EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2021

April 2020 to mid-July 2021

OCTOBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use etl@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – European Union Agency for Cybersecurity

CONTRIBUTORS

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of the ENISA ad hoc Working Group on Cyber Threat Landscapes for their valuable feedback and comments in validating this report. We would also like to thank the ENISA Advisory Group and the National Liaison Officers network for their valuable feedback.
We would also like to thank the ENISA Situational Awareness and Incident Notification teams for their active contribution and support in consolidating different pieces of information into the threat landscape.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

TABLE OF CONTENTS

1. THREAT LANDSCAPE OVERVIEW 7
1.1 PRIME THREATS 8
1.2 KEY TRENDS 9
1.3 EU PROXIMITY OF PRIME THREATS 10
1.4 PRIME THREATS PER SECTOR 11
1.5 METHODOLOGY 13
1.6 STRUCTURE OF THE REPORT 14
2. THREAT ACTOR TRENDS 16
2.1 STATE-SPONSORED ACTORS 16
2.2 CYBERCRIMINALS 23
2.3 HACKER-FOR-HIRE ACTORS 30
2.4 HACKTIVISTS 31
3. RANSOMWARE 34
3.1 TRENDS 35
3.2 RECOMMENDATIONS 43
4. MALWARE 46
4.1 TRENDS 46
4.2 RECOMMENDATIONS 49
5. CRYPTOJACKING 51
5.1 TRENDS 51
5.2 RECOMMENDATIONS 54
6. E-MAIL RELATED THREATS 56
6.1 TRENDS 56

6.2 RECOMMENDATIONS 58

7. THREATS AGAINST DATA 61

7.1 TRENDS 62

7.2 RECOMMENDATIONS 64

8. THREATS AGAINST AVAILABILITY AND INTEGRITY 67

8.1 TRENDS 67

8.2 RECOMMENDATIONS 72

9. DISINFORMATION - MISINFORMATION 75

9.1 TRENDS 78

9.2 RECOMMENDATIONS 79

10.NON-MALICIOUS THREATS 82

10.1 TRENDS 84

10.2 RECOMMENDATIONS 85

A ANNEX: MITRE ATT&CK 88

B ANNEX: MAJOR INCIDENTS 97

EXECUTIVE SUMMARY

This is the ninth edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape that identifies prime threats, major trends observed with respect to threats, threat actors and attack techniques, and also describes relevant mitigation measures. In the process of constantly improving our methodology for the development of threat landscapes, this year's work has been supported by a newly formatted ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

The time span of the ETL 2021 report is April 2020 to July 2021 and is referred to as the "reporting period" throughout the report. During the reporting period, the prime threats identified include:

- **Ransomware**
- **Malware**
- **Cryptojacking**
- **E-mail related threats**
- **Threats against data**
- **Threats against availability and integrity**
- **Disinformation – misinformation**
- **Non-malicious threats**
- **Supply-chain attacks**

In this report we discuss the first 8 cybersecurity threat categories. Supply chain threats, the 9th category, were analysed in detail, due to their particular prominence, in a dedicated ENISA report "ENISA Threat landscape for Supply Chain Attacks" [1].

For each of the identified threats, attack techniques, notable incidents and trends are discussed along with proposed mitigation measures. As regards trends, during the reporting period we highlight the following:

- **Ransomware** has been assessed as the **prime threat for 2020-2021.**
- **Governmental organisations have stepped up their game** at both national and international level.
- **Cybercriminals are increasingly motivated by monetisation** of their activities, e.g. ransomware. **Cryptocurrency** remains the most common pay-out method for threat actors.
- **Malware decline** that was observed in 2020 continues during 2021. In 2021, we saw an increase in threat actors resorting to relatively new or uncommon programming languages to port their code.
- The volume of **cryptojacking infections** attained a **record high** in the first quarter of 2021, compared to recent years. The **financial gain** associated with cryptojacking incentivised threat actors to carry out these attacks.
- **COVID-19 is still the dominant lure in campaigns** for e-mail attacks.
- There was a **surge in healthcare sector related data breaches**.
- **Traditional DDoS (Distributed Denial of Service) campaigns** in 2021 are more targeted, more persistent and increasingly multivector. The **IoT (Internet of Things)** in conjunction with **mobile networks** is resulting in a new wave of DDoS attacks.
- In 2020 and 2021, we observe a **spike in non-malicious incidents**, as the COVID-19 pandemic became a multiplier for **human errors** and **system misconfigurations**, up to the point that most of the breaches in 2020 were caused by errors.

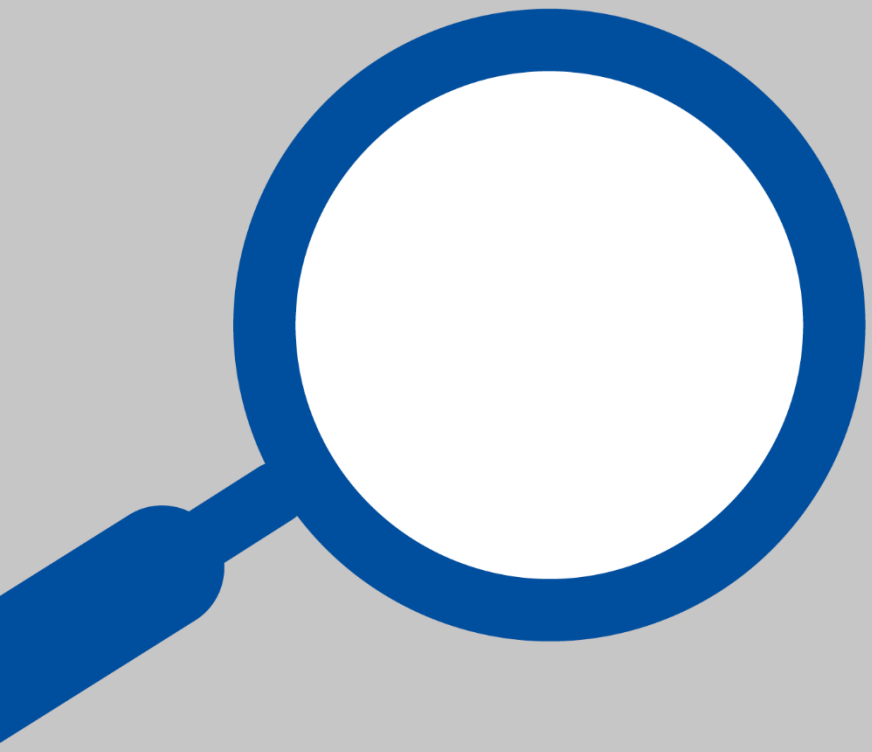
Understanding the trends related to threat actors, their motivations and their targets greatly assists in planning cybersecurity defences and mitigation strategies. This is an integral part of our overall threat assessment, since it

[1] ENISA Threat Landscape for Supply Chain Attacks, July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

allows security controls to be prioritised and a dedicated strategy to be devised based on the potential impact and likelihood of threat materialisation. With this in mind, for the purposes of the ETL 2021, the following four categories of cybersecurity threat actors are considered:

- **State-sponsored actors**
- **Cybercrime actors**
- **Hacker-for-hire actors**
- **Hacktivists**

Through continuous analysis, ENISA derived trends and points of interest for each of the major threats presented in the ETL 2021. The key findings and judgments in this assessment are based on multiple and publicly available resources which are provided in the references used for the development of this document. The report is mainly targeted at strategic decision-makers and policy-makers, but it will also be of interest to the technical cybersecurity community.



1. THREAT LANDSCAPE OVERVIEW

In its ninth edition, the ENISA Threat Landscape (ETL) report provides a general overview of the cybersecurity threat landscape. The ETL report is partly strategic and partly technical, with information relevant to both technical and non-technical readers. This year's work has been supported by a newly formatted ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL)[2].

Cybersecurity attacks have continued to increase through the years 2020 and 2021, not only in terms of vectors and numbers but also in terms of their impact. The COVID-19 pandemic has also –expectedly– had an impact on the cybersecurity threat landscape. One of the more enduring developments that resulted from the COVID-19 pandemic is a lasting shift to a hybrid office model. Therefore, cybersecurity threats related to the pandemic and exploiting the "new normal" are becoming mainstream. This trend has increased the attack surface and, as a result, we have seen a rise in the number of cyber-attacks targeting organisations and companies through home offices[3].

In general, cybersecurity threats are on the rise. Spurred by an ever-growing online presence, the transitioning of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity and the exploitation of new features of emerging technologies such as Artificial Intelligence (AI)[4][5], the cybersecurity landscape has grown in terms of sophistication of attacks, their complexity and their impact. Notably, the threat to supply chains and their significance due to their potentially catastrophic cascading effects has reached the highest position among major threats, so much so that ENISA produced a dedicated threat landscape for this category of threat[6].

It is worth noting that in this iteration of the ETL, particular focus has been given on the impact of cyber threats in various sectors, including the ones listed in the Network and Information Security Directive (NISD). Interesting insight may be drawn from the particularities of each sector when it comes to the threat landscape, as well as potential interdependencies and areas of significance. Accordingly, sectorial threat landscapes merit further attention.

There have also been some notable steps from the side of defenders in the cyber community this year, as well as the policy makers. The global community has begun to realise the importance of communication and cooperation in examining and tracking cybercriminals, with ransomware (the most prominent threat for the reporting period of ETL 2021) in particular becoming a prime item in agendas for meetings on strategy among global leaders.

Dedicated readers of past editions of the ETL 2021 will notice a difference in the mapping of prime threats. This year, ENISA took a step back and consolidated threat categories in a move towards integration and better representation of similar threats. This is part of ongoing efforts towards a revamped threat taxonomy and will help in establishing trends methodologically over the next few years.

The ETL 2021 is based on a variety of open-source information and cyber threat intelligence sources. It identifies major threats, trends and findings, and provides relevant high-level mitigation strategies. ENISA is currently working on solidifying the methodology for reporting on the threat landscape to promote transparency and consistency in the work.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Cost of a Data Breach Report 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA AI Threat Landscape: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISA Threat Landscape for Supply Chain Attacks, July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1 PRIME THREATS

A series of cyber threats emerged and materialised in the course of 2020 and 2021. Based on the analysis presented in this report, the ENISA Threat Landscape 2021 identifies and focuses on the following 8 prime threat groups (See Figure 1). These 8 threat groups are highlighted because of their prominence during the reporting period, their popularity and the impact that materialisation of these threats has had.

- **Ransomware**
  Ransomware is a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access. Ransomware has been the prime threat during the reporting period, with several high profile and highly publicised incidents. The significance and impact of the threat of ransomware is also evidenced by a series of related policy initiatives in the European Union (EU) and worldwide.

- **Malware**
  Malware is software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of a system. The threat of malware has been consistently ranked high for many years, albeit at a decreasing rate during the reporting period of ETL 2021. The use of new attach techniques and some major wins for the law enforcement community have impacted the operations of relevant threat actors.

- **Cryptojacking**
  Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. With the proliferation of cryptocurrencies and their ever-increasing uptake by the wider public, an increase in corresponding cybersecurity incidents has been observed.

- **E-mail related threats**
  E-mail related attacks are a bundle of threats that exploit weaknesses in the human psyche and in everyday habits, rather than technical vulnerabilities in information systems. Interestingly and despite the many awareness and education campaigns against these types of attacks, the threat persists to a notable degree. In particular, the compromise of business e-mails and advanced sophisticated techniques in extracting monetary gains are on the rise.

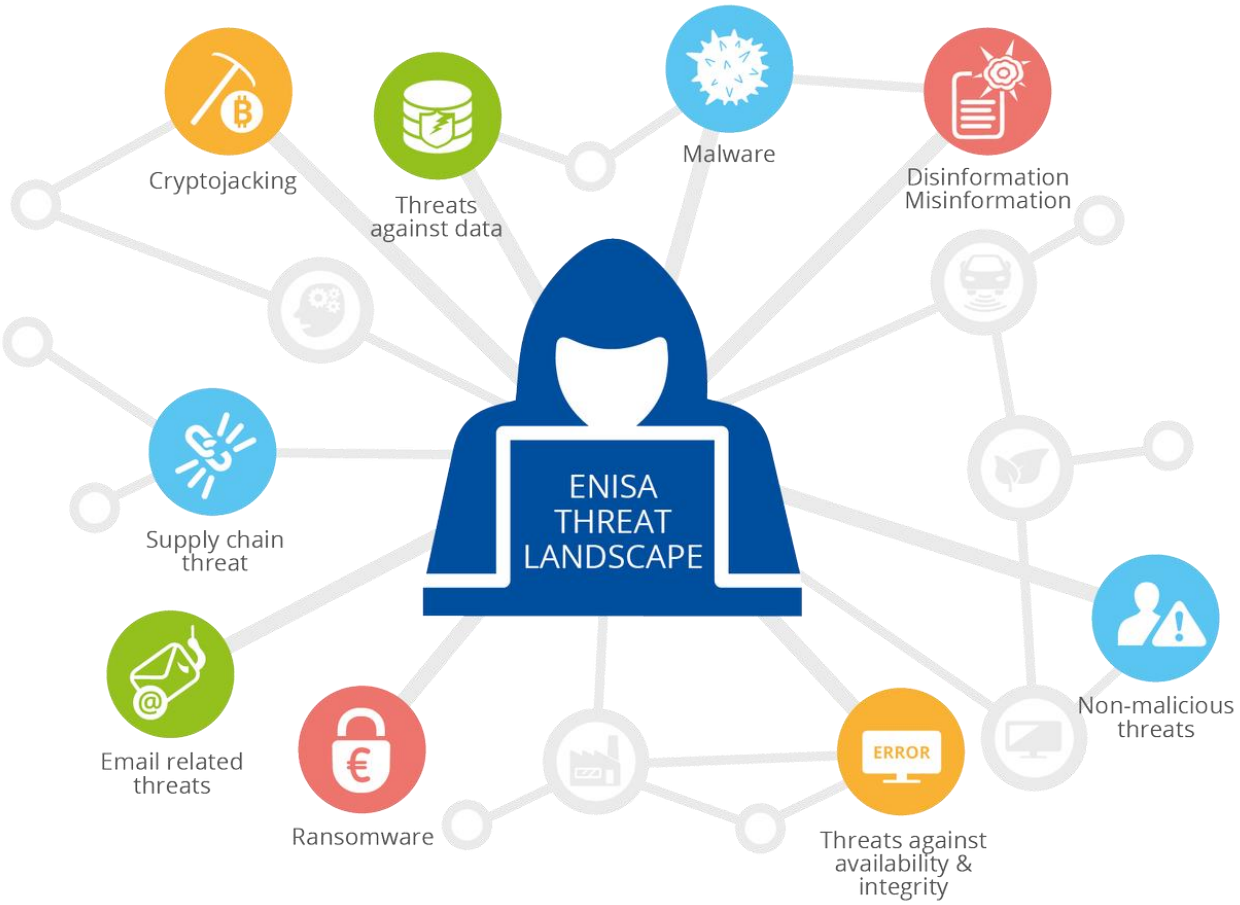
- **Threats against data**
  This category encompasses data breaches/leaks. A data breach or data leak is the release of sensitive, confidential or protected data to an untrusted environment. Data breaches can occur as a result of a cyber-attack, an insider job, unintentional loss or exposure of data. The threat continues to be high, since access to data is a prime target for attackers for numerous reasons, e.g. extortion, ransom, defamation, misinformation, etc.

- **Threats against availability and integrity**
  Availability and integrity are the target of a plethora of threats and attacks, among which the families of Denial of Service (DoS) and Web Attacks stand out. Strictly related to web-based attacks, DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages. The treat is consistently ranked high in the ENISA threat landscape, both because of its manifestation in actual incidents and its potential for high impact.

- **Disinformation – misinformation**
  Disinformation and misinformation campaigns are on the rise, spurred by the increased use of social media platforms and online media, as well as a result of the increase of people's online presence due to the COVID-19 pandemic. This group of threats is making its first appearance in the ETL; however its importance in the cyber world is high. Disinformation and misinformation campaigns are frequently used in hybrid attacks to reduce the overall perception of trust, a major proponent of cybersecurity.

- **Non-malicious threats**
  Threats are commonly considered as voluntary and malicious activities brought by adversaries that have some incentives to attack a specific target. With this category, we cover threats where malicious intent is not apparent. These are mostly based on human errors and system misconfigurations, but they can also refer to physical disasters that target IT infrastructures. Also attributed to their nature, these threats have a constant presence in the annual threat landscape and are a major concern for risk assessments.

Figure 1: ENISA Threat Landscape 2021 - Prime threats



It needs to be noted that the aforementioned threats involve categories and the collection of threats, consolidated into the eight areas mentioned above. Each of the threat groups is further analysed in a dedicated chapter of this report, which elaborates on its particularities and provides more specific information, findings, trends, attack techniques and mitigation vectors.

1.2 KEY TRENDS

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. These are also reviewed in detail throughout the various chapters comprising the ENISA threat landscape of 2021.

- **Highly sophisticated and impactful supply chain compromises** proliferated, as highlighted by the dedicated ENISA Threat Landscape on Supply Chain. **Managed service providers** are high-value targets for cybercriminals.
- **COVID-19 drove cyber espionage** tasking and created **opportunities for cybercriminals**.
- **Governmental organisations have stepped up their game** at both national and international level. Increased efforts have been observed from governments to disrupt and take legal action against state-sponsored threat actors.
- **Cybercriminals are increasingly motivated by monetisation** of their activities, e.g. ransomware. **Cryptocurrency** remains the most common pay-out method for threat actors.
- Cybercrime attacks **increasingly target and impact critical infrastructure**.
- **Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP)** remain the two most common **ransomware infection vectors**.
- The focus on **Ransomware as a Service** (**RaaS) type business models** has increased over 2021, making proper attribution of individual threat actors difficult.
- The occurrence of **triple extortion ransomware** schemes increased strongly over the course of 2021.

- **The malware decline** that was observed in 2020 continues during 2021. In 2021, we saw an increase in threat actors resorting to relatively new or uncommon programming languages to port their code.
- **Malware targeting container environments** have become much more prevalent, with novel evolutions like file-less malware being executed from memory.
- Malware developers keep finding ways to **make reverse engineering and dynamic analysis harder**.
- The volume of **cryptojacking infections** attained a **record high** in the first quarter of 2021, compared to the last few years. The **financial gain** associated with cryptojacking incentivised the threat actors to carry out these attacks.
- **The volume of Crypto mining in 2021 and cryptojacking activities are at a record high**.
- We can see that a **shift from browser to file-based cryptojacking** is taking place.
- **COVID-19 is still the dominant lure in campaigns** for e-mail attacks.
- **Business E-mail Compromise (BEC)** has **increased**, has grown in **sophistication** and become more **targeted**.
- **The Phishing-as-a-Service (PhaaS)** business model is gaining prevalence.
- Threat actors shifted their attention towards **vaccine information** in the context of threats to data and information.
- There was a **surge in healthcare sector related data breaches**.
- Traditional DDoS (Distributed Denial of Service) attacks are moving towards **mobile networks and IoT (Internet of Things)**.
- **Ransom Denial of Service (RDoS)** is the new frontier of denial of service attacks.
- **Sharing of resources in virtualised environments** acts as an amplifier of DDoS attacks.
- **DDoS campaigns** in 2021 have become more targeted and much more persistent and increasingly multivector.
- **Artificial Intelligence (AI)-enabled disinformation** supports attackers in carrying out their attacks.
- **Phishing is at the heart of disinformation attacks** and strongly exploits people's beliefs.
- **Misinformation and disinformation** are at the core of cybercrime activities and is increasing at an unprecedented rate.
- **Disinformation-as-a-Service (DaaS) business model** has grown significantly, spurred by the increasing impact of the COVID-19 pandemic and the need to have more information.
- In 2020 and 2021, we observed a **spike in non-malicious incidents**, as the COVID-19 pandemic became a multiplier for **human errors** and **system misconfigurations**, up to the point that most of the breaches in 2020 were caused by errors.
- There has been a **spike in cloud security non-malicious incidents**.

1.3 EU PROXIMITY OF PRIME THREATS

An important aspect to consider in the context of the ENISA Threat Landscape involves the proximity of a cyber threat with respect to the European Union (EU). This is particularly important to assist analysts in assessing the significance of cyber threats, correlate them with potential threat actors and vectors and even to guide the selection of appropriate targeted mitigation vectors. In line with the proposed classification for the EU Common Security and Defence Policy (CSDP)[7], we classify cyber threats into four categories as illustrated in Table 1.

Table 1: Classification of proximity of cyber threats

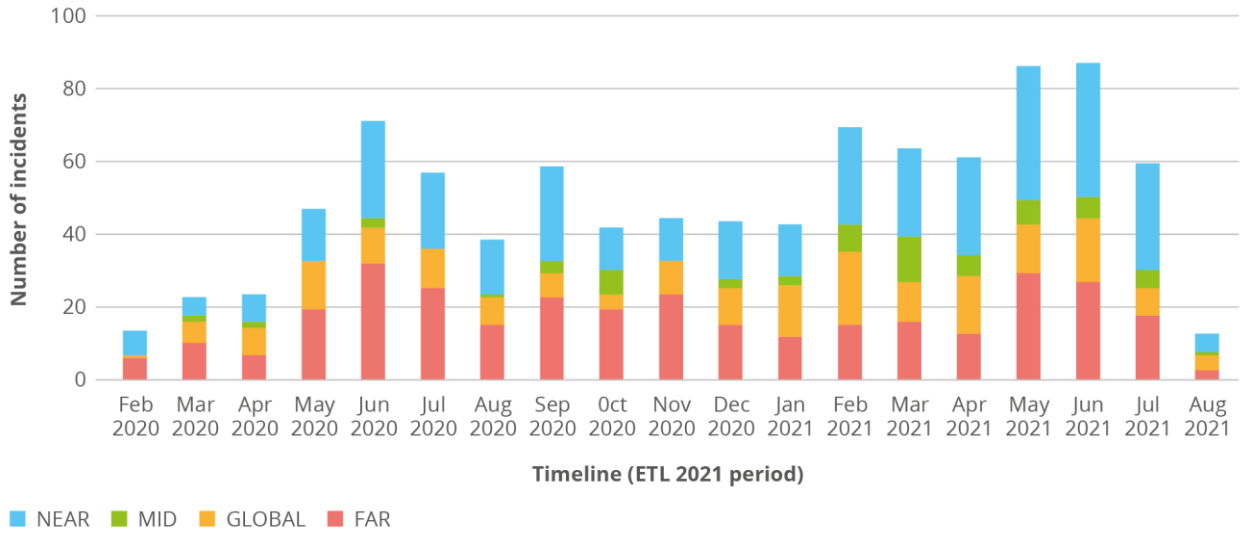
Proximity	Concerns
NEAR	Affected networks, systems, controlled and assured within EU borders. Affected population within the borders of the EU.
MID	Networks and systems considered vital for operational objectives within the scope of the EU digital single market and the NISD sectors, but their control and assurance relies on non-EU institutional or MS public or private authorities. Affected population in geographical areas close to EU borders.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Proximity	Concerns
FAR	Networks and systems that, if influenced, will have a critical impact on operational objectives within the scope of the EU digital single market and the NISD sectors. Control and assurance of those networks and systems lies beyond EU institutional or Member States' (MS) public or private authorities. Affected population in geographical areas far from the EU.
GLOBAL	All the aforementioned areas

Figure 2 illustrates a timeline of incidents related to the prime threat categories reported in the ETL 2021. It should be noted that the information in the graph is based on OSINT (Open Source Intelligence) and is a result of work by ENISA in the area of Situational Awareness[8].

Figure 2: Timeline of observed incidents related to major ETL threats (OSINT-based situational awareness) in terms of their proximity.



As evidenced by the above figure, 2021 has seen a higher number of incidents compared to 2020. In particular, the category NEAR has a constantly rising number of observed incidents related to prime threats, which implies their significance in the context of the EU. Unsurprisingly, the monthly trends (not shown in the figure for brevity) are quite similar among the different classifications since cybersecurity knows no border and in most cases threats materialise at all levels of proximity. It is noteworthy that, during the last months covered by ETL 2021, a higher EU NEAR proximity is observed, a trend that ENISA will continue monitoring to see how it evolves and how it relates to the activities of threat actors and ongoing threat vectors.

1.4 PRIME THREATS PER SECTOR

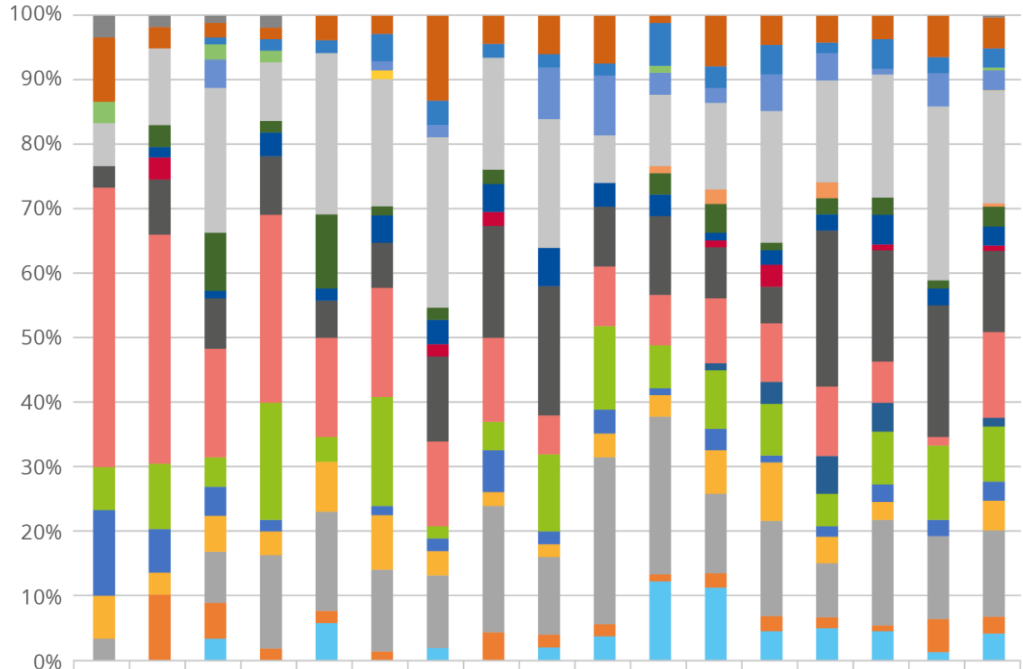
Cyber threats are usually not restricted to one particular sector and in most cases affect more than one of them. This is indeed true since in many cases the threats manifest themselves by exploiting vulnerabilities in underlying ICT systems that are being used in a variety of sectors. However, targeted attacks as well as attacks exploiting the differences in cybersecurity maturity across sectors and the popularity/prominence of certain sectors, are all factors that need to be considered. These factors contribute to threats manifesting themselves as incidents in specific sectors

[8] In accordance with the EU cybersecurity act Art.7 Par.6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

and this is why it is important to look deeply into sectorial aspects of observed incidents and threats. Moreover, trends noticed in each sector and cross-sector dependencies are observations that may be drawn from such an analysis.

Figure 3 and Figure 4 highlight the affected sectors concerning incidents observed based on OSINT (Open Source Intelligence) and is a result of work by ENISA in the area of Situational Awareness[9]. They refer to incidents related to the prime threats of ETL 2021. This is the first attempt by ENISA to map the impact of threats on specific sectors. In the coming years and in future iterations of the threat landscape, efforts will be made to align the sectors with the ones listed in the Network and Information Security Directive (NISD) and the proposal for its review (NISD 2.0).

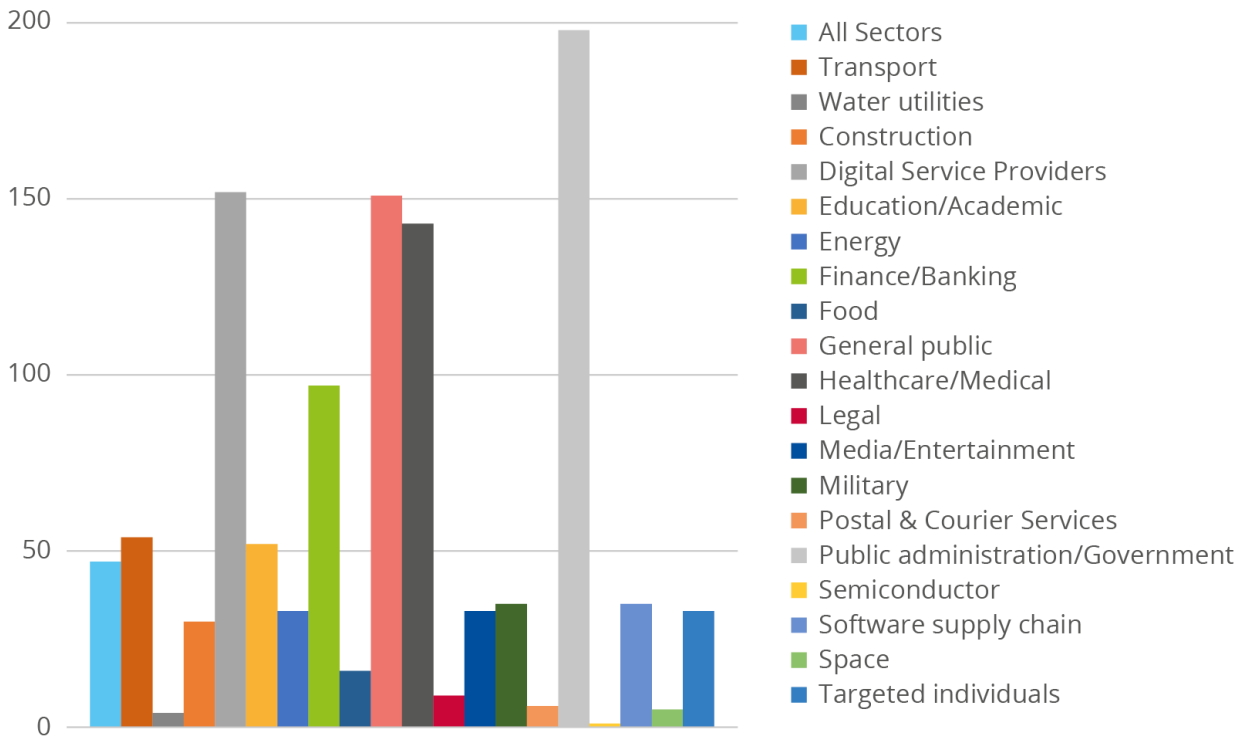
Figure 3: Timeline of observed incidents related to prime ETL threats in terms of the affected sector.



	4/20	5/20	6/20	7/20	8/20	9/20	10/20	11/20	12/20	1/21	2/21	3/21	4/21	5/21	6/21	7/21	Total
Water utilities	1	1	1	1													**4**
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	**54**
Targeted individuals			1	1	1	3	2	1	1	1	6	3	4	2	5	2	**33**
Space	1		2	1							1						**5**
Software supply chain			4			1	1		4	5	3	2	5	5	1	4	**35**
Semiconductor						1											**1**
Public administration/ Government	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	**198**
Postal & Courier Services											1	2		3			**6**
Military		2	8	1	6	1	1	1			3	4	1	3	3	1	**35**
Media/Entertainment		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	**33**
Legal		2					1	1				1	3		1		**9**
Healthcare/Medical	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	**143**
General public	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	**151**
Food												1	3	7	5		**16**
Finance/Banking	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	**97**
Energy	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	**33**
Education/Academic	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		**52**
Digital Service Providers	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	**152**
Construction		6	5	1	1	1		2	1	1	1	2	2	2	1	4	**30**
All Sectors			3		3		1		1	2	11	10	4	6	5	1	**47**

[9] In accordance with the EU cybersecurity act Art.7 Par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Figure 4: Targeted sectors per number of incidents (April 2020-July 2021)



During this reporting period, a large number of incidents targeted public administration and government and digital service providers. The latter is to be expected given the horizontal provisioning of services for this sector and thus its impact on many other sectors. We also observed a significant number of incidents targeting end users and not necessarily a particular sector. The health sector was also targeted significantly, and this activity shows signs of increasing during the last few months of the reporting period (May-July 2021). Interestingly, the finance sector faces a consistent number of incidents throughout the year. The supply chain of software also shows an increased number of incidents during 2021, which is also an observation in the ENISA Supply Chain threat landscape report[10].

1.5 METHODOLOGY

The ENISA Threat Landscape (ETL) 2021 report is based on information available from open sources, mainly of a strategic nature and ENISA's own Cyber Threat Intelligence (CTI) capabilities, and covers more than one sector, technology and context. The report attempts to be industry and vendor agnostic and references or cites the work from various security researchers, security blogs and news media articles throughout the text in multiple footnotes. The time span of the ETL 2021 report is April 2020 to July 2021 and is referred to as the "reporting period" throughout the report.

For the production of the ETL 2021 report, the following approach was used. Throughout the relevant time period ENISA, by means of situational awareness, gathered a list of major incidents as they appeared in open sources. This list served as the foundation for the identification of the list of prime threats, as well as the source material for several trends and statistics in the report.

Subsequently, an in-depth desk research of available literature from open sources such as news media articles, expert opinion, intelligence reports, incident analysis and security research reports was conducted by ENISA and external experts. Through continuous analysis, ENISA derived trends and points of interest for each of the major threats presented in ETL 2021. The key findings and judgments in this assessment are based on multiple and publicly available resources which are provided in the references used for the development of this document.

[10] ENISA Threat Landscape for Supply Chain Attacks, July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Within the report, we try to differentiate between what has been reported by our sources and what is our assessment. (We do so by specifically using the phrase “in our assessment”). Finally, when conducting an assessment, we convey probability by using words that express an estimate of probability (e.g. likely, very likely, certainly)[11].

MITRE ATT&CK® framework[12] was used in this report to highlight the attack tactics and techniques relevant to a given threat (see Annex A). For each ATT&CK® tactic, the techniques the adversary used are presented. This can lead to a list of ATT&CK Mitigations[13] that can be applied. MITRE ATT&CK® is a knowledge base, a common language for adversarial tactics and techniques based on real-world observations. The MITRE ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

The report was validated by the ENISA Ad Hoc Working Group on Cyber Threat Landscapes[14] that was established in April 2021, a group that consists of experts from European and international public and private sector entities.

For the future development of Threat Landscapes, ENISA is in the process of formalising a new methodology, to promote transparency and set the foundations for structured and well-aligned processes. In this endeavour, together with a revised threat taxonomy, the methodology for threat landscapes will be made public in the future.

1.6 STRUCTURE OF THE REPORT

The ENISA Threat Landscape (ETL) 2021 has maintained the structure of previous ETL reports by using a similar structure for highlighting the prime cyber threats in 2021. Readers of past iterations will notice that the threat categories have been consolidated in line with a move towards a new cybersecurity threat taxonomy to be used in the future.

This report is structured as follows:

Chapter 2 explores the trends related to threat actors (i.e. state-sponsored actors, cybercrime actors, hacker-for-hire actors and hacktivists).
Chapter 3 discusses major findings, incidents and trends regarding ransomware.
Chapter 4 presents major findings, incidents and trends regarding malware.
Chapter 5 describes major findings, incidents and trends regarding cryptojacking.
Chapter 6 highlights major findings, incidents and trends regarding e-mail related threats.
Chapter 7 discusses major findings, incidents and trends regarding threats to data.
Chapter 8 presents major findings, incidents and trends regarding threats against availability and integrity.
Chapter 9 underlines the importance of hybrid threats and describes major findings, incidents and trends regarding disinformation and misinformation.
Chapter 10 focuses on major findings, incidents and trends regarding non-malicious threats.
Annex A presents the techniques commonly used for each threat, based on the MITRE ATT&CK® framework.
Annex B includes notable incidents per threat, as observed during the reporting period.

[11] CIA - Words of Estimative Probability https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

2. THREAT ACTOR TRENDS

Cyber threat actors are an integral component of the threat landscape. They are entities aiming to carry out a malicious act by taking advantage of existing vulnerabilities, with the intent to do harm to their victims. Understanding how threat actors think and act, what their motivations and goals are, is an important step towards a stronger cyber incident response. Monitoring the latest developments with respect to the tactics and techniques used by threat actors to achieve their objectives, along with staying up-to-date with the long-term trends in motivations and targets, is crucial for an efficient defence in today's cybersecurity ecosystem.

Moreover, understanding the trends related to threat actors, their motivations and their targets assist greatly in planning cybersecurity defences and mitigation strategies. It is an integral part of the overall threat assessment since it allows security controls to be prioritised and a dedicated strategy based on potential impact and the likelihood that threats will materialise to be devised. Having no understanding of threat actors and the way they operate creates a significant knowledge gap in cybersecurity, because one ends up looking and analysing threats without considering the motivations and goals behind those threats.

In this section, we explore the trends related to threat actors. This assessment does not provide an exhaustive list of all trends during the reporting period, but rather a high-level view of major trends observed at a strategic level. We focus on the threat actors' motives, capabilities and targeting, and their evolution is assessed.

For the purposes of the ETL 2021, the following four categories of cybersecurity threat actors are considered:

- **State-sponsored actors**
- **Cybercrime actors**
- **Hacker-for-hire actors**
- **Hacktivists**

The list of potential threat actors is evidently large and encompasses other categories such as insider actors, etc. The focus on the particular four categories above does not imply that other categories of threat actors are deemed of lesser significance. The reasoning behind the focus on the four selected threat actor categories is based on their relative prominence during the ETL 2021 reporting period.

2.1 STATE-SPONSORED ACTORS

COVID-19 drove cyber espionage tasking. During the reporting period, we observed state-backed groups conducting cyber espionage operations related to COVID-19 as well as using COVID-19 related lures for social engineering. Regarding COVID-19 related cyber-espionage, threat actors have been tasked to pursue information related to recovery and vaccine development efforts[15]. According to publicly available reports, state-sponsored threat actors have been observed to be likely seeking data related to infection rates, country-level responses, and treatments.[15,16,17,18,19] Moreover, the collection of scientific information related to the COVID-19 vaccine was a high-priority requirement and thus the healthcare, pharmaceutical, and medical research sectors have been heavily targeted.[15,17,21]

[15] FireEye / Mandiant - M-Trends 2021 https://content.fireeye.com/m-trends/rpt-m-trends-2021
[16] NCSC-UK - Advisory: APT29 targets COVID-19 vaccine development https://www.ncsc.gov.uk/news/advisory-apt29-targets-COVID-19-vaccine-development
[17] CrowdStrike - 2021 Global Threat Report - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
[18] El Pais - Chinese hackers accused of stealing information from Spanish centers working on COVID-19 vaccine - https://english.elpais.com/society/2020-09-18/chinese-hackers-accused-of-stealing-information-from-spanish-centers-working-on-COVID-19-vaccine.html
[19] US Department of Justice - Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research - https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

Our assessment is that the targeting of the these sectors by state-sponsored actors will certainly continue as long as the pandemic lasts. In addition, we believe that the targeting of contact tracing systems as well as other COVID-19 related applications deployed by governments whose data can be valuable for intelligence gathering and spear phishing campaigns is likely. Finally, threat actors that have been ascribed as acting in the interests of nation states exploited the concern and confusion related to COVID-19 with spear-phishing lures.[17,20,21] In our opinion, cyber espionage groups will almost certainly continue to conduct (spear-) phishing attacks using COVID-19 themes.[22]

Highly sophisticated and impactful supply chain compromises. While supply chain compromises by state-backed threat actors are not new, during the reporting period, this type of attack reached new levels of sophistication and impact.[23,24] One of the major campaigns that took place during the reporting period is the SolarWinds supply chain compromise.[23,25,26,27,28,29,30] The SolarWinds supply chain compromise is a prominent example of how great an impact a supply chain attack can have. The state-backed group behind this supply chain attack meticulously planned the attack making almost no operational security mistakes.[17] Moreover, the threat actor showed exceptional knowledge of cloud environments,[17] something that highlights the threats and current gaps in our knowledge of cloud environments.[31,32] The threat actor had well-defined and long-term espionage objectives judging from the careful selection of the targets and subsequent post-compromise activity compared to the circa 18.000 organisations that have been affected.

Based on ENISA's analysis,[23] on at least 17 occasions between 2020 and 2021, investigations confirm that supply chain attacks were conducted by Advanced Persistent Threat (APT) groups, often state-sponsored, which constitutes more than 50% of the attributed supply chain attacks during this period. Moreover, software supply chain attacks are the most frequent type of supply chain attacks while the software services sector is the most targeted. From an attacker's perspective, the characteristics of the targeted software are usually the following:[33] i) cross-network communication capability, ii) has root/admin-level privileges, iii) cross-platform/cross-operating system, iv) often whitelisted, and v) acts as a centralised management platform.

Historically, the majority of supply chain attacks resulted, or had the potential to result, in remote code execution.[34] According to publicly available reports, various state actors have conducted software supply chain attacks. The most likely distribution vector of the supply chain attacks conducted by state-backed threat actors is via the hijacking of the software update process (others include the undermining of software certificates, open-source compromise, and mobile app store attacks).[34] This distribution vector is very sophisticated and is indicative of the complexity and the careful planning and execution that is needed for such operations (e.g. see SolarWinds campaign timeline[35]).

Summing up, the diversified and complex world of supply chains offers a wealth of targets for state-backed threat actors. Moreover, the move to teleworking, exacerbated by COVID-19, led organisations to maintain or even increase the third-party suppliers they depend on for their operational needs. In our assessment, state-backed threat actors will certainly continue conducting supply chain attacks (especially targeting software, cloud, and managed service

[20] Kaspersky - APT annual review: What the world's threat actors got up to in 2020 https://securelist.com/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99574/
[21] Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
[22] Kaspersky - Advanced Threat predictions for 2021 - https://securelist.com/apt-predictions-for-2021/99387/
[23] ENISA Threat Landscape for Supply Chain Attacks, July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[24] Kaspersky - APT Trends Report Q1 2021 - https://securelist.com/apt-trends-report-q1-2021/101967/
[25] Microsoft - Addressing cybersecurity risk in industrial IoT and OT - https://www.microsoft.com/security/blog/2020/10/21/addressing-cybersecurity-risk-in-industrial-iot-and-ot/
[26] FireEye - Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[27] Microsoft - Microsoft Internal Solorigate Investigation Update - https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/
[28] CrowdStrike - SUNSPOT: An Implant in the Build Process - https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
[29] SolarWinds - SolarWinds Security Advisory - https://www.solarwinds.com/sa-overview/securityadvisory
[30] European Commission - Answer given by Mr. Hahn on behalf of the European Commission - https://www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.pdf
[31] Atlantic Council - Broken Trust: Lessons from Sunburst - https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf
[32] CERT-EU - Threat Landscape Report (Volume 1) - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf
[33] Obscurity Labs – Software supply chain targeting – Who will the APTs target next? - https://obscuritylabs.com/blog/software-supply-chain-targeting-who-will-the-apts-target-next/
[34] Atlantic Council - BREAKING TRUST: Shades of Crisis Across an Insecure Software Supply Chain - https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
[35] kiuwan – SolaWinds Hack Timeline - https://www.kiuwan.com/solarwinds-hack-timeline/

providers) as they represent a unique initial access tactic.[17] We also assess the likely targeting of cloud-hosted development environments as enablers for supply chain attacks.[36] Finally, while many of these attacks were carried out by state-sponsored adversaries, cybercrime threat actors increasingly show the same patterns of behaviour.[21]

State-backed groups and their operators engaging in revenue generation activities. As we have observed in the past, there have been cases where state-sponsored adversaries have engaged in cybercrime operations.[37,38] Moreover, during the reporting period, we identified cases indicating this is an increasing trend among various threat groups that are linked to nation states:

- We observed for the first time that the Lazarus group conducted targeted ransomware intrusions for financial gain.[39] The likely motive behind these activities is monetary gain.
- The US Department of Justice has issued indictments against individuals linked with the threat group APT41/WICKED PANDA for conducting cybercrime operations targeting the video game sector whilst also conducting cyber espionage operations.[40,41] The APT41's cybercrime operations have been conducted for personal financial gain, e.g. obtain or generate video game currency via hacking to then sell it for profit.
- The PIONEER KITTEN threat group has been identified with advertising and selling corporate network access on an underground forum.[42] This activity has been likely conducted for personal gain.
- Various threat groups (Labyrinth Chollima, Stardust Chollima, Velvet Chollima[43]) have been observed to deploy malicious cryptocurrency applications, targeting cryptocurrency exchanges, stealing cryptocurrency wallet credentials, and other currency generation operations. The likely motive behind these activities is monetary gain.
- A member of the Sandworm threat group has been identified conducting spear-phishing campaigns against real estate companies, auto dealers, and cryptocurrency exchanges for personal gain[44] .
- According to the US Department of Justice, several Iran-based threat actors conducted both espionage and criminal operations[45]. Regarding the actors' money-making activities for personal gain (likely as a secondary income), they used the victims' stolen information to steal financial information and they attempted to extort the victims after stealing sensitive information from them.
- Cybercriminals allegedly acting on behalf of nation states have reportedly conducted cyber operations (ransomware attacks, cyber-enabled extortion, cryptojacking, and rank theft) for their personal gain[46].

It is our assessment that state-backed actors will certainly continue conducting revenue generating cyber intrusions (in pursuit of strategic objectives or for personal gain) with varying levels of national responsibility[47] and thus further blur the lines between cyberespionage and cybercrime operations. As states leverage cybercrime groups to conduct cyber operations, we expect this trend to increase and these state-affiliated groups to engage in money-making intrusions for themselves.

Governmental organisations step up their game. During the reporting period, we observed increased efforts from governments to disrupt, "name and shame", and take legal action against state-sponsored threat actors. We have

[36] Booz Allen - 8 Cyber Threat Trends To Watch Out For In 2021 - https://www.boozallen.com/c/insight/publication/8-cyber-threat-trends-for-2021.html
[37] FireEye - APT41: A Dual Espionage and Cyber Crime Operation - https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
[38] BBC - The Lazarus heist: How North Korea almost pulled off a billion-dollar hack - https://www.bbc.com/news/stories-57520169
[39] Kaspersky - Lazarus experiments with new ransomware - https://www.kaspersky.com/blog/lazarus-vhd-ransomware/36559/
[40] U. S. Department of Justice - Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally - https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
[41] PwC - Cyber Threats 2020: A Year in Retrospect - https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
[42] CrowdStrike – Who is PIONEER KITTEN? - https://www.crowdstrike.com/blog/who-is-pioneer-kitten
[43] CrowdStrike - 2021 Global Threat Report - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
[44] US Department of Justice - Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace - https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
[45] US Department of Justice - Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East - https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states?s=08
[46] White House - The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China - https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
[47] Atlantic Council - Beyond Attribution: Seeking National Responsibility in Cyberspace - https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/

observed (among others) several indictments issued and sanctions imposed by the US Department of Justice,[44,48, 49] public attribution statements from the NCSC-UK,[50] a public statement by the White House,[51] a joint advisory from NSA-FBI-CISA,[52] and the Norwegian government's public statement.[53] From the EU perspective, we have observed the first-ever sanctions announced by the European Council[54] against state-sponsored threat actors, a statement related to cyberattacks that have been undertaken from the territory of China,[55] and the new EU Cybersecurity Strategy that strengthens the EU Cyber Diplomacy Toolbox to prevent, discourage, deter and respond to cyberattacks against the EU.[56] Moreover, aligned with the US Cyber Strategy of "persistent engagement", we have observed US-based agencies (e.g. US Cyber Command, CISA, NSA) publicly disclosing Tactics, Techniques and Procedures (TTPs), campaigns, and tools of state-backed threat actors thus disrupting their operations and "burning" their toolsets. Finally, we observed the FBI obtaining court approval to remove web shells from Internet-connected and compromised Microsoft Exchange servers in the US.[57]

The goal of the activities described above is to disrupt the operations of adversaries, enable network defenders to detect and respond to malicious activities, act as a means of signalling to adversaries (potentially deterring them or influencing their behaviour), and establish a level of cyber norms in cyberspace.[58] We assess that it is likely that more countries will start using indictments, public disclosures and attribution statements as part of their cyber strategy.[59] On the flip side, it is still not yet clear how these activities will deter highly sophisticated and determined state-backed threat actors in the long term. The hacking of the e-mail accounts of the most prominent federal prosecutors in the US Department of Justice during the SolarWinds campaign suggests, though, that indictments against foreign cyber operators can have a deterrent effect[60].

Hindering defenders' efforts. During the past few years, we have observed threat actors monitoring threat intelligence reporting and attribution disclosures and responses from an operational and strategic perspective. Over the years, one can claim that state-backed threat actors have been learning from their past mistakes and they have been improving their operational security and leaving no high fidelity indicators during their intrusions[61].

[48] FireEye - APT41: A Dual Espionage and Cyber Crime Operation - https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
[49] US Department of Justice - Department of Justice and Partner Departments and Agencies Conduct Coordinated Actions to Disrupt and Deter Iranian Malicious Cyber Activities Targeting the United States and the Broader International Community - https://www.justice.gov/opa/pr/department-justice-and-partner-departments-and-agencies-conduct-coordinated-actions-disrupt
[50] NCSC-UK - Advisory: APT29 targets COVID-19 vaccine development https://www.ncsc.gov.uk/news/advisory-apt29-targets-COVID-19-vaccine-development
NCSC-UK - UK and partners condemn GRU cyber-attacks against Olympic and Paralympic Games - https://www.ncsc.gov.uk/news/uk-and-partners-condemn-gru-cyber-attacks-against-olympic-an-paralympic-games
NCSC-UK - UK and allies hold Chinese state responsible for pervasive pattern of hacking - https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking
[51] White House - The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China - https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
[52] NSA-CISA-FBI Joint Advisory on Russian SVR Targeting US and Allied Networks, April 2021 https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied
[53] BBC - Norway blames Russia for cyber-attack on parliament - https://www.bbc.com/news/world-europe-54518106
[54] European Council - EU imposes the first-ever sanctions against cyber-attacks - https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/
[55] European Council - China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory - https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/
[56] European Commission - New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient - https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
[57] ZDNet - Everything you need to know about the Microsoft Exchange Server hack - https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/
US Department of Justice - Justice Department Announces Court-Authorised Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities - https://www.justice.gov/opa/pr/justice-department-announces-court-authorised-effort-disrupt-exploitation-microsoft-exchange
[58] PwC - Five cyber threat trends to prepare for in 2021 - https://www.pwc.co.uk/issues/cyber-security-services/insights/five-cyber-threat-trends-to-prepare-for-in-2021.html
[59] Kaspersky - Advanced Threat predictions for 2021 - https://securelist.com/apt-predictions-for-2021/99387/
[60] AP News - Justice Department says Russians hacked federal prosecutors - https://apnews.com/article/technology-europe-russia-election-2020-5486323e455277b39cd3283d70a7fd64
[61] ZeroFOX - The Future of Digital Threats: 2020 Insights, 2021 Predictions - https://www.zerofox.com/blog/cyber-threat-trends-report/

An increasing number of state-sponsored threat actors have been observed to use offensive security tools (OSTs)[62] (especially Cobalt Strike[63] but also Empire, Metasploit[64], Mimikatz, etc.), living-off-the-land techniques,[65] and published proof-of-concept code.[61] These options provide them scalability of operations, ease of use, deniability, operational effectiveness, and reduced costs.[66] State actors utilise such tools and techniques (at least) in the early phases of their intrusions and before deploying their home-grown tools to reach their objectives. Moreover, the leveraging of cybercriminal contract hackers by states (for deniability) as well as the wide use of common tools and techniques by cybercrime and state-backed actors undermine credible attribution.[67]

Finally, the use of false flags can be regarded as an established method related to state-backed threat actors.[68] During the reporting period, we observed the cases of MontysThree[69] and DeathStalker[70] threat actors that utilised false flags.

In our assessment state-backed groups will certainly be leveraging offensive security tools, living-off-the-land techniques, published PoCs, false flags, criminal contract hackers, crimeware-as-a-service, and will also be exhibiting high levels of operational security to conduct cyber operations. All these will further complicate the detection, response, and especially the defenders' attribution efforts.[71]

Increased targeting of ICS networks. Historically, organisations have had less visibility in their ICS networks as compared to their IT networks. Moreover, digital transformation initiatives, the rise of Industrial IoT,[72] the cloud connectivity of ICS devices, as well as the remote access services for ICS networks provide opportunities for the threat actors[73] (For example, the abuse of valid accounts was the No1 technique used by threat groups targeting ICS networks[74]).

During the last 5-10 years, adversaries have increasingly invested resources to target ICS networks. According to publicly available reports, the number of threat groups targeting ICS networks is growing at a rate three times faster than they are going dormant[74] and, during the reporting period, at least four new groups were discovered: STIBNITE, TALONITE, KAMACITE, and VANADINITE.[75] The objectives of these groups vary from information collection and long-term persistence to disruption of ICS operations and potential physical destruction.

In our assessment the interest in targeting ICS networks will certainly grow in the near future. While we previously discussed the opportunities for ICS targeting, the drivers for such operations include the desire for technological independence, geopolitics (e.g. conflicts, long-term persistence, cyber warfare), as well as testing the capabilities of threat actors and preparing for future attacks (some threat actors are still learning about ICS domain, experimenting and developing ICS-targeting capabilities).

[62] Intezer – Offensive Security Tools (OST) Map - https://www.intezer.com/ost-map/
[63] Accenture - Threats Unmasked 2021 Cyber Threat Intelligence Report - https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf
Proofpoint - Cobalt Strike: Favorite Tool from APT to Crimeware - https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware
[64] ZDNet - Cobalt Strike and Metasploit accounted for a quarter of all malware C&C servers in 2020 - https://www.zdnet.com/article/cobalt-strike-and-metasploit-accounted-for-a-quarter-of-all-malware-c-c-servers-in-2020/
[65] Symantec/Broadcom - Living off the Land: Attackers Leverage Legitimate Tools for Malicious Ends - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/living-land-legitimate-tools-malicious
[66] Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
[67] White House - The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China - https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
[68] VirusBulletin - Wave your false flags! Deception tactics muddying attribution in targeted attacks - https://www.virusbulletin.com/virusbulletin/2016/11/vb2016-paper-wave-your-false-flags-deception-tactics-muddying-attribution-targeted-attacks/
[69] Kaspersky - MontysThree: Industrial espionage with steganography and a Russian accent on both sides - https://securelist.com/montysthree-industrial-espionage/98972/
[70] Kaspersky - Lifting the veil on DeathStalker, a mercenary triumvirate - https://securelist.com/deathstalker-mercenary-triumvirate/98177/
[71] Verizon – Cyber Espionage Report 2020-2021 - https://www.verizon.com/business/resources/reports/cyber-espionage-report/
BlackBerry - BlackBerry 2021 Threat Report - https://www.blackberry.com/us/en/forms/enterprise/report-bb-2021-threat-report
[72] Microsoft - Addressing cybersecurity risk in industrial IoT and OT - https://www.microsoft.com/security/blog/2020/10/21/addressing-cybersecurity-risk-in-industrial-iot-and-ot/
[73] Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
[74] Dragos - Year in Review - https://hub.dragos.com/2020-year-in-review-download
[75] Dragos - Threat Activity Groups - https://www.dragos.com/threat-activity-groups/

Cyber operations are driven by state strategies, geopolitical tensions, and armed conflicts. It is common knowledge, nowadays, that cyber operations are conducted by most states all over the world to accomplish their strategic objectives.[76] Thus, states are striving to develop, buy or hire cyber offensive capabilities to place themselves in a favourable position in this cyber arms race. The implementation of such cyber capabilities is important for their national strategies and their long-term planning. Currently, some of the trends we observe are that a) states with advanced cyber capabilities are using them to strategically shape global political, military, economic, and ideological power, b) middle powers are focusing on initiatives related to regulation, cyber norms, and protection of their critical infrastructure, and c) low-capability cyber powers are enhancing their defensive and offensive postures.[77]

During the reporting period, we observed that cyber operations were aligned with the strategic objectives of states as well as with the geopolitical landscape and real-world events. Notably, we observed increased cyber intrusion activities in regions of trade routes (e.g. between Europe and Asia[78]), in regions of armed conflict,[79,80,81] against strategic targets such as governmental organisations (e.g. SolarWinds supply chain attack), and cyber operations as enablers for large-scale espionage, personally identifiable information and the theft of intellectual property (e.g. the Microsoft Exchange hack[82]).

State-sponsored groups are increasingly testing and exhibiting their capabilities for disruptive operations. In our assessment state-backed actors will certainly continue pursuing their strategic objectives via cyber operations for intelligence gathering for advantages in decision-making, stealing intellectual property, and pre-positioning of military and critical infrastructure (preparation of the operational environment) for future conflicts.[83] It is also our assessment that state-backed groups will possibly develop (or buy or otherwise procure) and conduct disruptive/destructive operations masqueraded as ransomware to weaken, demoralise and discredit adversarial governments.[84] Finally, local conflicts will likely include cyber operations paired with drone attacks and media-driven misinformation in order to amplify impact.[85]

Information operations as a tool to pursue states' strategic goals. Information operations dominated the news headlines during the 2016 US elections. Currently, several states are leveraging information operations as a tool for hybrid conflicts exploiting societal divisions, undermining trust, and polarising societies over issues that are sensitive and important in certain countries.[96]

During the last few years, we observed an evolution in how threat actors are conducting information operations. First, we observed threat actors conducting more targeted information operations as compared to the "noisy" ones in the pas.t[95] Moreover, currently there are commercial actors that sell Information-Operations-as-a-Service, providing plausible deniability for their sponsors.[86] Threat actors have also adapted their TTPs and exhibit better operational security as well as platform diversification to survive takedowns[87].

[76] Ben Buchanan - The Hacker and the State: Cyber-Attacks and the New Normal of Geopolitics - https://www.amazon.com/Hacker-State-Attacks-Normal-Geopolitics/dp/0674987551
[77] Control Risks - Geopolitics and cyber in 2021 - https://www.controlrisks.com/our-thinking/insights/geopolitics-and-cyber-in-2021
[78] Kaspersky - Advanced Threat predictions for 2021 - https://securelist.com/apt-predictions-for-2021/99387/
[79] Recorded Future - China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions - https://www.recordedfuture.com/redecho-targeting-indian-power-sector/
[80] Cisco Talos - PoetRAT: Malware targeting public and private sector in Azerbaijan evolves - https://blog.talosintelligence.com/2020/10/poetrat-update.html
BBC - Nagorno-Karabakh: The Armenian-Azeri 'information wars' - https://www.bbc.com/news/world-europe-54614392
Azerbaycan 24 - Azerbaijani hackers broke into over 90 Armenian websites - https://www.azerbaycan24.com/en/azerbaijani-hackers-broke-into-over-90-armenian-websites-video/
[81] National Security and Defense Council of Ukraine - The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies - https://www.rnbo.gov.ua/en/Diialnist/4823.html
[82] NCSC-UK - UK and allies hold Chinese state responsible for pervasive pattern of hacking - https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking
[83] Control Risks - Geopolitics and cyber in 2021 - https://www.controlrisks.com/our-thinking/insights/geopolitics-and-cyber-in-2021
[84] Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
[85] Kaspersky - ICS threat predictions for 2021 - https://securelist.com/ics-threat-predictions-for-2021/99613/
[86] ZDNet - Disinformation for hire: PR firms are the new battleground for Facebook - https://www.zdnet.com/article/disinformation-for-hire-pr-firms-are-the-new-battleground-for-facebook/
[87] Facebook - The State of Influence Operations 2017-2020 - https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

During the reporting period, major topics of information operations included election interference and COVID-19. During the 2020 US elections[88] and the 2021 pre-election period in Germany,[89] there were reported cases of information operations as preparatory work for such operations. According to publicly available reports, intelligence services have been conducting information operations related to COVID-19 issues.[90] The EUvsDisinfo is a European task force that tracks disinformation threats and has 922 COVID-19 disinformation narratives in its database (as of 31st July 2021).[91] These narratives vary from promoting conspiracy theories about the origin of COVID-19, through vaccine rollout and disinformation about vaccination strategies, the handling of public health measures, undermining public trust in the European Medicines Agency (EMA), and to fuelling anti-vaccination movements in the EU.[92]

Our assessment is that threat actors will very likely continue pursuing their strategic objectives by conducting cyber-enabled information operations for the next decade focusing on important geopolitical issues like elections, public health, humanitarian crises, human rights, and security.[93] Also, in our opinion, threat actors will very likely continue leveraging the latest technology (e.g. Artificial Intelligence, deep fakes, voice biometrics) to impersonate individuals as part of their information operations.[94] Finally, in our view, it is possible that there will be increased leveraging of Information-Operations-as-a-Service together with increased competition of these disinformation networks.[94]

Hack-and-leak operations are an established tactic. Hack-and-leak operations include activities where a threat actor has unlawfully accessed information via a cyberattack and then leaks this information. This information is usually leaked in a specific context – sometimes the information is manipulated – and at a time that serves the threat actor's objectives to achieve the desired effect and influence public debate.[95] Targets for these operations can be businesses, politicians, as well as governmental organisations, and they are information operations impacting the confidentiality and integrity of the information leaked.[96]

Hack-and-leak operations are not a new tactic but they gained traction after the hack-and-leak operations during the 2016 US elections. For these operations, their impact, perpetrators (mostly using fake identities), and targets are hard to predict. However, if the stolen information is not sold on underground forums (showing a financial motivation by the threat actor) but rather shared with the public, one can assess that these operations likely have a political motivation.[97] Threat actors conducting hack-and-leak operations usually fall within the category of state actors, hacktivists, or front entities acting on behalf of nation-backed groups such as hacktivists. The latter is also a trend that has been identified in recent years as state-backed groups are increasingly using hacktivists as cover under which to conduct their operations; they even co-ordinate with hacktivists so that these operations look like the work of genuine hacktivists[97, 98, 99].

[88] The New York Times - Iran and Russia Seek to Influence Election in Final Days, US Officials Warn - https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html
CISA - Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data - https://us-cert.cisa.gov/ncas/alerts/aa20-304a
[89] Cyberscoop - Hackers target German lawmakers in an election year - https://www.cyberscoop.com/bundestag-germany-hackers-ghostwriter/
Der Taggesspiegel - Angriffswellen russischer Hacker auf Abgeordnete - https://www.tagesspiegel.de/politik/gefahr-fuer-die-bundestagswahl-angriffswellen-russischer-hacker-auf-abgeordnete/27418978.html
[90] APNews - US officials: Russia behind spread of virus disinformation - https://apnews.com/article/virus-outbreak-ap-top-news-health-moscow-ap-fact-check-3acb089e6a333e051dbc4a465cb68ee1
EU Disinfo Lab - How two information portals hide their ties to the Russian news agency InfoRos - https://www.disinfo.eu/publications/how-two-information-portals-hide-their-ties-to-the-russian-news-agency-inforos/
[91] EUvsDisinfo – Disinfo Database (COVID-19 related narratives) - https://euvsdisinfo.eu/disinformation-cases/?disinfo_keywords%5B%5D=106935&disinfo_keywords%5B%5D=88558&date=&per_page=
[92] EUvsDisinfo - EEAS SPECIAL REPORT UPDATE: SHORT ASSESSMENT OF NARRATIVES AND DISINFORMATION AROUND THE COVID-19 PANDEMIC (UPDATE DECEMBER 2020 - APRIL 2021) - https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-COVID-19-pandemic-update-december-2020-april-2021/?highlight=COVID
EUvsDisinfo - EEAS SPECIAL REPORT UPDATE: SHORT ASSESSMENT OF NARRATIVES AND DISINFORMATION AROUND THE COVID-19 PANDEMIC (UPDATE MAY - NOVEMBER) - https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-COVID-19-pandemic-update-may-november/?highlight=COVID
EUvsDisinfo - WHAT HAPPENED IN 2020? - https://euvsdisinfo.eu/what-happened-in-2020/?highlight=COVID
[93] World Economic Forum – Global Risks 2021 - https://www.weforum.org/reports/the-global-risks-report-2021
[94] Control Risks - Disinformation will affect more than elections in 2021 - https://www.controlrisks.com/our-thinking/insights/disinformation-will-affect-more-than-elections-in-2021
[95] Facebook - The State of Influence Operations 2017-2020 - https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf
[96] Dutch Ministry of Justice and Security – Cyber Security Assessment Netherlands 2020 - https://english.nctv.nl/documents/publications/2020/08/28/cyber-security-assessment-netherlands-2020
[97] CERT-EU - Threat Landscape Report (Volume 1) - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf
[98] Recorded Future - Return to Normalcy: False Flags and the Decline of International Hacktivism - https://go.recordedfuture.com/hubfs/reports/cta-2019-0821.pdf
[99] Thomas Rid - Active Measures: The Secret History of Disinformation and Political Warfare - https://www.amazon.com/Active-Measures-History-Disinformation-Political/dp/0374287260

During the reporting period, the European Medicines Agency (EMA) fell victim to a cyberattack. The stolen information was made public through the Internet and was picked up by the media.[100,101] Based on the EMA's investigation, not all the leaked documents were in their original form and this data manipulation could spread doubt about admission procedures and the safety of COVD-19 vaccines. Another interesting case was the operation conducted by the Ghostwriter threat group that targeted members of the German Parliament and Polish government officials (among others).[102,103,104,105] According to publicly available reports, documents from the personal e-mail accounts of government officials were leaked on Telegram[103] while the operation against German MPs was likely to be preparatory work for a future hack-and-leak information (especially taking into account that 2021 is an election year in Germany).[106107]

In our assessment hack-and-leak operations by state-backed and state-affiliated groups will very likely continue in the near future, as these operations require low to medium resource investment by the threat actors compared to their potential impact. Moreover, we expect these operations to intensify during periods of high interest (e.g. pre-election periods) and exploit political divisions or instability. Moreover, our assessment is that threat actors will likely conduct these operations through a series of releases so that they can sustain news media attention.[108] The latter highlights the importance of the target's response towards the leak operation in order to direct the media narrative more to the hack element rather than the leak element of the adversary's operation.

2.2 CYBERCRIMINALS

COVID-19 created opportunities for cybercriminals. Social engineering remains the most prevalent attack technique.[109] The effectiveness of a phishing campaign depends on whether it taps into strong emotions that drive action from the recipient's side.[110] During the pandemic, cybercriminals have been exploiting people's interest, concern, curiosity, and fear by using phishing lures related to COVID-19 for financial gain.[111] The COVID-19 lure themes matched the different stages of the pandemic.[112] The major ones used by the cybercriminals have reportedly been the following:[112,113]

- Exploitation of individuals looking for details on disease tracking, testing, and treatment;
- Impersonation of medical bodies, including the World Health Organisation (WHO) and US Centre for Disease Control and Prevention;
- Financial assistance and government stimulus packages;
- Tailored attacks against employees working from home;
- Scams offering personal protective equipment;
- Passing mention of COVID-19 with previously used phishing lure content (e.g. deliveries, invoices, and purchase orders);
- Vaccination-related lures;
- Phishing lures related to new variants of COVID-19.

[100] European Medicines Agency - Cyberattack on EMA - update 6 - https://www.ema.europa.eu/en/news/cyberattack-ema-update-6
[101] de Volkskrant - Russian and Chinese hackers gained access to EMA - https://www.volkskrant.nl/nieuws-achtergrond/russian-and-chinese-hackers-gained-access-to-ema~bdc61ba59/
[102] FireEye - Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity - https://www.fireeye.com/blog/threat-research/2021/04/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.html
[103] Reuters - Poland says it sees link between hacking and Russian secret services - https://www.reuters.com/world/poland-says-it-sees-link-between-hacking-russian-secret-services-2021-06-22/
[104] Cyberscoop - Hackers target German lawmakers in an election year - https://www.cyberscoop.com/bundestag-germany-hackers-ghostwriter/
[105] ABC News - Polish intelligence agencies link cyberattack to Russia - https://abcnews.go.com/International/wireStory/polish-intelligence-agencies-link-cyberattack-russia-78420183
[106] Der Taggesspiegel - Angriffswellen russischer Hacker auf Abgeordnete - https://www.tagesspiegel.de/politik/gefahr-fuer-die-bundestagswahl-angriffswellen-russischer-hacker-auf-abgeordnete/27418978.html
[107] Financial Times - Germany's spy chief warns of cyber-attacks on Bundestag election - https://www.ft.com/content/c41f14d4-e993-4a5d-b728-320223d652ef
[108] War on the Rocks – Hack-and-Leak operations and US Cyber Policy - https://warontherocks.com/2020/08/the-simulation-of-scandal/
[109] Verizon – 2021 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir
[110] Auth0 - Phishing Goes Viral: COVID-19 Themes in Cybercrime - https://auth0.com/blog/phishing-goes-viral-COVID-19-themes-in-cybercrime
[111] Kaspersky - APT annual review: What the world's threat actors got up to in 2020 https://securelist.com/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99574/
[112] PwC - Five cyber threat trends to prepare for in 2021 - https://www.pwc.co.uk/issues/cyber-security-services/insights/five-cyber-threat-trends-to-prepare-for-in-2021.html
[113] CrowdStrike - 2021 Global Threat Report - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Cybercriminals have also been observed selling tailored COVID-19 related phishing kits in underground forums[114] as well as spoofing domains designed for harvesting credentials and personal data e.g. as stimulus packages were announced.[112] When COVID-19 vaccine travel certificates were introduced by governments all around the world, cybercriminals were observed selling fakes ones on the dark web.[115]

We also observed cybercriminals, in their pursuit of money, spreading fake news about COVID-19 via digital advertisements and websites related to potential COVID-19 cures and other COVID-19 prevention measures.[116] The goal of these fraud schemes was to trick people into buying fake medicines and other goods related to COVID-19.[117]

COVID-19 also created opportunities for targeted ransomware attacks since the potential disruption of organisations within the healthcare and public health sector will have multiple impacts during the pandemic.[118] The top ransomware families that targeted the healthcare and public health sector were Maze, Conti, Netwalker, and Ryuk and we observed the focused targeting of small and medium-sised hospitals and clinics.[119]

Our assessment is that COVID-19 cybercriminal activities will continue and will adapt to emerging COVID-19 topics and regional phases of the pandemic.[118,119] It is also our considered view that the healthcare and public health sector will certainly continue to be heavily targeted by ransomware groups as long as the pandemic lasts. Finally, in our opinion the targeting of COVID-19 related applications deployed by governments, whose data can be valuable and be made available for sale in underground markets and phishing campaigns, is likely.[120]

The exploitation of Work-From-Home technologies. During the pandemic, organisations were forced to change their strategies and quickly adopt technologies that would support the new reality of remote working. This allowed cybercrime adversaries to take advantage of the rapid deployment of these teleworking technologies and exploit them for initial access. Technologies that have been heavily targeted by cybercrime actors are network appliances[121] and remote access services (especially Virtual Private Network[122], Citrix[123][124] and RDP services[125]). The exploitation of such technologies involved old, unpatched and newly discovered vulnerabilities as well as initial access via compromised credentials.[126]

In our view cybercrime threat actors will certainly continue targeting technologies that support teleworking and specifically VPN and remote access services. The organisation will be relying on these services as long as the pandemic lasts and their successful compromise by the adversaries gives the latter the opportunity of remote access to their victims without even deploying any malware.[127] Another interesting point is that the potential return to the office may leave these teleworking services orphaned and this will provide additional opportunities for adversaries.[124] All these highlight the importance of fundamentals such as patch and vulnerability management as well as the security hardening of these systems and applications.

[114] Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
[115] Euronews - Fake COVID vaccine certificates sold on dark web for €150 - https://www.euronews.com/2021/07/08/fake-COVID-vaccine-certificates-sold-on-dark-web-for-150
[116] Europol - Catching the virus cybercrime, disinformation and the COVID-19 pandemic - https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-COVID-19-pandemic
CTI League – Darknet Report 2021 - https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
[117] Council of Europe - Cybercrime and COVID-19 - https://www.coe.int/en/web/cybercrime/-/cybercrime-and-COVID-19
[118] Europol - Catching the virus cybercrime, disinformation and the COVID-19 pandemic - https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-COVID-19-pandemic
[119] CTI League – Darknet Report 2021 - https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
[120] FireEye / Mandiant - M-Trends 2021 https://content.fireeye.com/m-trends/rpt-m-trends-2021
[121] Bank Info Security - Attackers Exploiting F5 Networks' BIG-IP Vulnerability - https://www.bankinfosecurity.com/hackers-are-exploiting-critical-f5-networks-vulnerability-a-16238
[122] Hacker News - Hackers Exploit SonicWall Zero-Day Bug in FiveHands Ransomware Attacks - https://thehackernews.com/2021/04/hackers-exploit-sonicwall-zero-day-bug.html
[123] ZDNet - Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme - https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/
Verizon – 2021 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/
[124] CERT-EU - Threat Landscape Report (Volume 1) - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf
[125] ZDNet - Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme - https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme
[126] IBM – Cost of a Data Breach Report 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[127] Kaspersky - Advanced Threat predictions for 2021 - https://securelist.com/apt-predictions-for-2021/99387/

Cybercriminals go where money is (…to targeted ransomware). During the reporting period, the frequency and the complexity of ransomware attacks increased[124] (by more than 150% in 2020[128]) and became one of the greatest threats that organisations face today regardless of the sector to which they belong. We are observing the golden era of ransomware – it has become a national security priority[129]– and some argue that it has not yet reached the peak of its impact.[130] Ransomware attacks are such a big issue that the OFAC (Office of Foreign Assets Control) issued an advisory to instruct organisations about the risks of potential sanctions for facilitating ransomware payments.[131]

It has been observed that cybercriminals are less likely to target payment-related data (e.g. credit cards) and more likely to target any data that will have an impact on the victims' operations.[132] The successful business model of human-operated ransomware (aka Big Game Hunting) has been increasingly attracting cyber-criminal threat actors and it is also having an impact on their targeting.[133] An indicative example is the FIN11 threat group whose observed target has changed due to the likely shift of its operations from point-of-sale (POS) campaigns to targeted ransomware.[134]

Moreover, the Ransomware-as-a-Service (RaaS) business model is blooming.[135] During 2020, two-thirds of ransomware campaigns were attributed to operators using RaaS.[136] This trend sets a relatively low barrier for conducting this type of cybercrime and allows inexperienced cybercriminals to conduct ransomware attacks.[137]

Taking into account the increasing number of publicly reported ransom payments, the success of the RaaS business model, and the active recruitment of new members for the ransomware groups on Dark Web forums.[138] [139] Our assessment is that more cybercriminals will very likely be attracted to shifting their targeting to focus on targeted ransomware operations and replicate these successes.[140]

Multiple extortion methods. During the reporting period, the tactics that ransomware groups use to put pressure on their victims and force them to pay the ransom have evolved. In late 2019, the Maze group demonstrated double extortion tactics[141]: a) the systems and data of an organisation are encrypted and a ransom is requested, and b) the organisation's sensitive data are exfiltrated and Maze operators threaten to publish the exfiltrated data on "public shaming websites" as extra leverage to demand further ransom payments.

During the reporting period, we have observed further evolutions in the tactics used by ransomware groups:[134] [142]

- Monetisation of the stolen information through data auctions in the dark web;[143]
- Media amplification of their victim's compromise by contacting journalists;[144]
- Cold calling victims if they begin the ransomware recovery process without paying the ransom;[145]

[128] Group-IB - Group-IB: ransomware empire prospers in pandemic-hit world. Attacks grow by 150% - https://www.group-ib.com/media/ransomware-empire-2021/
[129] Coveware - Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority - https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
[130] DoublePulsar - The hard truth about ransomware: we aren't prepared, it's a battle with new rules, and it hasn't near reached peak impact - https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasn-t-a93ad3030a54
[131] OFAC - Ransomware Advisory - https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001
[132] Verizon – 2021 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/
[133] CrowdStrike - 2021 Global Threat Report - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
[134] FireEye / Mandiant - M-Trends 2021 https://content.fireeye.com/m-trends/rpt-m-trends-2021
[135] ZDNet - Ransomware as a service is the new big problem for business - https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/
[136] Group-IB - Group-IB: ransomware empire prospers in pandemic-hit world. Attacks grow by 150% - https://www.group-ib.com/media/ransomware-empire-2021
[137] Europol - Catching the virus cybercrime, disinformation and the COVID-19 pandemic - https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-COVID-19-pandemic
[138] Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf
[139] ZDNet - Ransomware: Why we're now facing a perfect storm - https://www.zdnet.com/article/ransomware-why-were-now-facing-a-perfect-storm/
[140] PwC - Five cyber threat trends to prepare for in 2021 - https://www.pwc.co.uk/issues/cyber-security-services/insights/five-cyber-threat-trends-to-prepare-for-in-2021.html
[141] Checkpoint - Ransomware Evolved: Double Extortion - https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/
[142] Flashpoint - Facing Five Types of Ransomware and Cyber Extortion - https://www.flashpoint-intel.com/blog/facing-five-types-of-ransomware-and-cyber-extortion/
[143] Computer Weekly - Sodinokibi gang begins dark web celebrity data auctions - https://www.computerweekly.com/news/252485589/Sodinokibi-gang-begins-dark-web-celebrity-data-auctions
[144] The Record - Ransomware Gang Threatens To Launch DDoS Attacks, Call Reporters and Business Partners - https://therecord.media/ransomware-gang-threatens-to-launch-ddos-attacks-call-reporters-and-business-partners/
[145] ZDNet - Ransomware gangs are now cold-calling victims if they restore from backups without paying - https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/

- Reaching out to business partners, investors, board members and other stakeholders disclosing information about the attack;[146]
- Conducting DDoS attacks against the victim in order to add more pressure to pay the ransom;[147]
- Reaching out to victim's customers and clients to action and demand a ransom payment;[148]
- Calling and harassing employees;[149]
- Turning to revenge porn as an extortion tactic.[150]

In the past, ransomware groups have been opportunistically targeting mostly small and medium-sised enterprises with security programs that are not very mature but currently we have observed a strong focus on targeting bigger organisations that could potentially pay higher ransoms.[151] The evolution and escalation of cybercriminals' extortion tactics are aligned with increased pressure to pay the ransom needed on these bigger organisations. Our assessment is that the extortion methods of cybercriminals will certainly evolve further so they keep succeeding in getting higher ransom payments from their victims.

Increasing collaboration and professionalisation. During the reporting period, we observed cybercrime groups that have developed specialised cybercrime services, and cybercriminals that have built relationships within the ecosystem as well as affiliate models.

The cybercrime ecosystem has a global presence. In this ecosystem, we observed different actors providing and specialising in different services. This "Cybercrime-as-a-Service" trend lowers the barriers for threat actors that want to conduct cybercrimes while it enhances the reach of cyberattacks. The different types of services offered in the cybercrime ecosystem include:[152]

- Main types of services: access brokers, phishing kits, credit/debit card testing services, malware packing services, web inject kits, hardware for sale, ransomware, loaders, (bulletproof) hosting and infrastructure, DDoS attack tools, anonymity and encryption, crime-as-a-service, counter antivirus service/checkers, recruiting for criminal groups;
- Distribution services: social network and instant messaging spam, exploit kit development, spam e-mail distribution, purchasing traffic and/or traffic distribution systems (TDS);
- Monetisation services: money mule and cashing services, reshipping fraud networks, dump shops, collection and sale of payment card information, money laundering, ransom payments and extortion, wire fraud cryptocurrency services.

Many of the cybercrime groups in this ecosystem provide services that support targeted ransomware operations, but access brokers play an increasingly critical role.[153] We have observed cybercriminal groups that had historically been operating banking trojans (e.g. Trickbot,[154] Qakbot[155]) capitalise on their access to compromised organisations by selling it (mostly to ransomware groups and operators). According to publicly available reports, there are at least 10 threat actors that act as access facilitators (or are ransomware affiliates) and sell their access to multiple ransomware operators[156]. While there is not a 1:1 relationship between these access-enabling malwares and ransomware attacks[156] there was a unique relationship between Emotet (malware distribution), Ryuk (ransomware), and Trickbot

[146] Bleeping Computer - Ransomware gang plans to call victim's business partners about attacks - https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/
[147] Threat Post - Ransomware's New Swindle: Triple Extortion - https://threatpost.com/ransomwares-swindle-triple-extortion/166149/
[148] Bleeping Computer - Ransomware gang urges victims' customers to demand a ransom payment - https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/
[149] FireEye / Mandiant - M-Trends 2021 https://content.fireeye.com/m-trends/rpt-m-trends-2021
[150] Motherboard - Ransomware Gang Turns to Revenge Porn - https://www.vice.com/en/article/z3xzby/ransomware-gang-revenge-porn-leaks-nude-images
[151] Flashpoint - Facing Five Types of Ransomware and Cyber Extortion - https://www.flashpoint-intel.com/blog/facing-five-types-of-ransomware-and-cyber-extortion/
[152] Europol - IOCTA 2020 - https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
[153] Digital Shadows - The Rise Of Initial Access Brokers - https://www.digitalshadows.com/blog-and-research/rise-of-initial-access-brokers/
[154] CISA – TrickBot Malware - https://us-cert.cisa.gov/ncas/alerts/aa21-076a
[155] AT&T – The risk of QakBot - https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot
[156] Proofpoint - The First Step: Initial Access Leads to Ransomware - https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

(backdoor) that suggests that the groups behind these different approaches to attack are either part of a larger criminal organisation or they increasingly collaborate and depend on each other[157].

We have also observed cybercrime groups that have developed affiliate programs where they exclusively sell the malware to the affiliates and share the money paid.[158] Finally, we have observed ransomware groups creating cartels to enhance collaboration, share tactics and help each other publish their victims' data on their "public shaming sites".[159]

Our assessment is that botnet operators will very likely capitalise on their infections by selling access to other cybercriminals.[160] It is also our opinion that access brokers and the threat actors behind them will very likely increase in sophistication and demand, while some of them are likely to abandon cybercrime forums and use private channels. Finally, state-backed threat actors will likely be buying initial access to organisations of interest from access brokers[161].

Managed service providers as high-value targets for cybercriminals. Nowadays, we observe that organisations are increasingly outsourcing their IT infrastructure management and are depending on other companies for various digital services. Managed service providers are high-value targets for cybercriminals since their compromise enables them to target their clients as well.

The compromise of a service provider introduces the following potential risks for its clients;[162]

- Confidentiality risks related to the clients' data as they can be exfiltrated and stolen;
- Availability risks related to the continuity of the service provider's business, with a subsequent impact on its clients;
- Risks related to the potential propagation of an infection from the service provider to its clients;
- Risks related to the misuse of clients' service accounts for further malicious activities.

According to the ENISA Threat Landscape on Supply Chain[10], attacks against managed service providers are increasing but it is still unclear whether the scope of the attackers was also to target their clients in all cases. Within the reporting period, some of the most prominent cybercriminal activities against service providers include the cases of Blackbaud,[163] SendGrid,[164] AG[165] and Kaseya.[166]

The cyberattack against Kaseya by the REvil ransomware group was one of the major cyberattacks observed during the reporting period.[167] Kaseya is a vendor that provides Kaseya VSA software that is widely used by Managed Service Providers to manage IT infrastructure. The impact of this supply chain attack was huge;[168] 50 Managed Service Providers (MSPs) had been using Kaseya's VSA software which was compromised while 800-1500 businesses that were managed by the compromised MSPs were infected with the ransomware. Moreover, about one

[157] https://intel471.com/blog/understanding-the-relationship-between-emotet-ryuk-and-trickbot
[158] Group-IB - Group-IB: ransomware empire prospers in pandemic-hit world. Attacks grow by 150% - https://www.group-ib.com/media/ransomware-empire-2021/
[159] Cyware – The Rise and Fall of Maze Cartel - https://cyware.com/news/the-rise-and-fall-of-maze-cartel-53bc9108
Analyst1 - Ransom Mafia - Analysis of the World's First Ransomware Cartel - https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
[160] Proofpoint - Q4 2020 Threat Report: A Quarterly Analysis of Cybersecurity Trends, Tactics and Themes - https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes
[161] Intel471 - Partners in crime: North Koreans and elite Russian-speaking cybercriminals - https://intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals
[162] CERT-EU - Threat Landscape Report (Volume 1) - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf
[163] ZDNet - Cloud provider stopped ransomware attack but had to pay ransom demand anyway - https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/
[164] Krebs on Security - Sendgrid Under Siege from Hacked Accounts - https://krebsonsecurity.com/2020/08/sendgrid-under-siege-from-hacked-accounts/
[165] ZDNet - German tech giant Software AG down after ransomware attack - https://www.zdnet.com/article/german-tech-giant-software-ag-down-after-ransomware-attack/
[166] PaloAlto - Understanding REvil: The Ransomware Gang Behind the Kaseya Attack - https://unit42.paloaltonetworks.com/revil-threat-actors/
[167] CISA / FBI - Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack - https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
[168] Bleeping Computer - Kaseya: Roughly 1,500 businesses hit by REvil ransomware attack - https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/

million computers were affected by this ransomware attack[169] and REvil operators have requested 50 million dollars for a universal decryptor. It is interesting to note that the threat group demanded ransom payments only from the end businesses that were impacted and not from the compromised MSPs. While MSPs have been (indirectly) targeted by supply chain attacks, the fact that they could deploy software (ransomware in this case) to their clients (this is part of the daily tasks of IT infrastructure management) amplified the effect of this attack.

Our assessment is that cybercriminal actors will certainly continue targeting (directly or indirectly via their suppliers) managed service providers as a way to target the clients of MSPs, especially with respect to ransomware attacks.[170]

Cybercriminals transitioning to the cloud. The pandemic fastened the adoption of cloud infrastructure and services by organisations globally and the "moving to the cloud" trend is expected to continue for the foreseeable future. However, apart from the apparent benefits of migrating to the cloud, there are also associated risks for organisations.[171] The rapid deployment of cloud infrastructure and services due to the urgent needs of the teleworking workforce during the pandemic as well as the gap in cloud-specific expertise[172] resulted in poorly secured and managed cloud deployments that provide opportunities for cybercriminals. According to publicly available reports, misconfigured cloud deployments were a leading cause of breaches[173] while external cloud systems were more common than on-premises assets in data breaches.[174]

Cybercriminals (as well as state-back actors) have already identified these opportunities and developed capabilities to breach cloud infrastructure and services. During the reporting period, we observed cybercriminals enumerating cloud environments,[175] deploying the first cryptomining worm to steal AWS credentials,[176] cryptomining on Linux servers in the cloud,[177] and targeting Docker and Kubernetes environments.[178,179] Moreover, there is an increasing trend of cloud providers being compromised by ransomware groups such as BlackBaud,[180] Swiss Cloud,[181] Equinix,[182] and Cloudstar.[183]. Finally, credential-based attacks against cloud services that are poorly secured or have not enabled Multi-Factor Authentication (MFA) proliferate.[184]

Our assessment is that attacks against cloud environments will almost certainly continue and will likely have a greater impact as more organisations adopt and implement Cloud-First strategies. Cloud downtimes will likely cause enough pressure (due to SLAs as well as a lack of tested recovery processes and cloud expertise) to coerce companies into paying ransoms in cases where they have been victims of ransomware attacks (even if they have backups in some cases)[185].

[169] Lawfare Blog - The Kaseya Ransomware Attack Is a Really Big Deal - https://www.lawfareblog.com/kaseya-ransomware-attack-really-big-dea l
[170] Canadian Center of Cybersecurity – National Cyberthreat Assessment - https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020
[171] CERT-EU - Threat Landscape Report (Volume 1) - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf
ZeroFOX - The Future of Digital Threats: 2020 Insights, 2021 Predictions - https://www.zerofox.com/blog/cyber-threat-trends-report/
[172] CloudHealth - The Cloud Management Skills Gap Is Real. Here Are 5 Ways to Adapt - https://www.cloudhealthtech.com/blog/gartner-report-cloud-management-skills-gap
[173] IBM – Cost of a Data Breach Report 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[174] Verizon – 2021 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/
[175] PaloAlto - TeamTNT Actively Enumerating Cloud Environments to Infiltrate Organisations - https://unit42.paloaltonetworks.com/teamtnt-operations-cloud-environments/
[176] Cado Security - Team TNT – The First Cryptomining Worm to Steal AWS Credentials - https://www.cadosecurity.com/post/team-tnt-the-first-cryptomining-worm-to-steal-aws-credentials
[177] Intezer - New Malware Variant Exploits Production Environment - https://www.intezer.com/blog/cloud-security/rocke-group-actively-targeting-the-cloud-wants-your-ssh-keys/
[178] AquaSec - TeamTNT Pwn Campaign Against Docker and Kubernetes Environments - https://blog.aquasec.com/teamtnt-campaign-against-docker-kubernetes-environment
[179] Intezer - New Attacks on Kubernetes via Misconfigured Argo Workflows - https://www.intezer.com/blog/container-security/new-attacks-on-kubernetes-via-misconfigured-argo-workflows/
[180] ZDNet - Cloud provider stopped ransomware attack but had to pay ransom demand anyway - https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/
[181] Latest Hacking News - Swiss Cloud Hosting Provider Suffered Ransomware Attack - https://latesthackingnews.com/2021/05/06/swiss-cloud-hosting-provider-suffered-ransomware-attack/
[182] ZDNet - Data center giant Equinix discloses ransomware incident - https://www.zdnet.com/article/data-center-giant-equinix-discloses-ransomware-incident/
[183] Fitch Ratings - Cloudstar Ransomware Highlights Multiple Issuer Exposure Potential - https://www.fitchratings.com/research/insurance/cloudstar-ransomware-highlights-multiple-issuer-exposure-potential-22-07-2021
[184] Verizon – 2021 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/
[185] The Record - Swiss Cloud becomes the latest web hosting provider to suffer a ransomware attack - https://therecord.media/swiss-cloud-becomes-the-latest-web-hosting-provider-to-suffer-a-ransomware-attack/

Cybercrime attacks increasingly target and impact critical infrastructure. During the reporting period, we observed increased targeting of critical infrastructure by cybercrime actors. Major critical infrastructure sectors being impacted are the healthcare, transportation, and energy sectors.

Ransomware attacks have disrupted the operations of public health agencies, hospitals, and emergency services.[186] Threat actors have been specifically targeting the healthcare and public health sector despite the promises of some ransomware gangs to stop doing so during the pandemic.[187] They grasped this opportunity during the pandemic since this sector became extremely significant and highly susceptible.[188] Ryuk is a ransomware gang that heavily targeted the healthcare sector in the USA[186] despite the attempts cybersecurity vendors to take them down.[189]

According to publicly available reports, the transportation industry has faced cybercrime threats related to initial access offerings, gift card fraud, and ransomware.[190] All four major shipping companies have fallen victim to ransomware attacks during recent years[191] while the trucking sector has experienced high-profile ransomware attacks.[192] Because the Courier, Express, and Parcel (CEP) business is blooming it could be regarded as critical infrastructure during the pandemic. Thus it attracted the attention of cybercriminals who targeted the CEP sector.[193] Finally, despite limited flights and air traffic during the pandemic, the aviation industry faced disproportional numbers of cyberattacks.[194]

The ransomware attack against Colonial Pipeline (a US fuel company) by the Darkside ransomware group had a high impact as a perceived gas shortage led to stockpiling and panic (although the IT network was impacted, operators stopped ICS operations for protection).[195] Colonial Pipeline's ransomware attack[196] also drove policy initiatives within the US with Joe Biden signing an Executive Order to strengthen cybersecurity[197] and restarting the discussion on the responsibility of states for cybercrime attacks.[198] [199] Regarding the targeting of ICS networks, there has been an increase in public and non-public ransomware events affecting ICS environments.[200] Ransomware families like EKANS,[201] Megacortex[202] and Clop[203] have already developed ICS-aware functionality to stop industrial processes.

It is our opinion that, as our society becomes increasingly dependent on technology and Internet connectivity, cybercrime attacks against critical infrastructure are very likely to become more disruptive. It is also likely that

[186] CISA - Ransomware Activity Targeting the Healthcare and Public Health Sector - https://us-cert.cisa.gov/ncas/alerts/aa20-302a
Wired - The untold story of a cyberattack, a hospital, and a dying woman - https://www.wired.co.uk/article/ransomware-hospital-death-germany
HHS - Ransomware Trends 2021 - https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
BBC - Cyber-attack on Irish health service 'catastrophic' - https://www.bbc.com/news/world-europe-57184977
[187] Bleeping Computer - Ransomware Gangs to Stop Attacking Health Orgs During Pandemic - https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/
[188] CTI League – Darknet Report 2021 - https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
[189] Microsoft - New action to combat ransomware ahead of US elections - https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
[190] Intel471 - How cybercriminals create turbulence for the transportation industry - https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry
[191] ZDNet - All four of the world's largest shipping companies have now been hit by cyber-attacks - https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/
[192] Freight Waves - 5 defining cyberattacks on trucking and logistics in 2020 - https://www.freightwaves.com/news/5-defining-cyberattacks-on-trucking-and-logistics-in-2020
[193] SRM - The Courier, Express and Parcel industry is booming. But cyber security must grow alongside revenues. Here's why - https://www.srm-solutions.com/blog/the-courier-express-and-parcel-industry-is-booming-but-cyber-security-must-grow-alongside-revenues-heres-why/
[194] EUROCONTROL EATM-CERT Services - Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope? - https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf
[195] Dragos - Recommendations Following the Colonial Pipeline cyber-attack - https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/
[196] CISA - Ransomware Impacting Pipeline Operations - https://us-cert.cisa.gov/ncas/alerts/aa20-049a
[197] White House - Executive Order on Improving the Nation's Cybersecurity - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[198] Atlantic Council - Assessing Russia's role and responsibility in the Colonial Pipeline attack - https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/
[199] New York Time - Biden Warns Putin to Act Against Ransomware Groups, or U.S. Will Strike Back - https://www.nytimes.com/2021/07/09/us/politics/biden-putin-ransomware-russia.html
[200] Dragos - ICS Threat Activity on the Rise in Manufacturing Sector - https://www.dragos.com/blog/industry-news/manufacturing-sector-cyber-threats/
[201] Dragos - EKANS Ransomware and ICS Operations - https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
SentinelOne - New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware - https://labs.sentinelone.com/new-snake-ransomware-adds-itself-to-the-increasing-collection-of-golang-crimeware/
[202] Dragos - EKANS Ransomware Misconceptions and Misunderstandings - https://www.dragos.com/blog/industry-news/ekans-ransomware-misconceptions-and-misunderstandings/
[203] Otorio - A New Variant of Clop Targets Industrial Companies - https://otorio.com/blog/ransomware-targeting-industry-4-0/

disruptive attacks against critical infrastructure may masquerade as ransomware attacks while having different objectives.[198] [204]

Dark web markets contribute to and follow the actors' business models. During the reporting period, we observed a general trend that applies to many of actors, predominantly to the cybercriminals given the financial implications. The dark web has become even more connected with the threat actors during the reporting period. In previous years we observed the growth of both the flow of cryptocurrencies and the anonymising of networks. These two key developments helped the dark wed become even more accessible due to the anonymisation it provided.[205]

Marketplaces have given the ability to threat actors to procure services and capabilities that they lack, and to promptly gain access to breached data.[206] Through the markets and underground forums threat actors that lack certain skills, for example to develop a custom ransomware, are able to identify RaaS providers and procure the necessary skillset. The providers offer to the customers various services (trading, payment and recovery). In exchange for these tools and services the providers receive a small portion of the ransoms[207]. A recent report also showed the average price listings of the most common requested services.[208] We have also seen cases in which the threat actors launched recruitment campaigns via the dark wed (Revil). [209]

In conclusion, the revenue of dark web markets hit a record during the reporting period at a total of 1.7 billion dollars' worth in cryptocurrency, even though this was mainly to the growth of Hydra.[210] This is a prime indicator that the dark wed has become an integrated part in the ecosystem of the threat actors.

2.3 HACKER-FOR-HIRE ACTORS

Rise of hacker-for-hire services. This category of threat actors refers to actors within the "Access-as-a-Service" (AaaS) market that is mostly comprised of firms that offer offensive cyber capabilities. Their clients are usually governments (but also corporations and individuals) and the service categories they offer are (usually bundled altogether as a single service):[211] Vulnerability Research and Exploitation, Malware Payload Development, Technical Command and Control, Operational Management, and Training and Support.

The hacker-for-hire companies operate legally in their country of operation and the market as a whole is currently semi-regulated.[211] The clients of these companies pay them mostly to conduct cyber espionage operations, get access to advanced offensive cyber capabilities and enjoy plausible deniability. These hacker-for-hire threat actors complicate the threat landscape and introduce the following challenges for defenders:[212]

- Their targeting cannot be predicted as it depends on the tasks their clients order; there is no focus on specific sectors and thus any sector has the potential to be targeted.
- These threat actors act as proxies and it is very difficult for defenders to identify their sponsors as well as their objectives.

[204] Kaspersky - ICS threat predictions for 2021 - https://securelist.com/ics-threat-predictions-for-2021/99613/
[205] Five Key Reasons Dark Web Markets Are Booming - https://www.forbes.com/sites/forbestechcouncil/2020/04/23/five-key-reasons-dark-web-markets-are-booming/?sh=378b3b3a6f6f
[206] Stolen data on the dark web is being accessed faster than ever - https://siliconangle.com/2021/10/19/stolen-data-dark-web-accessed-quicker-ever/
[207] Cybercrime - A Peek at the Cybercriminal Ecosystem - https://www.institutmontaigne.org/en/blog/peek-cybercriminal-ecosystem
[208] The cost of hiring a hacker on the dark web: report - https://www.comparitech.com/blog/information-security/hiring-hacker-dark-web-report/
[209] REvil Ransomware Gang Offers $1 Million As Part Of Recruitment Drive- https://www.forbes.com/sites/simonchandler/2020/10/06/revil-ransomware-gang-offers-1-million-as-part-of-recruitment-drive/?sh=2a40595d7bab
[210] Russian dark web marketplace Hydra cryptocurrency transactions reached $1.37bn in 2020- https://www.zdnet.com/article/russian-dark-web-marketplace-hydra-cryptocurrency-transactions-reached-1-37bn-in-2020/
[211] Atlantic Council - Countering Cyber Proliferation – Zeroing in on Access-as-a-Service - https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf
[212] PwC - Cyber Threats 2020: A Year in Retrospect - https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

During the reporting period, the major hacker-for-hire actor under discussion was the NSO Group and a leak that was related to the targeting of activists, journalists, and political leaders.[213] The impact of this leak is evidenced by several proposals across the globe on managing such a threat.[214] [215]

We also observed the alleged hacker-for-hire group called DeathStalker that has been targeting organisations within the Financial and Legal services sectors for corporate espionage.[216] While the group's TTPs are evolving (e.g. use of false flags[217]), its operations are representative of the fact that these threat actors can accomplish their goals without using highly sophisticated tools.[218]

Some groups have focused on cyber espionage activities in specific regions e.g. Bahamut targeted entities in the Middle East and South Asia, CostaRico mostly focused on targets in South Asia, etc.[212] Thus, we observed some regional targeting from some hacker-for-hire groups, which is likely due to their country of operations as well as their client base.

Our assessment is that hacker-for-hire companies will certainly continue targeting any sector based on their sponsors' requirements. While the operations of hacker-for-hire companies are disclosed from time to time, our assessment is that these companies will certainly complicate defenders' efforts in identifying their original clients.[219] Finally, in our opinion, the hacker-for-hire industry will likely experience increased state control and oversight (and potentially more attention from cybersecurity companies) due to potential national security risks as well as human rights abuse[220] [213].

2.4 HACKTIVISTS

Hacktivists' operations remain low in numbers, sophistication, and impact. After 2016, we observed a falloff in hacktivism following its peak during the period 2010-2015.[221] Nowadays, hacktivists act mostly in small groups of individuals, protesting against regional events and targeting specific organisations.[222] Their targets remain their traditional ones: financial institutions and governmental agencies. Massive public participation is missing.[222] This is likely due to the prosecution of various hacktivists in recent years which has acted as a deterrent.[223]

Regarding hacktivists' capabilities, their tactics remain "old school" [224] mostly focusing on DDoS attacks, defacements, releasing of sensitive data, and account takeovers.[222] During the reporting period, the frequency of hacktivists' operations was low and did not have the impact they had in the past. This is something that can be attributed to the limited sophistication of their operations and their limited resources as well as the improved security controls that their target organisations have developed over the years.

It was expected that there would be a rise in hacktivism during the pandemic as more people were staying at home and this would increase the potential for participating in online protests (and disruptions).[223,224] However, this

[213] Amnesty International - Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally - https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/
Google Sheets - Links to articles about Project Pegasus - https://docs.google.com/spreadsheets/d/1aWl8aTFTsEc2Q66picrIBiv5aXVyNZlmrrhYv10MLfw/edit#gid=0
[214] The Guardian - Israel 'creating task force' to manage response to Pegasus project - https://www.theguardian.com/world/2021/jul/21/israel-creating-task-force-to-manage-response-to-pegasus-project
[215] Enough is Enough – Joint statement from representatives TOM MALINOWSKI, KATIE PORTER, JOAQUIN CASTRO AND ANNA G. ESHOO ON THE ABUSES LINKED TO THE NSO GROUP'S PEGASUS SPYWARE https://malinowski.house.gov/media/press-releases/enough-enough-joint-statement-representatives-tom-malinowski-katie-porter
[216] Kaspersky - APT trends report Q3 2020 - https://securelist.com/apt-trends-report-q3-2020/99204/
[217] Kaspersky - Advanced Threat predictions for 2021 - https://securelist.com/apt-predictions-for-2021/99387/
[218] Kaspersky - APT annual review: What the world's threat actors got up to in 2020 https://securelist.com/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99574/
[219] Blackberry - BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps - https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf
[220] Atlantic Council - Countering Cyber Proliferation – Zeroing in on Access-as-a-Service - https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf
Citisen Lab - Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus - https://citisenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/
New York Times - Israeli Companies Aided Saudi Spying Despite Khashoggi Killing - https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.htm l
[221] IBM Security Intelligence - The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015 - https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/
[222] Recorded Future - Return to Normalcy: False Flags and the Decline of International Hacktivism - https://go.recordedfuture.com/hubfs/reports/cta-2019-0821.pdf
[223] Dark Reading - The State of Hacktivism in 2020 - https://www.darkreading.com/the-state-of-hacktivism-in-2020-/d/d-id/1338382
[224] ZeroFOX - The Future of Digital Threats: 2020 Insights, 2021 Predictions - https://www.zerofox.com/blog/cyber-threat-trends-report/

development did not materialise since hacktivism operations lacked technical capacity at scale and extensive public participation.[224] Moreover, the content moderation policies of some sharing platforms reduced the impact of some of the activists' operations.[225] Thus, the low hacktivism activity observed during the reporting period was mostly focused on regional events. During the reporting period, some of the most notable hacktivist activities were:

- Verkada hack – A group of hackers gained unauthorised access to 150,000 video archives of security cameras by taking over accounts. The hackers claimed responsibility for the attack and their motivation was to highlight the dangers of mass video surveillance as well as the insufficiency of security controls for securing these video recordings.[225] A Swiss hacker, who claimed hacktivism motives, was arrested and charged for this cyberattack.[226]
- Black Lives Matter – During the summer of 2020, the hacktivist group Anonymous re-emerged during the protests related to the death of George Floyd[227]. The group focused on DDoS attacks against the Minneapolis police department website as well as releasing e-mail addresses and credentials allegedly taken from police servers (but it is likely their source was old data breaches[228]).
- BlueLeaks hack – BlueLeaks was probably the most prominent hacktivist operation conducted during the reporting period. This anonymous hacktivist group leaked more than 1 million documents stolen from a Texas firm called Netsential that provided web-hosting services to several US law enforcement agencies.[224] The leaks were distributed via the DDoSecrets[229] platform whose Twitter account was later suspended for policy violations related to the distribution of hacked data.[230]

Our assessment is that the threat posed by hacktivists will very likely remain low in the near future. Our opinion is based on the number, sophistication, and impact of the hacktivists' operations during the reporting period. The focus of hacktivists' activity will remain regional although new movements are gaining traction (e.g. environmental and anti-discrimination) that are likely to develop hacktivism side-tactics and attract wider public participation for online protest (and disruption). Finally, It is our opinion that state-backed groups will almost certainly continue to leverage hacktivism as a disguise to achieve their strategic goals.

[225] ZDNet - Verkada disables accounts after reports its security cameras were breached - https://www.zdnet.com/article/verkada-disables-accounts-after-reports-its-security-cameras-were-breached/
[226] The Verge - 'Anti-capitalist' Verkada hacker charged by US government with attacks on dozens of companies - https://www.theverge.com/2021/3/19/22339625/tillie-kottmann-swiss-hacker-verkada-charged-us-government-verkada
[227] BBC - George Floyd: Anonymous hackers re-emerge amid US unrest - https://www.bbc.com/news/technology-52879000
[228] Troy Hunt - Analysing the (Alleged) Minneapolis Police Department "Hack" - https://www.troyhunt.com/analysing-the-alleged-minneapolis-police-department-hack/
[229] Krebs on Security - 'BlueLeaks' Exposes Files from Hundreds of Police Departments - https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/
[230] ZDNet - Twitter bans DDoSecrets account over 'BlueLeaks' police data dump - https://www.zdnet.com/article/twitter-bans-ddosecrets-account-over-blueleaks-police-data-dump/

3. RANSOMWARE

Ransomware is a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access. In some instances, attackers may also steal an organisation's information and demand additional payment in return for not disclosing the information to authorities, competitors, or the public.[231]

Compromise through phishing e-mails and brute-forcing on Remote Desktop Protocol (RDP) services remain the two most common infection vectors. During the reporting period in 2021, we saw that the Conti and REvil threat actors dominated the ransomware market from a financial as well as from a volume of infections point of view. Both actors provide separate ransomware-as-a-service (RaaS) platforms through which affiliates can efficiently orchestrate their attacks. The focus on RaaS-type business models increased during 2021, making proper attribution to individual threat actors difficult.

The occurrence of multiple extortion schemes also increased strongly during 2021. After initially stealing and encrypting sensitive data from organisations and threatening to release it publicly unless a payment is made, attackers also target the organisations' customers and/or partners for ransom to maximise their profits.

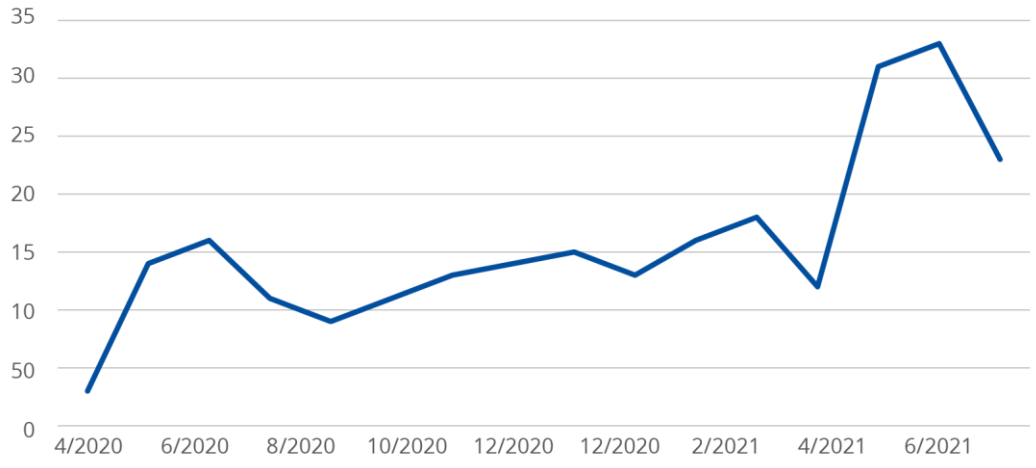
Cryptocurrency remains the most common pay-out method for threat actors. Attackers shifted to Monero as their cryptocurrency of choice because of its enhanced anonymity and the indistinguishability of transactions.

The average ransom amount doubled over the last year, though small amounts of ransom are still popular with threat actors. They tend to be paid more easily and result in less public exposure for the threat actor. The higher demands also increased. Over just a few months, the highest demand made in 2020 more than doubled in 2021.

Some large ransomware operations shut down, whether voluntary or due to actions carried out by law-enforcement agencies. However, groups have shut down in the past, only to resurface under another operation.

Several ransomware attacks were reported during the ETL reporting period. Figure 5 shows the incidents observed based on OSINT (Open Source Intelligence) collected by ENISA for the purposes of situational awareness.[232] The scope of the collection is global and multi-sectorial. Incidents, however, with a direct impact in the EU area are given priority. We have observed a steady increase in ransomware incidents being reported since 2020, and a sharp increase in May and June 2021. A list of notable ransomware incidents can be found in Annex B.

Figure 5: Ransomware incidents observed by ENISA (April 2020-July 2021)



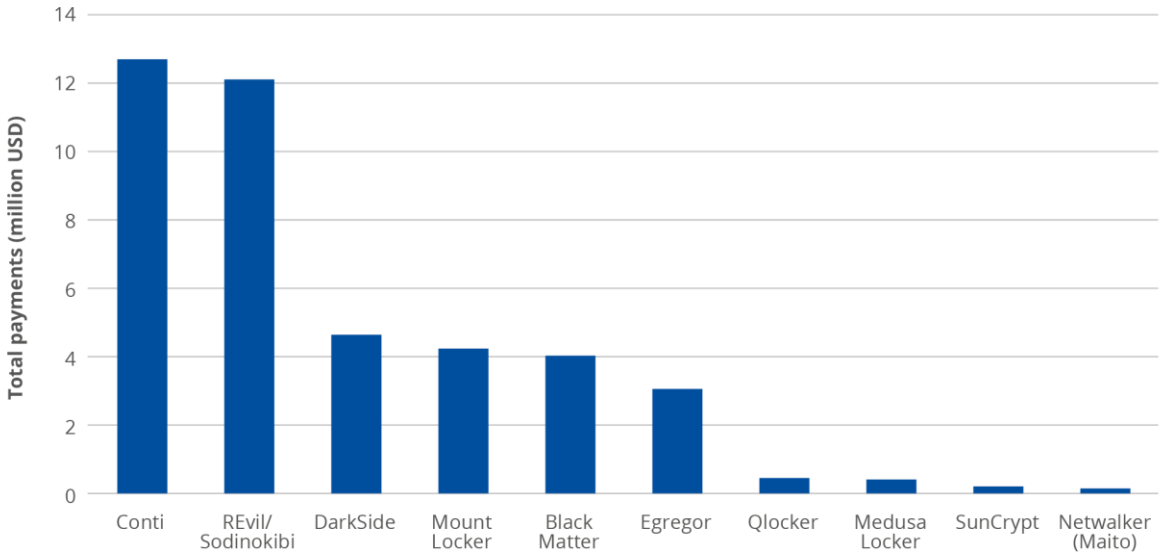
[231] NIST Preliminary Draft NISTIR 8374 - Cybersecurity Framework Profile for Ransomware Risk Management, https://csrc.nist.gov/CSRC/media/Publications/nistir//draft/documents/NIST.IR.8374-preliminary-draft.pdf
[232] In accordance with the EU cybersecurity act Art.7 Par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

3.1 TRENDS

3.1.1 Conti and REvil ransomware groups lead the market

Based on crowdsourced ransomware payment data (as illustrated in Figure 6), the ransomware groups with the most financial gains in 2021 are Conti ($12.7 million), REvil/Sodinokibi ($12 Million), DarkSide ($4.6 Million), MountLocker ($4.2 Million), Blackmatter ($4.0 Million) and Egregor ($3.1 Million).[233]

Figure 6: Ransomware data, grouped by family, in 2021. (Source: https://ransomwhe.re/)



When looking at statistics based on trends in responses to ransomware incidents, the ransomware groups with the most market share in 2021 Q1 are REvil/Sodinokibi (14.2%), Conti V2 (10.2%), Lockbit (7.5%), Clop (7.1%), and Egregor (5.3%). For 2021 Q2 the top is represented by Sodinokibi (16.5%), Conti V2 (4.4%), Avaddon (5.4%), Mespinoza (4.9%) and Hello Kitty (4.5%). These last two are newly emerging ransomware variants.[234]

Both from a financial and an incident perspective, we see that Conti and REvil dominated the ransomware market in 2021. We expect to see no infections from the original REvil/Sodinokibi and Darkside groups in the coming months, as these have shut down at the time of writing this report. We also waiting to see whether the arrest of Clop members, involved in money laundering, will impact the rest of their operations.

3.1.2 RDP and phishing remain the most common attack vectors

Initial compromise through RDP has been the major attack vector for the last few years. However, since 2020, we see that this attack vector is in decline. In contrast, attacks through phishing e-mails rose during 2020.[235] In Q2 2020, we see both vectors as the most used ways to gain an initial foothold. Note that these two vectors are also the cheapest and thus most profitable methods for threat actors.[235]

Compromise through RDP is mostly achieved by brute-forcing credentials. The advantage of this method is that threat actors enter the network using legitimate credentials, allowing them to stay unnoticed. Although organisations with a higher security maturity will monitor this type of activity, most medium to small businesses will not. Brute-forcing RDP credentials is possible due to weak credentials, lack of two-factor authentication or a secure tunnel (VPN) to access the RDP. Compromise of the RDP service itself due to a vulnerability happens but is less common.[236]

[233] Ransomwhere, https://ransomwhe.re
[234] Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority, https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
[235] Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority, https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
[236] Critical RDP Vulnerabilities Continue to Proliferate, https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/critical-rdp-vulnerabilities-continue-to-proliferate/

3.1.3 Ransomware-as-a-Service business model

The use of Ransomware-as-a-Service (RaaS) platforms during attacks has become the norm. This type of service offers a platform for other threat actors, groups, and individuals and is based on an affiliate model. The platform facilitates all the elements needed to cover a ransomware attack, from file encryption and storage to payment.

The RaaS provider takes a cut on the ransom payments received from the victim, while the affiliate stays in control of the bounty and the communication towards the victim. The platform makes all the tools needed for easy deployment on the compromised target, and these tools are under continuous development. Like a healthy business, the RaaS platforms are continuously adapting to changes in the environment in order to stay undetected by endpoint and network security tools. RaaS has made ransomware attacks available to any malicious actor, even when they lack technical knowledge.

3.1.4 Recruiting future insider threats

An upcoming trend in more elaborate ransomware attacks is the active recruitment of employees to assist during the ransomware campaign. In August 2020, a Russian national was convicted for actively targeting and recruiting an employee at Tesla. The employee needed to execute malware on his company's computer system, which would exfiltrate data from the company's network. He would then threaten to disclose the data online unless the company paid a ransom demand. The employee would receive $1,000,000 in bitcoins after the malware was installed.[237] Lockbit also promises the gain of 'millions' in its insider recruitment program.[238]

3.1.5 Profit maximisation: a shift from double to multiple extortion

Throughout 2020, double extortion was a common theme during ransomware attacks. This type of attack combines the traditional encryption of files on the victim's network and systems, as well as the exfiltration of it. The extracted data is then hosted and held hostage on a leak or dump-site owned by the ransomware group. These are also referred to as shame sites. While negotiations are ongoing, the files often remained locked. Some RaaS platforms include the feature of a timer to indicate the time a victim has left to resolve the payment or negotiate the ransom. Research showed that in Q3 2020, almost half of all ransomware incidents featured the threat of data release.[239]

Traditional ransomware attacks would only cripple the organisations' internal operations. By threatening to release the data, victims are not only pressured to meet the group's ransom demand but also by the threat to disclose the breach to their customers and partners. In previous ransomware incidents, this notification was often neglected due to fear of impacting business and public relations. Due to the public shaming aspect of breaches due to double extortion ransomware, companies are in a way incentivised to openly communicate about an incident. The threat to leak exfiltrated data has increased significantly, from 8.7% in 2020 to 81% in 2021 Q2.[240]

We see the requirement to report breaches to law enforcement agencies becoming an important theme for cybersecurity lawmakers.[241] An interview with a supposed member of the Lockbit ransomware group mentions that threat actors are aware of this. They predict that payments can become more difficult for United States-based victims. Supposedly, Europeans pay immediately out of fear for GDPR fines.[242]

In 2021, we see another evolution in the maximisation of profit: the emergence of the multiple extortion scheme. After initially stealing and encrypting sensitive data from organisations and threatening to release it publicly unless a payment is made, attackers now also target the organisations' customers and/or partners for ransom.[243] In April 2021, REvil targeted Quanta Computer, a notebook manufacturer. When the company refused to pay any ransom, the attackers turned their attention to Apple, and threatened to release blueprints they stole through the initial attack. The

[237] Case 3:20-mj-00083-WGC *SEALED*, https://www.justice.gov/opa/press-release/file/1308766/download
[238] LockBit ransomware recruiting insiders to breach corporate networks, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/
[239] Check Point - Cyber security report - 2021
[240] Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority, https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
[241] New Bill Could Force US Businesses to Report Data Breaches Quicker, https://www.tripwire.com/state-of-security/government/new-bill-could-force-u-s-businesses-to-report-data-breaches-quicker/
[242] Talos - Interview with a LockBit ransomware operator - 2021
[243] Check Point – Cyber-attack trends - Mid Year Report - 2021

campaign towards Apple was dropped and Apple did not officially comment on the incident.[244] The same tactic was seen used by the Clop ransomware gang in May 2021. After targeting RaceTrac Petroleum and threatening to release the companies' files, the actor moved forward to contact their customers and partners directly and threaten to release their files.[245] Note that some research describes the use of DDoS as the triple extortion vector, and the ransom towards the victim's client then becomes the quadruple extortion. However, a DDoS attack is only used to increase the pressure but adds no actual ransom or extortion to the process, as the company is already locked out at that time.[246] Through a ransomware breach, third parties themselves become exposed. Like a regular company, the ransomware actors are constantly on the lookout for more business opportunities. These third-party victims are ideal vectors to request new ransoms or even start new ransomware campaigns using the internal information that was previously obtained.

3.1.6 Cryptocurrency for ransom payment: a shift from Bitcoin to Monero

For a few years now, cryptocurrencies like Bitcoins have been preferred by cyber threat actors to receive ransom payments. The promise of a fast, secure, and anonymous channel to move the money made it a perfect solution. The transparent and decentralised structure makes it a reliable channel and protects the money. In addition, due to the higher computer power necessary to generate new hashes, and stricter regulations,[247] the value of bitcoin has dramatically increased over the last two years. While the wallet can offer anonymity, it is not untraceable. Due to the transparency of bitcoin transactions and the wallets associated with specific ransomware groups, it becomes possible to research the affiliation between groups and follow the payments being made. This data gives an insight to estimate the actual financial gains of threat actor groups more reliably.

In May 2021, Colonial Pipeline fell victim to a ransomware attack orchestrated by ransomware group DarkSide. The FBI was involved after the victim had already paid the ransom demand of around 75 bitcoins. By reviewing the Bitcoin public ledger, law enforcement could track multiple bitcoin transfers and identify that the group had transferred approximately 63.7 bitcoins to a specific wallet address. It turns out that the FBI had the "private key" needed to access assets from the specific Bitcoin address. With a seizure warrant, the FBI proceeded to seise the coins. It was not disclosed how the FBI obtained the private key.[248] This operation was a success and the first time law enforcement retrieved the larger part of a ransom in cryptocurrency.

After the seizure, a shift was noticed towards the use of Monero as cryptocurrency. Monero was launched as an open-source project to add anonymity and indistinguishability of transactions but quickly gained traction among users and has had stable growth over the last few years. Ransomware group REvil only accepted Monero in 2021. Other groups such as DarkSide and Babuk left the choice to the victim but added charges when choosing bitcoin to pay the ransom.[249]

While not all are originating from cybercrime, the US Internal Revenue Service (IRS) has seised $1.2 billion worth of cryptocurrency in 2021 alone.[250] Typically, seised wallets are auctioned publicly. In addition, crowdsourced projects give easy visibility to these payments and the malware families.[251]

[244] Hacker Group Mysteriously Removes Stolen Apple Schematics and Extortion Threat From Ransomware Website, https://www.macrumors.com/2021/04/26/revil-delists-stolen-apple-schematics-threat/
[245] Ransom Gangs E-mailing Victim Customers for Leverage, https://krebsonsecurity.com/2021/04/ransom-gangs-e-mailing-victim-customers-for-leverage
[246] Ransomware Double Extortion and Beyond: REvil, Clop, and Conti, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
[247] Bitcoin falls further as China cracks down on crypto-currencies, https://www.bbc.com/news/business-57169726
[248] Department of Justice Seises $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, https://www.justice.gov/opa/pr/department-justice-seises-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
[249] Monero emerges as crypto of choice for cybercriminals, https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6
[250] The IRS has seised $1.2 billion worth of cryptocurrency this fiscal year – here's what happens to it, https://www.cnbc.com/2021/08/04/irs-has-seised-1point2-billion-worth-of-cryptocurrency-this-year-.html
[251] Ransomwhere, https://ransomwhe.re/

3.1.7 Money laundering is the weak spot

At some point, threat actors want to convert their ransom from cryptocurrency to money. At that point, maintaining anonymity over the wallet becomes more challenging. Major cryptocurrency exchanges require proof of identity to keep a record of payments, which makes it difficult for threat actors to cash out their gains easily. This is where money laundering schemes come into play.

Researchers used interviews and the investigation of police files to investigate ransomware groups' modus operandi to launder their profits. Based on the results, two main models were identified; based on the payment of the ransom 1) via vouchers and 2) via bitcoins. In the crypto-based model, bitcoins are first sent through a mixer, a mechanism that groups crypto from different sources together and divides it back via random transactions, in time and value, to other destination wallets. This mixer makes it more difficult to track where and how the original transaction moves. Bitcoins are then either exchanged via 1) a bitcoin exchange for money, 2) a (human) bitcoin trader in exchange for physical money, 3) money laundering services, or 4) used directly as bitcoins.[252]

Ransomware groups are much more intertwined than was assumed. A large concentration is seen at the deposit address level, where only 199 addresses received 80% of all funds sent by ransomware addresses in 2020. An even smaller group of 25 addresses accounts for 46%. The key takeaway is that only the owners of a small pool of addresses support and control the ability to cash out ransomware gains.[253] This concentration is also the weakness of the ransomware groups. Successful operations against the owners of these addresses could impact their gains and ability to pay all people involved in the ransomware scheme.

The Nemty ransomware group shut down its operations in April 2020. Researchers discovered internal details of their operations between 2019 and 2020. The interesting part is that the list of affiliates was disclosed. Through the list, some well-known nicknames are found. These users can be found all over the place, showing that the affiliates of RaaS are not working exclusively with one provider. This overlap in users suggests that the core RaaS actors are a small group of people, which is consistent with the previous section regarding the concentration of deposit addresses.[254]

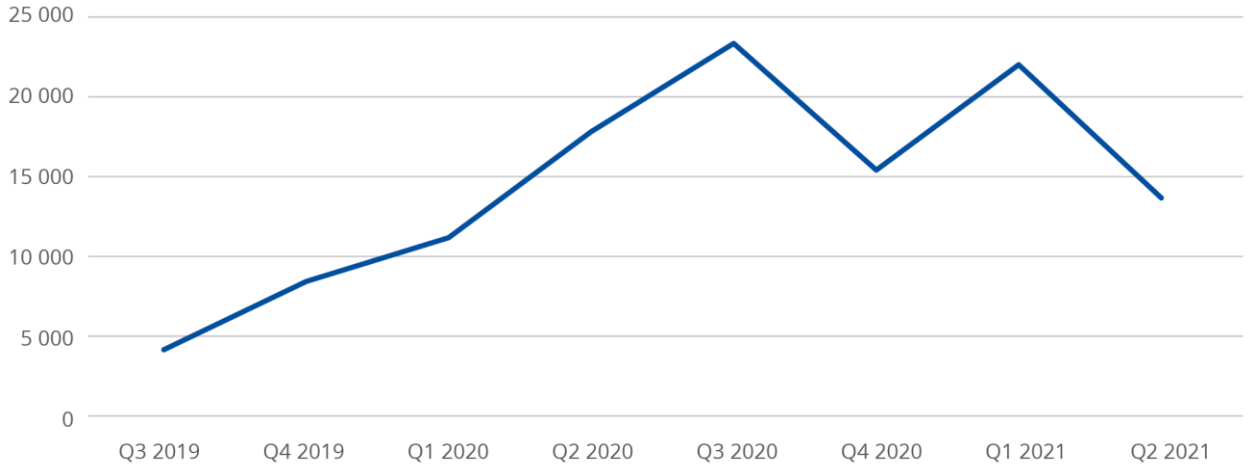
When ransomware groups are investigated, those involved in money laundering have more chances of getting caught. Transferring cryptocurrency to money is a process where true anonymity is hard to maintain. It was the case for the Clop ransomware group. Six people were arrested and charged with laundering $500 Million for the gang.[255]

The laundering schemes used are expected to further develop over the years. Only through proper international coordination of law-enforcement, but also cooperation with the private sector, e.g. exchanges markets, will we stand a chance to properly investigate money trails, to disrupt the ransomware operations.

[252] Laundering the profits of ransomware: money laundering methods for vouchers and cryptocurrencies, July 2020, European Journal of Crime Criminal Law and Criminal Justice 28(2):121-152
DOI:10.1163/15718174-02802002
[253] Chainalysis - Crypto crime report - 2021
[254] The Nemty affiliate model, https://medium.com/csis-techblog/the-nemty-affiliate-model-13f5cf7ab66b
[255] Clop ransomware is back in business after recent arrests, https://www.bleepingcomputer.com/news/security/clop-ransomware-is-back-in-business-after-recent-arrests/

3.1.7.1 The average ransom doubled in 2020

Figure 7: Average ransom, based on data from Coveware[256]



A study[257] suggests that in 2019, the average ransom paid was around $80,000. In 2020, this more than doubled to an average of $170,000. According to the same study, the average in 2021 Q1 and Q2 was around $180.000. Other research[258] finds that the average ransom increased from $115,123 in 2019 to $312,493 in 2020. Both of these findings show the same trend. For the first half of 2021, we can conclude that the average amount peaked further. These figures support the idea that small ransom amounts are still worthwhile for threat actors while also easier for companies to defend paying.

3.1.8 Highest ransom demands are skyrocketing

Another trend is an increase in the ransom demanded by threat actors. This amount is often the starting point for the ransom to be paid. If companies want to pay, negotiations are held and, usually, only a part of the initial sum is paid. The highest ransomware demand grew from $15 million in 2019 to $30 million in 2020.[259] Since this research, REvil has stepped up its game, demanding $50 million from Acer in March 2021.[260] A month later, in April, the ransomware group requested the same amount from Quanta Computer, a supplier to Apple.[261] In July 2021, after Kaseya got hit, they demanded a $70 million ransom to publish the universal decryptor to unlock every device affected.[262] Over just a few months, the highest demand of 2020 more than doubled in 2021. It is likely we will hit the cap of a $100 million ransom demand in 2022.

With record-high demands, we also see record-high pay-outs. The incidents that are publicly disclosed or that receive media attention are only the tip of the iceberg. There are other public ransomware incidents with high ransoms, where the actual amount discussed during negotiation leaked, but payment of the ransom was never confirmed, such as Garmin in 2020[263] ($10 million) and CNA in 2021 ($40 million).[264] As long as organisations keep paying, there is no reason for ransomware groups to lower their demands. The highest pay-outs become a goal or even a reference for existing and future ransomware groups.

[256] https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
[257] Group-IB "Ransomware Uncovered 2020 – 2021" Report
[258] Unit42 - Ransomware Threat Report - 2021
[259] Unit42 - Ransomware Threat Report - 2021
[260] Cyberattaque : une rançon de 50 millions de dollars demandée à Acer, https://www.lemagit.fr/actualites/252498175/Cyberattaque-une-rancon-de-50-millions-de-dollars-demandee-a-Acer
[261] Hacker Group Mysteriously Removes Stolen Apple Schematics and Extortion Threat From Ransomware Website, https://www.macrumors.com/2021/04/26/revil-delists-stolen-apple-schematics-threat/
[262] REvil gang asks for $70 million to decrypt systems locked in Kaseya attack, https://therecord.media/revil-gang-asks-70-million-to-decrypt-systems-locked-in-kaseya-attack/
[263] Garmin reportedly paid multimillion-dollar ransom after suffering cyberattack, https://www.theverge.com/2020/8/4/21353842/garmin-ransomware-attack-wearables-wastedlocker-evil-corp
[264] One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

3.1.9 Overall increase in costs and revenue loss due to ransomware

When a ransomware incident happens, organisations are confronted with a lot of cost. These costs include the amount of ransom, downtime, and the cost of people and actual operational and technical remediation, etc. A survey conducted across 30 countries showed that the overall cost of remediating a ransomware attack has vastly increased, from $761,106 in 2020 to $1.85 million in 2021.[265] The results suggest that the overall cost of a ransomware incident more than doubled in only one year.

During a ransomware attack, key infrastructure is often targeted to paralyse the organisation, causing the inability to provide proper service and run internal operations. The average downtime of organisations has increased over the last year. Research shows that the average downtime increased from 15 days in Q1 2020 to 23 days in Q2 2021.[266]

Aside from the costs related to the incident, repercussions on business opportunities and revenues have also been observed. A survey of 1,263 respondents reported that 66% of their organisations suffered significant revenue losses due to ransomware attacks, where company sise appears to have minimal impact on revenue loss.[267] The results underline the fact that every industry vertical is vulnerable to a statistically significant chance of revenue loss following successful ransomware.

3.1.10 The volatility of ransomware groups; shutdowns and arrests

Whether voluntary or based on actions from law-enforcement agencies, we saw large ransomware operations going offline. In the past, groups have shut down, only to resurface under another name.

In November 2020, the Maze ransomware group announced the end of its operations. Maze published data referring to more than 300 successful ransomware operations. It is believed that the group behind Maze will eventually reform as the Egregor group. [268]

In January 2021, a Canadian national was charged in relation to NetWalker ransomware attacks in which tens of millions of dollars were allegedly obtained.[269]

By the end of January 2021, the FonixCrypter or Fonix Ransomware group announced the shutdown of their operation and released the master decryption key.[270] While not confirmed, there are some indications that the group were arrested.

The threat actors behind Ziggy ransomware shut down their operation one week later, also releasing the decryption keys. They sent out a message about feeling guilty for their actions.[271] Research on their ransomware sample showed Gaza, Iran, Syria, Lebanon, and Palestine as white-listed countries.[272] Note that white-listing specific countries is a common practice in malware.

In February 2021, three people from the Egregor ransomware group were arrested in Ukraine following a joint operation between French and Ukrainian law enforcement.[273] Egregor operated a Ransomware-as-a-Service (RaaS) business for affiliates and had around 200 public victims. Because of Egregor's rapid growth and successful

[265] Sophos - The state of ransomware - 2021
[266] Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020, https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
[267] Ransomware: the true cost to business, https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf
[268] Maze Ransomware Shuts Down Operations After Recent Ransomware Attacks, https://www.zerofox.com/blog/maze-recent-ransomware-attacks/
[269] Department of Justice Launches Global Action Against NetWalker Ransomware, https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware
[270] Twitter fnx, https://twitter.com/fnx67482837/status/1355249547824521216
[271] Ziggy ransomware shuts down and releases victims' decryption keys, https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/
[272] Twitter MalwareHunterTeam, https://twitter.com/malwrhunterteam/status/1352339143750250507
[273] Cybersécurité : des pirates "Egregor", à l'origine de l'attaque contre Ouest-France, interpellés en Ukraine, https://www.franceinter.fr/amp/justice/cybersecurite-des-pirates-egregor-a-l-origine-de-l-attaque-contre-ouest-france-interpelles-en-ukraine

operations, victims even had to wait in a queue to negotiate a ransomware payment.[274] Blockchain analysis suggested affiliate overlap and other possible connections between Maze, Egregor, SunCrypt, and Doppelpaymer.[275]

In April 2021, the group behind Babuk ransomware announced the shutdown of their operations quickly after their successful attack against the District of Columbia's Metropolitan Police Department. After analysing their decryptor, researchers stated that it caused significant damage due to faulty code, leading to unreliable and sometimes faulty decryption, destroying the files in the process.[276]

In May 2021, the DarkSide ransomware group, which also operated with a RaaS model, announced the group's shutdown closely after the attack on Colonial Pipeline. After the attack, the group initially announced they would 'vet' the targets of their affiliates and explained that their motives were not political or destructive. Another announcement was later made that they would cease their operations and send out decryptors to all the victims. The statement, posted in the Russian language, claimed that an unspecified law enforcement agency disrupted part of its infrastructure.[277] It is still uncertain whether this information was factual or part of an exit strategy for the group. Note that the decryptor used by DarkSide was also not well designed, and the decryption process ran too slow for efficient recovery of their victims' operations. Therefore, even after paying for the decryptor, they had to resort to their own backups to help restore the system.[278]

In June 2021, a Latvian national faced charges stemming from her alleged role in a transnational cybercrime organisation responsible for creating and deploying a computer banking trojan and ransomware suite of malware known as Trickbot.[279]

Later in June, six members from the Clop ransomware group were detained in Ukraine after a joint operation between Ukraine, South Korea, and the United States.[280] While the authorities claimed to have shut down the group's infrastructure successfully, the ransomware operation is still in business and is listing new victims on their data leak site. The operations targeted the money-laundering side of the operation, while the platform core members were not apprehended.[281]

In July 2021, Avaddon, a ransomware group operating a RaaS platform, announced the shutdown of their operation. Along with the announcement, they released 2,934 decryption keys, one for each of their victims.[282] This number of decryption keys shows that the number of reported ransomware infections is just the tip of the iceberg.

Later in July, REvil/Sodinokibi shut down its operations.[283] Note that this is just days after the communication between the United States and Russia regarding the increase in ransomware attacks. High-profile victims of the group were Kaseya and its many managed service provider (MSP) customers and JBS Foods.

New groups have mysteriously emerged while these others shut down. Backmatter, for example, is a group that is actively recruiting affiliates or 'initial access brokers'.[284] However, encryption algorithms found in a decryptor show that the group is, in fact, a rebrand of the DarkSide ransomware operation. Grief, another new group, is a rebrand of

[274] Egregor ransomware affiliates arrested by Ukrainian, French police, https://www.bleepingcomputer.com/news/security/egregor-ransomware-affiliates-arrested-by-ukrainian-french-police/
[275] Chainanalysis = The 2021 Crypto Crime Report
[276] McAfee: Babuk ransomware decryptor causes encryption 'beyond repair', https://www.zdnet.com/article/mcafee-babuk-ransomware-decryptor-causes-encryption-beyond-repair/
[277] DarkSide Ransomware Shutdown: An Exit Scam or Running for Hills?, https://www.securityweek.com/darkside-ransomware-shutdown-exit-scam-or-running-hills
[278] Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom, https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
[279] Latvian National Charged for Alleged Role in Transnational Cybercrime Organisation, https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organisation
[280] Cuffed: Ukraine police collar six Clop ransomware gang suspects in joint raids with South Korean cops, https://www.theregister.com/2021/06/16/clop_ransomware_gang_arrests_ukraine/
[281] Clop ransomware is back in business after recent arrests, https://www.bleepingcomputer.com/news/security/clop-ransomware-is-back-in-business-after-recent-arrests/
[282] Avaddon ransomware shuts down and releases decryption keys, https://bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/
[283] Ransomware Giant REvil's Sites Disappear, https://threatpost.com/ransomware-revil-sites-disappears/167745/
[284] BlackMatter, a new ransomware group, claims link to DarkSide, REvil, https://blog.malwarebytes.com/ransomware/2021/07/blackmatter-a-new-ransomware-group-claims-link-to-darkside-revil/

DoppelPaymer, according to research.[285] Other newcomers are AvosLocker[286], and Haron. The latter is based on Avaddon source code and has the same look-and-feel. [287]

What this indicates is that these shutdown operations are often nothing more than rebranding operations. The goal is not always clear, whether to fool or distract law enforcement agencies and researchers or to deal with unhappy affiliates. The fact remains that all these groups share common malware writers, overlapping source code, and affiliates that use the platform. Over time, they will all disappear and re-emerge in one way or another. Overall, we see law enforcement actions taking place, but the impact on the operations of these groups remains limited.

3.1.11 Increased usage of zero-day vulnerabilities

In the past, zero-days were only used for targeted attacks by advanced threat actor groups and nation-states. The reason is, of course, the cost (value) of such a zero-day. Threat actors can only re-use it as long as the attack vector and payload are not discovered. Therefore, threat actors will carefully select the target and consider what it is potentially worth, and whether and when to 'burn' an exploit.

In December 2020, Accellion patched a zero-day vulnerability in its legacy *File Transfer Appliance* product. The vulnerability turned out to be one in a cascade of vulnerabilities. Four zero-days (CVE-2021-27101,[288] CVE-2021-27102,[289] CVE-2021-27103,[290] CVE-2021-27104[291]) were used to extract the data of its customers. The victims then received extortion e-mails from an actor claiming association with the Clop ransomware team gang. Technically speaking, no ransomware was deployed, but the actors threatened to expose the stolen data if no ransom was paid.[292]

REvil used CVE-2021-30116 [293] and two other CVEs,[294] to target Kaseya VSA management software and its MSP customers. A side note here is that the mentioned CVE had been discovered previously by security researchers and had been disclosed internally to Kaseya, which in the strictest of terms means that this wasn't a zero-day anymore, at least not for the companies involved.

After the initial publication of a zero-day vulnerability, we generally see an increase in attacks, where threat actors try to target as many unpatched victims as possible. In June 2021, The PrintNightmare vulnerability (CVE-2021-1675[295]) was initially discovered. Magniber ransomware was observed quickly adapting and weaponising the PrintNightmare vulnerability to target victims, mainly in South Korea.[296]

With the increase in ransoms, we see more zero-days being used to gain a foothold in an organisation and execute a ransomware attack. It shows that the potential revenue of a ransomware attack is higher than the cost of the exploit. Especially in operations at scale, this makes a lot of sense. The decrease in the number of attacks and the focus on large organisations allows for threat actors to ask for high ransoms. This focus on a high pay-out is referred to as big game hunting (BGH). Instead of targeting a large pool of targets using prevalent malware distribution vectors such as phishing, victims are carefully studied, and sophisticated methods are used to breach these high-value targets. The focus and potential of BGH dominated the ecosystem of cybercrime in 2020 and boosted the market for network access brokers. This way, BGH trends disrupted traditional targeted cybercrime behaviour.[297]

[285] DoppelPaymer ransomware gang rebrands as the Grief group, https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-gang-rebrands-as-the-grief-group/
[286] AvosLocker Under The Lens: A New Sophisticated Ransomware Group , https://blog.cyble.com/2021/07/15/avoslocker-under-the-lens-a-new-sophisticated-ransomware-group/
[287] New Haron ransomware gang emerges, borrows from Avaddon and Thanos, https://therecord.media/new-haron-ransomware-gang-emerges-borrowing-from-avaddon-and-thanos/
[288] CVE-2021-27101 Detail, https://nvd.nist.gov/vuln/detail/CVE-2021-27101
[289] CVE-2021-27102 Detail, https://nvd.nist.gov/vuln/detail/CVE-2021-27102
[290] CVE-2021-27103 Detail, https://nvd.nist.gov/vuln/detail/CVE-2021-27103
[291] CVE-2021-27104 Detail, https://nvd.nist.gov/vuln/detail/CVE-2021-27104
[292] Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11, https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/
[293] CVE-2021-20116 Detail, https://nvd.nist.gov/vuln/detail/CVE-2021-30116
[294] Kaseya VSA before 9.5.7 allows credential disclosure, as exploited in the wild in July 2021, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116
[295] Windows Print Spooler Remote Code Execution Vulnerability, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675
[296] Teaching an Old Dog New Tricks: 2017 Magniber Ransomware Uses PrintNightmare Vulnerability to Infect Victims in South Korea, https://www.crowdstrike.com/blog/magniber-ransomware-caught-using-printnightmare-vulnerability/
[297] Crowdstrike - Global Threat Report - 2021

3.1.12 Insurance fuels the ransomware industry economy

With the general increase in cybersecurity incidents, organisations are more prone to take out cybersecurity insurance. Taking out insurance is part of a risk strategy in which you transfer the risk to a third party. Being insured doesn't mean that the security risks are mitigated. Instead, the risk of associated costs in case of an incident is reduced. Companies faced with ransomware incidents will more readily pay, knowing that they have insurance coverage. Research points out that ransomware coverage in insurance policies is not only encouraging threat actors, but the practice may be fuelling the entire ransomware economy.[298] The insurance industry is facing criticism over this. The largest insurance organisation in the United States defends ransom payment reimbursements.[299] One of Europe's top five insurers announced in May 2021 it would suspend ransomware crime reimbursement. Note that this suspension only covered France.[300]

Ransomware coverage in cybersecurity insurance becomes unsustainable as the ransoms will only increase in value and numbers.[301] A survey showed that in 2020, 26% of the victims paid the ransom to get their data back. This number rose to 32% for 2021.[302] More victims are thus paying their ransom. This rise will impact insurance companies and the cost of an insurance policy. An insurer with 25.000 small and midsise customers in North America reported that in 2020, 41% of their customer claims were related to ransomware attacks.[303]

Insurance companies can play an important role by requiring their customers to improve their IT security. However, insurance companies often only impose basic risk assessments, including security tests, to validate whether a baseline is covered within the organisation. A common requirement is to do vulnerability scanning against the external perimeter of the organisation's IT infrastructure. While this is certainly a good initiative, it results in a narrow representation of the company's security posture and the associated risk. However, an article suggests that ransomware-related claims dropped by 65% following the insurance's security scans.[304] As previously discussed, RDP exposure on the external infrastructure has been a preferred way for intrusion for a long time and could explain why scanning for remote services on the external perimeter does reduce the likelihood of ransomware incidents.

3.2 RECOMMENDATIONS

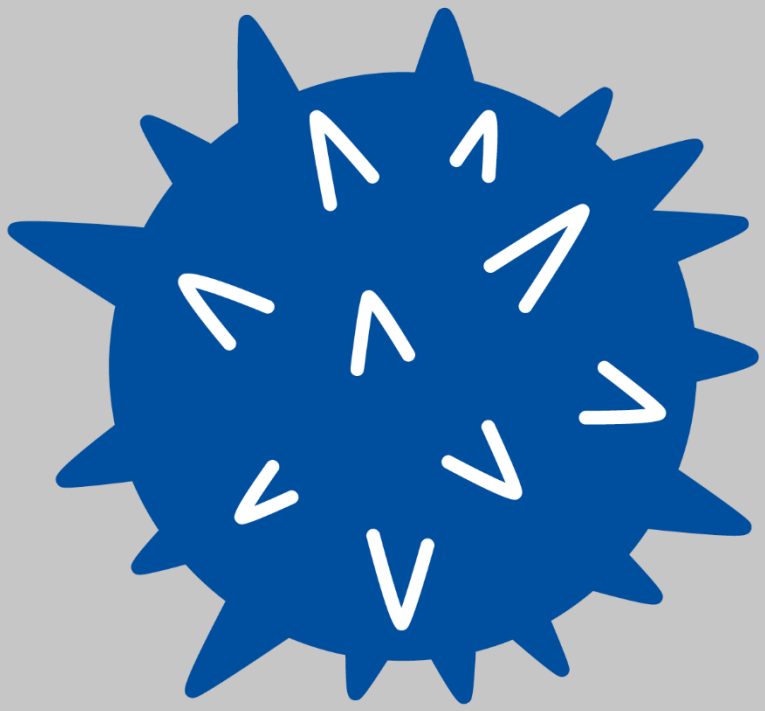
The following proposed recommendations provide the basis for the development of a mitigation strategy for the prevention of and response against ransomware.

- Implementation of secure and redundant backup strategies;
- Implementation and auditing of identity and access management (least-privilege and separation of duties);
- Training and raising the awareness of users (including privileged users);
- Separation of development and production environments;
- Information sharing on incidents with authorities and the industry;
- Restricting access to known ransomware sites;
- Identities and credentials should be issued, managed, verified, revoked, and audited for authorised devices, users, and processes;[305]
- Access permissions and authorisations should be managed, incorporating the principles of least privilege and separation of duties;[305]
- Separation of development and production environments;[305]
- Ransomware response and recovery plans should be tested periodically to ensure that risk and response assumptions and processes are current with respect to the evolving ransomware threats;[305]
- Use of security products or services that block access to known ransomware sites;[306]

[298] https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge
[299] https://www.insurancejournal.com/news/national/2021/07/02/621178.htm
[300] https://apnews.com/article/europe-france-technology-business-caabb132033ef2aaee9f58902f3e8fba
[301] Cyber Insurance and the Cyber Security Challenge Jamie MacColl, Jason R C Nurse and James Sullivan - Royal United Services Institute (RUSI)
[302] https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
[303] Cyber Insurance Claims Report – H1 2020 – Coalition - coalitioninc.com
[304] https://www.bleepingcomputer.com/news/security/cyber-insurers-security-scans-reduced-ransomware-claims-by-65-percent/
[305] Cybersecurity Framework Profile for Ransomware Risk Management (Preliminary Draft), https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf
[306] NIST Releases Tips and Tactics for Dealing with Ransomware, https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

- Execution of the Ransomware Readiness Assessment (RRA), a tool developed by CISA geared towards IT and ICS (industrial control system) networks, to evaluate their security against varying levels of ransomware threat readiness;[307]
- Report any attack or attempted attack to the authorities and help restrict its spread;[308]
- Systems' monitoring for fast identification of infections; and
- Keeping up with recent ransomware trends, developments and proposals for prevention.

[307] US CISA Introduced Ransomware Readiness Assessment (RRA), https://latesthackingnews.com/2021/07/06/us-cisa-introduced-ransomware-readiness-assessment-rra-in-its-cset-security-software/
[308] StopRansomware.gov – Report Ransomware https://www.cisa.gov/stopransomware/report-ransomware-0



4. MALWARE

Malware is an umbrella term that describes any software, firmware or code intended to perform a malicious unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of a system. Examples of malware could be a virus, worm, Trojan horse, or other code-based entities that infect a host. Spyware and some forms of adware are also part of the malware term.[309]

A malware can have various and different capabilities depending on the goal of the creator. For example RATs (Remote Access Trojans/Tools) are malware that allow an actor remote control of an infected system. Infostealers or Skimmers are designed to capture credit card information. Botnets are a robot network of computers infected by malware and controlled by C&C servers. Trojans, which can be either a banking Trojan or a mobile Trojan depending on the target, are malware that are often disguised as legitimate software.

The threat of malware appears consistently in the ETL, with new families and strains emerging every year despite the laudable efforts of law enforcement to take them down. In the following paragraphs, we describe general trends that emerged during the reporting period. A list of notable malware incidents can be found in Annex B. In addition, it needs to be emphasised' clarified that mitigation vectors are generic in nature and security professionals need to look for specific mitigation vectors for different malware families.

4.1 TRENDS

4.1.1 Decline of 2020 continues over 2021

Malware attacks decreased heavily during the reporting period. Research has shown that attacks in North America decreased by 43% in 2020 compared to 2019. This drop was almost same in Europe, while a decrease of 53% was noticed in Asia.[310] One of the key factors for this reduction could be linked to the COVID19 pandemic. Employees worked more from home and used their consumer ISPs and personal computers for work-related activities. This home environment and infrastructure doesn't have the same level of protection and detection, limiting the visibility of malware infections. The reduction in this visibility can cause a gap when collected statistical data is based only on detecting infections in the corporate environment.

In 2021, the decrease in malware infections is continuing. Research shows a further reduction of 22% over the first six months of 2021, compared to this period last year.[311] Note that a reduction in total malware volume does not mean that cybercrime declined. In the past, malware was used to infect a maximum of victims. Today, the focus is less on quantity and more on the quality of infections. In 2019, the number of malicious Office and PDF files was equal. Throughout 2020, the number of malicious Office files increased heavily until they exceeded PDF files by 150%. In 2021, the share of malware on both these file types dropped, with executable files gaining the ground they had lost.[311]

For 2020, the most detected malware categories in corporate environments included botnets (28%), cryptominers (21%), infostealers (16%), mobile (15%), banking (14%), and ransomware (4%).[312] In June 2021, the most common malware families detected were Trickbot (botnet and banking), XMRig (cryptominer), Formbook (infostealer), Glupteba (botnet), and Agent Tesla (infostealer).[313] Notice that these malware families did not change a lot over the last year. One noticeable difference is the fact that Emotet was taken down and Trickbot took over its market share[314].

[309] NIST Special Publication 800-171 Revision 2 (updated 01-28-2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
[310] 2021 SonicWall Cyber Threat Report
[311] Mid-Year Update: 2021 SonicWall Cyber Threat Report
[312] 2021 Checkpoint CYBER SECURITY REPORT
[313] June 2021's Most Wanted Malware: Trickbot Remains on Top - Check Point Software
[314] https://threatpost.com/trickbot-takes-over-emotet/164710/

4.1.2 Windows container malware

Malware targeting container environments has become much more prevalent. The technology of containerisation allows scaling easily. Malware focusing on the cloud-native stack, is in essence, not new. In November 2020, malicious container images had been already identified, and were used to find and exploit vulnerabilities on a particular victim's Kubernetes environment.[315] In December 2020, researchers also discovered the existence of file-less malware being executed from memory.[316] Common defence mechanisms or static scanners would not detect this type of infection. In March 2021, researchers uncovered the first known malware that targets Windows containers.[317] Other typical initial infection vectors include misconfigured container dashboards, APIs or daemons, or security issues in the application hosted on the container environment.

The most common goal of this type of malware is to escape the container, to infect the whole cluster. Clusters are generally collections of multiple applications, which increases the impact of such an infection heavily.

Common compromises include the leakage of sensitive information such as passwords, credit card numbers etc. In addition, container technology is often used as a best practice during the development lifecycle to spin up separate environments quickly. Compromise of development environments could result in further supply-chain attacks. Attackers stay under the radar and build in backdoors through source-code commits. The modified software is spread and used as an infection vector, targeting the software's users through genuine installers or the software's update functionality.

Patch management for container infrastructure is often disregarded because of the short lifespan of container instances. However, the discovered attacks underline the importance of protecting all exposed infrastructure. Automated tools execute attacks in a short time, enough to steal files or escape to the cluster. Once the cluster is owned, all data and code should be considered compromised.

4.1.3 Mobile Malware

In 2020, fake ad blockers, also referred to as adware, were on the rise on Android. This type of malicious application tempts the user with "add blocking" capabilities, asks for extensive permissions on the operating system, and starts using all sorts of notifications and browser redirects to present ads and thus generate revenue. A close variant is the hiddenAds mobile malware. In 2020, detection of this malware type increased from 280.000 to 700.000 compared to 2019.[318] The large proportion of adware in mobile malware continues throughout 2021. 45% Of mobile malware was identified as adware in the first half of 2021.[319] Installation of these applications usually happens through third-party app stores as well as in online forums.

Mobile banking malware saw an increase in 2020. The malware tries to steal online banking credentials and payment information by showing fake login screens. The malware is then capable of performing transactions on accounts with financial institutions. The most common malicious banking applications in 2021 include Ghimob, Eventbot, and Thiefbot. Other common malware is Blackrock, Wroba, and TrickMO.[320]

In May 2021, Flubot infections increased using SMS as a spreading mechanism. The increase was mainly noticed in Europe and the UK. In most messages, either government (COVID-19 related) or package delivery brands were impersonated to lure victims into installing a malicious application.[321]

Most malware is based on malicious applications that users install. In 2020 and 2021, there have been some cases of significant vulnerabilities in popular applications allowing remote code execution, but malicious applications were not reported to target these actively. There have been cases of zero-day vulnerabilities targeting the mobile platform instead of an application. However, the victims of these attacks are very specific and high profile. The Pegasus spyware for iOS is used worldwide to target journalists, activists, and politicians. The malware uses two zero-click malware variants: the

[315] https://blog.aquasec.com/kubernetes-vulnerability-security-threat
[316] https://blog.aquasec.com/fileless-malware-container-security
[317] https://unit42.paloaltonetworks.com/siloscape/
[318] State of Malware 2021 - Malwarebytes
[319] https://press.avast.com/avast-reports-continued-dominance-of-adware-among-android-threats
[320] Checkpoint – Cyber Security Report 2021
[321] https://www.welivesecurity.com/2021/05/17/take-action-now-flubot-malware-may-be-on-its-way/

Kismet exploit in 2020 and the Forcedentry (Megalodon) in 2021.[322] In July 2021, a list of 50.000 victims of these targeted attacks leaked.[323]

4.1.4 Detection is bypassed using exotic languages

Malware developers resort to relatively new or uncommon programming languages. While not entirely new, this trend has continued to evolve throughout 2020 and 2021. These uncommon languages include but are not limited to Rust, Nim, DLang, and Go[324]. The main motive is to bypass detection capabilities.

As most of the detection capability of malware is based on static indicators, these become irrelevant or ineffective when the source code is rewritten in a new language.[325] From a reverse engineering perspective, it also becomes more challenging to analyse these new malware samples. Either entire rulesets must be rewritten to match patterns in the newly written malware, or focus needs to be shifted to the detection of dynamic or behaviour-based signatures. An example of this trend was reported in May 2021, when the original Buer malware was shown to have been rewritten in Rust, named RustyBuer. Their similarity is based on nearly identical communication structures between the command-and-control servers and the infected host.[326]

Malware written in these emerging programming languages only represents a fraction of all the malware being developed today. Still, it is an important aspect for the future development of malware detection and code analysis techniques. Migrating to other languages could mean that the scanners and defenders of today lose effectiveness and ability to detect the malware of tomorrow.

4.1.5 Malware disruption

Emotet is a strain of computer malware. Initially, the malware acted as a banking trojan. Over the years, the malware evolved and gained more ground. The functionality shifted from a simple information stealer to malware used to create an advanced botnet. The malware featured a well-developed command and control (C2) infrastructure, frequent updates and was very effective in evading detection.

In 2020, the malware used Trickbot and QBot to steal credentials and spread inside networks.[327] Throughout 2020, Emotet had been the most prevalent malware. The victims, part of the botnet, were often sold to other threat actors for targeted cyber-crime, such as ransomware or information stealing.

In January 2021, Interpol announced a crackdown on the botnet. Law enforcement and judicial authorities worldwide cooperated and took control of the botnet's infrastructure in a coordinated international action.[328] Through the C2 infrastructure, they delivered 'updates' to the malware, which would cause it to uninstall itself in April 2021. The Ukrainian government arrested two individuals in relation to this investigation.[329]

The fight against cyber-crime is an ongoing and uneven battle. However, this case shows that through international cooperation, law enforcement can have an impact.

4.1.6 High-Risk Vulnerabilities Across Major Vendors increase in 2021

At the end of 2020 and on into 2021 a wide spread of products were affected by high-risk vulnerabilities. Critical, easily exploited vulnerabilities appeared in multiple products from vendors such as Microsoft, Apple, Google, Adobe, Dell, SonicWall, QNAP, and VMWare. Another example is the vulnerabilities found in Apple software which were also increasingly exploited in 2021. Attackers, such as the Silver Sparrow malware, have been targeting Apple products.

[322] https://citisenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/
[323] https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus
[324] https://www.zdnet.com/article/malware-developers-turn-to-exotic-programming-languages-to-thwart-researchers/
[325] OLD DOGS NEW TRICKS:ATTACKERS ADOPT EXOTIC PROGRAMMING LANGUAGES – https://blogs.blackberry.com/en/2021/07/old-dogs-new-tricks-attackers-adopt-exotic-programming-languages
[326] https://www.proofpoint.com/uk/blog/threat-insight/new-variant-buer-loader-written-rust
[327] https://www.globenewswire.com/news-release/2020/08/07/2074889/0/en/July-2020-s-Most-Wanted-Malware-Emotet-Strikes-Again-After-Five-Month-Absence.html
[328] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
[329] https://www.cyberpolice.gov.ua/news/kiberpolicziya-vykryla-transnaczionalne-ugrupovannya-xakeriv-u-rozpovsyudzhenni-najnebezpechnishogo-v-sviti-kompyuternogo-virusu-emotet-2504/

This malware is the second known piece of macOS malware to feature a program compiled for the new M1 chip that Apple introduced in November 2020.[330]

In many cases these vulnerabilities had already been exploited by the time they were disclosed. Accellion and the vulnerabilities affecting Microsoft Exchange in Q1 2021 were among the most prominent.[330]

4.1.7 Malware as a business

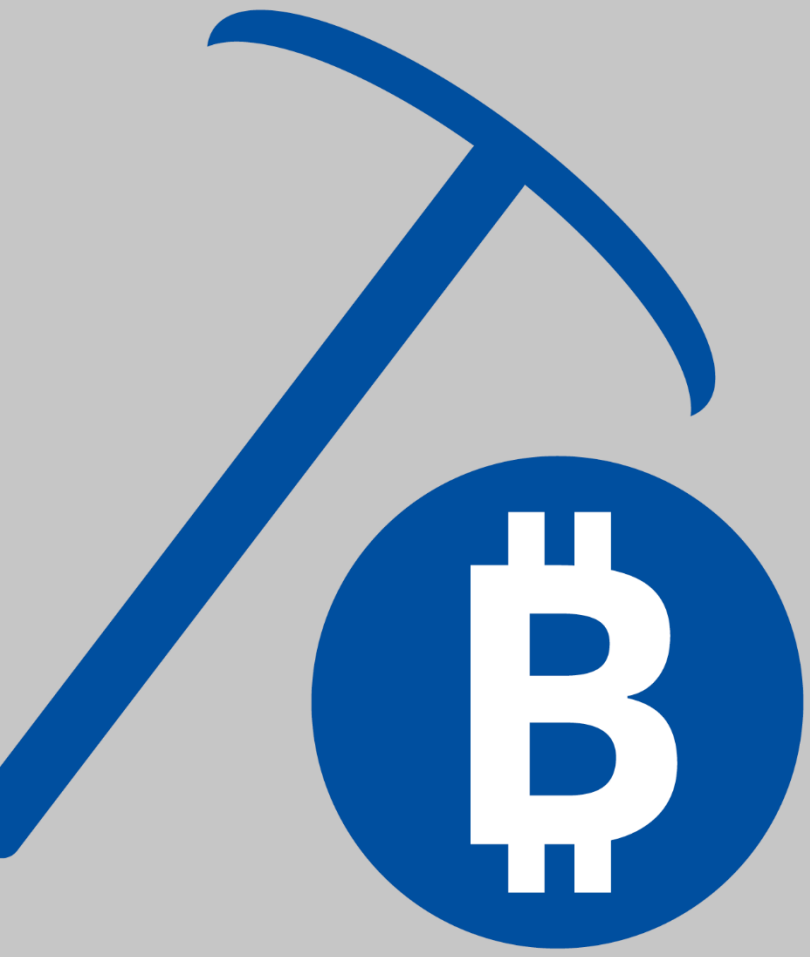
Malware as a service is not a new trend. The move from static exploit kits to cloud-based rental models were discovered in the past. We will not focus here on Ransomware-As-A-Service (RaaS), as this is covered in the previous chapter.

4.2 RECOMMENDATIONS

During the reporting period several good practices and mitigation vectors concerning malware were noted, as follows:

- Implement malware detection for all inbound/outbound channels, including e-mail, network, web and application systems in all applicable platforms (i.e. servers, network infrastructure, personal computers and mobile devices).
- Inspect the SSL/TLS traffic allowing the firewall to decrypt what is being transmitted to and from websites, e-mail communications, and mobile applications.
- Establish interfaces between malware detection functions (intelligence-led threat hunting) and security incident management to establish efficient response capabilities.
- Use the tools available for malware analysis for sharing malware information and malware mitigation (i.e. MISP).
- Develop security policies that specify the processes to be followed in the event of infection.
- Understand the capabilities of various security tools and develop new security solutions. Identify gaps and apply the defence-in-depth principle.
- Employ mail filtering (or spam filtering) for malicious e-mails and remove executable attachments.
- Regularly monitor the results of antivirus tests.
- Use patch management for container infrastructure.
- Make use of log monitoring using security incident and event management (SIEM) solutions. Indicative log sources are anti-virus alerts, endpoint detection and response (EDR), proxy server logs, Windows Event and Sysmon logs, intrusion detection system (IDS) logs, etc.
- Disable or reduce access to PowerShell functions.

[330] https://go.recordedfuture.com/hubfs/reports/cta-2021-0831.pdf



5. CRYPTOJACKING

Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. This usually occurs when the victim unwittingly installs a program with malicious scripts that allow the cybercriminal to access their computer or other Internet-connected devices, e.g. by clicking on an unknown link in an e-mail or visiting an infected website. Programs called 'coin miners' are then used by the criminal to create or 'mine' cryptocurrencies.[331]

During the reporting period we saw a growing trend in cryptojacking, which could perhaps be associated with the increasing volatility in the cryptocurrency market that was observed during the same period. Moreover, given that cryptocurrencies offer (pseudo) anonymity, they become a very attractive and convenient means of exchange by cybercriminals. Accordingly, it should be noted that cryptocurrencies in general are requested when asking for ransom in ransomware attacks. A list of notable cryptojaking incidents can be found in Annex B.

5.1 TRENDS

5.1.1 Cryptojacking volume in 2021 is record high

Since 2019, we have witnessed a steady decline in drive-by cryptominers, the dominant type for the past few years[332]. The decline, which is aligned to the diminishing value of drive-by mining profitability, was hastened by the shutdown of Coinhive in March 2019 and JSECoin in April 2020, as described in last year's ETL report.[333] [334] However, attackers have moved on to other types of malicious activities when it comes to cryptojacking/cryptomining, with Cisco reporting that 69% of its customers had been affected by cryptomining malware in 2020.[335] According to the same report, cryptomining generated the most DNS traffic out of any other malicious activity.

In March of 2020, a spike in infections was seen, after which the infection rate dropped dramatically. From the second to the last quarter of 2020, the volume of infections increased slowly and this continued in 2021.[335] In the first quarter of 2021, the volume of infections attained a record high compared to the last few years.[336] Other statistics confirm this trend, showing that during the first quarter of 2021, cryptomining malware increased by 117%.[337] This last report links this increase to the growth in 64-bit mining applications.[337] We can conclude that financial gain associated with cryptojacking incentivised the associated threat actors to carry out these attacks. Based on the fluctuating value of cryptocurrency, we assume this will remain an important attack vector over the coming year.

When comparing the exchange rate of Bitcoin with the volume of cryptominers, we clearly see how both are related. As mentioned in the ETL 2021 Ransomware report,[338] threat actors are shifting from Bitcoin, which provides pseudo-anonymity, to using strongly private cryptocurrency such as Monero.[339] Europol reports that cryptocurrencies continue to facilitate payments for various forms of cybercrime, as developments evolve with respect to privacy oriented crypto coins and services.[340]

[331] Interpol, Cybercrime-Cryptojacking September 2020, https://www.interpol.int/content/download/15670/file/Cybercrime-Cryptojacking-EN.pdf
[332] https://thenextweb.com/news/cryptojacking-cryptocurrency-million-hits-first-half-2019
[333] Check Point - Cyber security report - 2021
[334] ENISA Threat Landscape - Cryptojacking 2020
[335] https://blogs.cisco.com/security/threat-trends-dns-security-part-1
[336] SonicWall - Cyber Threat Report : Mid-Year Update: 2021 |
[337] McAfee Labs Threats Report - June 2021
[338] ENISA Threat Landscape - Ransomware 2021
[339] SonicWall - Cyber Threat Report - 2021
[340] IOCTA Internet Organised Crime Threat Assessment - 2020.

5.1.2 XMRig dominates the cryptomining market

In 2020, the global market of cryptomining malware was dominated by XMRig (35%), JSECoin (27%), Lucifer (7%), WannaMine (6%), RubyMiner (5%), and others (20%).[341] JSECoin was an open-source miner that shut down its services in April 2020 due to financial uncertainties after the COVID-19 pandemic.[342]

XMRig[343], an open-source miner, is used by attackers and most malware to perform cryptomining on victims unwillingly. Over the first half of 2021, its market share increased to 51%, accounting for more than half of all cryptomining malware. Other infections are related to Lucifer (10%), LemonDuck (5%), RubyMiner (5%), Wannamine (5%), and other miners (20%).[344] First discovered in May 2020, the Lucifer malware can, amongst other things, execute DDoS attacks, exploit vulnerable Windows hosts, and perform brute-force attacks. These features allowed the malware to propagate itself rapidly. Under the hood, the malware drops XMRig to mine.[345] The LemonDuck malware strain is already a few years old and is gaining more ground in 2021. It is also a self-propagating cryptominer, dropping XMRig on the victim to perform mining tasks. Since April 2021, the malware has been targeting unpatched Microsoft Exchange Servers, suffering back then from multiple zero-days.[346] Microsoft reported that cryptominers were some of the first payloads to target these vulnerabilities actively, illustrating how well these could adapt to use make of new exploits.[347]

Even though Wannemine and RubyMine are older XMRig dropping malware variants, they still retain a foothold in 2021. Wannamine further limits its malicious activity on the infected host, focusing solely on the mining.[348]

5.1.3 Shift from browser to file-based cryptojacking

Research showed that for the first trimester of 2021, desktop or file-based cryptojackers were almost seven times more frequent than browser-based miners, at 13% for browser-based compared to 87% for file-based.[349]

Other research confirms that since the shutdown of Coinhive, the share of browser-based cryptomining dropped. This gap is filled by file-based crypto-jackers, which first compromise the victim's host and then drop mining software on it.[350] In general, cryptojacking accounted for a mere 2.5% of malware used in breaches and only 1.5% of malware in incidents. Around 10% of organisations received (and blocked) cryptocurrency mining malware at some point throughout the course of the year[351].

5.1.4 Infection methods do not change

The techniques used to spread and deploy cryptominers do not differ much from other malware infection methods. A drive-by download is a technique used to deliver and install malicious files on a victim's device without its knowledge. This happens passively when visiting malicious websites, triggering a download that takes advantage of the operating system or the web browser, which contain security flaws. Notice that compromised websites are also used as a delivery vector for cryptominers. Another distribution method is malvertising, the act of spreading malware through advertisements.

Cryptominers are often delivered as applications that hide their malicious behaviour. Typical examples are mobile applications.[352] While these applications are subject to automated security validation before being published on the application store, these detections are not always adequate. Alternative stores are also used to spread malicious mobile applications.

[341] Check Point - Cyber security report - 2021
[342] JSEcoin Ltd, https://webcache.googleusercontent.com/search?q=cache:CZLnRC2thW4J:https://jsecoin.com/nl/home/+&cd=2&hl=nl&ct=clnk&gl=be
[343] XMRig, https://xmrig.com/
[344] Check Point - Cyber security: Mid year report - 2021
[345] Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices, https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/
[346] Lemon Duck spreads its wings: Actors target Microsoft Exchange servers, incorporate new TTPs, https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html
[347] Analyzing attacks taking advantage of the Exchange Server vulnerabilities, https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/
[348] INCIBE (National Cybersecurity Institute) - WannaMine analysis study – April 2021
[349] ESET - Threat report - T1 2021
[350] SonicWall - Cyber Threat Report - 2021
[351] Verizon DBIR 2020
[352] https://www.trendmicro.com/en_us/research/21/h/fake-cryptocurrency-mining-apps-trick-victims-into-watching-ads-.html

There are also deceptive mobile applications claiming to do cryptomining, but their only functionality is to lure users into expensive subscriptions.[353] Another example is malicious browser add-ons, which leverage JavaScript libraries. These are distributed through official browser add-on stores and forums.

Cryptomining software like XMRig is often incorporated in other malware and exploit kits.[354] Advanced malware can exploit other machines with known vulnerabilities or, through brute-forcing, can migrate over different machines and act like a cryptomining worm.[355]

Interestingly, cryptojacking malware is also reported to actively search and terminate other cryptomining instances running on their victim's host. The Kinsing cloud crypto-jacker is such an example. The Linux-based malware installs a Monero miner and then ensures maximum system resources by killing other processes and even docker containers that are resource-intensive.[356]

5.1.5 Cryptomining targeting cloud and container infrastructure

Cloud infrastructure allows processing power to be scaled up when needed. When cloud hosts are infected by crypto-jacking malware, the costs can become monumental. The cloud providers bill for the consumed CPU cycles, while the gains resulting from the computing operations only cover a fraction of the costs.[357]

Container infrastructure is also an interesting target, as these environments will spawn worker nodes based on needs. Cryptojacking was already seen on Kubernetes in the past but the entry vectors were either vulnerable web applications or malicious containers already containing mining malware. In June 2020, a large-scale campaign targeted Kubeflow, a machine learning toolkit, aiming to infect internet-facing Kubernetes instances and use them for cryptomining at the victims' expense. After gaining access to the cluster, they deployed a malicious container to run their XMRig-based miner.[358]

5.1.6 Disruption of illegal cryptomining operations

In May 2021, in the United Kingdom, law enforcement terminated a cryptomining operation, and the equipment was confiscated based on a charge of the theft of electricity. The bust happened in the context of a search warrant for a suspected cannabis farm.[359]

Later in May, China decided to ban financial institutions and payment companies from providing services related to cryptocurrency transactions.[360] The initial ban targeted three provinces, which according to research, accounted together for more than 65% of Bitcoin's hash rate.[361]

On the first of July, the security services of Ukraine (SBU) shut down a mining operation running on stolen electricity. The services acted on the threat to the region's critical infrastructure.[362] On the eighth of July, the SBU shut down a cryptomining operation and seized almost 5,000 computers. The seizure included 3800 game consoles and 500 graphic cards. The suspects were charged with the theft of electricity. The monthly loss was estimated to be up to USD 250.000.[363]

[353] Bogus Cryptomining Apps Infest Google Play, https://threatpost.com/bogus-cryptomining-apps-google-play/168785/
[354] https://www.trendmicro.com/vinfo/hk/threat-encyclopedia/malware/coinminer.win64.xmrig.yxbd2/
[355] https://arstechnica.com/gadgets/2021/04/windows-and-linux-devices-are-under-attack-by-a-new-cryptomining-worm/
[356] Threat Report: Kinsing Cloud Cryptojacker, 2021
[357] Sophos - Threat report - 2021
[358] Misconfigured Kubeflow workloads are a security risk, https://www.microsoft.com/security/blog/2020/06/10/misconfigured-kubeflow-workloads-are-a-security-risk/
[359] Bitcoin 'mine' uncovered during industrial unit raid, https://west-midlands.police.uk/news/bitcoin-mine-uncovered-during-industrial-unit-raid
[360] China bans financial, payment institutions from cryptocurrency business, https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/
[361] Cambridge Bitcoin Electricity Consumption Index, https://cbeci.org/mining_map
[362] СБУ знешкодила криптоферму, через яку без світла і води могла залишитися частина Чернігівської області, https://ssu.gov.ua/novyny/sbu-zneshkodyla-kryptofermu-cherez-yaku-bez-svitla-i-vody-mohla-zalyshytysia-chastyna-chernihivskoi-oblasti-video
[363] SBU exposes massive crypto mining in Ukraine, https://ssu.gov.ua/en/novyny/sbu-vykryla-naibilshu-kryptofermu-v-ukraini-maizhe-5-tys-kompiuteriv-mainyly-hroshi-na-vinnytsiaoblenerho

In July 2021, the Malaysian authorities reported having seised more than 1,000 bitcoin mining devices and arrested six persons on charges of theft of electricity over the course of six separate raids.[364] They destroyed the devices and put the images on YouTube, sending a message to other mining operators.

We see an increase in law enforcement operations against (illegal) cryptomining. The cost of energy associated with bitcoins pushes these mine operations to steal electricity. This practice is not new, as it has been used by farms that cultivate drugs. Disruptions in these operations will make the actors move to other locations and other means to mine crypto, such as leveraging infrastructure from compromised devices.

5.2 RECOMMENDATIONS

The following mitigation vectors were mentioned regarding cryptomining related attacks and incidents in the reported period.

- Monitor battery usage on users' devices and, in the case of suspicious spikes in CPU usage, scan for the presence of file-based miners.
- Implement web filtering of common cryptomining protocols, as well as blacklisting the IP addresses and domains of popular cryptomining IP pools.
- Monitor for network anomalies and block mining protocols.
- Install endpoint protection by means of anti-virus programs or crypto-miner blocking browser plug-ins.
- Conduct regular security audits to detect network anomalies.
- Implement robust vulnerability and patch management to protect against emerging threats and vulnerabilities.
- Implement patches and fixes against well-known exploits.
- Use whitelisting to prevent unknown executables from being executed at the endpoints.
- Use allow-listing to allow only the execution of known executables on the endpoints.
- Monitor and block common cryptomining executables.
- Invest in raising users' awareness of cryptojacking, especially with regard to secure browsing behaviour.
- Discuss crypto mining in the context of security awareness training.

[364] Police Destroy 1,069 Bitcoin Miners With Big Ass Steamroller In Malaysia, https://www.vice.com/en/article/7kv739/police-destroy-1069-bitcoin-miners-with-big-ass-steamroller-in-malaysia

6. E-MAIL RELATED THREATS

E-mail related threats have been consistently ranking high in the list of prime threats in the ETL for a number of years. This collection of threats exploits weaknesses in human behaviour concerning e-mails and human habits, and aims at manipulating humans to fall victims to an attack. E-mail related threats are in general less about the technical vulnerabilities of information systems, but mostly about end-user awareness and exploitation of the inherent trust people place on their e-mail communications. This threat canvas consists mainly of the following vectors: phishing, spear-phishing, whaling, smishing, vishing, business e-mail compromise (BEC) and spam.

Phishing aims at stealing important information like credit card numbers and passwords, through e-mails involving social engineering and deception. **Spear-phishing** is a more sophisticated version of phishing that targets specific organisations or individuals. **Whaling** is a spear-phishing attack aimed at users in high positions (executives, politicians etc.). **Smishing**, a term derived as a combination of "SMS" and "phishing",[365] occurs when financial or personal information of victims are gathered via the use of SMS messages. Another type of threat related to e-mail is **vishing,** a combination of phishing and voice that occurs when information is given via phone, where malicious actors using social engineering techniques extract sensitive information from users.

Business e-mail compromise (BEC) is a sophisticated scam targeting businesses and organisations, whereby criminals employ social engineering techniques to gain access to an employee's or executive's e-mail account to initiate bank transfers under fraudulent conditions.[366] Finally, **spam** is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via e-mail, but it can also be distributed via text messages, phone calls, or social media[367].

As expected, the COVID-19 pandemic has given rise to this category of threats, since people's online presence and need for communication has greatly risen during this period. Moreover, the digitalisation of many traditional services grew at an unprecedented rate during the pandemic, and given e-mail's lead role as a communications means, the increase in e-mail related threats was undeniable. A list of notable incidents related to e-mail threats can be found in Annex B.

6.1 TRENDS

6.1.1 COVID-19 still the lure in e-mail threat campaigns

Spam campaigns with COVID-19 related lures were major occurrences throughout the reporting period. In general, COVID-19 was exploited by adversaries to trick end users into falling victims to various types of e-mail related attacks. Exploiting the angst concerning the pandemic and the trust that people place on their e-mail as a principal means of communication, adversaries made use of COVID-19 to spread their campaigns. These campaigns ranged from attempts to trick users into ordering face masks from phony websites to infecting them with malware via malicious attachments. Three-quarters of attachments in these e-mails contained infostealers – a type of malware that steals sensitive information (such as passwords or other credentials).[368] As the pandemic continued and the vaccine was released the lure changed to incorporate that. The campaigns included advertisements or offers for early access to a vaccine upon payment of a deposit or fee and misinformation regarding the vaccines.[369]

[365] Bank Phishing E-mails, https://www.europol.europa.eu/sites/default/files/documents/4_ceo-bec_fraud.pdf
[366] Europol - IOCTA 2020 - https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
[367] What is spam? Definition & types of spam https://www.malwarebytes.com/spam
[368] COVID-19 spam, phishing e-mails, plagued users in first half of 2020 COVID-19 spam, phishing e-mails, plagued users in first half of 2020 | F-Secure Press Room
[369] Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines, https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-COVID-19-vaccines

6.1.2 Postal services used in phishing campaigns

Several phishing campaigns aiming to steal the credit card numbers of victims by sending phishing e-mails related to deliveries from national postal systems have been observed during the reporting period. The e-mails try to lead users to phishing websites that capture their credit information. This attempt has already affected at least 26 countries.[370] In 2021, postal services were also used in massive SMS spam messages that spread the Flubot Android malware across Europe. Malware gangs were sending malicious links to users via SMS posing as legitimate package delivery services.[371]

6.1.3 QRishing: new version of an old scheme

Social distancing during the pandemic has popularised QR (Quick Response) codes,[372] which are simple to use and may be pretty simple to generate. Identifying a fake QR message is not straightforward and it creates a suitable environment for malicious activity. A tactic that has been observed is embedding fake QR codes into phishing e-mails sent by large European banks. Upon scanning the code, users are directed to websites with realistic-looking landing pages, where the victim may be prompted to login in order to renew their credit cards.[373] A fake QR code also has the potential to connect to an unsecured Wi-Fi network or automatically navigate to a malicious link. Codes may also direct users to websites where malware can be automatically downloaded. Moreover, public QR codes could also cause a problem as cybercriminals may swap them out by replacing their own QR codes over genuine ones.

6.1.4 BEC has increased, has grown in sophistication and become more targeted

According to publicly available reports, BEC was the most costly cybercrime type in 2020 during which organisations reported total losses of more than 1.8 billion dollars[374]. During the reporting period, it was observed that BEC schemes have evolved, especially regarding credential phishing and the conversion of money into cryptocurrency.[375] As EU Member States report, there have been many cases where Office 365 accounts have been used for BEC scams. This implies that the actors have also conducted credential phishing operations or password spraying attacks (a technique similar to brute force attacks) against the victims[376].

Moreover, although cybercriminals target all sectors and businesses, BEC actors show an increased focus on small and medium-sise enterprises[377]. Historically, BEC actors were based in Nigeria but recent research has identified BEC actors in 50 different countries.[378] Half of the BEC-related cybercriminals are located in Nigeria (the reduction in this percentage is due to the efforts of law enforcement) and one-quarter of them are based in the United States. Moreover, the highly lucrative potential of this type of cybercrime has attracted more sophisticated cybercrime groups such as Cosmic Lynx[379].

Our assessment is that cybercriminals will certainly continue to take advantage of compromised business accounts and use them to make money through BEC scams. It is also likely that this lucrative type of cybercrime will attract sophisticated cybercrime actors globally, further diversifying the current geography of BEC actors and increasing the sophistication of BEC scams.

6.1.5 SMShing and Vishing have increased since users lack the awareness

According to security, new sites,[380] [381] such as various APTs groups, have started using SMShing and Vishing as part of their highly targeted campaigns. In recent attacks targeting political opponents, APT-C-23 appeared to have used a new technique, the use of voice-changing software to pose as women – the group's members who have been identified so far are all men – to engage victims in conversations. As the conversations continue, the group begin sending videos loaded with malware to infect the target's system.[381]

[370] Post Office Phishing Hits Credit Card Users in 26 Countries https://www.trendmicro.com/en_se/research/21/a/post-office-phishing-hits-credit-card-users-in-26-countries.html
[371] Despite arrests in Spain, FluBot operations explode across Europe and Japan - The Record by Recorded Future
[372] https://www.lexpress.fr/actualite/ne-pas-toucher-au-temps-du-covid-19-l-heure-de-gloire-du-qr-code_2131853.html
[373] https://www.hoxhunt.com/blog/banking-phishing-qr-codes/
[374] https://www.fbi.gov/contact-us/field-offices/anchorage/news/press-releases/fbi-releases-2020-internet-crime-report
[375] FBI – Internet Crime Report 2020 - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[376] Europol - IOCTA 2020 - https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
[377] https://www.comae.com/posts/keep-office-365-safe-from-bec-when-you-are-an-sme/
[378] Agari - The Global Reach of Business E-mail Compromise (BEC) - https://agari.com/e-mail-security-blog/business-e-mail-compromise-geography/
[379] Agari – Cosmic Lynx: The Rise of Russian BEC - https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf
[380] Iranian cyberspies behind major Christmas SMS spear-phishing campaign | ZDNet
[381] APT Group Using Voice Changing Software in Spear-Phishing Campaign | SecurityWeek.Com

In another instance Charming Kitten, (also known as APT35 or Phosphorus), used the 2021 holiday season to attack targets from all over the world using a spear-phishing campaign that involved both e-mails and SMS messages. While the SMS messages posed as Google security alerts, the e-mails used previously hacked accounts. The common indicator in both campaigns was that Charming Kitten operators managed to successfully hide their attacks behind a legitimate Google URL.[380]

In general, users are used to the idea of not clicking on suspicious e-mails, but still are not aware that they can also be phished via text messages or phone calls.

6.1.6 Phishing-as-a-Service (PhaaS)

Microsoft's recent analysis of the Bullet ProofLink campaign suggests that this operation is responsible for many of the phishing campaigns that have had an impact on organisations. BulletProofLink (also referred to as BulletProftLink or Anthrax by its operators in various websites, ads, and other promotional materials) is used by multiple malicious actors in either one-off or monthly subscription-based business models, creating a steady revenue stream for its operators[382].

Similar to ransomware-as-a-service (RaaS), phishing-as-a-service follows the software-as-a-service model. Attackers pay an operator to develop and deploy large portions of or complete phishing campaigns from false sign-in page development, website hosting, and credential parsing and redistribution, outsourcing capabilities that they may be lacking.

6.2 RECOMMENDATIONS

The following mitigation vectors were discussed regarding e-mail related attacks and incidents during the reporting period.

- Provide regular user training on how to identify suspicious links and attachments and how to report them.[383] [384] [385]
- Implement spam filters at the e-mail gateways; keep signatures and rules updated.[389] Whenever possible, use a secure e-mail gateway with automated maintenance of filters (anti-spam, anti-malware, policy-based filtering).
- Put security controls into place on the e-mail gateway to reduce the frequency or possibility of the lures arriving to your employees' inboxes.[386]
- Implement a need-to-know access policy to limit the impact of any compromise.[387]
- Consult the MITRE ATT&CK® framework for the tactics of adversaries and techniques pertaining to cybersecurity threats.[388]
- Ensure e-mails originating from outside the organisation are automatically marked before received.[389]
- Implement multifactor authentication (MFA) to accounts.[390]
- Check the lifespan of a suspected malicious domain and its ownership. If it has been active for less than a year, it could be a scam.
- Whenever possible, apply security solutions that use machine-learning techniques to identify phishing sites in real-time.
- Disable automatic execution of code, macros, rendering of graphics and preloading mailed links at the mail clients and update them frequently.[391]

[382] https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/
[383] Lessons in Cybersecurity: How education coped in the shift to distance learning, https://www.malwarebytes.com/resources/resource/malwarebytes-labs/lessons-in-cybersecurity-how-education-coped-in-the-shift-to-distance-learning
[384] 2020 Cyber Threats Report, https://www.netwrix.com/download/collaterals/2020_Cyber_Threats_Report.pdf
[385] Attack Landscape H1 2020, https://blog-assets.f-secure.com/wp-content/uploads/2020/09/17142720/F-Secure-attack-landscape-h12020.pdf
[386] Cyber Threat Landscape: Monthly Update For CIO/CISO, https://assets.kpmg/content/dam/kpmg/ca/pdf/2020/11/cyber-threat-landscape-report-nov-2020-en.pdf
[387] Cyber Threat Landscape Report 2020, https://www.ensigninfosecurity.com/analysis-insights/content/2020/05/18/cyber-threat-landscape-report-2020
[388] Cyberthreats: A 20-Year Retrospective, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf
[389] HHS Cybersecurity Program APT and Cybercriminal Targeting of HCS, https://www.hhs.gov/sites/default/files/apt-and-cybercriminal-targeting-of-hcs.pdf
[390] X-Force Threat Intelligence Index 2021, https://www.ibm.com/security/data-breach/threat-intelligence
[391] What is phishing? Everything you need to know to protect yourself from scam e-mails and more, https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-e-mails-and-more/

- Implement one of the standards for reducing spam e-mails.[392,393,394,395]
- Whenever possible, for critical financial transactions or when exchanging sensitive information, implement secure e-mail communications by using digital signatures or encryption.
- Whenever possible, implement fraud and anomaly detection at the network level for both inbound and outbound e-mails.
- Do not click on random links or download attachments if you are not absolutely confident about the source of an e-mail.
- Check the domain name of the websites you visit for typos, especially for sensitive websites (e.g. bank websites). Threat actors usually register fake domains that are similar to legitimate ones and use them to 'phish' their targets. Looking only for an HTTPS connection is not enough.[396]
- Use a strong and unique password for every online service. Re-using the same password for various services is a serious security issue and should be always avoided. Using strong and unique credentials for every online service limits the risk of a potential account takeover to only the affected service. Using a password manager software will make managing of the whole set of passwords easier.[397]
- Check how contact, registration, subscription, and feedback forms work on your website and add verification rules if necessary, so that they cannot be exploited by attackers.[398]
- Implement content filtering to locate unwanted attachments, e-mails with malicious content, spam, and unwanted network traffic.
- Avoid responding to new links received in e-mails or SMS messages by unknown senders and, most of all, do not enter your credentials when following such links.

[392] Guidance Using Domain-based Message Authentication, Reporting and Conformance (DMARC) in your organisation, https://www.gov.uk/government/publications/e-mail-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc
[393] Sender Policy Framework Project Overview, http://www.open-spf.org/
[394] What is DMARC? https://dmarc.org/
[395] DomainKeys Identified Mail, http://www.dkim.org/
[396] What is a Look-alike Domain? https://www.phishlabs.com/blog/what-is-a-look-alike-domain/
[397] How to create a strong password, https://blog.avast.com/strong-password-ideas
[398] Tricky 'Forms' of Phishing, https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html

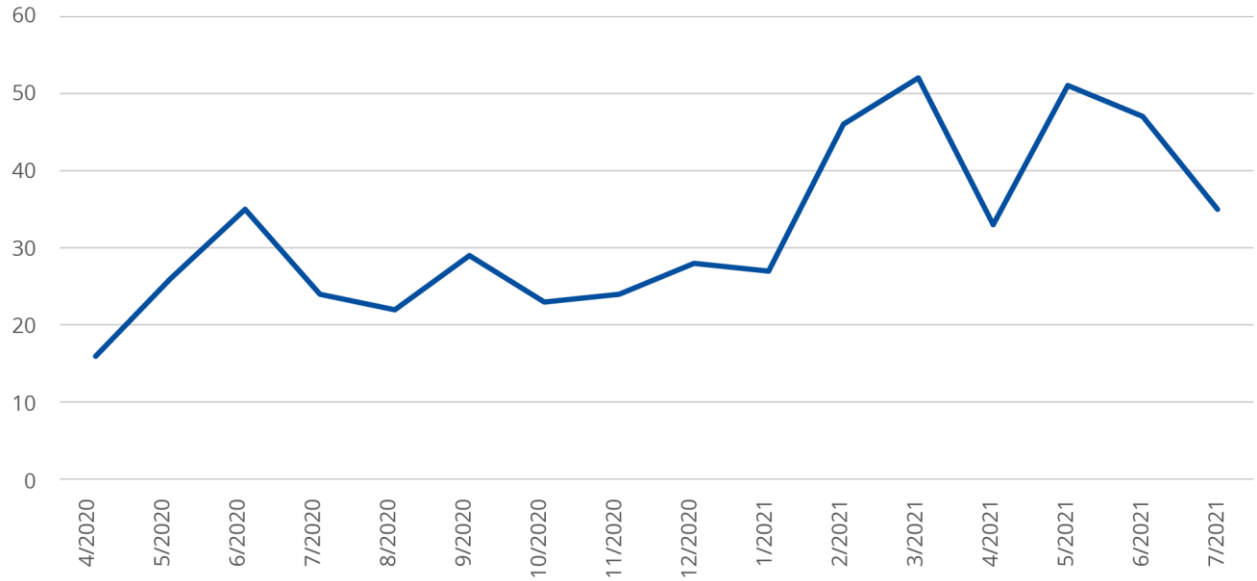
7. THREATS AGAINST DATA

Threats against data form a collection of threats that target data sources with the aim of gaining unauthorised access, disclosure, misinformation, disinformation, etc. They are mainly referred to as data breaches or data leaks and refer to the release of sensitive, confidential or protected data to an untrusted environment. Data breaches can occur as a result of a cyber-attack, an insider job, unintentional loss or exposure of data. Data exfiltration or data theft is a technique that is used by malicious actors to target, copy, and transfer sensitive data. A particular case of the use of exfiltrated data is identity theft, where malicious actors use personal identifiable information (PII) to impersonate a user.

Threats against data consistently rank high among the leading threats of the ETL and this trend continues in the reporting period of the ETL 2021. Adversaries explore a series of new techniques and exploit the increasing online presence and use of online services by the general public. Moreover, given the significance of data and in particular of private and sensitive data, adversaries are combining more sophisticated threats to target data, such as ransomware or supply chain attacks. It is noteworthy that in the ENISA threat landscape for supply chains,[399] for about 58% of the supply chain incidents analysed, the customer assets targeted were predominantly customer data, including personally identifiable information (PII) data and intellectual property.

Numerous incidents related to threats against data took place during the reporting period of ETL 2021. Figure 8 shows the incidents observed based on OSINT (Open Source Intelligence) collected by ENISA for the purposes of situational awareness.[400] The scope of the collection is global and multi-sectorial. Incidents, however, with a direct impact in the EU area are given priority. We observed an increasing trend in the number of incidents reported during 2021. This observation relates primarily to the surge of data breaches in the health sector (see trends below). Notable incidents related to threats against data can be found in Annex B.

Figure 8: Incidents related to threats against data observed by ENISA (April 2020-July 2021)



[399] https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[400] In accordance with the EU cybersecurity act Art.7 Par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

7.1 TRENDS

Considering data breaches,[401] the industry sectors suffering the most from internal errors are finance and insurance, public administration, healthcare and information. In the financial sector, 44% of the breaches are caused by internal actors, whose actions are, most of time, due to errors. It is noteworthy that internal actors have been growing constantly from 2018 in this industrial sector, while external actors have been decreasing at the same rate, to the point where the two are very close. In the public administration sector, social engineering is the primary pattern (70%), with errors the second pattern (15%) where misconfiguration and mis-delivery account for most errors. In the healthcare sector, errors are the primary cause, with the top three specific errors being mis-delivery, publishing errors and misconfiguration. Finally, in the information sector, basic web application attacks, errors and system intrusion are the main patterns, together accounting for 83% of all breaches. Misconfiguration covers the vast majority of all the breaches caused by errors (>70%).

According to Verizon,[401] 85% of data breaches involve a human element. This can be easily explained by considering that both social engineering and miscellaneous errors are among the main patterns. Breaches caused by errors differ with respect to other breaches in the variety of data being disclosed. Altogether, the most disclosed data are credentials (60%) and personal data (50%), while in breaches caused by errors the most disclosed are personal data (80%).

Most of breaches caused by errors are discovered within days or hours.[401] This claim can be explained by the fact that people quickly realise the errors they have made. Taking a more general look, the discovery time for breaches of every nature, broken down into organisation sise, show that enterprise-sised organisation do perform better than SMEs, discovering breaches within days in 55% of the cases. SMEs, instead, discover breaches within days in 47% of the cases. These results show that enterprises have significantly improved their performance, while SMEs have basically stayed the same as in 2019.

7.1.1 Threat actors shifted their attention towards COVID-19 vaccine information

Vaccine information became the centre of a few cyberespionage campaigns during the reporting period. In July 2020, the UK foreign secretary issued warnings about active large-scale phishing campaigns which appeared to specifically target COVID-19 research facilities and were believed to be sponsored by nation-states.[402] Later in 2020, phishing schemes with credential harvesting capabilities were found targeting organisations globally, with the intention to extract information regarding the transportation and distribution processes of the vaccines.[403] At the end of 2020, AstraZeneca employees where spear-phished[404] and the incident was attributed to state-sponsored APT groups. Lastly, at the end of 2020 the EMA was targeted and documents concerning the validation process of Pfiser and Moderna vaccines were accessed and leaked to the internet[405].

7.1.2 Surge in healthcare sector data breaches

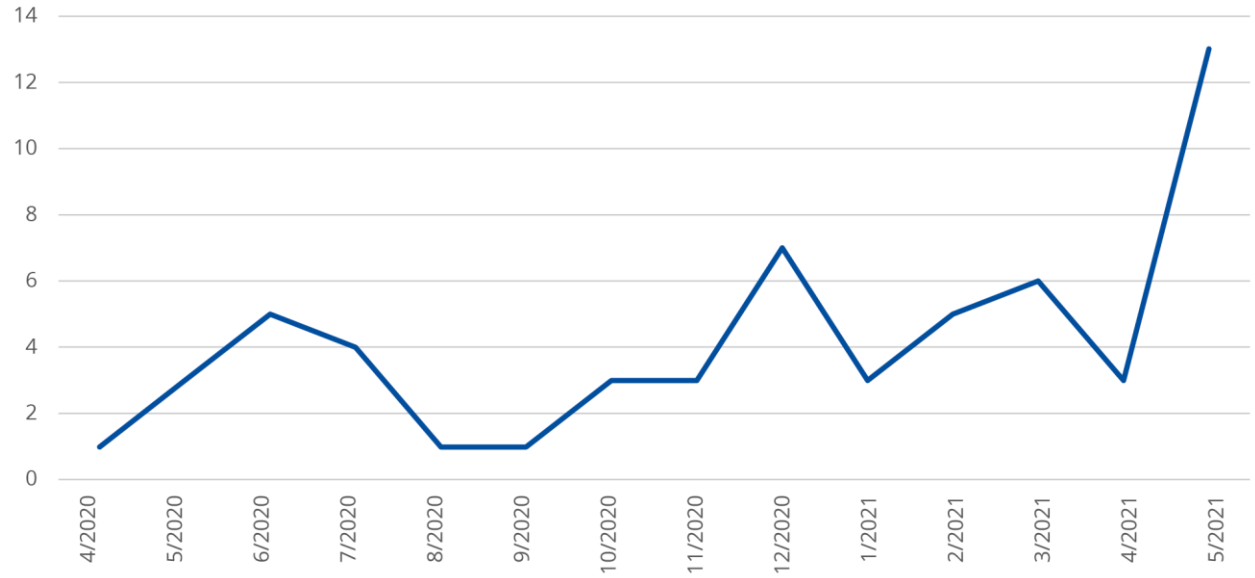
Healthcare data breaches are increasing rapidly (see Figure 14). This can be interpreted in a couple of ways. Due to the COVID-19 pandemic, the healthcare sector was put on the spotlight and threat actors took advantage of this crisis to hit an already suffering sector. In addition, due to the pandemic, a shift towards the online provisioning of healthcare services, remote eHealth and telemedicine approaches increased and thus the opportunities for adversaries to exfiltrate medical data increased greatly.

Moreover, the motivation for adversaries to access and exploit medical data is much higher than other types of data. A credit card for example can be easily cancelled, so the perceived value of having the data related to a card is much lower compared to medical records, which contain information, such as a patient's medical and behavioural health history and demographics, as well as their health insurance and contact information.

[401] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021
[402] UK condemns Russian Intelligence Services over vaccine cyber-attacks, https://www.gov.uk/government/news/uk-condemns-russian-intelligence-services-over-vaccine-cyber-attacks
[403] X-Force Threat Intelligence Index 2021, https://www.ibm.com/security/data-breach/threat-intelligence
[404] https://www.cybersecurity-insiders.com/cyber-attack-on-astrazeneca-COVID-19-vaccine-research/
[405] https://www.ema.europa.eu/en/news/cyberattack-ema-update-6

The increase in healthcare related incidents is also visible in relevant mandatory reporting in the US[406] that require victims to report the breaches. A similar trend is also observed in ENISA OSINT trend analysis as seen in Figure 9.

Figure 9: Data related incidents in healthcare as observed through OSINT by ENISA via situational awareness



7.1.3 Data breaches in the business environment rise

According to SANS Institute, in the last few years, approximately 74,000 employees, contractors, and suppliers were impacted by a data breach due to stolen company laptops.[407] This was exacerbated by the fact that data were not encrypted. In a 2021 study of 300 respondents - including top managers at US companies with over 5,000 employees in the most important business domains[408] - 34% of respondents has been the target of a theft of property or supply chain damage due to insiders abusing their privileges. Among observed physical threats, 27% of the respondents mentioned “insiders abusing authorised cyber and physical access points” in a list of the top-three physical threats, 26% “supply chain damage and/or disruptions”, and 23% “onsite theft/burglary”.

7.1.4 Motivations and attack vectors remain the same

During the reporting period, trends related to the motivations of adversaries as well as the main attack vectors remained generally the same. Phishing continues to be on the top causes of breaches (36%), as it has been for the past two years. It is followed by the use of stolen credentials (25%) and ransomware (10%).[409] As in past years, financially motivated attacks continue to be the most common. Nearly 80% of cyberattacks are for financial gain, such as stealing money directly from financial accounts, stealing credit card information or other types of data that can be monetised, or demanding ransom. In second place is espionage, which often involves the theft of intellectual property or other confidential information[409]

7.1.5 Identity theft and synthetic identity

Due to the increase in data breaches in previous years, personal and sensitive data has been easily accessible to malicious actors via online forums and the dark web. This has had a cascading effect on identity theft. According to the US Federal Trade Commission (FTC), complaints of identity theft rose in 2020 compared to the year before.[410] About a third of these involved US government benefits. Scams were geared towards the new COVID-19 reality such as using

[406] Health Insurance Portability and Accountability Act in US, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html
[407] RESOLVER, Physical and Cybersecurity Defense: How Hybrid Attacks are Raising the Stakes, August 2021, https://www.resolver.com/blog/physical-and-cybersecurity-defense-hybrid-attacks/
[408] The Ontic Center for Protective Intelligence, 2021 Mid-Year Outlook State of Protective Intelligence Report - The Escalating Physical Threat Landscape: A Clarion Call for Corporate Protective Intelligence https://www.prnewswire.com/news-releases/intelligence-failures-regularly-occur-at-large-us-companies-resulting-in-physical-threats-or-harm-and-business-continuity-disruption-study-finds-301334484.html, https://ontic.co/wp-content/uploads/2021/07/2021-Mid-Year-Outlook-State-of-Protective-Intelligence-Report.pdf
[409] https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
[410] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

stolen personal data to apply for and receive government benefits, stealing money by offering to deliver goods to people that were confined indoors due to the lockdowns, or by impersonating government agencies[411].

A lot of these incidents could have involved synthetic identities. Synthetic identity theft is a type of fraud in which criminals combine real and fake information to create a new identity. Incidents with synthetic identities tend to be more common in the United States because of static personally identifiable information, which is used to verify someone's identity, according to the Federal Reserve[412].

7.1.6 Actors taking advantage of bad user behaviour in order to commit identity abuse

The Identity Theft Resource Centre reported in early 2021 that the motivation of cybercriminals has shifted and instead of targeting consumers in order to steal large amounts of personal information they have started taking advantage of bad user behaviour[413] that are then used against organisations. A typical example involves stolen credentials.

As reported by CERT-EU, "identity abuse essentially consists of using valid accounts and legitimate applications to perpetrate malicious activities in a persistent and stealthy way. Attackers abuse the inherent trust in any action associated with authenticated users or authorised applications. Identity abuse can be seen as an extension of the living-off-the land (LOTL) tactic where an attacker makes use of legitimate tools to remain undetected, whereas, through identity abuse, the attacker will additionally make use of legitimate accounts. Observed tactics showed the unprecedented level of sophistication the adversaries leveraged to abuse their victims' identities for lateral movement and stealthy operations. They remained undetected for more than six months in the network of hundreds of compromised organisations". [414] In the SolarWinds Orion campaign, the adversaries abused the high-privileged accounts the application uses; these accounts ultimately underpin identity in an organisation's environment.

7.1.7 Rising Impact of Supply Chain Attacks

As reported in ENISA's dedicated threat landscape for supply chains, based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organisations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organisations remain secure.

Around 58% of the supply chain attacks were aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people. When it comes to suppliers' data, 20% of attacks were aimed at gaining access to that data and 66% to their source code.

7.2 RECOMMENDATIONS

The following mitigation vectors were mentioned regarding data related attacks and incidents in the reporting period.

- Develop and maintain a cybersecurity awareness plan. Provide training and simulation scenarios for identifying social engineering and phishing campaigns for employees.[415]
- Limit user access privileges under the need-to-know principle. Revoke access privileges to anyone who is not an employee[416].
- Establish and maintain an incident response team and evaluate incident response plans frequently.[417]
- Discover and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest. In other words, deploy data loss prevention capabilities.

[411] COVID + Credit: New Scams Put Identity at Risk during the COVID-19 Pandemic, https://www.equifax.com/personal/education/COVID-19/prevent-identity-theft-coronavirus-scams/
[412] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf
[413] https://www.idtheftcenter.org/data-breaches-are-up-38-percent-in-q2-2021-the-identity-theft-resource-center-predicts-a-new-all-time-high-by-years-end/
[414] https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf#page=13&zoom=auto,-274,51
[415] Discover security awareness trends and best practices for 2021, https://terranovasecurity.com/how-to-build-a-strong-security-awareness-program-in-2021/
[416] Need to Know Access Control Guideline, https://security.berkeley.edu/need-know-access-control-guideline
[417] Incident Response Team: What are the Roles and Responsibilities?, https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team

- Increase investments related to detection, alerting tools and ability to contain and respond to a data breach.
- Develop and maintain strong policies enforcing strong passwords (password management) and usage of multi-factor authentication (MFAs).
- Consider models that take the least privileged approach to provide security for both on premises and off premises resources (i.e. zero-trust).
- Invest in and create policies and plans for engaging with governance, risk management and compliance teams.
- Store data only on secure IT assets.
- Educate and train the personnel periodically.
- Use technology tools to avoid possible data leaks, such as vulnerability scans, malware scans and data loss prevention (DLP) tools. Deploy data and portable system and device encryption, and secure gateways.
- A Business Continuity Plan (BCP) is critical in the event of a data breach. This plan outlines the type of data being stored, their location and what potential liabilities could emerge when implementing data security and recovery actions. A BCP entails an effective incident response, which aims at addressing, managing, and rectifying the damages due to such an incident.
- Apply 'threat hunting' within a company to strengthen security plans. Threat hunting is conducted by skilled members of the Security Operation Centre (SOC) team to proactively identify vulnerabilities and prevent breaches.
- Policies such as velocity-based rules can be used to mitigate identity fraud, especially for payment card transactions. The machine data of valid transactions can provide sufficient information for the optimal policy definition.
- The Single Sign On (SSO) authentication method, when available, allows a user to access several applications with the same set of digital credentials. It is highly recommended to minimise the number of user accounts and stored credentials using SSO.
- URLs that are sent via e-mail or are randomly visited should first be checked based on their IP address, the ASN that associates with the IP, the owner of the domain and the relation between this domain and others, before any further step is taken.
- Organisations that are adopting cloud services should have strong cloud security operations and prefer an architecture of on-premises storages, private cloud storages and public cloud storages simultaneously to protect their customer's personal information.
- Use strong and updated encryption methods such as TLS 1.3 (uses ephemeral keys) for sensitive data to prevent hacking.
- Adequately protect all identity documents and copies (physical or digital ones) against unauthorised access.
- Identity information should not be disclosed to unsolicited recipients and their requests by phone, e-mail or in person should not be answered.
- Install and use content filtering to filter out unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Use Data Loss Prevention (DLP) solutions.


ERROR

8. THREATS AGAINST AVAILABILITY AND INTEGRITY

Availability and integrity are the target of a plethora of threats and attacks, among which the families of Distributed Denial of Service (DDoS) and Web Attacks stand out.

Distributed Denial of Service (DDoS) targets system and data availability, and though it is not a new threat (it celebrated its 20th anniversary in 2019) it remains a significant threat in the cyber landscape.[418] [419] Attacks occur when users of a system or service are not able to access relevant information, services or other resources. This can be accomplished by exhausting the service or overloading the component of the network infrastructure[420].

Web-based attacks mainly target data integrity and availability. They are an attractive method by which threat actors can delude victims using web systems and services as the threat vector. This covers a vast attack surface, for instance facilitating malicious URLs (Uniform Resource Locators) or malicious scripts to direct the user or victim to the desired website or downloading malicious content (watering hole attacks, drive-by attacks) and injecting malicious code into a legitimate but compromised website to steal information (i.e. formjacking) for financial gain, information stealing or even extortion via ransomware[421].

DDoS and web-based attacks are often coordinated activities. DDoS attacks can be built on a web-based attack, which are often distributed through web applications. For instance, web-based attacks can be adopted to build a botnet that is then used to carry out a denial of service attack aimed to make a system unavailable.

8.1 TRENDS

Both web attacks and DDoS attacks have remained stable over the years, while some interesting points on their evolution may be noted. According to EUROPOL, "*the threat potential of DDoS attacks is higher than its current impact in the EU.*"[419] Notable incidents for these two types of attacks can found in Annex B.

8.1.1 Ransom Denial of Service (RDoS) is the new trend of DDoS attacks

During 2020, Ransom DDoS (RDDoS) campaigns got a substantial boost from August 2020 onwards, with hacking groups such as Fancy Bear, Cozy Bear, Lazarus Group, and Armada Collective carrying out these campaigns. Targeted sectors include e-commerce, finance, and travel on a global scale.[422] Extortion attacks have also experienced a boost in terms of numbers and dimensions, reaching capacities of 500Gbps in 2020.[423]

Ransom Denial of Service substantially reduces the need of resources to carry out an attack. Cybercriminals analyse target businesses to find those with weak and vulnerable systems. They then blackmail these businesses by asking a ransom so as not to attack the system[424] [425]. Thanks to cybercrime-as-a-service tools, in fact, launching an RDDoS

[418] Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020
[419] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
[420] CISA, Understanding Denial-of-Service Attacks, November 2019. https://www.uscert.gov/ncas/tips/ST04-015
[421] ENISA Threat Landscape (ETL) 2020 – Web-Based Attacks, 2020
[422] ETH Zürich, Center for Security Studies (CSS), The Evolving Cyber Threat Landscape during the COVID Crisis, 2020
[423] Tom Emmons, PART I: Retrospective 2020: ddos was back -- bigger and badder than ever before, https://blogs.akamai.com/2021/01/part-i-retrospective-2020-ddos-was-back-bigger-and-badder-than-ever-before.html
[424] Sergiu Gatlan, "FBI: Thousands of orgs targeted by RDoS extortion campaign," September 2020, https://www.bleepingcomputer.com/news/security/fbi-thousands-of-orgs-targeted-by-rdos-extortion-campaign/
[425] CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/

attack is increasingly simple, while it is still difficult to spot its origin. Infecting a target with malware or ransomware would otherwise require more effort in terms of time and planning[426].

RDDoS comes in two flavours: i) attack-first, ii) extortion first. In the first case, a DDoS attack is implemented and a ransom is requested to stop it. In the second case, an extortion letter and proof in the form of a small-scale DoS is sent with a request to pay a ransom. RDDoS attacks are even more dangerous than traditional DDoS since they can be completed even if the attacker does not have sufficient resources.[427]

8.1.2 COVID-19 Pandemic has been used as an amplifier

DDoS attacks were boosted substantially in 2020 due to COVID-19 with more than 10 million attacks (1.6 million more than 2019) and a 22% increase in attack frequency in the last 6 months of 2020. In March 2020, a new norm began with over 800,000 DDoS attacks registered, an average of 839,083 attacks per month over the year and with more than 929,000 attacks in May 2020. Global DDoS extortion attacks also increased by 125% becoming one of the most critical approaches to DDoS.[428]

In addition, videoconferencing and remote collaboration software, such as Microsoft Teams, Skype or Zoom, experienced a peak of usage. However, their usage comes with some concerns. First, these tools are often built on weak communications possibly leading to attacks. Then, their high demand in terms of bandwidth can stress the network.[429] Furthermore, the massive adoption of remote working increased the risk for organisations of becoming a target of a DDoS attack. In addition, the bandwidth originally devoted to counteracting DDoS is currently used for remote working, reducing an enterprise's ability to defend itself against a DDoS attack.[430] In this context, the impact of DDoS attacks against RDPs and virtual private networks (VPNs) increased with the pandemic.[422]

Due to COVID-19, malicious actors increasingly targeted home networks as a starting point for more complex attacks, making DNS not only an attack vector but also a target of attacks. According to Neustar (NISC Survey, Q4 2020), Domain Hijacking (31%) has been the most observed DNS threat, followed by DNS Spoofing/Cache Poisoning (27%), DNS Tunnelling (26%), and Zombie Domain Attacks (18%).[426]

8.1.3 Cybercrime-as-a-Service works as an amplifier of web-based and DoS attacks

Cybercrime-as-a-Service is becoming a cornerstone for spreading DDoS, opening the door of DDoS to a wider population of attackers. Illegal online markets providing accesses to attack tools and services, as well as fast internet connections are further supporting cybercriminals in driving more complex and sophisticated campaigns, and disruptive attacks.[423] State-sponsored actors aim to develop their capabilities to disrupt critical infrastructure and conduct espionage against businesses, academia, and governments to steal intellectual property.

DDoS is increasingly implemented using cybercrime-as-a-service: a criminal pays for a DDoS attack-as-a-service and the paid service launches the DDoS attack.[431] [423] These services reduce the effort needed to manage high-volume and complex attacks, making DDoS adaptive, lightweight, and heterogeneous. DDoS is increasingly targeting smaller businesses and requiring less financial and technical resources. Potentially disruptive attacks can target third-party providers (e.g. financial, energy and telecommunication services), with cascading effects in the supply chain.[419] [432]

Cybercrime-as-a-Service in fact provides a set of online tools and services that simplify the execution of targeted attacks. We then have a coordinated effort between expert cybercriminals that provide tools and expertise and low-

[426] Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020, https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pd f
[427] CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/
[428] https://www.helpnetsecurity.com/2021/04/14/ddos-attack-activity/
[429] New York Times, "'Zoombombing' Becomes a Dangerous Organised Effort". https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html
[430] Accenture, Cyber Threatscape Report, 2020
[431] Europol, EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2021), 2021
[432] CrowdStrike, 2021 Global Threat Report, 2021

skilled cybercriminals who identify vulnerable targets, who share revenues. DDoS-For-Hire-Services are among the most adopted tools for cyberattacks.[431] In general, we may note that DDoS attacks are today mostly multivector and amplified by COVID-19. They also show a boost in dimension and impact, while impacting almost all businesses' domains thanks to the rise of extortion attacks.[433] Finally, according to research conducted by Digital Shadows, "*three main trends that can be expected to persist throughout 2021 include leveraging IoT devices, offering DDoS service solutions, and DDoS extortion.*"[434]

8.1.4 Traditional DDoS is moving towards mobile networks and IoT

The success of internet of things (IoT) in conjunction with 5G is resulting in a new wave of DDoS attacks, possibly inducing victims to pay a ransom.[435] On one hand, 5G makes IoT more vulnerable to cyberattacks, supporting localised DDoS where an attacker interferes with the connectivity of a specific area covered by a slice through a set of compromised devices.[436] On the other hand, IoT can be used as a threat vector for DDoS. Attackers can build massive botnets to launch DDoS attacks or distribute malware.[437] This is particularly critical in Industrial IoT (IIoT), where device vulnerabilities can disrupt business operations and cause significant damage (e.g. in the health domain, vulnerable medical devices can affect people's safety).[438]

Sensors and devices are in fact a suitable target of DDoS attacks due to their limited resources that often result in poor security protection. Devices are simple to corrupt, often coming with misconfigurations (e.g. weak passwords).[419] At the same time, the increasing complexity of these mobile systems makes users' shortage of security skills increasingly pertinent. In this context, DDoS aims to threaten the availability of components, as well as disrupt the operation of other networks or systems. It also has the potential to threaten the safety of users. The increasing number of devices and applications connected to the cloud gives adversaries a larger playing field on which to target attacks.

Lack of industry standards, network capabilities, and hardware can challenge service uptime and reliability.[439] This problem is exacerbated in IIoT, where vulnerabilities in third-party software components clearly point to a lack of standardisation and safe coding guidelines.[438]

8.1.5 New amplifiers and advanced sophistication for DDoS attacks emerge

Sharing of resources in virtualised environments acts as an amplifier of DDoS attacks.[436] Physical resource overloading can cause disruption in communications, services, and access to data.

DDoS attackers are adopting intelligent strategies based on technically advanced and smart attacks. In 2020-21, smart attacks used publicly available information to monitor the countermeasures adopted by their targets and adapt their attack strategies at run time.[418] In this context, the duration of short attacks decreased, while the duration of long attacks increased.[440] Focusing on absolute numbers, the number of short attacks had a sharp increase in Q1 2021, while long attacks decreased though their overall duration increased[588].[440] Sharing the same view, Akamai, at the end of March 2021, observed more attacks over 50 Gbps than during the whole of 2019. Even more important, in the first quarter of 2021, they recorded three of the six biggest DDoS attacks by volume, including the two largest known DDoS extortion attacks.[441]

[433] Jai Vijayan, DDoS Attacks Spiked, Became More Complex in 2020, December 2020, https://www.darkreading.com/attacks-breaches/ddos-attacks-spiked-became-more-complex-in-2020/d/d-id/1339814
[434] H-ISAC. Distributed Denial of Service (DDoS) Attacks, March 2021 https://www.aha.org/system/files/media/file/2021/03/distributed-denial-of-service-ddos-attacks-march-2021.pdf
[435] Cyber Threats Report - Acronis 2020.pdf
[436] H2020 EU Project CONCORDIA, Deliverable D4.1 - 1st year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf
[437] FortiGuard Labs, FORTINET, Global Threat Landscape Report 2020, August 2020, https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-h1-2020.pdf
[438] Trend Micro, Securing the Pandemic Disrupted Workplace, 2020
[439] H2020 EU Project CONCORDIA, Deliverable D4.2 - 2nd year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.2.pdf
[440] Alexander Gutnikov, Oleg Kupreev, Ekaterina Badovskaya, DDoS attacks in Q1 2021, May 2021, https://securelist.com/ddos-attacks-in-q1-2021/102166/
[441] Tom Emmons, 2021: Volumetric DDoS Attacks Rising Fast, March 2021, https://blogs.akamai.com/2021/03/in-our-2020-ddos-retrospective

8.1.6 DDoS campaigns in 2021 have become more targeted, multi-vector and persistent

The attackers look for weaknesses to exploit and try different attack vector combinations. 65% of DDoS attacks were multi-vector.[441] Independently from the statistics, DDoS attacks are increasingly becoming multi-vector.[433] According to NEUSTAR,[442] built-in access protocols have been used as attack vectors, resulting in the FBI releasing a warning in July 2020 that common network protocols like Apple Remote Management Services (ARMS), Web Services Dynamic Discovery (WS-DD) and Constrained Application Protocol (CoAP) were abused by hackers to conduct DDoS reflection and amplification attacks. Furthermore, some DDoS threats build on TCP-based attacks, including TCP SYN and fragmented packet floods. NEUSTAR shares the view that the majority of attack vectors for DDoS attacks focus on UDP protocols, such as Network Time Protocol (NTP), Connection-less Lightweight Directory Access Protocol (CLDAP), Internet Control Message Protocol (ICMP) and Domain Name System (DNS).

NETSCOUT, with its intelligent threat report, provided a detailed discussion of DDoS threat vectors. It claimed that the total number of vectors for individual attacks increased substantially, culminating in an attack composed of 26 attack vectors in 2020. Multi-vector attacks are mostly in the range 15-25 vectors and showed an increase in cardinality between 9% and 312%, with the most notable growth in the range of 15-21 vectors.[443]

8.1.7 Smaller organisations are being targeted

DDoS is increasingly targeting small enterprises by building on the rental of skill and tools to implement attacks (Cybercrime-as-a-Service).[444] This finding was previously discussed in IOCTA 2020, claiming that cybercriminals increasingly target smaller organisations with lower security standards, ensuring successful attacks with smaller volumes of data and maximum revenue. Public institutions and critical infrastructures remain among the main targets of DDoS attacks.[419]

Kaspersky, instead, monitored DDoS activities in 2020-21, focusing on trends in quarters[445,446,447]. In particular, in Q2 2020 (probably due to the pandemic), the number of attacks were more than the triple the same period of 2019. In Q3 2020, figures came back to normality and the number of attacks dropped around one third compared to Q2 2020 (with an increase of 50% compared to Q3 2019). In Q4 2020, the number of attacks dropped further by around one third compared to Q3 2020 (with comparable numbers with respect to Q4 2019). In Q1 2021, the attacks increased by more than 40% compared to Q4 2020. This increase was mostly observed in January (with peaks of 1,800 attacks per day) and, according to Kaspersky, was linked to the price of cryptocurrencies. In general, the increase in DDoS attacks in 2020 and 2021 was also due to COVID-19 and remote working, which provided a plethora of new vulnerable targets.

8.1.8 Increased combination of web-based and DDoS attacks

Recalling that DDoS and web-based attacks are often coordinated activities, web applications are still vulnerable to web-related threats, such as injections and cross-site scripting, and can become a vector for DDoS attacks. According to a recent report[448], SQL injection vulnerabilities and PHP injection vulnerabilities are the most commonly exploited, though XSS is the most discovered vulnerability. According to the Verizon 2020 Data Breach Investigations Report (DBIR),[449] cross-site scripting (XSS) traffic experienced a substantial increase in Q4 2020; blocked cross-site scripting (XSS) traffic nearly doubled in volume from Q2 2020 to Q4 2020, with more than 15 million attacks, representing 10% of blocked traffic.[450] Furthermore, 43% of all data breaches involved a web application and around 90% of all hacking

[442] Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020, https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf
[443] NETSCOUT, NETSCOUT THREAT INTELLIGENCE REPORT, DDoS in a Time of Pandemic, 2020, https://www.netscout.com/threatreport
[444] Emma Woollacott, Surge in malware and cyber-attacks set to continue, Europol warns in SOCTA 2021 report, April 2021, https://portswigger.net/daily-swig/surge-in-malware-and-cyber-attacks-set-to-continue-europol-warns-in-socta-2021-report
[445] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, DDoS attacks in Q4 2020, February 2021, https://securelist.com/ddos-attacks-in-q4-2020/100650/
[446] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, DDoS attacks in Q2 2020, August 2020, https://securelist.com/ddos-attacks-in-q2-2020/98077/
[447] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, DDoS attacks in Q3 2020, October 2020, https://securelist.com/ddos-attacks-in-q3-2020/99171/
[448] Verizon, Data Breach Investigations Report (DBIR) 2020, 2020
[449] David Warburton, F5 Labs, DDoS Attack Trends for 2020, May 2021, https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020
[450] Verizon, Cross-site scripting (XSS) attacks in Q4 2020: Trends and best practices, March 2021, https://www.verizondigitalmedia.com/blog/cross-site-scripting-attacks-trends-and-best-practices/

vectors targeted web applications.[448] The latter data was also confirmed in the Verizon 2021 Data Breach Investigations Report (DBIR).[451]

8.1.9 Trends on classifying DDoS attacks

The geographical spread of DDoS attacks in 2020-21 depends on attack classification, though some commonalities emerge[445] [446]:

- China and USA are always mentioned in the first two places both as targets and sources of DDoS attacks.
- Netherlands, Germany and France are often at the top places in the EU as targets and sources of DDoS attacks.
- In 2021, Canada, Netherlands, France, Great Britain, Germany, Brazil and Australia had sharp increases as sources of attacks, with Canada moving to spot #3. Similarly, Great Britain, Germany, France, Brazil and Australia experienced sharp increase as targets of attacks, with The Netherlands moving to spot #3. Also, unexpectedly, Poland entered the top ten.
- According to Cloudflare, Malaysia and India are the #3 and #4 source countries, while Morocco became the #3 target country.[452]

Concerning the sector spread, Akamai monitored data from 2017 to the end of 2020 and observed an increase in the number of DDoS attacks over the 50 Gbps threshold. Moreover, a general increase in attacks in 7 out of 11 of the analysed sectors was observed with a sharp increase in Business Services (960%), Education (180%), Financial Services (190%), Retail & Consumer Goods (445%), and Software & Technology (196%).[453]

Confirming these results, F5 labs claimed, "*the education sector saw a large increase in DDoS attacks in January 2021, with more than 56% of all education incidents for the past 15 months occurring in Q1 2021*". Concerning the domains attacked, technology, telecommunications, and finance are in the first three places, while if we compare the number of attacks with the average attack sise, healthcare is the most critical domain.[454]

8.1.10 Web-based attack main trends persist

Web Attacks includes threats, such as injection and application malfunctioning, affecting IT systems in their entirety. Modern IT systems are based on services composed at run time, which can be the target of attacks and breaches. These services often expose a standard API interface (e.g. REST, RPC) and interact on virtual networks or orchestration platforms, introducing new security challenges to cope with. At the same time, "traditional" (i.e. desktop, client-side) applications suffer from long-standing issues that are still a source of bugs and attacks. Though web attacks have remained stable over the years, we can note some interesting points as follows.

- **Security Misconfiguration.** Unpatched software, use of default accounts or unused pages are the preferred means exploited by attackers to bypass security protections and gain unauthorised access to systems.[455] These holes can be found at all layers of a system and are difficult to manage.
- **Automated brute force, dictionary, and session management attacks are increasingly adopted.**[455] For instance, Remote Desktop Protocols (RDPs) are exploited by attackers for malware infection; to do this, attackers search for specific open ports in order to implement brute force attacks.
- **Cyber-attackers are turning security defences into weapons.** For instance, secure channels can be used to cover malware distribution, to disrupt secured transactions, and for data exfiltration.[455]
- **Untrusted compositions.** Composite services are increasingly composed of atomic services to provide advanced functionalities, while introducing new risks that go beyond the risks faced by atomic services.[456] On one hand, composite services can increase the risk of data breaches by combining the different sources

[451] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021
[452] Vivek Ganti, Omer Yoachimik, DDoS attack trends for 2021 Q1, April 2021, https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1/
[453] Tom Emmons, PART I: Retrospective 2020: ddos was back -- bigger and badder than ever before, https://blogs.akamai.com/2021/01/part-i-retrospective-2020-ddos-was-back-bigger-and-badder-than-ever-before.html
[454] David Warburton, F5 Labs, DDoS Attack Trends for 2020, May 2021, https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020
[455] H2020 EU Project CONCORDIA, Deliverable D4.1 - 1st year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf
[456] M. Anisetti, C. Ardagna, E. Damiani e G. Polegri, Test-Based Security Certification of Composite Services, ACM Transactions on the Web, vol. 13, pp. 1-43, February 2019

of information they have. On the other hand, the composition of atomic services could entail an endemic risk related to the fact that the strength of a composite application is the one of its weakest link.[457]

- **Many of the OWASP Top 10 Vulnerabilities are due to misconfigurations**[458]**,** an issue discussed in Chapter 10 of the ETL 2021**.** Injection and cross-site scripting (respectively number 1 and number 7 in the list of the OWASPs most critical web application security risks) exploit system misconfigurations, such as insufficient data validation. In addition, default configurations are often insecure and cause web-based attacks. Finally, a lack of server-side verification or access controls introduces a level of risk, especially when auxiliary services are requested.
- According to the OWASP[458], **web-based attacks exploit components with known vulnerabilities.** Also, they benefit from insufficient logging and monitoring.

8.2 RECOMMENDATIONS

Both DDoS and web-based attacks are long-standing threats and several mitigation measures are well known and established. In summary, we present in the following some fundamental mitigation vectors for DDoS and web-based attacks, with a particular focus on trends that emerged during the reporting period.

- A denial-of-service response plan is fundamental for organisations where resilience is a priority and should integrate system checklists, response teams, and efficient communication and escalation procedures.
- The security process should be a continuous activity that follows and adapts system and network evolutions and life cycles.[434]
- Collaboration and coordination between relevant organisations is important to multiply and strengthen mitigation efforts.
- Implement DDoS protection using an on-premises solution, DDoS scrubbing service, or a hybrid solution.[454]
- Use both network and web application firewalls[442]. The first can be coupled with approaches mitigating peaked traffic such as a Content Delivery Network (CDN), a load balancer and scalable resources. The latter is particularly useful in case DDoS is based on injection or XSS.[459]
- Use antivirus solutions to curb malware infections.
- Use a network-based intrusion-detection system.
- Apply patches promptly, especially when many employees use their personal machines for work. Organisations should give high priority to system updates and deliver them to users remotely.
- Traffic profiling and traffic filtering may assist in providing early warning signs of abnormal traffic patterns that are an indicator of DDoS attacks.
- Use DDoS mitigation services to detect abnormal traffic flows and redirects traffic away from your network, as well as rate limiting to restrict the volume of incoming traffic.
- Protect web-based APIs and monitor for related vulnerabilities.
- Fortify DNS or even consider a managed DNS service. Cache poisoning or similar exploits can be prevented by the use of DNSSEC, or even better a managed DNS vendor supporting the DNSSEC specification.
- Consider a multi-layered solution mixing detection, investigation, and response capabilities across multiple platforms.
- Build a threat intelligence program based on a proactive approach that adapts the security posture to the evolving threat environment.
- Use staff training and cybersecurity exercises to increase capacity building and preparedness.

Countermeasures for mitigating web-based attacks are as follows:

- Set up a web application firewall (WAF) to identify and filter malicious requests.[459] WAF must be kept updated to protect the system against newly discovered vulnerabilities.
- Strengthen the code base (e.g. input sanitisation, parametrised statements) to protect against injection-based attacks.

[457] H2020 EU Project CONCORDIA, Deliverable D4.2 - 2nd year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.2.pdf
[458] OWASP Top Ten, https://owasp.org/www-project-top-ten/
[459] Tripwire, The 10 Most Common Website Security Attacks (and How to Protect Yourself), December 2020, https://www.tripwire.com/state-of-security/featured/most-common-website-security-attacks-and-how-to-protect-yourself/

- Promptly update software to avoid zero-day attacks.
- Properly configure and harden web servers and regularly patch all servers exposed on the Internet.
- Continuously verify the effectiveness of your security hardening, using attack tools, vulnerability scanners, and penetration test services.
- Enable logging and inspect those logs.

9. DISINFORMATION - MISINFORMATION

The rise in the use of digital technologies and social media has changed the way in which people access information and news. Unlike traditional media (e.g. newspapers, TV), social media guarantees direct access to information with no filters. The price we pay for such a convenient way of accessing information is the increasing risk of retrieving fake news and manipulated information.[460] In this context, social media assumes the role of preferred amplifier of information, much more than what happened with the advent of traditional media. This information may be fake (therefore changing perception of reality in people) or real (information about incidents, errors, losses, opinions, and reputation regarding a company). The amplification effect of (social) media is an important threat to individuals, enterprises and even states, because an item of false news can be perceived as real, while an apparently minor problem might become a major incident in public opinion. In addition, social media can be manipulated to distort the market or become effective vectors of misinformation/smear campaigns against a company or the reputation of some of its most representative individuals. The brand reputation, financial solidity of the company, and the trustworthiness of the management as well as the honesty and trustworthiness of individuals are therefore put at risk.

Media-driven market manipulations and misleading public-opinion campaigns were boosted in recent years thanks to new technologies that increase the ability to spread fabricated information.[455] Two main attacks emerged, namely, disinformation and misinformation. Though often perceived as similar, since they refer to inaccurate, incorrect, or misleading information, they entail fundamentally different concepts.[461] [462] [463]

Disinformation is an intentional attack that consists of the creation or sharing of false or misleading information. Disinformation attacks experienced an exponential boost in the COVID-19 pandemic era, for instance, targeting people's trust on vaccines.

Misinformation is an unintentional attack, where sharing of information is done inadvertently. Inaccuracy carried by the information is unintentional and could happen for example when a journalist reports wrong information in good faith or reports information by mistake. The spread of misinformation also includes scenarios where people believe a news item regardless of veracity because it supports their worldview.

One may argue about the how these threats relate to cybersecurity. It is important to note that disinformation and misinformation attacks are among the preparatory activities at the basis of other attacks (e.g. phishing, social engineering, malware infection). Moreover, such threats are often used in tandem with other cybersecurity threats, thus leading to advanced hybrid threats. It should also be underlined that the main aim of these threats is to undermine trust, which is the foundation of cybersecurity. By shattering that foundation, cascading effects ripple throughout the whole cybersecurity ecosystem and may have severe implications.

The success of these attacks is due to the spread guaranteed by social media, and has both technical and social foundations.[464] [465] Social media amplifies news and circulates information independently of its accuracy. Technical

[460] Infographic: Beyond Fake News – 10 Types of Misleading News – Seventeen Languages, https://eavi.eu/beyond-fake-news-10-types-misleading-info /
[461] Caroline Jack, "Lexicon of Lies: Terms for Problematic Information" (New York: Data & Society, 2017), https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf .
[462] Alice E. Marwick, "Why Do People Share Fake News? A Sociotechnical Model of Media Effects," Georgetown Law Technology Review (474) (2018), available at https://georgetownlawtechreview.org/why-do-people-share-fake-news-a-sociotechnical-model-of-media-effects/GLTR-07-2018/
[463] Erin Simpson, Adam Conner, Fighting Coronavirus Misinformation and Disinformation
Preventive Product Recommendations for Social Media Platforms, August 2020, https://www.americanprogress.org/issues/technology-policy/reports/2020/08/18/488714/fighting-coronavirus-misinformation-disinformation/
[464] Caroline Jack, "Lexicon of Lies: Terms for Problematic Information" (New York: Data & Society, 2017), https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf .
[465] Europol, EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2021), 2021

features such as lists of trending topics contribute further to this circulation. In addition, many sites flourish because their intent is to make money through advertising. Their goal is not to circulate true or false information but rather to collect clicks (clickbait), which has the side effect of spreading misleading information.[466]

The complexity of this scenario is due to the difficulty in distinguishing the real intent of a piece of information or even its originator. This is even more difficult when information campaigns are analysed in detail. Different campaigns exist and their boundaries are quite difficult to draw. For instance, the differences between advertising, public relations, public diplomacy (or public affairs), information operations, and propaganda are quite blurred, since they all represent information campaigns whose understanding depends on personal interpretation.[467]

This huge flow of dis- or mis-information is flooding people with the goal of causing uncertainty, apathy towards truth, exhaustion in trying to find it, and fear. It is becoming increasingly clear that policy-makers should put disinformation at the core of their agenda, while also including security and privacy implications.[468]

Social media are the most critical vector for misinformation and disinformation attacks. They permit direct access to information with no filters, increasing the risk of encountering fake news and manipulated information. Social media are also the preferred amplifier of misinformation and disinformation attacks, bringing those attacks on a large-scale. Technical peculiarities of social networks also increase the circulation of (fake) news such as trending topic lists. This is further amplified when people are in social relations and exchange information with like-minded people sharing the same beliefs, creating the so called “Echo Chamber” effect.[469]

Examples of social media-based attack vectors are celebrities or influencers spreading disinformation, social media groups promoting material for supporters. Traditional approaches are also used to carry out disinformation or misinformation attacks such as the spread of malicious accounts: bots, spammers, fake domains, and cyborgs.[470] Social bots have attracted a huge interest and have been massively adopted.[471] Some studies, on Twitter, claimed that social bots can represent between 5 and 15% of users and are responsible for misinformation campaigns, phishing attacks, election and market manipulation.[472]

Starting from the above vectors, two main classes of threat agents are playing the disinformation/misinformation role. On one hand, we have state-backed groups implementing state-sponsored attacks. On the other hand, we have cybercriminals, that is, non-state and private commercial organisations benefiting from the increasing availability of Disinformation-as-a-Service. For instance, conspiracy narratives are distributed by terrorists, extremists and organised criminal groups to manipulate people. In general, a large part of attacks is managed by non-state domestic actors, while both types of agents are increasingly targeting the private sector to spread misinformation, and manipulate the market or attack the reputation of competitors.[473] [474] Misinformation and disinformation are increasingly distributed as chains of messages, social media content, deepfakes, and phishing via voice, text, and e-mail.[475]

[466] Alice E. Marwick, “Why Do People Share Fake News? A Sociotechnical Model of Media Effects,” Georgetown Law Technology Review (474) (2018), available at https://georgetownlawtechreview.org/why-do-people-share-fake-news-a-sociotechnical-model-of-media-effects/GLTR-07-2018/
[467] Caroline Jack, “Lexicon of Lies: Terms for Problematic Information” (New York: Data & Society, 2017), https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf.
[468] The Global Economic Forum, The Global Risks Report 2021 16th Edition, 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[469] Wayne Rash, Cyber-Attacks, Disinformation, Pre-Election Chaos And The Pandemic Combine To Produce New Strategic Threats Against The US, July 2020, https://www.forbes.com/sites/waynerash/2020/07/31/cyber-attacks-disinformation-pre-election-chaos-and-the-pandemic-combine-to-produce-new-strategic-threats-against-the-us/
[470] Tanveer Khan, Antonis Michalas, Adnan Akhunzada, Fake news outbreak 2021: Can we stop the viral spread?, Journal of Network and Computer Applications, Volume 190, 2021, https://www.sciencedirect.com/science/article/pii/S1084804521001326
[471] H2020 EU Project CONCORDIA, Deliverable D4.1 - 1st year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf
[472] Cloudflare Inc. What is a Social Media Bot?, Cloudflare, 2020., available at: https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot/
[473] Control Risks, Disinformation will affect more than elections in 2021, February 2021, https://www.controlrisks.com/our-thinking/insights/disinformation-will-affect-more-than-elections-in-2021
[474] Rodney Joffe, How security teams can combat disinformation attacks, November 2020, https://www.securityinfowatch.com/security-executives/article/21162305/how-security-teams-can-combat-disinformation-attacks
[475] Zarmeena Waseem, Scams and Misinformation Challenges, May 2021, https://staysafeonline.org/blog/scams-and-misinformation-challenges/

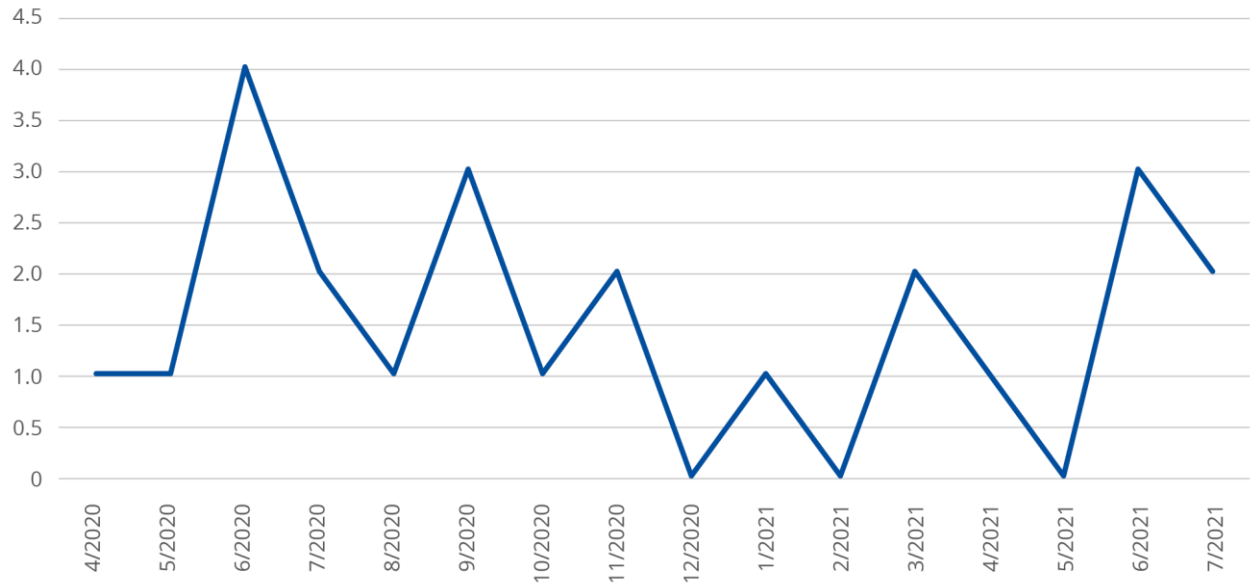
Misinformation and disinformation have different targets and means, as well as goals. They may aim to cause financial and reputational damage and arouse a lack of trust in society at all levels. An overview is presented in Table 2. [476]

Table 2: Misinformation and Disinformation: Target, Means, and Goals

Target	Means	Goal
People	Disinformation, misinformation, fake news	Reduce perceived honesty and trustworthiness of individuals
Enterprises	Market distortion, misinformation, disinformation, smear campaigns, fake news, propaganda	Affect brand reputation, financial solidity of the company, and the trustworthiness of the management.
Society	Disinformation, fake news	Inability to distinguish real and fake news, apathy, exhaustion in trying to find the truth, manipulating and misleading public-opinion
Any	Sharing of inaccurate information	Make money based on advertisement

Figure 10 shows incidents based on OSINT (Open Source Intelligence) collected by ENISA for the purposes of situational awareness.[477] The scope of the collection is global and multi-sectorial. Incidents, however, with a direct impact in the EU area are given priority. Notable misinformation and disinformation incidents are included in Annex B. More work is needed to better classify cyber incidents related to disinformation and misinformation, since a lot of them are classified in other categories given that they are commonly used in complex, hybrid attacks. This is the reason why there is a constant fluctuation throughout the year as evidenced by the figure.

Figure 10: Misinformation and disinformation incidents observed by ENISA (April 2020-July 2021)



[476] PwC, The disinformation age has arrived. Are you ready? https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html
[477] In accordance with the EU cybersecurity act Art.7 Par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

9.1 TRENDS

The Global Risks Report of the World Economic Forum[478] reports that "*disinformation and misinformation campaigns can erode community trust in science, threaten governability and tear the social fabric. According to the GRPS, a 'backlash against science' will heighten the risks of 'climate action failure' and 'infectious diseases' over the next decade.*" Dissemination of disinformation on elections, humanitarian crises, and public health, security and cultural issues is expected to increase over the next decade. Political divisiveness acts as an amplifier of disinformation and is affecting public trust, especially in those countries (e.g. US) where a non-negligible number of individuals primarily access political news through social media (2020).[479]

Some interesting and important points emerge and are summarised in the following.

- Phishing is at the heart of disinformation attacks and it strongly exploit the beliefs of people.
- Human-centric threats are difficult to analyse in pragmatic terms, including the ability to describe, decompose, classify, and reproduce them to feed quantitative analyses, graphical or numerical simulations, or coding into algorithms.[436]
- Disinformation attacks benefit from the difficulty of quantifying everything connected with humans. When the threat involves or depends on people's behaviour (e.g. errors, cognitive bias, skill shortages), measurements and data collection are complex processes that often result in poor-quality data.[436]
- The problem around disinformation is not the ability to distinguish true or false information; instead it is a social and epistemic crisis amplified by the evolving media and political context.[463]
- Disinformation that is moving from political/social spheres to the corporate world is growing in scope and impact thanks to social media platforms and content creation technologies.[480]

9.1.1 AI-enabled disinformation supports attackers in carrying out their attacks

AI is used to build realistic profiles and images, to vary the content and wording of posts and to get unnoticed.[481] [482] AI-powered social media is at the basis of the spread of disinformation, causing social chaos.[483]

Deepfakes technology is evolving quickly. Supporting technology makes the creation of deepfakes simpler, while social media help in spreading them[484]. Additionally, misinformation and disinformation campaigns are becoming more credible thanks to deepfakes, which cannot yet be fully counteracted.[485] [486]

9.1.2 Coronavirus pandemic used for amplification of attacks

COVID-19 is a top topic for disinformation attacks, resulting in what the World Health Organisation (WHO) warned as an infodemic of online dis/misinformation.[487] [463] Disinformation campaigns aim to spread fear, uncertainty and doubt around the effectiveness of Coronavirus vaccines. This is used as the basis for social engineering attacks. It also targets the beliefs of individuals, reducing trust in information sources and impacting business brands. Businesses and individuals are targeted by disinformation campaigns focused on green pass, mandatory vaccination, health passports, mass immunity testing, and lockdowns.

[478] The Global Economic Forum, The Global Risks Report 2021 16th Edition, 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[479] Miles Parks, Trump Is No Longer Tweeting, But Online Disinformation Isn't Going Away, March 2021, https://www.npr.org/2021/03/05/971767967/trump-is-no-longer-tweeting-but-online-disinformation-isnt-going-away?t=1624004975614
[480] PwC, The disinformation age has arrived. Are you ready? https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html
[481] John Villasenor, how to deal with AI-enabled disinformation, November 2020, https://www.brookings.edu/research/how-to-deal-with-ai-enabled-disinformation/
[482] Fabio Rugge, AI in the Age of Cyber-Disorder: Actors, Trends, and Prospects, 2020, https://www.ispionline.it/sites/default/files/pubblicazioni/ispi_report_ai_in_the_age_of_cyber-disorder_2020.pdf
[483] The Global Economic Forum, The Global Risks Report 2021 16th Edition, 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[484] Avast, 2020: The Year of Fake News, COVID-related Scams and Ransomware, November 2020, https://www.prnewswire.com/news-releases/2020-the-year-of-fake-news-COVID-related-scams-and-ransomware-301180568.html
[485] Chuck Brooks, Alarming Cybersecurity Stats: What You Need To Know For 2021, March 2021, https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/
[486] Europol, EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2021), 2021
[487] Managing the COVID-19 infodemic: Promoting healthy behaviors and mitigating the harm from misinformation and disinformation, Joint statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC, September 2020 , https://www.who.int/news/item/23-09-2020-managing-the-COVID-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation

COVID-19 pandemic resulted in an infodemic of online misinformation as stated by the WHO, on the one hand, and disinformation services, on the other hand.[463] Focusing on disinformation and the COVID-19 pandemic, AVAST went a step further and indicated that ***2020 was the year of fake news and COVID-related scams***.[488] Cybercriminals used the pandemic for financial and reputational damage, reducing the trust in the scientific community and vaccines, as well as trying to spread malware using COVID-related ads and apps distributed through social networks (e.g. TikTok, YouTube, Instagram). As an example, during the lockdown imposed to flatten the COVID-19 curve, experts were competing with substantial campaigns of online misinformation and disinformation[463]. In more detail, fake shops related to COVID-19 proliferated, as well as scams targeting people interested in information related to COVID-19. Six hundred malicious apps proposing COVID-19 services contained trojans/spyware. Avast also reported the rise of deepfakes especially related to pornographic domains and targeting normal people (e.g. TikTok users). The UK's National Cyber Security Centre, in April 2020, removed 2,000 scams, including 471 fake online shops, and 200 phishing sites.[489] [490] In this context, politicians, policy makers, legislators are pressing social media enterprises (e.g. Google, Facebook, Twitter) to find countermeasures and limit the proliferation of misinformation/disinformation campaigns.[491]

9.1.3 Disinformation-as-a-Service (DaaS)

Professional disinformation is produced on a large scale by major governments, political parties, and public relations firms.[492] Since 2019, a growing number of third parties have been offering disinformation services, providing targeted attacks on behalf of clients.[493] Services are provided in numerous countries and an increasing number of non-state and private commercial organisations are using them.[494] In this context, disinformation has moved from political and social spheres to the corporate world.[495] The University of Oxford monitored the manipulation of public opinion using social media by governments and political parties, and the various private companies and other organisations they work with to spread disinformation.[496] From a geographical point of view, disinformation and misinformation are targeting every country in the world.

9.2 RECOMMENDATIONS

Mitigation vectors include both technical and non-technical domains. On one side, mitigation vectors are manual and human-based approaches targeting training and awareness, fact checking and debunking, regulations, and communication. On the other side, technical solutions are important to limit the spread of mis/disinformation through social networks. Co-operation between all actors is important to further limit the impact of mis/disinformation attacks.

In general, the following approaches may be explored to mitigate misinformation and disinformation campaigns.

- **Training and awareness**: is the process preparing employees in managing disinformation attacks, and also in assessing any e-mail and report.[497] [498] In this context, following a vaccine-like approach, prebunking aims to expose users to a small amount of mis/disinformation to prepare them to manage mis/disinformation later on. Other approaches focus on gamification, where a simulation of social media feeds is used to teach users in distinguishing real and fake news. For instance, online game, "Go Viral!"[499] aimed to prebunk common misinformation surrounding COVID-19.[500]

[488] Avast, 2020: The Year of Fake News, COVID-related Scams and Ransomware, November 2020, https://www.prnewswire.com/news-releases/2020-the-year-of-fake-news-COVID-related-scams-and-ransomware-301180568.html
[489] Paul McEvatt, Fujitsu, 2021 Prediction: The Age of Disinformation Attacks, January 2021, https://blog.global.fujitsu.com/fgb/2021-01-12/2021-prediction-the-age-of-disinformation-attacks/
[490] Fujitsu, Top 10 Cyber Security Predictions for 2021, 2021, https://www.fujitsu.com/global/services/security/insights/predictions-2021/
[491] Jane Wakefield, Google, Facebook Twitter grilled in US on fake news, March 2021, https://www.bbc.com/news/technology-56523378
[492] Samantha Bradshaw, Hannah Bailey, Philip N. Howard, Industrialised Disinformation 2020 Global Inventory of Organised Social Media Manipulation, 2020, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf
[493] CTI League, Darknet Report 2021, 2021
[494] Control Risks, Disinformation will affect more than elections in 2021, February 2021, https://www.controlrisks.com/our-thinking/insights/disinformation-will-affect-more-than-elections-in-2021
[495] PwC, The disinformation age has arrived. Are you ready?,https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html
[496] Samantha Bradshaw, Hannah Bailey, Philip N. Howard, Industrialised Disinformation 2020 Global Inventory of Organised Social Media Manipulation, 2020, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf
[497] Paul McEvatt, Fujitsu, 2021 Prediction: The Age of Disinformation Attacks, January 2021, https://blog.global.fujitsu.com/fgb/2021-01-12/2021-prediction-the-age-of-disinformation-attacks/
[498] Fujitsu, Top 10 Cyber Security Predictions for 2021, 2021, https://www.fujitsu.com/global/services/security/insights/predictions-2021/
[499] Go Viral!, https://www.goviralgame.com/en
[500] Zara Abrams, Controlling the spread of misinformation, Monitor on Psichology, Vol. 52, No. 2, March 2021, https://www.apa.org/monitor/2021/03/controlling-misinformation

- **Mis/disinformation identification**: guidelines are emerging to identify fake content as well as to access content properly. For instance, examine sources, authors, cross-references, cited data and dates are some examples.[501] [502]
- **Fact Check and Debunking False Stories**: many efforts by both non-profit organisations and government agencies have been undertaken to reduce the impact of misinformation and disinformation.[503] [504] These actors aim to debunk publications and content carrying false information and fake news.[505] Many efforts have been undertaken to counteract the infodemic around COVID-19.[506]
- **Regulations**: new regulations (such as the proposed EC Digital Services Act[507]) and punishments for sites, including social networks, spreading fake news are under way. In the context of the GDPR (General Data Protection Regulation), it is possible to limit access to information that enables targeted advertising.[508] Accordingly, GDPR can help against misinformation by regulating the processing of personal data by online targeted advertising – which is also a tool used for spreading fake news. So GDPR, by regulating online targeted advertising, could also indirectly contribute in a broader way to the limitation of misinformation. The Code of Practice on disinformation provides self-regulatory standards to fight disinformation with the support of industry.[509] The EU recently released the Fifth Progress Report on "the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats". The report discussed the need to protect free and fair elections, the role of strategic communications and a centre of excellence for countering hybrid threats, the importance of cooperation among countries and resilience against radicalisation and extremism.[510]
- **Strategic and transparent communication**: that is factual and separate from political communication.[511]
- **Technical countermeasures**: [512] [513] [514] [515] [516] [455]
    - Rewriting search engine algorithms
        - Social network detection and mitigation: i) suspension of fake accounts (e.g. accounts that post duplicate or redundant information), ii) mechanisms to filter and flag fake news, iii) reductions of automatic activities (e.g. Bots), iv) artificial Intelligence tools and platforms to detect fake news based on online approaches, v) data science/big data visualisation to identify the large-scale spread of disinformation, vi) mobile apps and chatbots powered by factcheckers targeting the general public, vii) web-browser extensions for the general public, viii) digital media information literacy platforms and tools
    - Awareness campaigns through advertisements
    - Credibility rating, flagging suspicious behaviour
    - Digital watermarking (tagging visual content)
    - Creation of protection strategies centred around sentiment tracking and dark web monitoring.

[501] Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, Trend Micro, The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public, 2017, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
[502] CIS Center for Internet Security, Election Security Spotlight – Disinformation and Misinformation, https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disinformation-and-misinformation/
[503] Trend Micro, Fake News and Cyber Propaganda: The Use and Abuse of Social Media, June 2017, https://www.trendmicro.com/vinfo/it/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media
[504] Tanveer Khan, Antonis Michalas, Adnan Akhunzada, Fake news outbreak 2021: Can we stop the viral spread?, Journal of Network and Computer Applications, Volume 190, 2021
[505] Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, Trend Micro, The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public, 2017, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
[506] COVID-19 Resource Hub, https://www.disinfo.eu/coronavirus
[507] See https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[508] Control Risks, Disinformation will affect more than elections in 2021, February 2021, https://www.controlrisks.com/our-thinking/insights/disinformation-will-affect-more-than-elections-in-2021
[509] European Commission, Code of Practice on Disinformation, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[510] European Commission, Report on Countering Hybrid Threats and security package, June 2021, https://ec.europa.eu/defence-industry-space/report-countering-hybrid-threats-and-security-package_en
[511] OECD Policy Responses to Coronavirus (COVID-19), Transparency, communication and trust: The role of public communication in responding to the wave of disinformation about the new Coronavirus, July 2020, https://www.oecd.org/coronavirus/policy-responses/transparency-communication-and-trust-bef7ad6e/
[512] Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, Trend Micro, The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public, 2017, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
[513] John Villasenor, How to deal with AI-enabled disinformation, November 2020, https://www.brookings.edu/research/how-to-deal-with-ai-enabled-disinformation/
[514] United Nations Interregional Crime and Justice Research Institute (UNICRI), Stop the Virus of Disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it, November 2020, http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf
[515] Control Risks, Disinformation will affect more than elections in 2021, February 2021, https://www.controlrisks.com/our-thinking/insights/disinformation-will-affect-more-than-elections-in-2021
[516] Bruce Potter, Misinformation campaigns will dominate cybersecurity headaches in 2021, January 2021, https://www.securitymagazine.com/articles/94097-misinformation-campaigns-will-dominate-cybersecurity-headaches-in-2021

10. NON-MALICIOUS THREATS

Threats are commonly considered as voluntary and malicious activities carried out by adversaries who have some incentives to attack a specific target. In these sections, we cover threats where malicious intent is not apparent.

Non-malicious threats are mostly based on human errors and system misconfigurations[517] , but they can also refer to physical disasters that target IT infrastructures. Non-malicious threats can be classified in two categories:

Errors and Misconfigurations are caused by negligence, lack of awareness or, simply, human errors. These include:

- errors when managing an IT system: i) misconfigurations introduced when specific applications and systems are (re-)configured and updated; ii) erroneous system management including errors in patching and updating a system; iii) erroneous system administration, for instance, in distributing privileges among users; iv) issues in the management of traditional systems such as network security, access control, identity management.
- development-time errors: i) issues with the management of dependencies; for instance, libraries that are used without developers even noticing; ii) long-standing issues, for instance, memory safety, unsanitised inputs and, in general, issues with well-known solutions involving the use of modern tools,[518] [519] [520] [521] iii) other forms of negligence, for instance, storing application credentials on public repositories.[522] [523] [524]
- application-level errors: i) errors introduced when using an application/system, ii) misconfigured (cloud) applications and poor password and key management; for instance, publicly available buckets, unencrypted databases, iii) minor errors, such as sending an e-mail to the wrong recipient.[525]
- physical errors: i) unattended devices, ii) unsecured documents/information, iii) exceptions to physical access rules.

Physical Disasters can be classified as:

- damages to or failures of physical infrastructure, such as inadvertent damage to fibre cables, loss of Internet connection, fire, unstable power supply,
- natural disasters, such as floods and earthquakes, causing the unavailability of the IT infrastructure and related services/applications.

For non-malicious threats, we can distinguish between four **main actors**:

- **Normal Users** interact and use a system with all privileges needed to carry out a specific and limited activity on it.
- **Privileged users (Admins)** have root privileges on the system and are responsible for system configuration and management. Intuitively, and confirmed by some reports, the damage caused by an error committed by these users is typically much higher.[526] These also include users responsible for physical IT infrastructure.

[517] H2020 EU Project CONCORDIA, Deliverable D4.2 - 2nd year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.2.pdf
[518] JSOF. Ripple20. https://www.jsof-tech.com/disclosures/ripple20
[519] Lily Hay Newman, Wired, An Operating System Bug Exposes 200 Million Critical Devices, July 2019 https://www.wired.com/story/vxworks-vulnerabilities-urgent11/
[520] Lily Hay Newman, Wired, Decades-Old Code Is Putting Millions of Critical Devices at Risk, October 2019 https://www.wired.com/story/urgent-11-ipnet-vulnerable-devices/
[521] Ben Seri, Armis. URGENT/11 Affects non-Vxworks Operating Systems, October 2019 https://www.armis.com/blog/urgent11-affects-additional-rtoss-highlights-risks-on-medical-devices/
[522] Jelle Ursem and DataBreaches.net, No need to hack when it's leaking, August 2020, https://www.databreaches.net/wp-content/uploads/No-need-to-hack-when-its-leaking.pdf
[523] Forescount. Amnesia:33, https://www.forescout.com/research-labs/amnesia33/
[524] Lily Hay Newman, Wired, Critical Flaws in Millions of IoT Devices May Never Get Fixed, December 2020, https://www.wired.com/story/amnesia33-iot-vulnerabilitiesmay-never-get-fixed/
[525] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[526] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021

- **Developers** design, code, implement and maintain a specific software, service or system.
- **Service/Cloud providers** supply a service or cloud functionality that is then integrated within the system. This category can also be broadened to include third-party providers of software libraries and components.

Depending on their role, different types of non-malicious threats can be associated to actors as seen in Table 3:

Table 3: Mapping between non-malicious threats and actors

Threat Category	Threat Type	Actors
Errors and Misconfigurations	Errors made when managing an IT system	Privileged Users
	Development-time errors	Developers, Service/Cloud Providers
	Application-level errors	Users, Privileged Users
	Physical errors	All
Physical Disasters	Damages to or failures of physical infrastructure	Privileged Users, Cloud Providers
	Natural disasters	None

Non-malicious threats represent a major threat vector for many existing malicious threats. For instance, security vulnerabilities, misconfigurations, inadequate vulnerability and patch management can open the door to DDoS attacks, malware and ransomware. At the same time human errors are a major vector for phishing and social engineering. Notable non-malicious incidents are included in Annex B.

Misconfiguration is the most common attack vector (approximately 50%), followed by misdelivery (approximately 30%), based on a 2021 report by Verizon on data breaches.[527] Programming errors account for a very small percentage, stressing the fact that often security measures do exist and work correctly but are not applied. Cloud misconfigurations substantially boosted and, according to Palo Alto Networks, can be classified in two main categories: *i)* storage and encryption issues, *ii)* network issues.[528] Encryption of data at rest and in transit remains among the major misconfigurations, as well as permissive policies, lack of sophisticated protections and storage available publicly.[529] Also, non-malicious vectors/threats are rising in the case of the Internet of Things (IoT) with i) exploitation of device vulnerabilities (41%, including 3% zero-day) and ii) user practices (26%, 13% password-based) in the top spots.[530]

Considering non-malicious threat agents and vectors, the statement that points to “humans as the weakest part in a system” is becoming increasingly relevant. Major threat vectors are lack of training and skills, as well as awareness, in the users, developers and administrators. Lack of standardised processes, as well as weak configurations by default (e.g. encryption disabled by default), are increasing the probability of an error/misconfiguration.[531] All these vectors coupled with the increasing complexity of modern systems that mix Cloud, Edge and IoT make current scenarios a ticking time bomb. At the same time, weak physical infrastructures not ready to face destructive natural events, as well as lack of proper plans for utility management open the doors to disasters that might impact the availability of the system.

Major inadvertent threat agents are therefore individuals who have different roles in system life cycles as end users, privileged users, developers and cloud/services providers. Considering errors and misconfigurations, in virtually all cases the threat actor is internal, for instance, an employee inadvertently publishing some records, or an IT manager not securing properly an S3 bucket. In more detail,[532] internal actors account for 99% of breaches, the remaining percentage is divided among partners and a combination thereof. Among internal actors, the three most frequent are

[527] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021
[528] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[529] Aqua Security - Cloud Security Report - Cloud Configuration Risks Exposed
[530] https://unit42.paloaltonetworks.com/iot-threat-report-2020/
[531] Aqua Security - Cloud Security Report - Cloud Configuration Risks Exposed
[532] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021

system admin (approximately 50%), developer (approximately 30%), and end user (approximately 20%). However, the possible damage of such breaches is typically much higher in the first two cases, since i) system admins are the most powerful users controlling virtually all the systems; ii) developers frequently have privileged access to data. Regarding physical disaster, threat agents are either the users acting on and managing the physical infrastructure, or natural events impacting the physical infrastructure.

10.1 TRENDS

In summary, non-malicious threats have historically had an important impact on the working of IT systems and applications, but their impact is being exacerbated by i) the increasing complexity of the systems and infrastructures; ii) the increasing migration to cloud environments and integration of IoT devices and edge computing, often with limited amount of time, skills and resources;[533] and iii) the COVID-19 pandemic. On top of this, skills shortages and well-known vulnerabilities or misconfigurations continue to be an issue.

10.1.1 Errors and system misconfigurations are the most frequent reported root cause

In 2020, out of the incidents with significant impacts reported under the NIS directive[534], 17% were flagged as human errors, while system failures remain the most frequent root cause of reported incidents at a rate of 48%. The causes these incidents were software bugs and hardware failures. This was a continuing trend as similar figures were reported in 2019.[535]

Similar trends are also observed for Telecommunication and Trust services in 2020:

- System failures in the telecom sector maintained the widest impact with almost 50% of the total user hours lost and were the most likely root cause of incidents (61%).[536] Faulty software changes/updates accounted for 41% of the total user hours lost and 24% of the total incidents. Human errors accounted for 41% of the total user hours lost, and were the root cause of 26% of total incidents (an increasing trend). Third party failures remain stable at 29%.
- System failures accounted for more than half of the incidents in the trust services sector in 2020, and were the major root cause (53%). Human errors were the root cause of 39% of the incidents.[537]

10.1.2 COVID-19 increased the number of non-malicious incidents due to migration to the cloud

The pandemic forced a migration to the cloud, causing a substantial increase in cloud workloads between October 2019 and February 2021 all over the world: 70% in the APAC region, 69% in the EMEA region, 65% in the AMER region and 58% in Japan[538]. According to Palo Alto networks,[538] the industries with the highest increase in security incidents (Retail 402%, Manufacturing 230%, Government 205%, and Pharma and Life sciences 127%) were among those that increased their cloud workloads significantly due to the pandemic.

A huge number of recent data breaches is caused by misconfigured buckets.[539] While many of them revealed personal information, it is also common to find credentials and secrets stored in buckets. Using simple crawling techniques, Truffle Security built an initial list of 4,000 open S3 buckets which, due to file name patterns, were likely to contain environmental variables and other secrets. Files matching those patterns contained an average of 2.5 secrets. Furthermore, some of them also contained credentials to open authenticated buckets and secrets for other services, from database passwords to PayPal credentials and JWT secrets.

[533] Security Today, The IoT Rundown For 2020: Stats, Risks, and Solutions, January 2020, https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2
[534] Annual Report NIS Directive Incidents 2020 CG Publication, to be released. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[535] Annual Report NIS Directive Incidents 2019, CG Publication 03/20, December 2020. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[536] ENISA, Telecom Security Incidents 2020 - Annual Report, July 2021, https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020
[537] ENISA, Trust Services Security Incidents 2020 - Annual Report, July 2021, https://www.enisa.europa.eu/publications/trust-services-security-incident-2020-annual-report
[538] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[539] Truffle Security, An API Worm in The Making: Thousands of Secrets Found in Open S3 Buckets, August 2021, https://trufflesecurity.com/blog/an-s3-bucket-worm-in-the-making-thousands-of-secrets-found-in-open-s3-buckets

10.1.3 Vulnerabilities and bugs continue to play a prominent role

In 2020, NIST received more than 18,000 new CVEs (fourth year in a row that this number grows)[540], and this trend seems to be continuing in 2021[541].

The 2020 also saw a never-seen-before spike in IoT malware, exploiting devices that are, in most cases, unsecure and never patched properly. The challenges behind unsecure IoT are well-known and detailed, for instance, the IoT Top Ten by OWASP contains vulnerabilities such as Insecure Ecosystem Interfaces, Lack of Secure Update Mechanisms, Use of Insecure or Outdated Components and Lack of Device Management.[542] Sonicwall reports an even faster increase in the first half of 2021.[543] In homes due to school reopenings, the rise in COVID-19 cases and the growth in the number of IoT devices.

On the contrary, the exploitation of vulnerabilities accounts for only 3% of breaches[544]. When organisations expose some vulnerable hosts on the Internet, such vulnerabilities are quite old and attackers still actively exploit them. According to Verizon, 20% of organisations expose vulnerabilities as old as 2010. SonicWall discovered similar old vulnerabilities still being exploited.[545]

These findings stress once again how organisations do not deal effectively with patch management. The scenario of unpatched vulnerabilities and legacy software is particularly critical in the healthcare sector. For instance, 83% of all imaging devices run on operating systems which are not actively supported, including Windows 7.[546] They are also responsible for a high number of security issues, compared to the number of deployed devices, where the imaging systems, patient monitoring and medical device gateways (which account for 34% of all devices) are at the basis of 86% of all security issues.

According to a recent report[547], the top 30 ecommerce retailers in the US use 1,131 third-party resources each and 23% of them include at least one critical vulnerability. This results in possible cascading effects where a compromise of a system can open the door to compromises in other domains. The total cost of a breach caused by a third party is $4.29 million on average. In this context, Verizon claims that web applications are involved in 43% of the breaches and 80% of organisations experienced an attack from a vulnerability in their third-party software.

According to Aqua Security,[548] SMEs do fix issues faster than enterprises, 75 days vs 88 days (on average).

10.1.4 Physical and natural threats affect digital infrastructures and telecommunications

According to the Annual Report NIS Directive Incidents 2020[549], natural phenomena were reported to affect only the digital infrastructure and the communication sector. About half of the incidents affecting the digital infrastructure sector (38 incidents – 9%) and one incident affecting the communication sector were reported as natural disasters. Regarding telecom security incidents in the EU reported in 2020[550], natural phenomena come third as the root cause at almost a tenth of total incidents (9%, 109 incidents in total).

10.2 RECOMMENDATIONS

It is important to note that, since non-malicious threats are among the major threat vectors for any type of attack, mitigation vectors in this section might overlap with the ones in other chapters of this report. The following proposed

[540] https://www.redscan.com/news/nist-nvd-analysis/
[541] https://nvd.nist.gov/general/nvd-dashboard
[542] OWASP. Top 10 Internet Of Things 2018. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
[543] Sonicwall, Sonicwall Cyber Threat Report, 2021 Midyear Update, sonicwall.com
[544] https://unit42.paloaltonetworks.com/iot-threat-report-2020/
[545] SonicWall. Attackers actively targeting vulnerable AVTECH devices, October 2020, https://securitynews.sonicwall.com/xmlpost/attackers-actively-targeting-vulnerable-avtech-devices/
[546] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[547] Juta Gurinaviciute, 5 biggest cybersecurity threats, February 2021, https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats
[548] Aqua Security - Cloud Security Report - Cloud Configuration Risks Exposed
[549] Annual Report NIS Directive Incidents 2020 CG Publication, to be released. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[550] ENISA, Telecom Security Incidents 2020 - Annual Report, July 2021, https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020

recommendations provide the basis for the development of a mitigation strategy for the prevention of and response to non-malicious threats.

- Holistic approach to security must be adopted, where traditional security is enriched with physical protection and disaster recovery.[551]
- Adopting a risk management process that considers non malicious threats, as well as cloud services.
- Avoiding shadow IT (and shadow IoT in particular)[552], coupled with good asset management.
- Continuous monitoring and testing to spot errors and misconfigurations in a timely manner.[553]
- Organisational policies: while basic cyber practices are often lacking, attacks are becoming more sophisticated and relying much more on the supply chain or on the human factor[554] [555]. In the latter case, attacks driven by AI (e.g. deepfakes) can trigger a human error, which is very difficult to prevent in a wholly technical way. Hence, robust organisational policies are needed to mitigate human errors.[556]
- Adopting a governance-based approach to data and security, allowing data to be thoroughly considered and followed.[557] [558] [559]
- A patch management plan to deal with vulnerabilities: a proper plan does not require everything to be patched but means what is needed must be patched, eventually using priorities coming, for instance, from a risk management process.[560,561]
- Adopting a wider definition of patch management, it should also refer to organisations pushing for updates rather than only receiving them (i.e. software and hardware producers). There are many cases of IoT vulnerabilities that have been around for years and it is difficult to understand who should actually publish the patches.[562] [563]
- Updates should be delivered in a secure way (e.g. Tesla Model X's lack of code signing[564]).
- Patch management must account for supply chain risk.[565,566]
- Training and awareness for all types of users. Properly trained developers can introduce many security and safety practices into their products,[567] leveraging modern languages and frameworks giving more security guarantees. This is crucial also for developing secure IoT devices without some long-standing issues such as those related to memory safety.[568] Admins should be trained on the security (and compliance) aspects of their activities, relying on solutions which ensure security by default. Finally, training and awareness are fundamental for end users to help them, for instance, in recognising early signs of incidents and making the right choice at the right moment.[569] [570] [571] [572] [573] [574]
- Engineering of physical infrastructures to be more robust against natural events, as well as a proper management of utilities guaranteeing business continuity in case of unexpected events or shortages.
- Zero-trust security approach,[575] assuming everything is considered malicious and untrusted. This approach moves from implicitly trusting assets because of their location or ownership towards a dynamic approach

[551] Andi Hendrickson, Top 5 Physical Security Considerations, July 2021, https://securityboulevard.com/2021/07/top-5-physical-security-considerations/
[552] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[553] Booz Allen Hamilton, Securing the Data Supply Chain, May 2021
[554] Accenture, State of Cybersecurity Report, 2020
[555] Booz Allen Hamilton, Supply Chain Vulnerability Trends to Watch Out For, February 2021
[556] Sophos Threat Report 2020
[557] Anna Larkina, Roman Dedenok, Doxing in the corporate sector, March 2021, https://securelist.com/corporate-doxing/101513/
[558] Booz Allen Hamilton, Securing the Data Supply Chain, May 2021
[559] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[560] Accenture, Cyber Threatscape Report, 2020
[561] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021
[562] Forescount Amnesie:33
[563] Lily Hay Newman, Wired, Critical Flaws in Millions of IoT Devices May Never Get Fixed, December 2020, https://www.wired.com/story/amnesia33-iot-vulnerabilitiesmay-never-get-fixed/
[564] Andy Greenberg, This Bluetooth Attack Can Steal a Tesla Model X in Minutes, November 2020, https://www.wired.com/story/tesla-model-x-hack-bluetooth/
[565] Booz Allen Hamilton, Securing the Data Supply Chain, May 2021
[566] Booz Allen Hamilton, Rethink Cyber Defense After the SolarWinds Hack, June 2021
[567] Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021
[568] Forescout Amnesia:33
[569] Kaspersky, Financial Cyberthreats in 2020, March 2021, https://securelist.com/financial-cyberthreats-in-2020/101638/
[570] Shasya Sharma, Monitor, review, and protect Amazon S3 buckets using Access Analyzer for S3, December 2019, https://aws.amazon.com/blogs/storage/protect-amazon-s3-buckets-using-access-analyzer-for-s3/
[571] AWS IAM access analysis features, https://aws.amazon.com/iam/features/analyze-access/
[572] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021
[573] Blackberry Threat Report, 2020
[574] Booz Allen Hamilton, Securing the Data Supply Chain, May 2021
[575] NIST SP 800-207. Zero Trust Architecture. 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

where authentication and authorisation are explicitly granted, following the motto of ''identity is the new perimeter''.[576] [577] [578]

- Increasing awareness at the level of top management that cybersecurity and physical security must be integrated. Despite increasing physical attacks, corporate leaders are reluctant to believe their companies could be physical threat targets.[579]
- Recovery plans and backups are fundamental to increasing system resilience.
- Physical breaches can facilitate attacks. For instance, vulnerabilities in physical access control, tailgaters, unattended devices can help an adversary in executing an attack.[580] [581]
- Errors and malfunctioning in internal equipment (heating, ventilation, and air-conditioning) can bring on scenarios in which fire, humidity and unstable power supplies can damage IT infrastructures.[582]
- Climate changes are posing a new set of challenges on system availability and resilience. Flooding, fire, and earthquakes are happening at an increasing rate with an exponential power and impact on all infrastructures.[583] Risk assessment, disaster recovery techniques, and personnel training are fundamental.

[576] Booz Allen Hamilton, Rethink Cyber Defense After the SolarWinds Hack, June 2021
[577] Gartner, Top security and risk management trends 2021, 2021
[578] Blackberry 2021 Threat Report, 2021
[579] The Ontic Center for Protective Intelligence, 2021 Mid-Year Outlook State of Protective Intelligence Report - The Escalating Physical Threat Landscape: A Clarion Call for Corporate Protective Intelligence https://www.prnewswire.com/news-releases/intelligence-failures-regularly-occur-at-large-us-companies-resulting-in-physical-threats-or-harm-and-business-continuity-disruption-study-finds-301334484.html, https://ontic.co/wp-content/uploads/2021/07/2021-Mid-Year-Outlook-State-of-Protective-Intelligence-Report.pdf
[580] https://www.boonedam.com/en-us/pillar-page/making-physical-security-part-of-cybersecurity-best-practices
[581] Andi Hendrickson, Top 5 Physical Security Considerations, July 2021, https://securityboulevard.com/2021/07/top-5-physical-security-considerations/
[582] Karoline Gore, Physical threats to Cybersecurity that you must address, October 2019, https://cybersecurity.att.com/blogs/security-essentials/physical-threats-to-cybersecurity-that-you-must-address
[583] Warren Cornwall, Europe's deadly floods leave scientists stunned, July 2021, https://www.sciencemag.org/news/2021/07/europe-s-deadly-floods-leave-scientists-stunned

A ANNEX: MITRE ATT&CK

RANSOMWARE

The figure illustrated below highlights the techniques in MITRE ATT&CK® Framework associated with ransomware software, ransomware groups or both according to the legend.[584] Notice that this is a dynamic representation, based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its specific tools and attack patterns. This overview groups all common techniques.

TA0001: Initial Access	T1189: Drive-by Compromise
TA0002: Execution	T1203: Exploitation for Client Execution T1106: Native API T1047: Windows Management Instrumentation
TA0003: Persistence	T1197: BITS Jobs T1554: Compromise Client Software Binary T1205: Traffic Signaling
TA0004: Privilege Escalation	T1134: Access Token Manipulation T1055: Process Injection
TA0005: Defense Evasion	T1134: Access Token Manipulation T1197: BITS Jobs T1140: Deobfuscate/Decode Files or Information T1480: Execution Guardrails T1070: Indicator Removal on Host T1036: Masquerading T1112: Modify Registry T1027: Obfuscated Files or Information T1055: Process Injection T1205: Traffic Signaling T1497: Virtualization/Sandbox Evasion
TA0006: Credential Access	T1110: Brute Force
TA0007: Discovery	T1482: Domain Trust Discovery T1083: File and Directory Discovery T1046: Network Service Scanning T1135: Network Share Discovery T1120: Peripheral Device Discovery T1057: Process Discovery T1012: Query Registry T1018: Remote System Discovery T1518: Software Discovery T1082: System Information Discovery T1614: System Location Discovery T1016: System Network Configuration Discovery T1049: System Network Connections Discovery T1033: System Owner/User Discovery T1007: System Service Discovery T1124: System Time Discovery T1497: Virtualization/Sandbox Evasion

[584] Ransomware techniques in ATT&CK, https://healthcyber.mitre.org/blog/resources/attack-navigator/

TA0008: Lateral Movement	T1210: Exploitation of Remote Services T1570: Lateral Tool Transfer T1080: Taint Shared Content
TA0009: Collection	T1005: Data from Local System T1039: Data from Network Shared Drive
TA0011: Command and Control	T1568: Dynamic Resolution T1008: Fallback Channels T1105: Ingress Tool Transfer T1104: Multi-Stage Channels T1095: Non-Application Layer Protocol T1219: Remote Access Software T1205: Traffic Signaling T1102: Web Service
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel
TA0040: Impact	T1531: Account Access Removal T1485: Data Destruction T1486: Data Encrypted for Impact T1490: Inhibit System Recovery T1489: Service Stop T1529: System Shutdown/Reboot

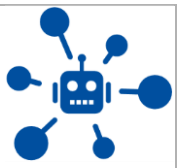
MALWARE

The term malware, or malicious software, covers a range of technology, tools, and tactics. Software is the interaction layer with information technology. This report focuses on malware in general, which we cannot unambiguously map to the ATT&CK Framework. Instead, malware is defined as a single building block of Capability Development. MITRE ATT&CK® describes malware as a means to support the threat actor's operations, obtaining a means for maintaining control of remote machines, evading defences, and executing post-compromise behaviours.[585] For illustration purposes, we describe the mapping to the MITRE ATT&CK® Framework concerning one notable malware, namely Emotet, which may be seen to be using a variety of different techniques in different stages.

Techniques used by EMOTET			
T1087	0.003	Account Discovery: Email Account	Emotet has been observed leveraging a module that can scrape email addresses from Outlook.[3][4]
T1560		Archive Collected Data	Emotet has been observed encrypting the data it collects before sending it to the C2 server. [5]
T1547	0.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Emotet has been observed adding the downloaded payload to the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run key to maintain persistence.[6][7][8]
T1110	0.001	Brute Force: Password Guessing	Emotet has been observed using a hard coded list of passwords to brute force user accounts. [9][6][7][10][3]
T1059	0.001	Command and Scripting Interpreter: PowerShell	Emotet has used Powershell to retrieve the malicious payload and download additional resources like Mimikatz. [6][2][8][11][12]
	0.003	Command and Scripting Interpreter: Windows Command Shell	Emotet has used cmd.exe to run a PowerShell script. [8]
	0.005	Command and Scripting Interpreter: Visual Basic	Emotet has sent Microsoft Word documents with embedded macros that will invoke scripts to download additional payloads. [6][13][2][8][12]
T1543	0.003	Create or Modify System Process: Windows Service	Emotet has been observed creating new services to maintain persistence. [7][10]

[585] Obtain Capabilities: Malware, https://attack.mitre.org/techniques/T1588/001/

T1555	0.003	Credentials from Password Stores: Credentials from Web Browsers	Emotet has been observed dropping browser password grabber modules. [2][4]
T1114	0.001	Email Collection: Local Email Collection	Emotet has been observed leveraging a module that scrapes email data from Outlook.[3]
T1573	0.002	Encrypted Channel: Asymmetric Cryptography	Emotet is known to use RSA keys for encrypting C2 traffic. [2]
T1041		Exfiltration Over C2 Channel	Emotet has been seen exfiltrating system information stored within cookies sent within an HTTP GET request back to its C2 servers. [2]
T1210		Exploitation of Remote Services	Emotet has been seen exploiting SMB via a vulnerability exploit like EternalBlue (MS17-010) to achieve lateral movement and propagation. [6][7][10][11]
T1040		Network Sniffing	Emotet has been observed to hook network APIs to monitor network traffic. [1]
T1571		Non-Standard Port	Emotet has used HTTP over ports such as 20, 22, 7080, and 50000, in addition to using ports commonly associated with HTTP/S.[13]
T1027		Obfuscated Files or Information	Emotet has obfuscated macros within malicious documents to hide the URLs hosting the malware, CMD.exe arguments, and PowerShell scripts. [13][2][8][14]
	0.002	Software Packing	Emotet has used custom packers to protect its payloads.[2]
T1003	0.001	OS Credential Dumping: LSASS Memory	Emotet has been observed dropping password grabber modules including Mimikatz. [2]
T1566	0.001	Phishing: Spearphishing Attachment	Emotet has been delivered by phishing emails containing attachments. [15][9][6][7][13][2][8][12][4]
	0.002	Phishing: Spearphishing Link	Emotet has been delivered by phishing emails containing links. [1][16][15][9][6][7][13][13][8]
T1057		Process Discovery	Emotet has been observed enumerating local processes.[17]
T1055	0.001	Process Injection: Dynamic-link Library Injection	Emotet has been observed injecting in to Explorer.exe and other processes. [8][1][7]
T1021	0.002	Remote Services: SMB/Windows Admin Shares	Emotet leverages the Admin$ share for lateral movement once the local admin password has been brute forced. [9]
T1053	0.005	Scheduled Task/Job: Scheduled Task	Emotet has maintained persistence through a scheduled task. [7]
T1552	0.001	Unsecured Credentials: Credentials In Files	Emotet has been observed leveraging a module that retrieves passwords stored on a system for the current logged-on user. [7][3]
T1204	0.001	User Execution: Malicious Link	Emotet has relied upon users clicking on a malicious link delivered through spearphishing.[1][12]
	0.002	User Execution: Malicious File	Emotet has relied upon users clicking on a malicious attachment delivered through spearphishing.[1][12][4]
T1078	0.003	Valid Accounts: Local Accounts	Emotet can brute force a local admin password, then use it to facilitate lateral movement.[9]
T1047		Windows Management Instrumentation	Emotet has used WMI to execute powershell.exe.[12]

BOTNET	
TA0043: Reconnaissance	T1595: Active Scanning T1595.001: Scanning IP Blocks
TA0042: Resource Development	T1583: Acquire Infrastructure T1583.005: Botnet T1584: Compromise Infrastructure T1584.005: Botnet
TA0003: Persistence	T1176: Browser Extensions
TA0011: Command and Control	T1071: Application Layer Protocol T1092: Communication Through Removable Media T1132: Data Encoding T1001: Data Obfuscation T1568: Dynamic Resolution T1573: Encrypted Channel T1008: Fallback Channels T1105: Ingress Tool Transfer T1104: Multi-Stage Channels T1095: Non-Application Layer Protocol T1571: Non-Standard Port T1572: Protocol Tunneling T1090: Proxy T1219: Remote Access Software T1205: Traffic Signaling T1102: Web Service
TA0010: Exfiltration	T1020: Automated Exfiltration T1030: Data Transfer Size Limits T1048: Exfiltration Over Alternative Protocol T1041: Exfiltration Over C2 Channel T1011: Exfiltration Over Other Network Medium T1052: Exfiltration Over Physical Medium T1567: Exfiltration Over Web Service T1029: Scheduled Transfer T1537: Transfer Data to Cloud Account
TA0040: Impact	T1531: Account Access Removal T1485: Data Destruction T1486: Data Encrypted for Impact T1565: Data Manipulation T1491: Defacement T1561: Disk Wipe T1499: Endpoint Denial of Service T1495: Firmware Corruption T1490: Inhibit System Recovery T1498: Network Denial of Service T1498.001: Direct Network Flood T1498.002: Reflection Amplification T1496: Resource Hijacking T1489: Service Stop T1529: System Shutdown/Reboot

CRYPTOJACKING

The anatomy of cryptojacking related attacks is depicted in the following figure, which includes the techniques that may be used in each kill chain phase. The MITRE ATT&CK® Navigator view below highlights the common techniques associated with cryptojacking software and provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions.

TA0043: Reconnaissance	T1595: Active Scanning T1595.001: Scanning IP Blocks
TA0042: Resource Development	T1583: Acquire Infrastructure T1583.005: Botnet T1584: Compromise Infrastructure T1584.005: Botnet T1608: Stage Capabilities
TA0003: Persistence	T1176: Browser Extensions
TA0005: Defense Evasion	T1535: Unused/Unsupported Cloud Regions T1600: Weaken Encryption
TA0006: Credential Access	T1606: Forge Web Credentials T1056: Input Capture T1539: Steal Web Session Cookie
TA0040: Impact	T1499: Endpoint Denial of Service T1498: Network Denial of Service T1498.001: Direct Network Flood T1498.002: Reflection Amplification T1496: Resource Hijacking

E-MAIL RELATED THREATS

The anatomy of e-mail related attacks is depicted in the following table, which includes the techniques that may be used in each kill chain phase and lead to a phishing, spear-phishing, smishing, BEC or spam attack. The MITRE ATT&CK® provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques leading to e-mail attacks are selected using the MITRE ATT&CK® for the Enterprise and Mobile domains which cover the behaviour against access to enterprise IT networks, cloud, and mobile devices, while focuses on the behaviour against network-based access on the Mobile domain.

PHISHING

TA0043: Reconnaissance	T1595: Active Scanning T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/Domains T1594: Search Victim-Owned Websites

TA0042: Resource Development	T1583: Acquire Infrastructure T1586: Compromise Accounts T1584: Compromise Infrastructure T1585: Establish Accounts T1608: Stage Capabilities
TA0001: Initial Access	T1566: Phishing
TA0002: Execution	T1203: Exploitation for Client Execution T1204: User Execution
TA0003: Persistence	T1176: Browser Extensions
TA0005: Defense Evasion	T1221: Template Injection T1535: Unused/Unsupported Cloud Regions T1600: Weaken Encryption T1220: XSL Script Processing
TA0006: Credential Access	T1187: Forced Authentication T1606: Forge Web Credentials T1528: Steal Application Access Token T1539: Steal Web Session Cookie
TA0008: Lateral Movement	T1534: Internal Spearphishing
TA0040: Impact	T1499: Endpoint Denial of Service T1498: Network Denial of Service T1496: Resource Hijacking

BEC

TA0001: Initial Access	T1078: Valid Accounts
TA0002: Execution	T1609: Container Administration Command T1203: Exploitation for Client Execution
TA0003: Persistence	T1205: Traffic Signaling T1078: Valid Accounts
TA0004: Privilege Escalation	T1078: Valid Accounts
TA0005: Defense Evasion	T1553: Subvert Trust Controls T1205: Traffic Signaling T1550: Use Alternate Authentication Material T1078: Valid Accounts
TA0007: Discovery	T1033: System Owner/User Discovery
TA0008: Lateral Movement	T1563: Remote Service Session Hijacking T1550: Use Alternate Authentication Material
TA0011: Command and Control	T1095: Non-Application Layer Protocol T1205: Traffic Signaling
TA0010: Exfiltration	T1011: Exfiltration Over Other Network Medium
TA0040: Impact	T1485: Data Destruction T1499: Endpoint Denial of Service T1496: Resource Hijacking

THREATS AGAINST DATA

The anatomy of data exfiltration is depicted in the following table, which includes the techniques that may be used in each kill chain phase and lead to data exfiltration or data breach or identity theft. The construction of the table is based on the MITRE ATT&CK®[586] knowledge base. MITRE ATT&CK® provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques leading to data exfiltration were selected using the MITRE ATT&CK® part for Enterprise, which covers behaviours against enterprise IT networks and the cloud

DATA EXFILTRATION

TA0003: Persistence	T1197: BITS Jobs
TA0005: Defense Evasion	T1197: BITS Jobs T1599: Network Boundary Bridging
TA0009: Collection	T1560: Archive Collected Data T1005: Data from Local System T1039: Data from Network Shared Drive T1025: Data from Removable Media T1074: Data Staged
TA0010: Exfiltration	T1020: Automated Exfiltration T1048: Exfiltration Over Alternative Protocol T1041: Exfiltration Over C2 Channel T1011: Exfiltration Over Other Network Medium T1052: Exfiltration Over Physical Medium T1567: Exfiltration Over Web Service T1029: Scheduled Transfer T1537: Transfer Data to Cloud Account

THREATS AGAINST AVAILABILITY AND INTEGRITY

The anatomy of Denial of Services attacks and web attacks are depicted in the following figures, which includes the techniques that may be used in each kill chain phase. The table is constructed based on the MITRE ATT&CK®[587] knowledge base. MITRE ATT&CK® provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques are selected using the MITRE ATT&CK® part for Enterprise, which covers behaviours against enterprise IT networks and the cloud.

DOS

TA0042: Resource Development	T1583: Acquire Infrastructure T1583.005: Botnet T1584: Compromise Infrastructure T1584.005: Botnet
TA0005: Defense Evasion	T1553: Subvert Trust Controls T1553.003: SIP and Trust Provider Hijacking
TA0040: Impact	T1499: Endpoint Denial of Service T1499.003: Application Exhaustion Flood T1499.004: Application or System Exploitation T1499.001: OS Exhaustion Flood T1499.002: Service Exhaustion Flood T1498: Network Denial of Service T1498.001: Direct Network Flood T1498.002: Reflection Amplification

[586] MITRE ATT&CK®, https://attack.mitre.org/
[587] MITRE ATT&CK®, https://attack.mitre.org/

WEB BASED ATTACK

TA0001: Initial Access	T1189: Drive-by Compromise T1133: External Remote Services
TA0002: Execution	T1610: Deploy Container
TA0003: Persistence	T1133: External Remote Services
TA0005: Defense Evasion	T1610: Deploy Container T1550: Use Alternate Authentication Material T1550.004: Web Session Cookie
TA0006: Credential Access	T1606: Forge Web Credentials T1606.001: Web Cookies T1539: Steal Web Session Cookie
TA0007: Discovery	T1613: Container and Resource Discovery
TA0008: Lateral Movement	T1550: Use Alternate Authentication Material T1550.004: Web Session Cookie
TA0040: Impact	T1499: Endpoint Denial of Service T1499.003: Application Exhaustion Flood

In 2021, the most widespread attack vector is UDP flooding (41.87%), while SYN flooding dropped to third place (26.36%), after TCP flooding (29.23%)[588]. GRE (1.43%) and HTTP flooding (1.10%) showed modest growth. Linux botnets continued to account for almost all DDoS traffic (99.90%).

Web application security is a prime threat vector for both large and small organisations[589,590,591]. F5 Labs classified DDoS attacks into three categories: volumetric, application, protocol, and analysed their frequency. 73% of all incidents was due to volumetric attacks; 53% of the attacks built on reflection attacks.[590] For example, application DDoS includes HTTP, HTTPS, and DNS requests to a server. Volumetric DDoS includes standard UDP flooding, along with reflection attacks, including NTP and DNS.

DISINFORMATION - MISINFORMATION

It is important to note that disinformation and misinformation attacks are among the preparatory activities at the basis of other attacks (e.g. phishing, social engineering, malware infection). The MITRE ATT&CK® graph below can give an idea of the link between disinformation/misinformation and connected attacks

TA0043: Reconnaissance	T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/Domains T1594: Search Victim-Owned Websites
TA0042: Resource Development	T1586: Compromise Accounts T1585: Establish Accounts

[588] Alexander Gutnikov, Oleg Kupreev, Ekaterina Badovskaya, DDoS attacks in Q1 2021, May 2021, https://securelist.com/ddos-attacks-in-q1-2021/102166/
[589] Verizon, Cross-site scripting (XSS) attacks in Q4 2020: Trends and best practices, March 2021, https://www.verizondigitalmedia.com/blog/cross-site-scripting-attacks-trends-and-best-practices/
[590] David Warburton, F5 Labs, DDoS Attack Trends for 2020, May 2021, https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020
[591] Verizon, Data Breach Investigations Report (DBIR) 2021, 2021

TA0001: Initial Access	T1566: Phishing
TA0002: Execution	T1203: Exploitation for Client Execution T1204: User Execution
TA0040: Impact	T1565: Data Manipulation T1491: Defacement

B ANNEX: MAJOR INCIDENTS

In what follows, we present a non-exhaustive list of relevant incidents, alongside their geographic spread/proximity and the associated timeline. It is important to note that by analysing the incidents presented as well as the full list of incidents related to threats mentioned in the ETL, ENISA determined the trends described in the previous sections.

The incidents that constitute each list were selected based on the following criteria: (a) the geographical spread of the attack, (b) the impact of the incident, (c) an innovative technique used for the attack, and (d) the existence of an unprecedented element (e.g. first incident in which a patient died because of a ransomware attack).

RANSOMWARE

Table 4: Notable ransomware incidents

Time	Geographical Spread	Description
July 2021	NEAR	Spain's 4th largest telecom operator, MasMovil, became aware of an attack by the REvil ransomware operator. This attack is believed to have occurred sometime around the end of June 2021. In the beginning of July 2021, screenshots started appearing on REvil's blog on the Tor network of what appears to be stolen data.
June 2021	NEAR	City of Liege incident: the attack that occurred in June of 2021 affected the city's civil status and population services, including the ordering and collection of identification documents, driving licenses and the ability to make appointments for marriage registrations. Early information points to the Ryuk ransomware.
June 2021	FAR	Fujifilm incident: the company's infrastructure was brought down due to a security incident identified in early June 2021.[592] Although investigations are currently underway, early findings indicate that ransomware was installed using a 13-year-old trojan called Qbot, currently controlled by the REvil crime group[593].
May 2021	FAR	In the beginning of May 2021, a major US Pipeline operator fell victim of a double extortion attack based on the DarkSide ransomware. The colonial pipeline provides about 45% of the fuel delivered to the US east coast. The attack led to the shutdown of its pipelines, resulting in the disruption of its refineries, and ultimately leading to fuel shortages. The company reportedly paid $4.4M in ransom fees.[594] It was later discovered that the attackers stole 100GB worth of data, used as part of a double-extortion scheme.[595]
April 2021	NEAR	The Conti crime gang is believed to be behind the breach on the HSE systems, which occurred in the end of April 2021. They claim to have stolen 700GB worth of personal data, before encrypting computers and restricting access to diagnostics and medical records.

[592] Unauthorised access to Fujifilm servers, https://www.fujifilm.com/uk/en/news/hq/6642
[593] Fujifilm becomes the latest victim of a network-crippling ransomware attack, https://techcrunch.com/2021/06/03/fujifilm-becomes-the-latest-victim-of-a-network-crippling-ransomware-attack/
[594] Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom, https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636
[595] Colonial Hackers Stole Data Thursday Ahead of Shutdown, https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

November 2020	FAR	Foxconn incident: attackers demanded $34 million in ransom from the electronics giant Foxconn in November 2020. The attackers claimed to have encrypted 1200 servers, destroyed at least 20TB of backups and acquired 100GB of data. A month later, parts of the data was released on the DoppelPaymer's leak site.[596]
September 2020	FAR	Universal health services (UHS) incident: the attack took place in September 2020. UHS was forced to shut down its IT infrastructure affecting 250 healthcare facilities across the US costing them $67 million.[597] The Ryuk ransomware was detected on some systems, suggesting that the attack most likely started with phishing, leading to the delivery of the Emotet and Trickbot trojans, which were later used by the Ryuk threat actors to install the ransomware payload.
September 2020	NEAR	Patient dies after ransomware attack on Düsseldorf University Hospital. The hospital's IT systems gradually started to be paralysed on the 10th of September 2020 because of ransomware. In response, the hospital announced that it could no longer receive patients in need of emergency care[598]. Regrettably, a patient died while being transferred to another hospital 30km away. Initial information suggests that the DoppelPaymer ransomware was used, and that the attackers' entry point was an unpatched Citrix VPN product
June 2020	FAR	In June 2020, it became known that the HONDA car manufacturer suffered a cyber-attack that affected its sale activities, as well as its production systems. A later study identified the Snake ransomware family as the probable cause of the cyber-attack and RDP as a possible attack vector.
April 2020	NEAR	Portuguese energy company (EDP) threatened with data public release. Hacking group Ragnarok demanded $10.9 million from EDP following a double-extortion attack in April of 2020. The group also threatened to release 10TB of information containing private client and financial information

[596] DoppelPaymer Ransomware Attack Disrupts Foxconn's Operations in the Americas, Hackers Delete Terabytes of Data, Demand $34 Million, https://www.cpomagazine.com/cyber-security/doppelpaymer-ransomware-attack-disrupts-foxconns-operations-in-the-americas-hackers-delete-terabytes-of-data-demand-34-million/
[597] Cyberattacks Cost Hospitals Millions During COVID-19, https://www.wsj.com/articles/cyberattacks-cost-hospitals-millions-during-COVID-19-11614346713
[598] Update 16 Uhr - Uniklinik Düsseldorf: Massiver Netzwerkausfall, https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-16-uhr-uniklinik-duesseldorf-massiver-netzwerkausfall

MALWARE

Table 5. Notable malware incidents

Time	Geographical Spread	Description
March 2021	GLOBAL	Hafnium targeted Microsoft Exchange servers. In March 2021, multiple zero day exploits were used to attack on-premise Microsoft Exchange Servers, through which attackers gained access to the servers. From there, attackers were able to access e-mail accounts, and install additional malware.[599]
March 2021	GLOBAL	Password manager Passwordstate hacked to deploy malware on customer systems. A threat actor compromised the update mechanism of enterprise password manager application Passwordstate and deployed malware on its users' devices. At least 29,000 companies were reportedly affected.[600]
January 2021	GLOBAL	In January 2021 EMOTET was taken down by law enforcement and judicial authorities worldwide. The worldwide coalition of law enforcement agencies involved the US, Canada, the UK, the Netherlands, Germany, France, Lithuania, and Ukraine, and Europol.[601]
December 2020	GLOBAL	In December 2020, a supply chain attack targeted large organisations. Attackers leveraged SUNBURST to breach SolarWinds, a tool used for asset inventory. Through this breach, they were able to compromise public and private companies worldwide, including more than 40 United States government agencies.[602]
July & August 2020	GLOBAL	KISMET zero-click zero-day. Pegasus spyware from NSO was used to breach 36 personal cell phones belonging to journalists, producers, anchors, and executives at *Al Jazeera*. The attack leveraged an exploit chain called KISMET. NSO is used by state actors to breach the phones of dissident voices.[603]

[599] HAFNIUM targeting Exchange Servers with 0-day exploits, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[600] Password manager Passwordstate hacked to deploy malware on customer systems - The Record by Recorded Future
[601] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
[602] Highly evasive attacker leverages Solarwinds supply chain to compromise multiple global victims with SUNBURST backdoor, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[603] Highly evasive attacker leverages Solarwinds supply chain to compromise multiple global victims with SUNBURST backdoor, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

CRYPTOJACKING

Table 6: Notable cryptojacking incidents

Time	Geographical Spread	Description
April 2021	GLOBAL	Prometei cryptocurrency mining botnet took advantage of Microsoft Exchange vulnerabilities. Threat actors behind the botnet were exploiting the four zero-day vulnerabilities in the Microsoft Exchange e-mail server, collectively referred to as the ProxyLogon vulnerabilities, that were first exploited by Hafnium in order to mine cryptocurrencies (Monero).[604]
March 2021	NEAR, GLOBAL	Attacks targeted QNAP network-attached storage (NAS) devices to abuse them in cryptocurrency mining.[605]
August 2020	FAR	Vietnamese state-backed hackers deployed cryptocurrency mining malware to monetise the networks of victim organisations on whom they are also spying on. From July to August 2020 the APT32 Group (aka Ocean Lotus, BISMUTH) deployed Monero coin miners in attacks targeting private and public sector organisations in France and Vietnam. Doing so could have been part of a plan to generate extra revenue alongside such attacks, or an attempt to stay hidden.[606]
August 2020	GLOBAL	Hildegard' Malware Targeted Kubernetes Systems. During the summer of 2020, TeamTNT was targeting Docker and Kubernetes systems with a cryptomining worm capable of stealing local credentials, including Amazon Web Services (AWS) login details.[607]

[604] Prometei cryptocurrency mining botnet takes advantage of Microsoft Exchange vulnerabilities (cybersecurity-help.cz)
[605] UnityMiner targets unpatched QNAP NAS in cryptocurrency mining campaignSecurity Affairs
[606] Vietnamese State Hackers Deploy Coin Miners to Victims - Infosecurity Magazine (infosecurity-magazine.com)
[607] New 'Hildegard' Malware Targets Kubernetes Systems | SecurityWeek.Com

E-MAIL RELATED THREATS

Table 7: Notable incidents related to threats targeting e-mail

Time	Geographical Spread	Description
May 2021	NEAR, FAR	A spear-phishing campaign was detected on 28 May 2021,[608] targeting non-governmental organisations (NGOs), government organisations and intergovernmental organisations (IGOs). According to the US Federal Bureau of Investigation (FBI) and the US Cybersecurity and Infrastructure Security Agency (CISA), through the use of a compromised account of a software company called "Constant Contact", hackers sent spear-phishing messages to a US government organisation containing links to malicious sites. The threat actor, probably being APT29 (also known as Cozy Bear, Nobelium, and The Dukes), sent spoofed e-mails with a link that redirected to a malicious URL that prompted the victim to download an ISO image with malicious content. CISA and FBI reported that at least 7,000 accounts distributed among 350 NGOs, government organisations and IGOs, received these phishing e-mails.
March 2021	GLOBAL	Office 365 fake sites used in BEC campaign. In March 2021, a BEC campaign took place[609] that targeted senior employees working in financial services, insurance, and retail industries. The attackers used phishing lures that appeared to be Office 365 updates. The lures directed the targets to phishing pages masquerading as the Office 365 login page in order to harvest credentials. Access to these accounts gave the attackers key information that helped them send fraudulent messages requesting bank transfers to accounts held by them [610].
November 2020	GLOBAL	In November 2020, hackers suspected to be nation sponsored used LinkedIn and WhatsApp to approach a broad set of COVID-19 researchers with fake job offers[611] by pretending to be recruiters. Then, they e-mailed documents with fake job descriptions that contained malicious code designed to gain access to the victims' computers. The attacks were not successful. This attack targeted 6 vaccine producing pharmaceutical companies (including AstraZeneca PLC).
October 2020	GLOBAL	Universities across the world were targeted via a spear-phishing campaign. In October 2020, a hacker group named "Silent Librarian" (also referred to as TA407 and Cobalt Dickens), which has a history of attacking academic institutions, launched a new series of phishing campaigns, according to a Malwarebytes report[612]. This hacking group, instead of targeting particular countries, aims to obtain wider coverage by targeting university staff and students by weaponising a great number of phishing sites. It is mentioned that 25 Universities were targeted during the campaign.
October 2020	FAR	North Korean group accused of phishing attack against Russian defence industry[613]. In October 2020, a researcher of the Russian IT security company GROUP-IB revealed that the North Korean hacker group named "Kimsuky" (aka "Velvet Chollima" and "Black Banshee") launched a phishing campaign targeting Russian aerospace and defence companies. Using the pandemic as the main topic, these e-mails contained information about supposed job vacancies.
October 2020	NEAR, FAR	State-sponsored hackers targeted attendees at security conferences. According to Microsoft research published in October 2020,[614] the Charming Kitten group (also known as APT35 or Phosphorus), were sending spear-phishing messages to

[608] https://us-cert.cisa.gov/ncas/alerts/aa21-148a
[609] Office 365 Phishing Attack Targets Financial Execs, https://threatpost.com/office-365-phishing-attack-financial-execs/164925/
[610] Sophisticated Microsoft Spoof Targets Financial Departments, https://www.area1security.com/blog/microsoft-365-spoof-targets-financial-departments/
[611] Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca, https://www.reuters.com/article/uk-healthcare-coronavirus-astrazeneca-no-idUKKBN28719Y
[612] https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
[613] North Korean hackers attack the Russian defence industry, https://www.kommersant.ru/doc/4538451
[614] https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/

		individuals who were possibly attending two significant security conferences: the "Munich Security Conference" held in Germany and the "Think 20 Summit" held in Saudi Arabia. The hackers managed to steal the credentials of many of their victims and, according to Microsoft researchers, the attacks were executed for the purposes of collecting intelligence. At least 100 high-profile possible attendees were targeted during this campaign.
September 2020	GLOBAL	Worldwide phishing attack jeopardised the supply chain of COVID-19 vaccine. In September 2020 organisations associated with the transportation of the COVID-19 vaccine received phishing messages from hackers pretending to be senior executives of a legitimate company involved in the COVID-19 vaccine supply chain.[615]
August 2020	GLOBAL	United Nations under attack. On 28 August 2020, the hacker group named "Kimsuky" launched a phishing campaign against individuals and officials of the United Nations. During this attack, which took place in March and April 2020, victims received spear-phishing messages in their e-mail accounts, either from hackers posing as reporters requesting interviews or containing supposed UN security alerts.[616] The fraudulent e-mails contained links to phishing sites or malicious software. According to this UN report, more than 28 officials were targeted, out of whom six were Security Council members.
March 2020	FAR	Starting in Spring 2020 and continuing for the remainder of that year[617], a hacking group named "Water Nue" leveraged the SendGrid customer communication cloud platform to send phishing messages. In this campaign, senior executives of companies in Canada and the US received phishing messages leading them to expose their passwords to scammers. Scammers then used these user credentials to send messages to employees of these companies, requesting bank transfers to accounts held by them. During this campaign more than 800 accounts were breached.

[615] IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain (securityintelligence.com)
[616] North Korea has tried to hack 11 officials of the UN Security Council, https://www.zdnet.com/article/north-korea-has-tried-to-hack-11-officials-of-the-un-security-council/
[617] Water Nue Phishing Targets Execs' Office 365 Accounts, https://www.trendmicro.com/en_us/research/20/h/water-nue-phishing-targets-execs-office-365-accounts.html

THREATS AGAINST DATA

Table 8: Notable incidents related to threats against data

Time	Geographical Spread	Description
May 2021	FAR	In a data breach that became known in May 2021, data was stolen from the IT systems of Rehoboth McKinley Christian Health Care Services that contained personal data of around 200,000 patients including names, date of birth, social security numbers as well as other contact information.[618]
May 2021	NEAR	In May 2021, Ireland's Health Service Executive (HSE) fell victim to a ransomware attack. It was reported that this was part of the Conti malware and that there were major outages in the IT systems.[619] The adversaries launched a double extortion attack by threatening to disclose data obtained. The HSE has confirmed that 520 patients' data was exposed.[620]
May 2021	FAR	A data breach at Canada Post through a supply chain attack occurred in May 2021. Shipping information of 950,000 parcel recipients was stolen in a data breach that became known in May 2021 and was attributed to a malware attack on one of the Post's key partners. The stolen records contained names, addresses, but only a few e-mail addresses and phone numbers.[621]
February 2021	FAR	4.5 million travel records belonging to passengers of an affected airline dating all the way back to August 2011 were stolen in a cyber-attack that became known in February 2021. The records in question included personal data, such as names, date of birth, contact and passport information, as well as credit card numbers. The attack was carried out through the airliner's data processor partner SITA.[622,623]
December 2020	NEAR	In December 2020, the European Medicines Agency (EMA) was subject to a cyber-attack.[624] An initial review revealed that a limited number of documents belonging to third parties were unlawfully accessed. The companies concerned were informed. The ongoing investigation into the cyberattack on the EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines had been leaked on the internet.[625]
December 2020	FAR	University of California (UC) has had sensitive information leaked, affecting staff and students, after a successful attack in December 2020 against a third-party product (Accellion FTA) used by the university for file transfers. The leaked records are believed to include full names, addresses, social security numbers, financial information and health related information as well as other personal information.[626]
September 2020,	NEAR	Hackers threatened patients with the release of leaked medical data records. In late September 2020, Finnish psychotherapy practice Vastaamo was asked to pay $0,5 million by attackers who had breached their infrastructure in two separate incidents between 2018 and 2019. Towards the end of 2020, the attackers extorted money from patients, by threatening to release records with sensitive and confidential health information.[627]
August 2020	GLOBAL	Maze group released data obtained from LG and Xerox. Two separate breaches are believed to have occurred in August 2020, both attributed to a flaw in the Citrix

[618] Notice of Data Breach, https://response.idx.us/rmchcs/
[619] https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/
[620] https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136
[621] Canada Post informs 44 large business customers of supplier data breach involving shipping information, https://www.newswire.ca/news-releases/canada-post-informs-44-large-business-customers-of-supplier-data-breach-involving-shipping-information-888678957.html
[622] SITA data breach affected 4.5 million flyers, Air India reveals, https://www.teiss.co.uk/air-india-sita-data-breach/
[623] Notification to Passengers, http://www.airindia.in/images/pdf/Data-Breach-Notification.pdf
[624] https://www.ema.europa.eu/en/news/cyberattack-ema-update-1
[625] https://www.ema.europa.eu/en/news/cyberattack-ema-update-5
[626] UC Notice of Data Breach, https://www.businesswire.com/news/home/20210510005214/en/UC-Notice-of-Data-Breach
[627] Vastaamo psychotherapy data breach sees the most vulnerable victims extorted https://blog.malwarebytes.com/cybercrime/2020/10/vastaamo-psychotherapy-data-breach-sees-the-most-vulnerable-victims-extorted/

		Application Delivery Controller (CVE-2019-19781). Large amounts of data with intellectual property were stolen from LG and Xerox. After failed negotiations, the data was leaked on the dark web.[628]
May 2020	MID	In May 2020, it became known that booking data of 9 million customers of an airline company was stolen, including credit/debit card info with CVV numbers belonging to 2,208 customers. The data was personal, such as names and e-mail addresses, as well as related flight information.[629,630]

[628] Ransomware gang publishes tens of GBs of internal data from LG and Xerox, https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/
[629] Chinese Hackers Attacked EasyJet, https://www.cybersecurityintelligence.com/blog/chinese-hackers-attacked-easyjet-5009.html
[630] EasyJet admits data of nine million hacked, https://www.bbc.com/news/technology-52722626

THREATS AGAINST AVAILABILITY AND INTEGRITY

Table 9: Notable Denial of Service incidents

Time	Geographical Spread	Description
February 2021	NEAR	The largest known ransom DDoS attack peaked at 800Gbps; it targeted a gambling company in Europe.[631]
October 2020	GLOBAL	The operators of SunCrypt ransomware used a DDoS attack to force a victim to pay a ransom.[632]
February 2020	GLOBAL	Largest ever DDoS cyber-attack targeting Amazon fired 2.3Tbps.[633] [634]
Attacks on Docker APIs[635]		
December 2020	GLOBAL	DDoS Capable IRC Bot. TeamTNT added propagation functionalities and the ability to steal Amazon Web Services (AWS) Secure Shell (SSH) credentials.[636]
October 2020	GLOBAL	An attack on Docker APIs has been reported based on Metasploit Framework.**Error! Bookmark not defined.**
May 2020	GLOBAL	Coinminer, a malicious cryptocurrency miner and Distributed Denial of Service (DDoS) actor, targeted open Docker daemon ports.[637]
Reflection/Amplification Attacks[638]		
January-February 2021	GLOBAL	Powerhouse VPN servers, Plex Media Server and Microsoft Remote Desktop Protocol (RDP) used for Reflection/Amplification of DDoS attacks. [640]
Q4 2020	GLOBAL	Citrix ADC (application delivery controller) devices exploited as an amplifier tool, by abusing their DTLS interface. [643]
August 2020	NEAR	A wave of DDoS attacks targeted several European ISPs in France, Belgium and the Netherlands. The attacks were based on DNS amplification and LDAP.[639]

[631] Tom Emmons. 2021: Volumetric DDoS Attacks Rising Fast, March 2021, https://blogs.akamai.com/2021/03/2021-volumetric-ddos-attacks-rising-fast.html
[632] CrowdStrike, 2021 Global Threat Report, 2021
[633] Amazon, AWS Shield Threat Landscape Report – Q1 2020, 2020, https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf
[634] BBC, Amazon thwarts largest ever DDoS cyber-attack. June 2020, https://www.bbc.com/news/technology-53093611
[635] Another particular case of DoS incidents includes attacks on Docker APIs, a category of attacks that appeared prominently during the reporting period. Attacks on Docker APIs give cybercriminals access to the host with root privileges, leading to distributed denial of service (DDoS) attacks, remote code execution (RCE), and unauthorised cryptocurrency mining activity. These attacks require some form of misconfiguration or security gap in the infected system. In particular, the group needed to perform remote code execution on the system by taking advantage of instances of misconfiguration, weak or stolen credentials, or other vulnerabilities.
Alfredo Oliveira, David Fiser, Metasploit Shellcodes Attack Exposed Docker APIs, October 2020, https://www.trendmicro.com/en_hk/research/20/j/metasploit-shellcodes-attack-exposed-docker-apis.html
Trend Micro, A constant State of Flux – Trendmicro, 2020
[636] David Fiser, TeamTNT Now Deploying DDoS-Capable IRC Bot TNTbotinger, December 2020, https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html
[637] Trend Micro, Coinminer, DDoS Bot Attack Docker Daemon Ports, May 2020, https://www.trendmicro.com/vinfo/us/security/news/virtualisation-and-cloud/coinminer-ddos-bot-attack-docker-daemon-ports
[638] Reflection/amplification incidents are listed under DoS events as a special case. A reflection/amplification attack builds on reflection (i.e. an attacker spoofs an IP address to send at attack as a request for information) and amplification (i.e. an attacker exploits protocols to generate a huge amount of traffic). It allows attackers to enlarge the amount of malicious traffic and at the same time obscure the attack source.
NETSCOUT, What is a Reflection Amplification Attack?, https://www.netscout.com/what-is-ddos/what-is-reflection-amplification-attack
[639] Catalin Cimpanu, European ISPs report mysterious wave of DDoS attacks, August 2020, https://www.zdnet.com/article/european-isps-report-mysterious-wave-of-ddos-attacks/

Attacks on remote teaching and learning		
March 2021	NEAR	DDoS attack targeted CSG Comenius Mariënburg, a school in Leeuwarden, Netherlands. [640]
February 2021	FAR	DDoS attack targeted a US schools in Winthrop, Massachusetts, and Manchester Township, New Jersey.[641]
December 2020	FAR	Canada's Laurentian University reported a DDoS attack.[642]
October 2020	FAR	DDoS attack targeted schools in Sandwich and Tyngsboro, Massachusetts, causing network outages. [640]
Attacks on entertainment and gaming domain		
March 2021	GLOBAL	LittleBigPlanet servers were taken down for several days. [640]
February 2021	MID	A DDoS attack targeted Icelandic provider Siminn, disabling the television service. [640]
January 2021	GLOBAL	A DDoS attack was reported against Blizzard, causing players to experience delays in online gaming services. [640]
January 2021	GLOBAL	Cybercriminals attacked League of Legends causing login issues and intermittent connection failures. [640]
December 2020	GLOBAL	Gaming platforms targeted by DDoS attacks exploiting Citrix devices as attack vector. According to ZDNet, Xbox and Steam were the targets of amplification attacks through Citrix devices. [643]
Attacks on internet and telecommunication providers		
May 2021	NEAR	Nova Broadband, an Irish Internet service provider hit by a DDoS attack causing network downtime.[644]
March 2021	GLOBAL	Mirai variant used to hack routers and switches.[645]
February-March 2021	NEAR	DDoS attacks targeted Austrian provider A1 Telekom and Belgian telecommunications firm Scarlet. [640]
January 2021	NEAR	Maltese Internet service provider Melita hit by a DDoS attack disrupting some services, with the aim of extorting money.[646] [588]
September 2020	NEAR	Hungarian banks and telecom services hit by DDoS attacks coming from Russia, China and Vietnam.[647]
First half of 2020	GLOBAL	Dark Nexus, an IoT botnet exploited an authentication-bypass vulnerability in ASUS and D-Link routers to assemble dangerously large botnets. Mozi, a peer-to-peer botnet, is another botnet built from exploited routers and DVRs including D-Link devices with the command execution flaw.[648]

[640] Alexander Gutnikov, Oleg Kupreev, Ekaterina Badovskaya, DDoS attacks in Q1 2021, May 2021, https://securelist.com/ddos-attacks-in-q1-2021/102166/
[641] Securelist by Kaspersky, DDoS attacks in Q1 2021 Report, https://securelist.com/ddos-attacks-in-q1-2021/102166/
[642] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, DDoS attacks in Q4 2020, February 2021, https://securelist.com/ddos-attacks-in-q4-2020/100650/
[643] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, DDoS attacks in Q4 2020, February 2021, https://securelist.com/ddos-attacks-in-q4-2020/100650/
[644] Steve Neville, Cork-based broadband provider hit by cyberattack, May 2021, https://www.irishexaminer.com/news/munster/arid-40292231.html
[645] Sean Lyngaas, CyberScoop, Another Mirai variant used in attempted hacks on routers, switches, https://www.cyberscoop.com/mirai-unit-42-research-botnet/
[646] Internet slows for Melita customers as company faces cyberattack, January 2021, https://timesofmalta.com/articles/view/internet-slows-for-melita-customers-as-company-combats-cyber-attack.844715
[647] Reuters, Hungarian banks, telecoms services briefly hit by cyber-attack: Magyar Telekom, September 2020, https://www.reuters.com/article/us-hungary-cyber-idUSKBN26H0CB
648 FortiGuard Labs, FORTINET, Global Threat Landscape Report 2020, August 2020, https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-h1-2020.pdf

Table 10: Notable Web attacks

Time	Geographical Spread	Description
May 2021	FAR	Attacks based on cross-site scripting (XSS) targeted e-commerce site in Japan. The attack was executed using orders stuffed with JavaScript.[649]
December 2020	GLOBAL	A DDoS attack targeted Bitcoin.org, which hosts Bitcoin Core, a major software versions of bitcoin. [650]
September 2020	NEAR	A DDoS attack targeted the web site and DNS providers of Tutanova, a popular German encrypted mail service.[651]
August 2020	FAR	According to Freepik, hackers stole e-mails and password hashes for 8.3M Freepik and Flaticon users using an SQL injection attack against the company's Flaticon website.[652]
June 2020	FAR	George Floyd death: Anti-racism sites hit by wave of cyber-attacks. Many sites went offline and became unavailable to interested people.[653]
Web attacks on Government, Finance and Health domains		
May 2021	NEAR	A DDoS attack targeted more than 200 organisations across Belgium including the government and parliament, taking part of the country's internet offline.[654]
Early 2021	MID	DDoS attacks targeted government agencies in Russia and Ukraine, including the websites of the Russian Federal Penitentiary Service and the National Guard, the Kiev City State Administration, the Security Service of Ukraine, the National Security and Defence Council, as well as other Ukrainian security and defence institutions. [640]
September 2020	FAR	One of the largest medical cyberattacks in the history of the United States took place, hitting a major hospital system and causing denial of service.[655]
September 2020	NEAR	A denial of service event in a German hospital due to a ransomware attack may have caused a death.[656]
August 2020	FAR	The New Zealand stock exchange was the target of a global campaign of DDoS extortion attacks managed by Lazarus Bear Armada.[657]
2020	NEAR	Greece's four main banks replaced approximately 15,000 customer credit or debit cards, after an incident involving a Greek travel website.[658]

[649] John Leyden, XSS in the wild: JavaScript-stuffed orders used to compromise Japanese e-commerce sites, May 2021, https://portswigger.net/daily-swig/xss-in-the-wild-javascript-stuffed-orders-used-to-compromise-japanese-e-commerce-sites
[650] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov, DDoS attacks in Q4 2020, February 2021, https://securelist.com/ddos-attacks-in-q4-2020/100650/
[651] Pierluigi Paganini, German encrypted e-mail service Tutanota suffers DDoS attacks, September 2020, https://securityaffairs.co/wordpress/108502/hacking/tutanota-suffers-ddos-attacks.html
[652] Sergiu Gatlan, Freepik data breach: Hackers stole 8.3M records via SQL injection, August 2020, https://www.bleepingcomputer.com/news/security/freepik-data-breach-hackers-stole-83m-records-via-sql-injection/
[653] BBC, George Floyd death: Anti-racism sites hit by wave of cyber-attacks, June 2020, https://www.bbc.com/news/technology-52912881
[654] Danny Palmer, This massive DDoS attack took large sections of a country's internet offline, May 2021, https://www.zdnet.com/article/this-massive-ddos-attack-took-large-sections-of-a-countrys-internet-offline/
[655] Kevin Collier, Major hospital system hit with cyberattack, potentially largest in US history, September 2020, https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254
[656] Robert Hackett, Ransomware attack on a hospital may be first ever to cause a death, September 2020, https://fortune.com/2020/09/18/ransomware-police-investigating-hospital-cyber-attack-death/
[657] NETSCOUT, NETSCOUT THREAT INTELLIGENCE REPORT, DDoS in a Time of Pandemic, 2020, https://www.netscout.com/threatreport
[658] Frank Downs, ISACA, Top Cyberattacks of 2020 and How to Build Cyberresiliency, November 2020, https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency

MINSINFORMATION AND DISINFORMATION

Table 11: Notable misinformation and disinformation incidents observed by ENISA (April 2020-July 2021)

Time	Geographical Spread	Description
July 2021	GLOBAL	It is reported that Pegasus spyware has been used against thousands of dissidents, journalists and politicians, including French President Emmanuel Macron.[659] [660] A wave of (claims against) disinformation emerged from these attacks, with political effects.
April 2021	NEAR	The social media accounts of Polish officials have been compromised to disseminate narratives critical of NATO.[661]
March 2021	FAR	A North Korean campaign has targeted infosec professionals using fake social media profiles and a fake website. [661]
January 2021	FAR	The Capitol Hill Attack was just the result of a long-term wave of misinformation and disinformation attacks,[662] which continued even after the assault to Capitol Hill.[663]
January 2021	FAR	State-sponsored hackers started a social engineering campaign against cybersecurity researchers. The campaign was based on fake twitter accounts and a fake blog trying to mislead targets of the attack to open infected sites or infected attachments in e-mails asking them to collaborate on a research project.[664]
2021	NEAR	The German election has been reported to be the target of disinformation attacks.[665] [666]
July 2020	FAR	QAnon conspiracy theorists against Wayfair, the US-based furniture and home décor company, falsely claimed that Wayfair was managing a vast child trafficking operation.[667]
July 2020	FAR	A major bitcoin scam attack targeted Twitter. Major US accounts (e.g. Kim Kardashian West, Kanye West, Elon Musk, Bill Gates and Barack Obama, as well as Uber and Apple) were compromised and used to tweet about Bitcoin. Short-time tweets requested Bitcoins from followers with a promise to return the double the amount received.[668] [669] The attack was caused by human error and a spear-phishing attack on Twitter employees.[670]
June 2020	FAR	T-Mobile outages due to network configuration issues were falsely reported as the biggest DDoS attack ever on the US.[671]

[659] Elliot Smith, Israeli Pegasus spyware saga could sow diplomatic rifts in Africa, July 2021, https://www.cnbc.com/2021/07/27/the-pegasus-spyware-saga-could-sow-diplomatic-rifts-in-africa-.html
[660] Dana Priest, Craig Timberg and Souad Mekhennet, Private Israeli spyware used to hack cellphones of journalists, activists worldwide, July 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/
[661] Center for Strategic and International Studies, Significant Cyber Incidents, July 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[662] Philip Bump, Questions of culpability for the Capitol violence must start with Trump's lies about fraud, January 2021, https://www.washingtonpost.com/politics/2021/01/11/questions-culpability-capitol-violence-must-start-with-trumps-lies-about-fraud/
[663] New report analyzes new and dangerous trends of disinformation in wake of US Capitol attack, March 2021, https://www.securitymagazine.com/articles/94908-new-report-analyzes-new-and-dangerous-trends-of-disinformation-in-wake-of-us-capitol-attack
[664] Center for Strategic and International Studies, Significant Cyber Incidents, July 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[665] Janosch Delcker, Cyber threat looms large over German election, May 2021, https://www.dw.com/en/cyber-threat-looms-large-over-german-election/a-56775960
[666] Kate Martyr, Russian disinformation mainly targets Germany: EU report, March 2021 https://www.dw.com/en/russian-disinformation-mainly-targets-germany-eu-report/a-56812164
[667] Alethea Group, QAnon Conspiracy Theorists Target Wayfair In Disinformation Campaign, August 2020, https://14ed461d-cb57-414f-a4b7-6e72361febb1.usrfiles.com/ugd/14ed46_368cff2044dd4c5bb0ee2dd6e0e4c65a.pdf
[668] BBC, Major US Twitter accounts hacked in Bitcoin scam, July 2020, https://www.bbc.com/news/technology-53425822
[669] Frank Downs, Dustin Brewer, Top Cyberattacks of 2020 and How to Build Cyberresiliency, November 2020, https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency
[670] BBC, Twitter hack: Staff tricked by phone spear-phishing scam, July 2020, https://www.bbc.com/news/technology-53607374
[671] Byron Muhlberg, Biggest DDoS cyber-attack on US Just Rampant Social Media Speculation, June 2020, https://www.cpomagazine.com/cyber-security/biggest-ddos-cyber-attack-on-u-s-just-rampant-social-media-speculation/

March 2017-2021	NEAR	The "Ghostwriter" campaign targeted Lithuania, Latvia, and Poland with narratives critical of the North Atlantic Treaty Organisation's (NATO) presence in Eastern Europe[672]. Hackers compromised websites and e-mail accounts and used them to publish fabricated documents. They then donned fake personas of local officials to promote the fabricated documents on social media[673]. Analysts aligned it with Russian security interests.[673]

Particular attention is given to incidents related to the pandemic, which found a sharp increase during the course of last year. Although not an incident per se, we also need to highlight that the World Health Organisation (WHO) declared an "infodemic" to describe the scale of fake news and its potential impact on efforts to limit the virus's spread.[674] [675] In general, COVID campaigns targeted three main themes: i) connection between vaccine and neurological effects; ii) hidden target of global depopulation; iii) more effective medications than the vaccines.[676] Accordingly, pandemic related misinformation/disinformation incidents are not exhaustively listed in the table below.

Table 12: Pandemic related misinformation/disinformation incidents

Time	Geographical Spread	Description
June 2021	NEAR	Denmark soccer star Christian Eriksen suffered a cardiac arrest during the match with Finland. This fact was the target of a disinformation attack against COVID-19 vaccine, which was blamed as the cause of Christian Eriksen's Collapse.[677]
2021	NEAR	Pharmaceutical companies Pfiser, Moderna, AstraZeneca and Johnson & Johnson are the target of disinformation campaigns about the effects and effectiveness of COVID-19 vaccines.[678]
2020-21	NEAR	2020-21: On one hand, contact tracing apps have been the target of disinformation attacks and fake news around mass surveillance and tracking.[679] On the other hand, fake apps have been used to distribute banking trojans.[680]
2020-21	NEAR	2020-21: Hundreds of deaths and thousands of hospitalisations around the world were due to COVID-19 misinformation, including rumours, conspiracy theories, and stigmas.[681]
2020-21	MID/NEAR	2020-21: 5G has been held responsible for spreading coronavirus. This has resulted in physical attacks on 5G towers.[682] [683]

[672] Mandiant, Ghostwriter' Influence Campaign: Report, Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests. https://www.mandiant.com/resources/ghostwriter-influence-campaign
[673] Council on Foreign Affairs, Ghostwriter. https://www.cfr.org/cyber-operations/ghostwriter
[674] Joyce Hakmeh, Emily Taylor, Allison Peters and Sophia Ignatidou, The COVID-19 pandemic and trends in technology: Transformations in governance and society, February 2021, https://www.chathamhouse.org/sites/default/files/2021-02/2021-02-16-COVID-19-trends-technology-hakmeh-et-al.pdf
[675] European Commission, Tackling coronavirus disinformation, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_en
[676] CTI League, Darknet Report 2021, 2021
[677] Tommy Beer, Conspiracy Blames Christian Eriksen's Collapse On COVID Vaccine—But He Hasn't Even Been Vaccinated, June 2021, https://www.forbes.com/sites/tommybeer/2021/06/14/conspiracy-blames-christian-eriksens-collapse-to-COVID-vaccine-but-he-hasnt-even-been-vaccinated/
[678] Lisa Kaplan, Disinformation attacks are spreading. Here are 4 keys to protecting your company, March 2021, https://fortune.com/2021/03/08/disinformation-solarwinds-capitol-riots-hacking-cybersecurity-defense/
[679] Jack Goodman, Flora Carmichael, Coronavirus: Contact-tracing rumours debunked, June 2020, https://www.bbc.com/news/53021722
[680] Alex Scroxton, Fake contact-tracing apps delivering banking trojans, June 2020, https://www.computerweekly.com/news/252484584/Fake-contact-tracing-apps-delivering-banking-trojans
[681] M.S. Islam et al., COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis, The American Journal of Tropical Medicine and Hygiene, Vol. 103, No. 4, 2020, https://www.ajtmh.org/view/journals/tpmd/103/4/article-p1621.xml
[682] The New York Times, Burning Cell Towers, Out of Baseless Fear They Spread the Virus, April 2020, https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html
[683] Zara Abrams, Controlling the spread of misinformation, Monitor on Psychology, Vol. 52, No. 2, March 2021, https://www.apa.org/monitor/2021/03/controlling-misinformation

2020-21	MID	2020-21: Conspiracy theorists are claiming that democratic governments distributed the virus to turn democracies into autocracies.[684]
2020-21	FAR	2020-21: Fake news is alleging that someone "*... has created or financed the creation of COVID-19 to sell vaccines and gain power over the world*". [684]
2020	FAR	2020: Copies of benign tools like the original John Hopkins COVID map have been used to infect users.[685]
2020	MID	2020: Avast identified fake shops selling COVID-19 cures with the World Health Organisation's logo, which were just a preparatory activity for a malware-based attack.[686]

[684] Avast, 2020: The Year of Fake News, COVID-related Scams and Ransomware, November 2020, https://www.prnewswire.com/news-releases/2020-the-year-of-fake-news-COVID-related-scams-and-ransomware-301180568.htm l
[685] CTI League, Darknet Report 2021, 2021
[686] Saj Huq, It's time to accept that disinformation is a cyber security issue, December 2020, https://www.computerweekly.com/opinion/Its-time-to-accept-that-disinformation-is-a-cyber-security-issue

NON-MALICIOUS THREATS

Table 13: Notable incidents related to errors and misconfigurations made when managing an IT system

Time	Geographical Spread	Description
June 2021	FAR	A misconfigured cloud storage system was discovered, containing information on about 1,000 customers of Mercedes Benz USA, including payment information and social security numbers.[687]
June 2021	FAR	An open ElasticSearch database was discovered, containing 25 GBs of data of users who had subscribed to a family history search platform named Ancestry. The database belonged to another company which syncs data from such a platform, and contained information such as names and geolocation data.[688]
April 2021	FAR	A publicly accessible datastore was discovered, containing thousands of records belonging to Skild, a US company delivering services for business challenges and competitions. Breached data contained personal information (e.g. names) and details about some competitions.[689]
February 2021	NEAR	An unsecured staging server was discovered, containing almost 2 million customer e-mails of e-Ticketing, a Dutch ticketing platform.[690]
January 2021	FAR	A misconfigured Git server leaked the source code of several applications developed and used by Nissan North American, including mobile apps and other internal software. The server was exposed with default username and password.[691]
July 2020	FAR	A cluster of unsecured ElasticSearch databases of an online booking and patient management platform, called Adit,[692] was discovered containing the details of 3.1 million patients.
June 2020	GLOBAL	47% of all MongoDB databases accessible online have been wiped. Around 23,000 databases were exposed with no passwords.[693]
May 2020	NEAR	A misconfigured ElasticSearch database was discovered, containing 7 TB of data (logs) of the adult live-streaming website CAM4.com. The database contained billions of user logs, including names, countries and payment details.[694]
April 2020	NEAR	A misconfigured ElasticSearch database was discovered, containing 8 TB of data (logs) of the French daily newspaper Le Figaro. The database contained billions of logs of subscribed users, including name, e-mails and passwords, sometimes in cleartext or poorly secured (e.g. MD5 or salted MD5).[695]

[687] Ax Sharma, Mercedes-Benz data breach exposes SSNs, credit card numbers, June 2021 https://www.bleepingcomputer.com/news/security/mercedes-benz-data-breach-exposes-ssns-credit-card-numbers/
[688] WizCase. Family History Search Software Leaks Users' Private Data, July 2020 https://www.wizcase.com/blog/mackiev-leak-research/
[689] TurgenSec. New York Startup Competitions Data Breach Disclosure (Skild), April 2021, https://community.turgensec.com/new-york-startup-competitions-data-breach-disclosure-skild/
[690] Lawrence Abrams, European e-ticketing platform Ticketcounter extorted in data breach, March 2021 https://www.bleepingcomputer.com/news/security/european-e-ticketing-platform-ticketcounter-extorted-in-data-breach/
[691] Catalin Cimpanu, Nissan source code leaked online after Git repo misconfiguration, January 2021, https://www.zdnet.com/article/nissan-source-code-leaked-online-after-git-repo-misconfiguration/
[692] Volodymyr Bob Diachenko. 3.1 million patients' details exposed by a medical software company, August 2020, https://www.linkedin.com/pulse/31-million-patients-details-exposed-medical-software-diachenko/
[693] Catalin Cimpanu, Hacker ransoms 23k MongoDB databases and threatens to contact GDPR authorities, July 2020, https://www.zdnet.com/article/hacker-ransoms-23k-mongodb-databases-and-threatens-to-contact-gdpr-authorities/
[694] SafetyDetectives. Live streaming adult site leaves 7 terabytes of private data exposed, May 2020, https://www.safetydetectives.com/blog/cam-leak-report/
695 Safety Detectives, French Subscribers to Famous News Site at Risk from Hacking, Fraud, April, 2020, https://www.safetydetectives.com/blog/lefigaro-leak-report/

Table 14: Notable incidents related to errors and misconfigurations at application level

Time	Geographical Spread	Description
June 2021	FAR	A misconfigured Microsoft Azure Blob bucket was discovered, containing information on more than 3.3 million customers of Volkswagen group North America. In some cases, the bucket contained very sensitive information, e.g. loan eligibility. [696] [697]
March 2021	FAR	The results of COVID-19, influenza and breathe alcohol tests of 162,021 residents of Wyoming (US) were discovered on public Github repositories. Apparently, the leak had been caused by an employee's error.[698]
February 2021	FAR	Two misconfigured AWS S3 buckets are discovered, containing more than 50,000 patient records of a Utah COVID-19 testing services. The bucket contained personal and sensitive data, such as passports and medical insurance cards.[699]
February 2021	FAR	A misconfigured AWS storage server was discovered, containing all the update documents managed by JamCOVID19. It is a website where travellers who want to go to Jamaica need to upload several documents such as COVID-19 negative tests.[700]
January 2021	GLOBAL	Misconfigured Microsoft Azure Blob buckets were discovered, containing 63 GBs of pitches and source codes for part of Microsoft Dynamics.[701]
August 2020	FAR	Using an unrecycled AWS access key, attackers leaked (at least) 35 million customer account records from Juspay, a company offering payment services. The breach included masked information about credit cards.[702]
July 2020	FAR	A misconfigured Google Cloud bucket was discovered, containing hundreds of personal identifiable information of users of Pfiser's drugs.[703]
June 2020	GLOBAL	A misconfigured AWS S3 bucket was discovered, containing 7 GBs of CVS files consisting of 350,000,000 of e-mails.[704]

[696] Lorenzo Franceschi-Bicchierai, Hackers Are Selling Data Stolen From Audi and Volkswagen, June 2021 https://www.vice.com/en/article/xgxaq4/hackers-are-selling-data-stolen-from-audi-and-volkswagen
[697] Zack Whittaker, Volkswagen says a vendor's security lapse exposed 3.3 million drivers' details, June 2021, https://techcrunch.com/2021/06/11/volkswagen-says-a-vendors-security-lapse-exposed-3-3-million-drivers-details/
[698] Wyoming Department of Health, Exposure of Laboratory Test Result Data Described, April 2021, https://health.wyo.gov/exposure-of-laboratory-test-result-data-described/
[699] Paul Bischoff, Utah COVID-19 testing services exposed 50,000 patients' photo IDs, personal info on the web, March 2021, https://www.comparitech.com/blog/information-security/utah-COVID-test-center-leak/
[700] Zack Whittaker, Jamaica's immigration website exposed thousands of travelers' data, February 2021, https://techcrunch.com/2021/02/17/jamaica-immigration-travelers-data-exposed
[701] vpnMentor. Report: Software Companies Exposed to Hacking in Major Data Breach, https://www.vpnmentor.com/blog/report-microsoft-dynamics-leak/
[702] Soumik Ghosh, CSO, Juspay data breach could have far-reaching consequences, January 2021, https://www.csoonline.com/article/3603473/juspay-data-breach-could-have-far-reaching-consequences.html
[703] vpnMentor. Report: Major Pharmaceutical Company Exposes Private Data of US Prescription Drug Users, October 2020 https://www.vpnmentor.com/blog/report-pfiser-breach/
[704] Edvardas Mikalauskas, 350 million decrypted e-mail addresses left exposed on an unsecured server, August 2020, https://cybernews.com/security/350-million-e-mail-addresses-left-exposed-on-an-unsecured-server/

Table 15: Notable incidents related to errors and misconfigurations made during development

Time	Geographical Spread	Description
July 2021	GLOBAL	An issue in the DNS server of content delivery network provider Akamai was the cause of a major outage of many websites and apps.[705] [706] [707]
July 2021	GLOBAL	Google released a patch to fix several vulnerabilities in Chrome, including a zero-day vulnerability that was being actively exploited.[708]
July 2021	NEAR	Italian hosting company Aruba revealed it has suffered from a breach due to a vulnerability in third-party software. Names, addresses and the Italian version of the social security numbers were among the exposed data.[709]
June 2021	GLOBAL	The edge-cloud platform Fastly experienced an outage that brought down part of the Web.[710] Many sites went offline due to a problem in the Fastly CDN. According to Fastly, outage was "*due to an undiscovered software bug that surfaced on June 8 when it was triggered by a valid customer configuration change*."
June 2021	GLOBAL	Microsoft's patch released several fixes, six zero-day vulnerabilities, that, according to Microsoft, were actively exploited.[711]
April 2021	GLOBAL	Apple released some patches to fix an zero-day vulnerability in WebKit that was actively exploited.[712]
March 2021	NEAR	Microsoft released patches for five zero-day vulnerabilities in Exchange Server that were actively exploited in targeted attacks. Notable victims include the Czech Labour Ministry and European Banking Authority. [713] [714] [715]
February 2021	GLOBAL	Adobe released some patches to fix an actively exploited zero-day vulnerability in Adobe Acrobat and Reader. [716]
December 2020	FAR	SolarWinds revealed a supply chain attack delivered through a (compromised) update on SolarWind's Orion (a monitoring solution). This was the attack with the greatest impact in US history, as it permitted access to many systems including government-related ones.[717] [718]

[705] Rhiannon Williams, what is Akamai? How DNS outage brought down many of the internet's biggest sites weeks after Fastly problems, July 2021, https://inews.co.uk/news/technology/what-is-akamai-how-dns-outage-brought-down-many-of-the-internets-biggest-sites-weeks-after-fastly-problems-1117900
[706] Chris Morris, Massive outage hits major sites across the Internet, July 2021, https://fortune.com/2021/07/22/internet-outage-psn-website-playstation/
[707] Peter Judge, CDN outages like Akamai's point to deeper problems, July 2021, https://www.datacenterdynamics.com/en/opinions/cdn-outages-like-akamais-point-to-deeper-problems/
[708] Google Chrome Releases, Stable Channel Updated for Desktop, July 2021, https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html
[709] Alessandro Longo, Data breach Aruba, "esposti dati anagrafici, password": ecco che devono sapere i clienti (in Italian), July 2021, https://www.cybersecurity360.it/nuove-minacce/data-breach-aruba-rubati-dati-anagrafici-password-ecco-che-devono-sapere-i-clienti/
[710] Nick Rockwell, Fastly, Summary of June 8 outage, https://www.fastly.com/blog/summary-of-june-8-outage
[711] Charlie Osborne, Microsoft June 2021 Patch Tuesday: 50 vulnerabilities patched, six zero-days exploited in the wild, June 2021, https://www.zdnet.com/article/microsoft-june-2021-patch-tuesday-50-vulnerabilities-patched-including-six-zero-days-exploited-in-the-wild/
[712] Apple, About the security content of iOS 14.4.2 and iPadOS 14.4.2, March 2021, https://support.apple.com/en-us/HT212256
[713] Microsoft, HAFNIUM targeting Exchange Servers with 0-day exploits, March 2021, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[714] Shannon Vavra, Victims of Microsoft Exchange Server zero-days emerge, March 2021, https://www.cyberscoop.com/microsoft-exchange-server-czech-republic-norway-hafnium-chinese-hackers/
[715] EBA, Cyber-attack on the European Banking Authority - UPDATE 3, March 2021, https://www.eba.europa.eu/cyber-attack-european-banking-authority-update-3
[716] Adobe Security Bulletin, Security update available for Adobe Acrobat and Reader | APSB21-09, https://helpx.adobe.com/security/products/acrobat/apsb21-09.html
[717] SonicWall CyberThreat Report 2021
[718] Lucian Constantin, CSO, SolarWinds attack explained: And why it was so hard to detect, December 2020, https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organisations-were-not-prepared.html

October 2020	GLOBAL	The Zerologon vulnerability (a privilege escalation, zero-day vulnerability discovered in August 2020 that allows attackers to impersonate even a Windows root domain controller) is being exploited by Iran-sponsored attackers. At the end of 2020, it was the most exploited vulnerability.[719] [720] [721]
August 2020	FAR	Tesla was notified of an attack vector that exploits some vulnerabilities allowing an attacker to unlock and drive a Model X.[722]
June 2020	GLOBAL	19 novel vulnerabilities were discovered in Treck's TCP/IP stack. The library is so widespread that international coordination among many CERTs (Computer Emergency Response Team) was needed. This set of vulnerabilities is known as Ripple20.[723]

Table 16: Notable incidents caused by physical disasters[724]

Time	Geographical Spread	Description
March 2021	NEAR	The OVH cloud was destroyed by the fire in the OVH data centre in Strasbourg. One of the four data centres was destroyed and one damaged. Millions of websites went offline for several days.[725]
February 2021	FAR	An unusual ice storm in Texas made critical utilities unavailable across the state. The entire state suffered power outages. Some data centres went close to run out of fuel, while many shared with competitors to maintain availability.[726]

[719] SonicWall CyberThreat Report 2021
[720] Carnegie Mellon CERT Coordination Center, Microsoft Windows Netlogon Remote Protocol (MS-NRPC) uses insecure AES-CFB8 initialisation vector, March 2021, https://www.kb.cert.org/vuls/id/490028
[721] Catalin Cimpanu, Microsoft says Iranian hackers are exploiting the Zerologon vulnerability, October 2020 https://www.zdnet.com/article/microsoft-says-iranian-hackers-are-exploiting-the-zerologon-vulnerability/
[722] Andy Greenberg, This Bluetooth Attack Can Steal a Tesla Model X in Minutes, November 2020, https://www.wired.com/story/tesla-model-x-hack-bluetooth/
[723] JSOF. Ripple20. https://www.jsof-tech.com/disclosures/ripple20
[724] In general, outages affect every day clouds and networks, causing a decrease in systems availability and loss of money. Total Uptime monitored these outages to provide a picture of the problem, Total Uptime, Notable Network and Cloud Outages of 2021 (so far), 2021, https://totaluptime.com/notable-network-and-cloud-outages-of-2021/
[725] Mathieu Rosemain, Raphael Satter, Millions of websites offline after fire at French cloud services firm, March 2021, https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU
[726] Tom Kiblin, A Near Miss and a Total Loss: Lessons from 2021 in Data Center Resiliency, May 2021, https://www.networkcomputing.com/data-centers/near-miss-and-total-loss-lessons-2021-data-center-resiliency

TP-AE-21-293-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citisens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-536-4
DOI: 10.2824/324797