ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS

JULY 2022

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 at: www.enisa.europa.eu.

CONTACT

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

EDITORS

Ifigeneia Lella, Eleni Tsekmezoglou, Rossen Naydenov, Apostolos Malatras – European Union Agency for Cybersecurity
Sebastian Garcia, Veronica Valeros, Alya Gomaa – Czech Technical University in Prague

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.

LEGAL NOTICE

COPYRIGHT NOTICE

For any use or reproduction of photos or other materials that are not under ENISA copyright, permission must be sought directly from the copyright holders.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

During the last decade ransomware has become one of the most devastating types of attacks, impacting organisations of all sizes worldwide. Quickly adapting to new business models with advanced threat actors leveraging the cybercrime ecosystem for a better distribution of labour, ransomware has managed to increase its reach and impact significantly. No business is safe.

This report aims to bring new insights into the reality of ransomware incidents through mapping and studying ransomware incidents from May 2021 to June 2022. The findings are grim. Ransomware has adapted and evolved, becoming more efficient and causing more devastating attacks. Businesses should be ready not only for the possibility of their assets being targeted by ransomware but also to have their most private information stolen and possibly leaked or sold on the Internet to the highest bidder.

The main highlights of the report include the following:

- A novel **LEDS matrix** (Lock, Encrypt, Delete, Steal) that accurately maps ransomware capabilities based on the actions performed and assets targeted;
- A detailed and in-depth analysis of the **ransomware life cycle**: initial access, execution, action on objectives, blackmail, and ransom negotiation;
- **Collection and in-depth analysis of 623 ransomware incidents** from May 2021 to June 2022;
- More than **10 terabytes of data stolen monthly** by ransomware from targeted organisations;
- Approximately **58.2% of all the stolen data contains GDPR personal data** based on this analysis**;**
- In **95.3%** of the incidents it is not known how threat actors obtained initial access into the target organisation;
- It is estimated that **more than 60% of affected organisations may have paid ransom** demands;
- At **least 47 unique ransomware threat actors** were found.

The report also highlights issues with the reporting of ransomware incidents and the fact that we still have limited knowledge and information regarding such incidents. The analysis in this report indicates that publicly disclosed incidents are just the tip of the iceberg.

Along with a general recommendation to contact the competent cybersecurity authorities and law enforcement in cases of ransomware attacks, several other recommendations are put forward, both to build resilience against such attacks and to mitigate their impact.

1. INTRODUCTION

The threat of ransomware has consistently ranked at the top in the ENISA Threat Landscape for the past few years and, in particular, in 2021 it was assessed as being the prime cybersecurity threat across the EU[1]. Motivated mainly by greed for money, the ransomware business model has grown exponentially in the last decade[2] and it is projected to cost more than $10 trillion by 2025[3]. The evolution of the business model to a more specialised and organised distribution of labour through a cybercrime-as-a-service model has turned ransomware into a commodity. Nowadays, it seems simpler for anyone with basic technical skills to quickly perform ransomware attacks. The introduction of cryptocurrency, the fact that affected companies actually do pay the ransom, and the more efficient division of work, have greatly fuelled the growth of ransomware, generating a catastrophic global effect[4],[5].

Even though ransomware is not new, technologies evolve and with them so do attacks and vulnerabilities, thus pressurising organisations to be always prepared for a ransomware attack. In many cases, staying in business requires difficult decisions, such as paying or not paying the ransom[6], since this money ends up fuelling ransomware activities. This is despite year-long and consistent recommendation not to pay ransom demands and to contact the relevant cybersecurity authorities to assist in handling such incidents.

This report brings new insights into the ransomware threat landscape through a careful study of 623 ransomware incidents from May 2021 to June 2022. The incidents were analysed in-depth to identify their core elements, providing answers to some important questions such as how do the attacks happen, are ransom demands being paid and which sectors are the most affected. The report focuses on ransomware incidents and not on the threat actors or tools, aiming to analyse ransomware attacks that actually happened as opposed to what could happen based on ransomware capabilities. This ransomware threat landscape has been developed on the basis of the recently published ENISA Cybersecurity Threat Landscape Methodology[7].

The report starts by clearly defining what ransomware is since it has proven to be an elusive concept spanning various dimensions and including different stages. The definition is followed by a novel description of the types of ransomware that breaks the traditional classification and instead focuses on the four actions performed by ransomware, i.e. Lock, Encrypt, Delete, Steal (LEDS), and the assets at which these actions are aimed. By defining the types of ransomware, it is then possible to study the life cycle of ransomware and its business models. This characterisation of ransomware leads into the core of this report which is the deep analysis of 623 incidents and its summary in precise statistics. The report ends by highlighting recommendations for readers and key conclusions.

The report is structured as follows:

---

[1] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 , October 2021
[2] '2021 Trends Show Increased Globalized Threat of Ransomware | CISA'. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a (accessed Jul. 02, 2022)
[3] Cybercrime To Cost The World $10.5 Trillion Annually By 2025', Cybercrime Magazine, Dec. 08, 2018. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed Jul. 02, 2022)
[4] Kaseya VSA ransomware attack', Wikipedia. Apr. 07, 2022. Accessed: Jul. 02, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Kaseya_VSA_ransomware_attack&oldid=1081509343
[5] J. Dossett, 'A timeline of the biggest ransomware attacks', CNET. https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/ (accessed Jul. 02, 2022)
[6] '83% of ransomware victims paid ransom: Survey', ZDNet. https://www.zdnet.com/article/83-of-ransomware-victims-paid-ransom-survey/ (accessed Jul. 02, 2022)
[7] https://www.enisa.europa.eu/news/enisa-news/how-to-map-the-cybersecurity-threat-landscape-follow-the-enisa-6-step-methodology

- **Chapter 1, Introduction**, provides a brief introduction to the problem of ransomware attacks and the dedicated ENISA ransomware threat landscape report;
- **Chapter 2, Focus on Ransomware**, discusses what ransomware is and its key elements, as well as proposing the LEDS matrix to accurately map ransomware capabilities based on the actions performed and assets targeted;
- **Chapter 3, Ransomware Life Cycle**, gives a detailed overview of the life cycle of a ransomware attack;
- **Chapter 4, Ransomware Business Models**, discusses the evolution of ransomware business models and how trust is the key to the ransomware business;
- **Chapter 5, Analysis of Ransomware Incidents**, presents a detailed study of ransomware incidents from May 2021 to June 2022, including a timeline of incidents;
- **Chapter 6, Recommendations**, provides high-level recommendations to better protect against ransomware incidents;
- **Chapter 7, Conclusions**, highlights the most important conclusions of the study and how they can potentially impact the future of the threat landscape.

2. FOCUS ON RANSOMWARE

2.1 DEFINING RANSOMWARE

Defining what ransomware is has been elusive and has presented mismatching descriptions that were modified as ransomware evolved. Therefore, based on previous work [8] [9] [10], in this report ransomware is defined as follows.

*Ransomware **is a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality**.*

There are **three key elements** in every ransomware attack: **assets, actions and blackmail**. Assets and actions will be discussed in the next section. Blackmail[11] is the final key element of ransomware attacks, where threat actors coerce the target through the use of threats demanding something in return for asset availability. Many coercion methods are used to force the target to comply with the ransom demands: publicity of the attack, partial or full data leaks, distributed denial of service (DDoS) attacks against the target infrastructure and others. While blackmail is more commonly financially motivated, there is precedence for ransomware threat actors demanding other things in exchange, such as a change in corporate policy, new software features[12], or asking targets to infect their social circle[13].

Note that this definition does not depend on the action done, such as encrypt or steal, or the type of demand done, monetary or not, and is inherently generic.

2.2 TYPES OF RANSOMWARE

Defining the types of ransomware is difficult because the concept of ransomware has evolved and the technical capabilities of ransomware are similar to those of other malware. Up to the mid-2010s, ransomware used to only focus on one or two actions, such as encryption or locking. This made it easy to group ransomware in simple categories such as *Encryption Ransomware* or *Lock Screen Ransomware*. However, ransomware is not tied to such descriptions anymore and its evolution has made such simple categories no longer sufficient to represent it.

This was further complicated by the lack of homogeneity in the naming of ransomware by the cybersecurity industry, and the tradition in believing that the *types* where mutually exclusive, e.g. Encryption Ransomware was only expected to encrypt files and not do anything else. We therefore propose to talk about ransomware not in terms of *type* but in terms of **actions** they perform and **assets** they target.

---

[8] Ransomware Attack - What is it and How Does it Work?' Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware / (accessed Jul. 02, 2022)
[9] 'What Is Ransomware? - Definition, Prevention & More | Proofpoint US'. https://www.proofpoint.com/us/threat-reference/ransomware (accessed Jun. 28, 2022).
[10] ENISA Threat Landscape 2021| https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (accessed Jul. 5, 2022).
[11] 'BLACKMAIL | Meaning & Definition for UK English | Lexico.com', Lexico Dictionaries | English. https://www.lexico.com/definition/blackmail (accessed Jul. 02, 2022)
[12] A. Hope, 'Nvidia Data Leak Exposed Proprietary Information but Wasn't a Russian Ransomware Attack, Company Says', CPO Magazine, Mar. 11, 2022. https://www.cpomagazine.com/cyber-security/nvidia-data-leak-exposed-proprietary-information-but-wasnt-a-russian-ransomware-attack-company-says/ (accessed Jul. 02, 2022)
[13] New ransomware offers to restore your files for free - if you infect two friends – ExtremeTech https://www.extremetech.com/internet/240933-new-ransomware-offers-restore-files-free-infect-two-friends (accessed Jul. 02, 2022)

There are four core **actions** ransomware can execute: **lock, encrypt, delete and steal.** We refer to these four core actions as *LEDS (Lock, Encrypt, Delete, Steal)*. Ransomware can **lock** access to an asset, such as locking the screen, or lock access to a particular application. It can **encrypt** an asset, making it unavailable to the target. It can **steal** an asset, compromising its availability and in the end its confidentiality. Lastly, it can **delete** an asset, making it permanently unavailable.

Assets are anything of value for a business or organisation. The most common targeted assets by ransomware are files and folders. Most assets are technically a *file* in the majority of operating systems, therefore the distinction needs to be made to show the differences between, for example, ransomware that encrypts all the files in a target, compared with ransomware that only encrypts parts of a file with the code to run a web server. However, it would be misleading to assume that these are the only assets targeted. Other targeted assets may include databases, web services, content management systems, screens, master boot records (MBR), master file tables (MFT), and others.

Using **actions** and **assets** allows us to represent the capabilities of current ransomware in Table 1. This table only shows the capabilities of current ransomware as they were analysed, and it is clear that many combinations are missing and there is room for variability as the threat landscape evolves. Accordingly, this will be monitored by ENISA in future updates of this work.

Table 1: Capabilities of current ransomware in terms of actions they perform and assets they target

Assets	Lock	Encrypt	Delete	Steal
Files	✖	✔	✔	✔
Memory	✖	✔	✔	✔
Folders	✖	✔	✔	✔
Database Content	✖	✔	✔	✔
MFT	✔	✔	✔	✖
MBR	✔	✔	✔	✖
Cloud	✖	✔	✔	✔
CMS	✖	✔	✔	✖
Screen	✔	✔	✔	✖

2.3 LEDS ACTIONS

2.3.1 Lock
The action to lock an asset can imply very different things. In the case of mobile screens, it can be simple to change the PIN of the mobile phone and lock the screen. In the case of an application, it can be to change the credentials to access it, the same with hardware. In particular, we don't consider the act of encryption as *locking* since that is covered in the action to encrypt.

2.3.2 Encrypt
Encrypt refers to the action of using an encryption algorithm to make the content of a file, folder or text available only to those who know the encryption algorithm used and who possess the encryption key to decrypt it. There are different types of encryption algorithms that can be used, assets that can be encrypted partially, different encryption types and a difference regarding *where* the encryption takes place: only in the client, or in the client and server.

2.3.3 Delete
The act of deletion refers to the action of ordering the operating system to delete a file by (i) the official OS procedure (which only deletes the reference to the file in the folder structure in most operating systems) or (ii) by deleting the file by rewriting its bytes. In the case of in-memory databases, deletion is the action of asking the database to delete the file. Deletion can also be done to virtual machines in cloud environments using official dashboards, which do not involve the operating system. Deletion of a file does not imply that the file was encrypted or stolen.

2.3.4 Steal
The action of stealing refers to copying the asset into the control of the attacker. It can be by exfiltrating data to the Internet, or by copying data to a *secret local* folder unknown to the owner of the asset. In particular, stealing does not imply deleting, or encrypting.

2.4 ASSETS TARGETED BY RANSOMWARE
The following assets are the most commonly observed assets targeted by ransomware in our study. The list will likely expand in the future as ransomware continues to exploit vulnerable systems.

Table 2: Commonly observed assets in Ransomware incidents

ASSETS TARGETED BY RANSOMWARE

FILES	We refer to files used by the user, traditionally searched by ransomware using file extensions due to their potential value. These can also be system files that contain configurations. Files also include network files as remotely mounted in the local computer.
FOLDERS	We refer to user and system folders that attackers may be interested in due to the files they may contain.
MEMORY	Some ransomware actually uses memory mapped I/O to encrypt cached documents in memory and force applications to save the encrypted file back to disk
DATABASE CONTENT	We refer to the content of databases, including rows and tables, and not particularly to the files where the dataset is stored. Some databases have the whole content in one file. Some databases have some of their rows and tables encrypted, but not all. And some databases are in-memory databases without any files.
SCREEN	We refer to the screen of the graphical user interface of an operating system. Ransomware is known for creating a special screen where users can interact with and disabling any other screen of the operating system.
MASTER FILE TABLE (MFT)	The MFT is a special file stored in the hard drive that contains an index of all files and folders in the volume.
MASTER BOOT RECORD (MBR)	The MBR is a special partition in a hard disk used in the booting process of the operating system. This partition can be locked by ransomware that modifies it.
CLOUD	Cloud assets fall into a very broad category, but these assets are purposely searched and attacked. It refers to third-party cloud providers (no private cloud) that are used as part of the operation of the target.
CONTENT MANAGEMENT SYSTEM (CMS).	CMS refers both to the web server running the web page and to the files of the web service. The files can be the configuration, data and code. This asset was especially distinguished due to a large number of attacks on web services.

M. Loman, 'LockFile ransomware's box of tricks: intermittent encryption and evasion', Sophos News, Aug. 27, 2021. https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/ (accessed Jul. 03, 2022)

3. RANSOMWARE LIFE CYCLEE

The life cycle of ransomware remained unchanged until around 2018 when ransomware started to add more functionality and blackmailing techniques matured. We can identify five stages of a ransomware attack: initial access, execution, action on objectives, blackmail, and ransom negotiation. These stages do not follow a strictly sequential path which can vary.

We need to clarify and highlight that ransom negotiation is not a suggested recommendation for victims of ransomware attacks. Contacting the competent cybersecurity authority and/or law enforcement is the recommended approach to handling such incidents. However, in describing the life cycle of typical ransomware incidents, we opted to include this stage in order to be inclusive as in several cases this stage did take place.

Figure 1 describes the life-cycle stages of a ransomware attack, following a typical flow of events from initial access to ransom negotiation, including actions and assets, and what constitutes blackmail. Each of these stages is further discussed in the following subsections.

Figure 1: The five stages of the ransomware life cycle
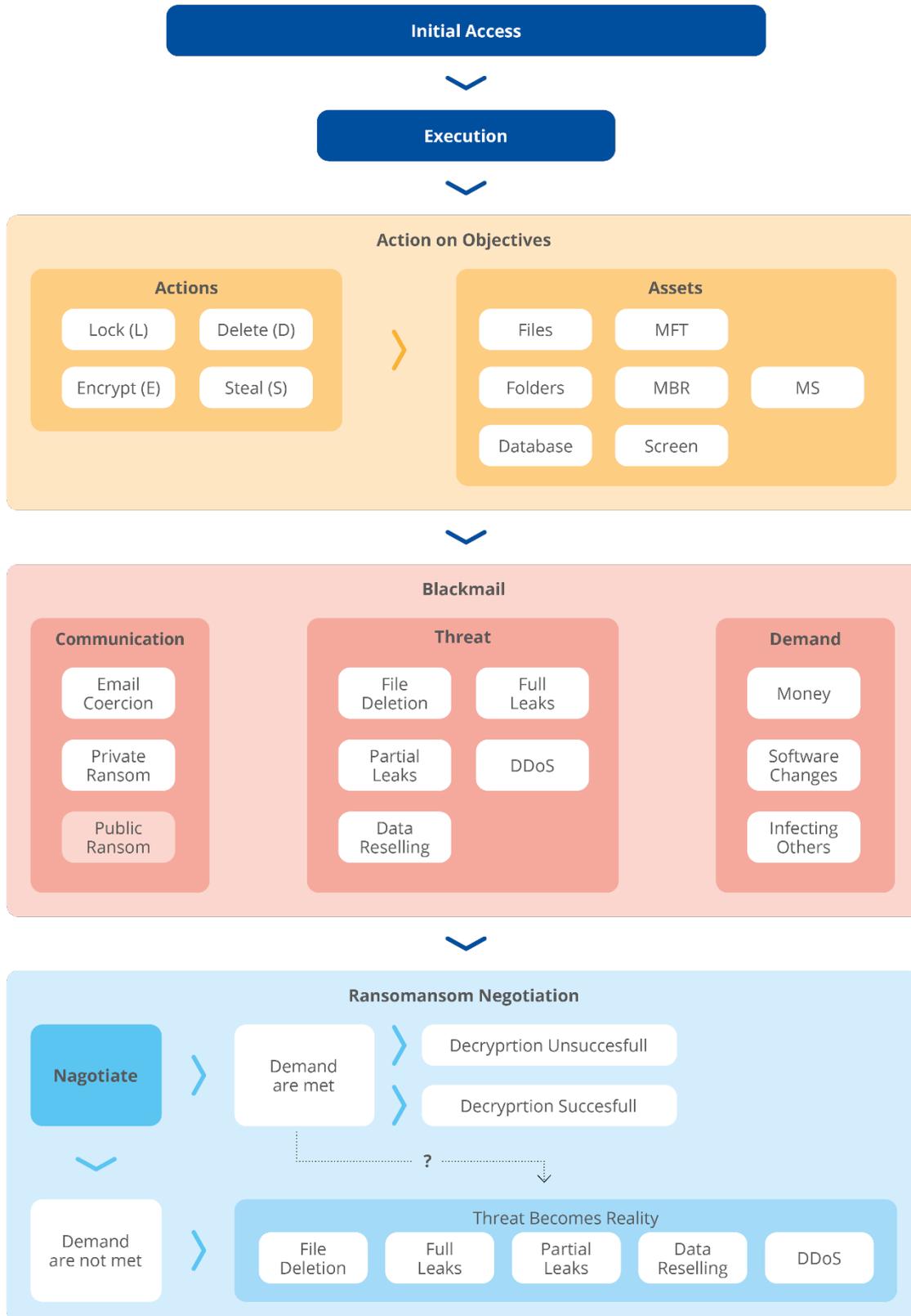
3.1 INITIAL ACCESS

The first stage of a ransomware attack is the initial access to the target. Ransomware uses the same techniques for getting access as other attacks may use, including exploiting software vulnerabilities, access through stolen credentials, phishing and others. In this report, we will not cover how these techniques have changed.

It is very challenging to find out what were the current initial access techniques used by ransomware against targets. The problem is due to the lack of incident reporting by compromised organisations which leads to reduced information sharing and relevant lessons learned. Public statements reporting the incidents are rare, and in the few cases where they are reported, they do not include details on how the attack happened, what ransomware attacked them, what they possibly took and what ransom was demanded. Many times, information is not shared because it may not be known or because the victims fear further adversarial actions by the threat actors or, most commonly, because they wish to avoid perceived reputational damages.

3.2 EXECUTION

After initial access, threat actors may study the target, move laterally to other computers and employ attack techniques[14] to ensure more assets are found to be exploited. This activity may take several weeks depending on the threat actor and the size and defences in place by the target. This movement is usually completed before the ransomware starts working, although when the ransomware starts it can also move laterally inside the victim's network.

Once the assets are located and before the ransomware is executed, there is usually a cleaning part where some actions are taken to ensure the correct working of the ransomware, such as: kill the security software, stop programs like databases that can interfere with the writing, stop the recovery features of systems, shadow copies, logs, etc.

The next step is the deployment of the ransomware. The ransomware can be deployed directly or it can be deployed by third parties using botnet-based malware delivery, such as in the case of Ryuk ransomware that used TrickBot and Emotet as delivery mechanisms[15].

3.3 ACTION ON OBJECTIVES

Once deployed, the ransomware attacks the availability and/or the confidentiality of the targeted assets through a series of actions. This stage is traditionally known as Action on Objectives[16]. The full capabilities of ransomware are discussed and mapped in Table 1. Ransomware actions are not immediate and can take place weeks after the initial infection of the system, giving attackers additional time to access more internal systems.

There is no guarantee that the encryption has been done correctly and that files could be decrypted after payment is completed. This is one additional reason why paying a demand for ransom is not a recommended approach, since there are no guarantees that it will be effective.

3.4 BLACKMAIL

After the availability of assets has been compromised, the threat actor then proceeds to blackmail the target to obtain a ransom in return for the availability of the assets. The three main components of blackmail are communication, threat and demand. *Communication* is the act of informing the target what is happening, e.g. the asset is no longer available. The *threat* is the

---

[14] Tactics - Enterprise | MITRE ATT&CK®'. https://attack.mitre.org/tactics/enterprise/ (accessed Jul. 02, 2022).
[15] Ryuk 2020: Distributing Ransomware via TrickBot and BazarLoader - Security News'. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader (accessed Jul. 02, 2022)
[16] Lockheed Martin, 'GAINING THE ADVANTAGE. Applying Cyber Kill Chain® Methodology to Network Defense', 2015. Accessed: Jul. 02, 2022. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

loss or damage that will occur if the demand is not met. The *demand* is what the threat actor expects to obtain from the situation.

The communication of ransom demands changed in the last decade, moving from private communication to more public communication. Earlier, a ransom note was shown on the affected systems with instructions on what to do to pay and get the data back, and how to communicate privately with the threat actors to negotiate. Nowadays it is common for threat actors to publicly showcase ransom incidents, including information on the assets affected, the ransom demands, and often publicly discrediting the target. It is also nowadays common for some threat actors to coerce not only the targets but also their customers, partners and interested parties thus piling up the pressure on the target.

The threats made in ransom demands have also evolved, with new forms of coercion being introduced. Currently, organisations are threatened with partial and full data leaks, deletion of the assets, and reselling data to the highest bidder (oftentimes competitors of the target). Targets are also threatened with distributed denial of service attacks (DDoS) against an organisation's infrastructure, which will only stop after successful negotiation of the ransom payment.

Ransomware demands have also evolved but in a smaller proportion. The primary demand is still monetary, attempting to obtain a financial profit from the ransom payments. When the target pays and the threats do not materialise, the threat actor gains reputation and notoriety with the public, allowing them to continue their operations. However, demands are not always monetary. There is ransomware that has requested companies to add or remove software features in their products[12] or ransomware that asks targets to infect other people in order to obtain free decryption keys[13].

3.5 RANSOM NEGOTIATION

The ransomware negotiation is generally a private communication, if any, between the target and the threat actors. We need to stress again that this is not a recommended step, nonetheless from an incident life cycle perspective we need to examine it since it has taken place in some incidents. There are two outcomes to this negotiation: targets pay the ransom or do not pay. It is not uncommon to hear that target organisations or individuals have successfully negotiated with the threat actors to lower the ransom money demanded.

Unfortunately, it is extremely hard to quantify who paid or did not pay the ransom and in which cases a lower ransom was agreed upon. This information is not commonly made publicly available. Often, there are reports where the total earnings of the threat actors are reported but not on an individual level. There are also threat actors that, after a successful payment, remove the compromised target name from their public website. However, it is not safe to generalise and assume that all targets that are no longer on the web page paid a ransom fee, as in many cases ransomware websites are buggy and unstable. Moreover, basing assessments on the claims of cyber criminals is not a reliable source.

4. RANSOMWARE MODELS

Ransomware has significantly evolved, both technically and organisationally, since the first incident was observed in 1989[17]. The market has matured to such a degree that ransomware has become a commodity[18]. With the new ransomware-as-a-service business models, almost anyone can conduct a ransomware attack. You can buy it as a part of your larger operation, and there are no significant differences between one ransomware family and another. However, the ransomware organisation, like other malware underground, is complex, with multiple actors, roles, problems, solutions and culture. Our exploration of the business models of ransomware depicts a high level view of how threat actors create, organise and obtain value from ransomware attacks[19].

4.1 INDIVIDUAL ATTACKERS

Initially, ransomware attacks were conducted by single individuals or very small groups. These ransomware attacks were less complex than attacks today, often focusing on automatic encryption that did not require operational coordination. The focus of the attackers was on the development and spread of the ransomware. It is very hard to know which groups started as single individuals and how long they remained like that. Many threat actors probably started as small groups as it seems the operation required plenty of work and coordination so eventually all actors needed the organisation of a small group[20].

4.2 GROUP THREAT ACTORS

In what is now considered the *traditional* ransomware business model, a single group threat actor is composed of multiple individuals that share and split and coordinate all the stages of the operation: picking the target, analysing the target for vulnerabilities, conducting the attacks, producing the malware and infection, coordinating the file encryption keys, negotiating the ransom payment, and getting the revenue. The same group also generally develops all their tools, sets the payment system, and buys exploits or the information required to conduct successful attacks. This business model is still the main organisational choice even though new opportunities have appeared, such as ransomware-as-a-service.

4.3 RANSOMWARE-AS-A-SERVICE

Ransomware-as-a-Service (RaaS) is a type of business model where threat actor groups offer their software platform to external affiliates to conduct attacks[21]. Affiliate markets are well known in the cybercrime organisation. The affiliate programme is operated by a threat actor group (RaaS operator) and it incorporates external affiliates that use the malware and payment platform. This RaaS model probably emerged due to the success in the *Group Threat Actor* type

[17] KnowBe4, 'AIDS Trojan | PC Cyborg | Original Ransomware | KnowBe4'. https://www.knowbe4.com/aids-trojan (accessed Jul. 02, 2022).

[18] '2021 the year of commodity ransomware, says Sophos', ComputerWeekly.com. https://www.computerweekly.com/news/252492290/2021-the-year-of-commodity-ransomware-says-Sophos (accessed Jul. 02, 2022)

[19] A. Osterwalder and Y. Pigneur, Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. John Wiley & Sons, 2010.

[20] D. S. Wall, 'Inside a ransomware attack: how dark webs of cybercriminals collaborate to pull them off', The Conversation. http://theconversation.com/inside-a-ransomware-attack-how-dark-webs-of-cybercriminals-collaborate-to-pull-them-off-163015 (accessed Jul. 02, 2022).

[21] Abnormal, 'The Evolution of Ransomware: Victims, Threats, Actors, and What to Expect in 2022', 2022. Accessed: Jul. 03, 2022. [Online]. Available: https://cdn2.assets-servd.host/gifted-zorilla/production/files/Ransomware-Trends-Victims-Threat-Actors.pdf

of business model where, after earning substantial money, the opportunity arose to share the malware platform developed, the data obtained, the targets infected, and the expertise in the area.

The *RaaS operators* develop the ransomware and provide the software platform for affiliates to operate. The *RaaS affiliates* conduct the ransomware attacks, the payment negotiation, collect the ransom and also purchase additional exploits or information needed to conduct the attacks[22]. This type of business model allows the RaaS operators to have multiple revenue streams. One source of income is a percentage of the ransom payment to the affiliates, often 10-20% or more[23]. Other sources of income can be selling data about targets, monthly subscriptions that affiliates pay to access the platform[24], or consultancy to other threat actors[25].

RaaS has lowered the entry-level barrier to conduct ransomware attacks. Attackers now do not need to know how to write their own ransomware. They need to know only how to conduct an attack, and the RaaS operators will provide the ransomware and the platform to operate. Anyone can attack, and anyone can become a target. RaaS platforms also introduce a new level of anonymity into the cybercrime operations, as it is rarely known who the attacker really is while operating as an affiliate. It is now easier than ever to get into ransomware as an affiliate, profit and retire quickly, as has already been witnessed with some threat actors[25].

4.4 DATA BROKERAGE

Ransomware threat actors are moving towards a new business model referred as *Data Brokerage*. In this model, threat actors take further advantage of the stolen data by selling it to the highest bidders[26]. This also includes reselling the access obtained to the target to other threat actors for additional exploitation[2] [27] https://www.zotero.org/google-docs/?qKoeHt.

4.5 NOTORIETY AS KEY TO A SUCCESSFUL RANSOMWARE BUSINESS

Ransomware demands are mostly financially motivated. In order to succeed in the business, ransomware needs to demonstrate a guarantee that decryption will work. Usually, threat actors have mechanisms to show that the decryption works, such as decrypting sample files.

The ransomware operators need to maintain a certain reputation of notoriety, otherwise, victims will not pay the ransom. The reputation of ransomware groups also depends on how well they keep their word. Many attackers promise that upon payment they will remove the companies from their websites, delete the stolen data and not leak data to the public. A report shows that in 18% of cases the companies that paid the ransom still got their data leaked, and 35% of the victims that paid the ransomware were unable to retrieve their data[28].

Notoriety and reputation is nearly impossible to measure, however, a 2021 report showed that 60% of respondents that reported ransomware incidents did actually negotiate with their attackers, showing that victims perceive threat actors to be worthy interlocutors[28].

Although ransomware threat actors seem to have kept their word in some cases, one needs to realise that there is no guarantee that payment of a ransom will lead to solutions and standing

---

[22] V. Ray, 'Understanding REvil and the Rise of Ransomware Business Models'. https://www.thefastmode.com/expert-opinion/20759-understanding-revil-and-the-rise-of-ransomware-business-models (accessed Jul. 02, 2022)
[23] Threat Assessment: BlackCat Ransomware', Unit 42, Jan. 27, 2022. https://unit42.paloaltonetworks.com/blackcat-ransomware/ (accessed Jul. 02, 2022).
[24] 'Ransomware as a Service' as a Business Model: Why the Business of Extortion Flourishes', Greenbone Networks, Nov. 26, 2021. https://www.greenbone.net/en/ransomware-as-a-service/ (accessed Jul. 02, 2022).
[25] Ransomware Unmasked: Dispute Reveals Ransomware TTPs', May 26, 2021. https://geminiadvisory.io/ransomware-unmasked-dispute-reveals-ransomware-ttps/ (accessed Jul. 02, 2022).
[26] What Is a Data Broker and How Does It Work? - Clearcode Blog', Clearcode | Custom AdTech and MarTech Development, Feb. 04, 2019. https://clearcode.cc/blog/what-is-data-broker/ (accessed Jul. 02, 2022).
[27] '3 Dark Web Intelligence Trends for Security Teams to Monitor', ZeroFox, May 05, 2021. https://www.zerofox.com/blog/3-dark-web-intelligence-trends-for-security-teams-to-monitor/ (accessed Jul. 02, 2022).
[28] Ransomware extortion doesn't stop after paying the ransom', BleepingComputer. https://www.bleepingcomputer.com/news/security/ransomware-extortion-doesnt-stop-after-paying-the-ransom/ (accessed Jul. 02, 2022)

down operations by threat actors. Negotiating with cyber criminals is not recommended and, in the case of ransomware incidents, contacting law enforcement and national cybersecurity authorities is the recommended course of action.

Moreover, there are operational problems that directly impact the trust of the ransomware actors and the whole ecosystem. Ransomware threat actors need infrastructure to work, but this infrastructure has turned out to be very unreliable, with websites not updated, links to public leaks expiring, data not available, and websites going down. This instability generates uncertainty among victims, since it is not easy to confirm whether a ransomware attack actually happened and whether files were really stolen, hence once again contacting authorities should be pursued.

5. ANALYSIS OF RANSOMWARE INCIDENTS

After presenting and defining ransomware, this section provides an analysis of sample incidents between May 2021 and June 2022, showing the lay of the ransomware landscape and its characteristics.

Before presenting the results it is important to clarify what is considered a ransomware incident for the purposes of this analysis. A *ransomware incident* is a successful attack in which a threat actor manages to access a target, perform any LEDS action (Lock, Encrypt, Delete, Steal) on the target's assets, and perform blackmail. Note that the ransom negotiation is not needed – and certainly not encouraged – to consider an attack a ransomware incident.

Our analysis considers **623** ransomware incidents worldwide with a special focus on Europe, the United Kingdom and the United States. These incidents were selected from news reports, the reports of security companies, government reports and the original sites of the ransomware threat actors. Each incident was explored in depth and confirmed from multiple sources.

5.1 DATA SAMPLING TECHNIQUE

It is important to understand the limitations of the data gathering process. To search, find and collect the ransomware incidents in this report, different sources of data were used, such as government reports, security company reports, news media reports, the dark web and sometimes verified blogs. The sources were then processed, analysed and aggregated to extract as much information about an incident as possible. In some ransomware incidents the research has been a challenging task, as there was not enough available information.

The real total number of ransomware incidents in the period May 2021 to June 2022 is very hard to estimate, due to many organisations not reporting the incidents and threat actors deleting incidents from their pages.

Classifying the numbers of incidents on the basis of the source from which the relevant information has been extracted is important, as it illustrates the level of trust in the collected data.

 Four types of *number of incidents* can be considered in this regard:

1. The real number of ransomware incidents

2. The number of ransomware incidents reported to governments

3. The number of ransomware incidents reported by news media and security companies

4. The number of ransomware incidents reported by ransomware groups on their web pages

The real number of ransomware incidents is the real population of ransomware incidents in the world. It is known that many organisations do not acknowledge incidents publicly, thus making this number almost impossible to obtain.

The number of ransomware incidents reported to governments is the number of organisations that contacted a government to ask for assistance and report the attack. For example, in 2021, the FBI Crime Report from the Internet Crime Complaint Centre (IC3)[29] received **3,729** complaints identified as ransomware.

The number of ransomware incidents reported by news media and security companies is more commonly reported but heavily biased towards the importance of the attacked organisation. For example, from April 2021 to April 2022 the Sophos IT security company indirectly reported **3,696** ransomware incidents (from 5,600 respondents in a survey of whom 66% had ransomware)[30].

The number of ransomware incidents reported by ransomware groups on their web pages is the most real account of incidents, but it is difficult to measure due to the instability of the ransomware infrastructure. These incidents are often deleted or changed, web pages are taken down or have migration issues. However, some organisations web-scraping threat actors' websites[31] reported **2,252** incidents in 2021, and **1,858** from January to June 2022.

We estimated that the total number of incidents from May 2021 to June 2022 was **3,640**[32] . Since this report analyses 623 incidents, it therefore covers **17.11%** of the total estimated cases in that time frame. All results and conclusions as presented should take into account this disclaimer concerning the number of incidents used in this analysis.

More importantly, it becomes evident from the varying numbers concerning how many ransomware incidents took place that there is an issue with reporting such incidents. Making detailed analysis and mitigating the ransomware threat necessitates a better understanding of the threat landscape and to do so, more efficient and effective incident reporting is necessary. In addition, the fact that we were able to find publicly available information for 17.11% of the cases highlights that when it comes to ransomware, only the tip of the iceberg is exposed and the impact is much higher than what is perceived.

5.2 STATISTICS ABOUT THE INCIDENTS
To qualitatively analyse the 623 incidents we studied each incident in further detail (using publicly available information) and extracted information about the following categories.

Categories	Description
Target	Name of the organisation targeted.
Industry sector	Industry sector of the target
Country	Country of the target
Threat actor	Name of the threat actor
Initial access techniques	MITRE ATT&CK® category of the technique used to compromise and access the target

---

[29] 'Internet Crime Report 2021', Federal Bureau of Investigation, 2021. Accessed: Jul. 02, 2022. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[30] Ransomware Report: Sophos State of Ransomware Report Download', SOPHOS. https://www.sophos.com/en-us/content/state-of-ransomware (accessed Jul. 02, 2022).
[31]josh!, ransomwatch 👀 🕵. 2022. Accessed: Jul. 02, 2022. [Online]. Available: https://github.com/joshhighet/ransomwatch/blob/fe3b0cf47bf439b10c3e69581a47346404a491b3/posts.json
[32] The IC3 for 2021 reported 3,743 incidents, an average of 312 incidents per month. Ransomware Watch for 2021 reported 2,252, an average of 188 incidents per month. Sophos for Apr 2021 to Apr 2022 reported 3,696 incidents, an average of 308 incidents per month. Ransomware Watch from Jan 2021 to June 2022 reported 1,858 incidents, an average of 310 incidents per month. The average of the average incidents per month is (312 + 188 + 308 + 310) / 4, which equals 280 incidents per month. Therefore, from May 2021 to June 2022 (inclusive) there are 13 months and an estimated total of 280*13 = 3,640 incidents.

Was the ransom paid?	Any confirmation on whether the ransom was paid
Was data stolen?	Whether any type of data was stolen
Volume of data stolen	The size of the data stolen in Gigabytes
Type of data stolen	The category of the type of data stolen (personal data, financial data, intellectual property, etc.)
Leaked data	Confirmation whether the data was partially or fully leaked after the blackmail

5.3 VOLUME OF DATA STOLEN

Of the 623 incidents included in the report, we found proof of data leaks for 288, which is 46.2% of the total incidents. The total accumulated stolen data for all incidents is 136.3 TB with an average of 518 GB per incident and an average of 10 TB per month. The maximum volume of stolen data found in one incident alone was 50 TB; this was stolen from Brazil's Ministry of Health (MoH) by the Lapsus$ threat actor[33]. The timeline shown in Figure 5 illustrates the cumulative amount of data stolen per month.

5.4 AMOUNT OF LEAKED DATA

There are two main ways in which data can be leaked in a ransomware incident. First, data can be *partially leaked* by threat actors to prove that they actually stole the data or to blackmail targets to pay the ransom. Second, as a result of a failed ransom negotiation where threat actors usually do a *full data leak* of the stolen data. The full data leak usually contains all the stolen data.

Many different platforms are used to leak the stolen data. Threat actors may use their own websites, cloud providers, or the group's Telegram channel. Cloud providers usually take down the leaks due to privacy concerns, but the leaks hosted on the attackers' website remain available, as well as on Telegram.

Of the 623 incidents analysed, evidence was found of partially leaked data in 62 incidents, 9.95% of the total incidents. Similarly, evidence was found of fully leaked data in 236 incidents, which is 37.88% of the incidents. In total, in almost half of the cases (47.83%) stolen data was leaked.

5.5 TYPE OF LEAKED DATA

More than 136 terabytes of data was stolen in the 623 incidents analysed. In 31% of the incidents, attackers provided an insight into the type of data stolen, which often included personal and business information.

5.6 PERSONAL DATA

In Europe, the General Data Protection Regulation (GDPR) defines personal data as 'any information which is related to an identified or identifiable natural person'[34].and protects them[35].

---

[33] 'Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes', ZDNet. https://www.zdnet.com/article/brazilian-ministry-of-health-suffers-cyberattack-and-covid-19-vaccination-data-vanishes/ (accessed Jul. 02, 2022)
[34] Personal Data', General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/personal-data/ (accessed Jul. 02, 2022).
[35] EUR-Lex - 32016R0679 - EN - EUR-Lex'. https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed Jul. 02, 2022).

Our analysis shows that 58.2% of all the stolen data contains GDPR personal data. This personal data ranges from protected health information (PHI), passport numbers and visas, to addresses and covid status.

In countries outside the European Union, personal data is classified into two types, personal identifiable information (PII) and personal protected information (PPI). PII is any data that could potentially identify a specific individual[36], whereas PPI is personal information that is important but not necessarily used to identify an individual[37].

Our analysis shows that 33% of the stolen data includes employee PII and 18.3% includes customer PII. In contrast, only 0.4% of the stolen data includes employee PPI and 3.8% includes customer PPI.

5.7 NON-PERSONAL DATA

Additionally, 41.7% of the stolen data contains non-personal data. *Non-personal data* is any information that is not related to identifiable natural persons. This data contains information that directly impacts the targeted business, such as financial information, blueprints, insurance, market research, internal network data, and more.

Of the stolen data, 19% contains financial information. *Financial information* refers to business data related specifically with the financial aspects of the business. This data may include departmental budgets, receipts, income declarations, financial statements, and more.

More than 24% of the data stolen contains business information. *Business information* refers to data that is important for the company business, such as production data, administrative documents, legal files, commercial registrations, NDAs (Non-Disclosure Agreements), and more.

5.8 INCIDENTS PER COUNTRY

The estimation of incidents per country (shown in Figure 2) is biased by our data selection process since this report focuses on incidents primarily in Europe, the United States and the United Kingdom. Accordingly, the results present an interesting yet not fully representative overview, since as discussed above, reported incidents and publicly available information is scarce.

Of the 623 incidents analysed, we found that the top three countries attacked are the United States with 112 incidents, Germany with 96 incidents, and France with 78 incidents.

---

[36] 'What is PII (Personally Identifiable Information)? Definition from SearchSecurity', SearchSecurity. https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII (accessed Jul. 02, 2022)
[37] Protected personal information Definition', Law Insider. https://www.lawinsider.com/dictionary/protected-personal-information (accessed Jul. 02, 2022)

Figure 2: Number of ransomware incidents in each country based on 623 incidents analysed
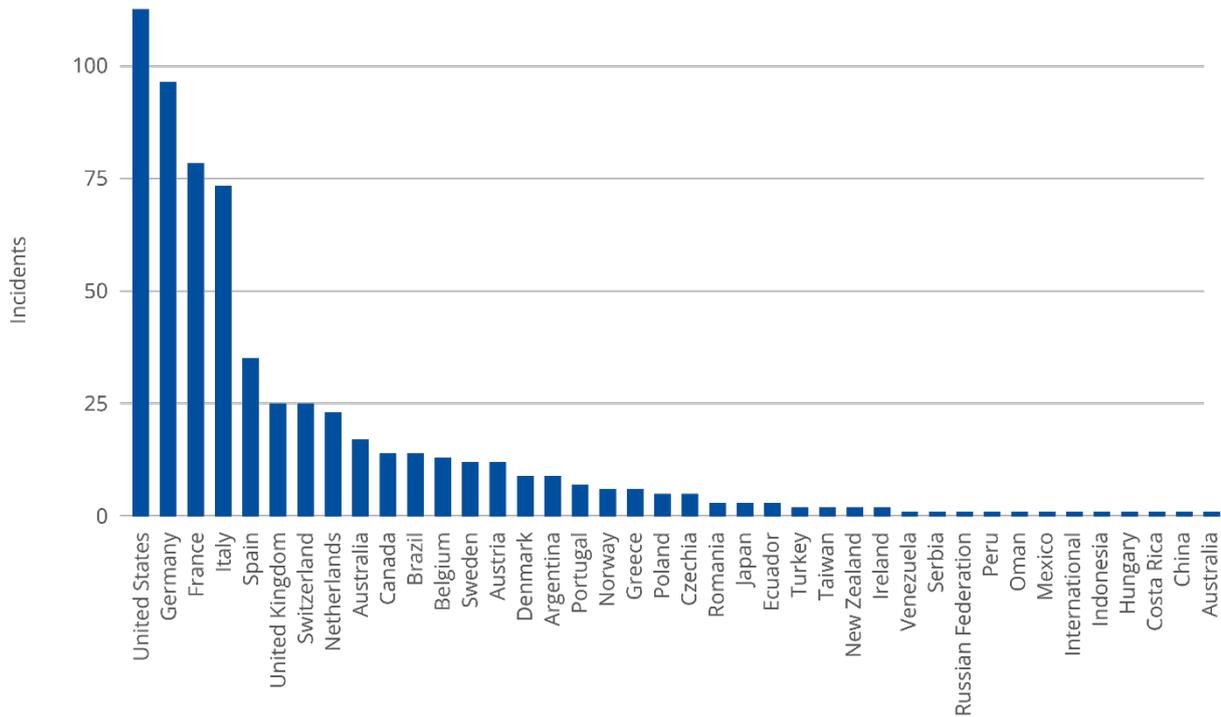
5.9 INITIAL ACCESS TECHNIQUES

To understand how ransomware initially accessed the targets we analysed reports of the incidents and the capabilities of the ransomware threat actors[38]. We have summarised some of the most common initial access techniques observed according to the MITRE ATT&CK framework[39].

MITRE ATT&CK techniques for initial access
T1133 External Remote Services: Exploited remote desktop
T1133 External Remote Services: RDP Brute Force[40]
T1133 External Remote Services: Exploited terminal services
T1189 Drive-by Compromise
T1189 Drive-by Compromise: Exploit kits
T1203 Exploitation for Client Execution: Exploiting Software Vulnerability
T1068 Exploitation for Privilege Escalation Error! Bookmark not defined.
T1078 Valid Accounts
T1566.001 Phishing: Spear phishing Attachment
T1566.002 Phishing: Spear phishing Link
T1195 Supply Chain Compromise

---

[38] Protected personal information Definition', Law Insider. https://www.lawinsider.com/dictionary/protected-personal-information (accessed Jul. 02, 2022)
[39] MITRE ATT&CK framework https://attack.mitre.org/
[40] AdvIntel, 'Adversary Dossier: Ryuk Ransomware Anatomy of an Attack in 2021', AdvIntel, Apr. 16, 2021.
https://www.advintel.io/post/adversary-dossier-ryuk-ransomware-anatomy-of-an-attack-in-2021 (accessed Jul. 02, 2022)

Out of the studied 623 incidents, it was not reported how the threat actors got initial access in 594 of them, which is an overwhelming 95.3%. It is understandable that targets don't want to share how they were (or still are) vulnerable for security reasons but at the same time the lack of information does not help others to realise what they should improve or how they can also be a victim in the future.

From the rest of the known 29 incidents for which initial access was leaked, there is small amount of data upon which to draw conclusions; the distribution is as follows.

INITIAL ACCESS according to MITRE	No of Incidents
T1133 External Remote Services	12
T1566 Phishing	8
T1195 Supply Chain Compromise	4
T1078 Valid Accounts	4
T1068 Exploitation for Privilege Escalation	1

5.10 PAID RANSOM

It is very difficult to know whether targets paid the ransom or not, since most targets do not share this information publicly and in many countries it is illegal to pay and in any case it is discouraged. Moreover, sometimes targets want to pay a smaller amount of ransom but the threat actor refuses, and the data is leaked anyway[41]. **From all the incidents analysed, it was not possible to confirm whether a ransom was paid in 588 cases, which is 94.2%. Out of the rest of the incidents in our analysis, 8 paid the ransom and 58 did not pay the ransom.** Once again, this gap in incident reporting limits our understanding and thus our ability to perform a proper analysis and mitigate the threat of ransomware; therefore solutions to this problem need to be examined.

Interestingly, from our previous analysis of leaked data, we found that 37.88% of the targets had their data fully leaked on the Internet. This *suggests*, but does not *imply*, that around 62.12% of the incidents might have actually paid the ransom, and that is why their data was not leaked. Of course, there are many mitigating situations, such as targets that paid and their data was leaked anyway, or targets that did not pay and their data was not leaked. However, the estimation of 62.12% is very close to the result of a survey from the *Claroty* security company that found that 62.14% of the respondents confirmed that their company paid the ransom[42]. Although these numbers should not be taken as a guide because they are merely indicators, they certainly bring the problem into focus.

5.11 INCIDENTS IN EACH TYPE OF SECTOR

A meaningful statistic can be derived from the number of ransomware incidents in each sector. However, special attention must be paid to the fact that the categorisation process we did of each target in a sector is slightly biased because a target can belong to many categories. **Figure 3 shows a comparison of the number of incidents in each sector. This graph suggests that ransomware is targeting all sectors indiscriminately and that no type of industrial sector is safe.**

---

[41] 'Hackers post hundreds of pages of purported internal D.C. police documents', Washington Post. Accessed: Jul. 02, 2022. [Online]. Available: https://www.washingtonpost.com/local/public-safety/dc-police-hackers-ransomware-babuk/2021/05/13/d0280fb4-b3f7-11eb-a980-a60af976ed44_story.html
[42] The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption'. https://security.claroty.com/report/global-state-industrial-cybersecurity-survey-2021 (accessed Jul. 02, 2022).

Figure 3: Comparison of the number of ransomware incidents for each sector
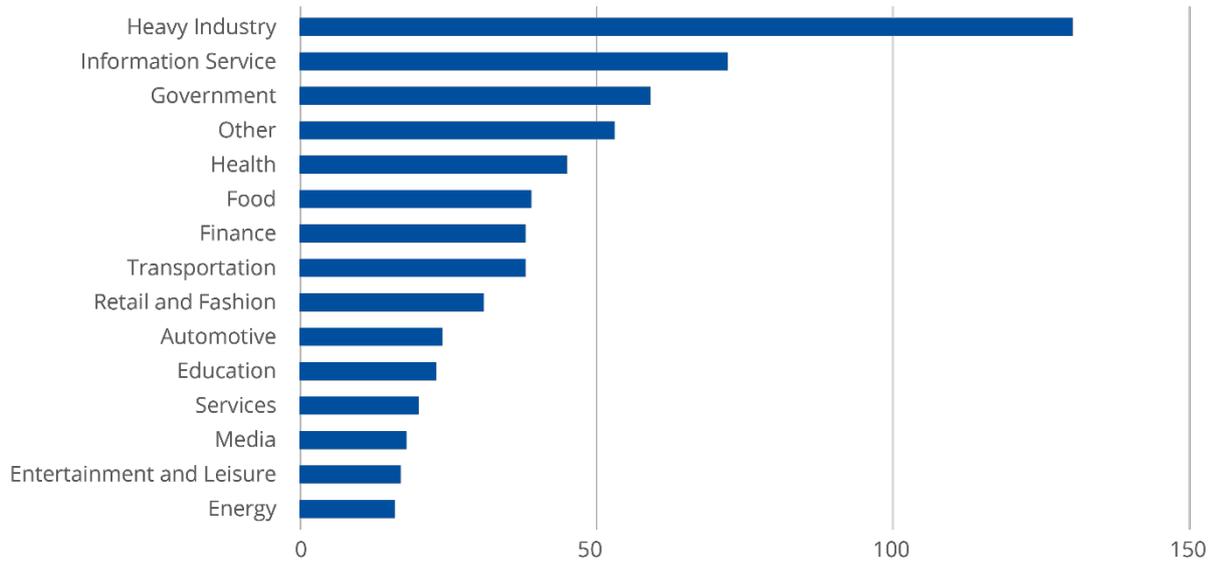

5.12 NUMBER OF INCIDENTS CAUSED BY EACH THREAT ACTOR

Ransomware threat actors, as with any other group of cybercriminals, are often taken down or they go out of business. However, unlike other cyberthreat groups, when it comes to ransomware threat actors publicly share and take attribution for their attacks. **From the 623 incidents analysed, only 22 incidents show no confirmation of** *which threat actor* **was behind the attack, amounting to only 3.5% of all incidents. Therefore the threat actor was known in 96.5% of cases.** This is in stark contrast to other cybersecurity threats, where the identity of the threat actors is not actively published. However, the ransomware business model works on increasing the visibility and notoriety of ransomware groups and actors, hence the difference.

Our analysis in Figure 4 shows that the incidents were carried out by 47 unique ransomware threat actors. The top 3 attackers are Conti, LockBit and Hive, which should come as no surprise given how prolific these threat actors have been in the past year[43]. However, these total numbers should not be taken as a strong guideline since our selection process slightly biased this evaluation by choosing at least 5 incidents from each threat actor.

---

[43] 'LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022 - Security News'. https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022 (accessed Jul. 02, 2022)

**Figure 4**: Number of ransomware incidents caused by each threat actor
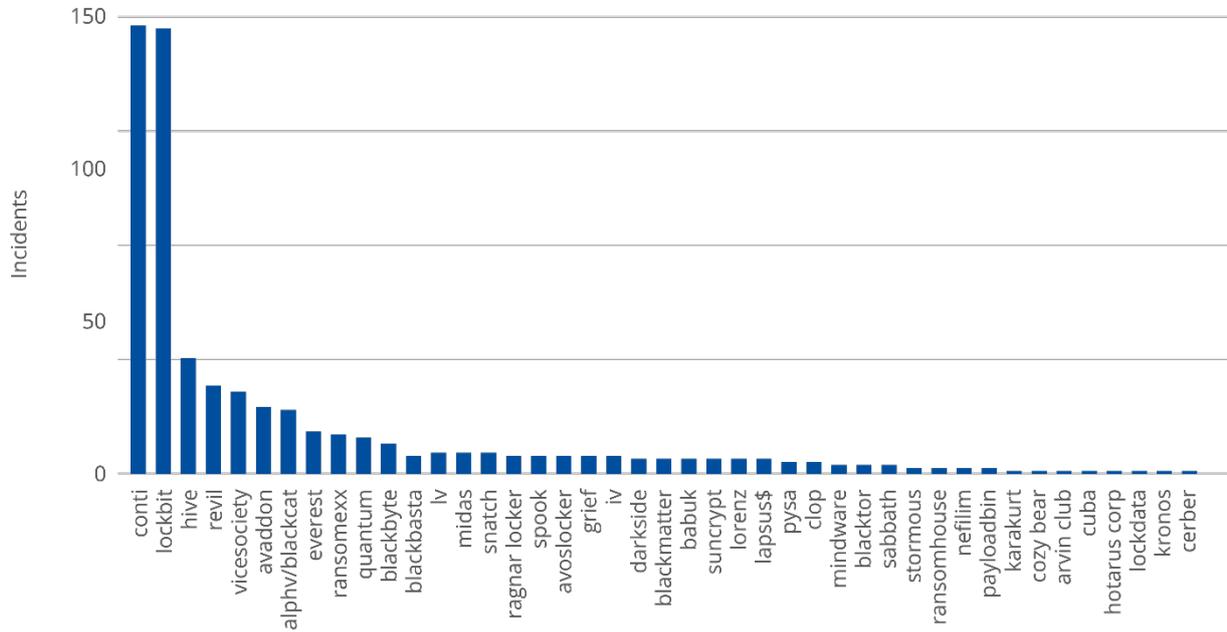
5.13 TIMELINE OF RANSOMWARE INCIDENTS

The 623 ransomware incidents analysed from May 2021 to June 2022 are shown in a timeline in Figure 5. This timeline highlights the number of incidents and the cumulative data stolen.

The number of incidents each month, shown in the vertical red colour bars above the horizontal line, is built using the date of when the incident was reported and not when the attack happened, which could have taken place weeks before. Curiously enough, researchers often need to rely on ransomware websites to obtain this data due to the lack of transparency when it comes to reporting ransomware incidents.

The cumulative amount of data stolen in terabytes (TB), shown in the vertical blue colour bars below the horizontal line, should be understood as a base value, given that in more than 50% of the incidents this information was unknown. **The cumulative amount of data stolen should also highlight the impact of ransomware, given that in at least 47% of the incidents the stolen data was partially or fully leaked.**

Figure 5: Timeline of ransomware incidents from May 2021 to June 2022. In red bars the number of ransomware incidents is shown. In blue bars the cumulative amount of stolen data is shown

.
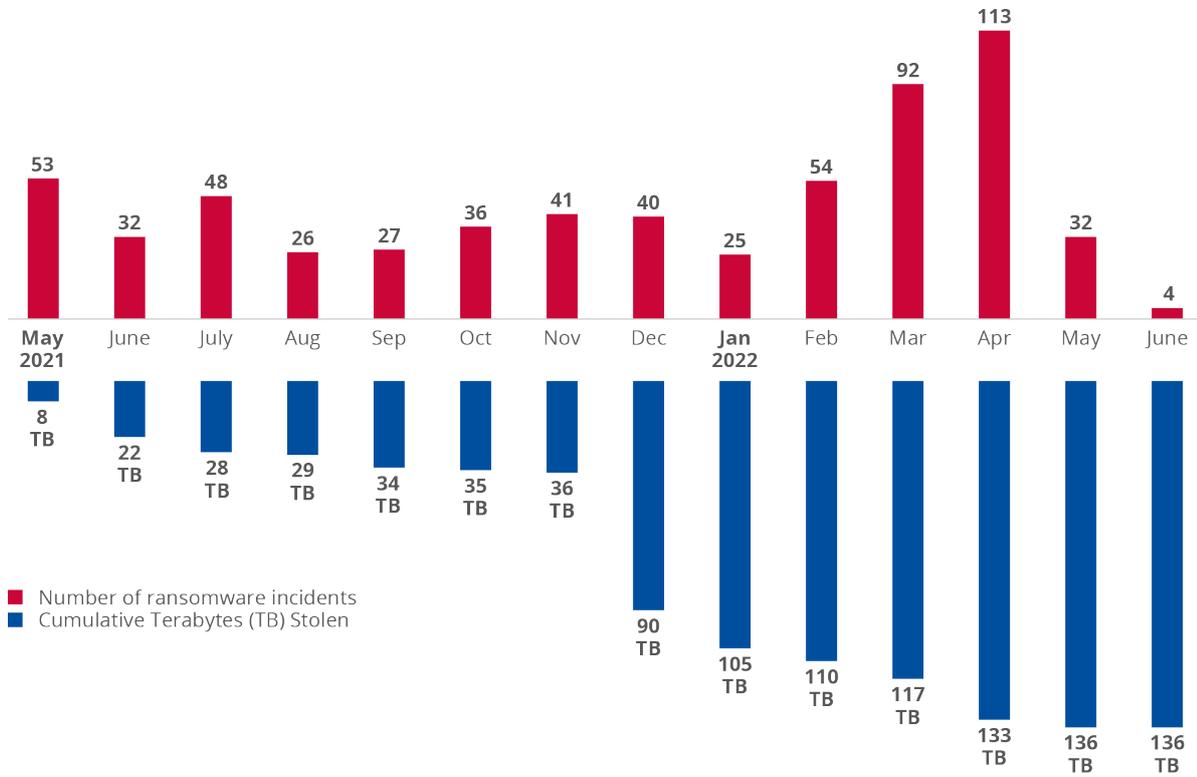
6. RECOMMENDATIONS

Ransomware attacks are a global problem, affecting organisations of all sizes across all sectors. This threat landscape aims to identify the issues and challenges related to ransomware, to highlight important trends and identify opportunities on how to improve the fight against ransomware.

The reality shows that ransomware can have devastating effects on organisations if they are not well prepared. In this section we present general recommendations that can help organisations deal better with the problem of ransomware. The recommendations focus on several key aspects: preparing against ransomware attacks and decreasing the impact of ransomware as well as the decision to pay.

6.1 RESILIENCE AGAINST RANSOMWARE

The techniques attackers use are continuously evolving and they are finding new ways to compromise targets. Organisations should not think whether they may suffer a ransomware attack but when it will happen. These recommendations should help organisations prepare for a ransomware attack before it happens and during its aftermath.

- Have a good and verified backup of all your business-critical files and personal data and keep it updated, and isolated from the network[44].

- Apply the 3-2-1 rule of backup. For all data: 3 copies, 2 different storage media, 1 copy offsite[45].

- Keep personal data encrypted according to the provisions of GDPR and using appropriate risk-based controls[46].

- Run security software in your endpoint devices that can detect most ransomware.

- Maintain your security awareness[47], security policy, and privacy protection policy up to date and working on your information systems and assets to accomplish desired hygiene by industry best practices such as network segmentation, up to date patches, regular backups, and appropriate identity, credential, and access management (ICAM) preferably with support of MFA. This that basically result in a good security hygiene[48]

- Conduct regular risk assessment and consider taking out ransomware insurance[49] based on this assessment.

- Restrict administrative privileges: use caution when handing out administrative privileges as the admin account has access to everything, including changing configurations or bypassing critical security settings. Always employ the Principle of Least Privilege (PLOP) when granting any type of access[50].

---

[44] Simple Steps for Internet Safety', Federal Bureau of Investigation. https://www.fbi.gov/news/stories/simple-steps-for-internet-safety (accessed Jul. 04, 2022)
[45] 'Backup', Wikipedia. Jun. 29, 2022. Accessed: Jul. 04, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Backup&oldid=1095660717
[46] See https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures
[47] The Avira Security Wordbook', Official Avira Support | Knowledgebase & Customer Support | Avira. https://support.avira.com/hc/en-us/articles/360002408618 -The-Avira-Security-Wordbook (accessed Jul. 04, 2022)
[48] Ransomware Guide | CISA'. https://www.cisa.gov/stopransomware/ransomware-guide (accessed Jul. 04, 2022)
[49] 'Cyber Insurance is Supporting the Fight Against Ransomware'. https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-supporting-fight-against-ransomware.html (accessed Jul. 04, 2022)
[50] K. Yasar, '10 Critical Steps to Take After a Ransomware Attack', MUO, Dec. 15, 2021. https://www.makeuseof.com/ransomware-attack-steps-to-take/ (accessed Jul. 04, 2022)

- Familiarise yourself with local government agencies that provide assistance on ransomware incidents and define protocols to follow in case of an attack.

6.2 RESPONDING TO RANSOMWARE

Should an organisation or an individual fall victim to ransomware attacks, several recommendations have been put forward, but the most important one is the first one, namely, contacting the authorities.

- Contact the national cybersecurity authorities or law enforcement on how to handle and how to deal with ransomware[51].

- Do not pay the ransom and do not negotiate with the threat actors.

- Quarantine affected systems: cutting off affected systems from the network is suggested in order to contain the infection and stop the ransomware from spreading[50].

- Visit The No More Ransom Project, a Europol initiative that can decrypt 162 variants for ransomware[52].

- Lock down access to backup systems until after the infection gets removed[50].

Furthermore, sharing information with the authorities about the ransomware incident is highly recommended. Such information sharing can lead to better lessons learned to assist other potential victims, can assist the authorities and security researchers and responders to better handle incidents and identify threat actors, and can provide more reliable data to map the threat landscape and its evolution. **Information sharing is one of the cornerstones of cybersecurity.**

When it comes to negotiating with threat actors about making ransom payments, this is not recommended as repeatedly mentioned in this report. From a **legal standpoint**, organisations should be aware of the current regulations about ransom payments. In some countries paying a ransom is illegal. One should consult with the legal team and the local government agencies on how to deal with ransomware attacks.

From a **technical standpoint**, it should be clear to every organisation that paying the ransom does not always result in the recovery of the assets and a successful decryption. Businesses should consider the cost of paying the ransom and not having the business back online. Additionally, paying the ransom and recovering the assets does not mean that the stolen information is not going to be leaked or sold afterwards; all stolen information should be considered as compromised. Sophos reported that only 4% of the companies that paid the ransom got all their data back and the majority that paid only got approximately 60% of their data back[53].

From a **business standpoint,** organisations should evaluate and consider the option of recovering the business without the compromised assets, how much it would cost, and what is the real impact of the stolen information being leaked even if the ransom is paid. Before considering paying the ransom, organisations should consider the cost of a publicity backlash, and be aware of the ethical standpoint.

From an **ethical standpoint**, organisations should be aware that they were attacked because of ransomware's fast growth, **a growth caused primarily because organisations previously infected paid the ransomware operators and funded their operations**. **Ransom payments are undoubtedly fuelling the rapid growth of ransomware.** Therefore, organisations should

---

[51] 'Report Ransomware | CISA'. https://www.cisa.gov/stopransomware/report-ransomware-0 (accessed Jul. 04, 2022)
[52] No More Ransom', The No More Ransom Project. https://www.nomoreransom.org/en/index.html (accessed Jul. 02, 2022).
[53] Sophos, 'The State of Ransomware 2022', Apr. 2022. Accessed: Jul. 04, 2022. [Online]. Available: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

consider the global position of the industry fighting against ransomware versus the position of recovering the organisation itself.

7. CONCLUSIONS

The analysis of the ransomware threat landscape from May 2021 to June 2022 resulted in some conclusions that can be regarded as takeaways for the community.

7.1 LACK OF RELIABLE DATA

In general, ransomware security incidents are seldom reported. Most organisations prefer to deal with the problem internally and avoid bad publicity. Some countries have laws regulating the mandatory reporting of incidents, but in most cases a security attack is first disclosed by the attacker.

A recent legislative initiative in the United States requires the reporting of all security incidents and ransom payments to the Department of Justice Cybersecurity and Infrastructure Security Agency (CISA)[54]. In the EU, the arrival of the revised Network and Information Security Directive 2[55] and the enhanced notification provisions for security incidents is expected to support a better understanding of relevant incidents.

The lack of reliable data from targeted organisations makes it very hard to fully understand the problem or even know how many ransomware cases there are. To this day, the most reliable sources for finding out which organisations have been infected are the web pages of the ransomware threat actors. This lack of transparency is not good for the industry, since the majority of the data leaked, as was found in this report, is personal data that belongs to employees and customers.

Even using the data from the web pages of threat actors (an undeniably unreliable source), it is very hard to keep track of the number of attacks, particularly because a large majority is ignored by the media, goes unreported by the victims and gets no coverage. The most important information that is missing is the technical explanation as to how the attackers obtained access to the targets. This is usually private data that describes the security posture of the target, so it is never shared with the public. As a consequence, our learning as a community of the problems to be solved remains fragmented and isolated.

Lastly, the trend in RaaS makes it hard to identify the threat actor behind an attack, since now the ransomware tool and command and control are shared between many different affiliates and threat actor groups.

7.2 THREAT LANDSCAPE

The study conducted on ransomware attacks from May 2021 to June 2022 showed that on average **more than 10 terabytes of data a month were stolen by ransomware threat actors**. Our research shows that **58.2% of the stolen data contains personal data from employees**. Given the sensitivity of such data, coordinated actions are needed to counter this threat. Ransomware threat actors are motivated mostly in terms of the acquisition of money, which increases the complexity of the attacks and, of course, the capabilities of the adversaries.

In 94.2% of the incidents it is not known whether the company paid the ransom or not. However, 37.88% of the incidents had their data leaked on the webpages of the attackers, indicating that the ransom negotiations failed. This allows us to estimate that

---

[54] 'Reporting of cyber incidents becomes law in the USA | Pen Test Partners'. https://www.pentestpartners.com/security-blog/reporting-of-cyber-incidents-becomes-law-in-the-usa/ (accessed Jul. 04, 2022)
[55] See https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-new-rules-cybersecurity-network-and-information-systems May 2022

approximately 62.12% of the companies might somehow have come to an agreement or solution concerning the ransom demand.

Ransomware is thriving, and our research shows that threat actors are conducting indiscriminate attacks. Companies of every size across all sectors are affected. Anyone can become a target. We urge organisations to prepare for ransomware attacks and consider possible consequences before attacks occur.

APPENDIX A: NOTABLE INCIDENTS

This appendix presents the life cycles of two distinct cases. These two incidents resulted in significant damage caused by the attacks and demands for quite large amounts of ransom. Each of these cases helps illustrate the life cycle of ransomware incidents as explained in Chapter 4.

A.1 COLONIAL PIPELINE RANSOMWARE INCIDENT

The Colonial Pipeline is the largest pipeline system for refined oil products in the United States[56] and provides roughly 45% of the United States East Coast's fuel, including gasoline, diesel, home heating oil, jet fuel, and military supplies[57].

On May 7, 2021, attackers gained initial access to the Colonial Pipeline network through exposed VPN account credentials (T1078 [58]). The execution phase consisted of deploying DarkSide ransomware[59]. The ransomware then proceeded to steal and encrypt files and folders in the target. Nearly 100GBs of company data was stolen. The threat actor threatened to publish leaked files if their demand was not met. The group demanded money, specifically 75 bitcoin in ransom, equivalent to approximately $4.4 million dollars, in exchange for a file decryptor to restore the files. The result of the negotiations was that Colonial Pipeline paid the ransom, received a file decryptor from the attackers, and used it to decrypt affected files and folders. The life cycle is shown in Figure 6.

Although the payment of the ransom was made, the decryption tool had a very long processing time so the company could not get the system back up quickly enough. This forced the Colonial Pipeline Company to halt all pipeline operations and freeze IT systems to contain the attack. Apart from the downtime, the ransomware attack also caused fuel shortages at several filling stations and affected several airports leading to changes in flight schedules and more economic loss.

The US Department of Justice stated that it had seized 63.7 Bitcoins from the original ransom payment which was only $2.3 million because the trading price of Bitcoin had fallen since the date the ransom was paid.

Darkside ransomware locks security software and event logging processes, deletes backups, and steals and encrypts files and folders.

---

[56] Colonial Pipeline ransomware attack', Wikipedia. Jun. 08, 2022. Accessed: Jul. 02, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Colonial_Pipeline_ransomware_attack&oldid=1092151580
[57] Colonial Pipeline attack: Everything you need to know', ZDNet. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/ (accessed Jul. 02, 2022).
[58] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®'. https://attack.mitre.org/techniques/T1078/ (accessed Jul. 02, 2022)
[59] A. Kleymenov, 'Colonial Pipeline Ransomware Attack: Revealing How DarkSide Works', Nozomi Networks, May 19, 2021. https://www.nozominetworks.com/blog/colonial-pipeline-ransomware-attack-revealing-how-darkside-works/ (accessed Jul. 02, 2022)

Figure 6: Life cycle of the attack against Colonial Pipeline in May 2021
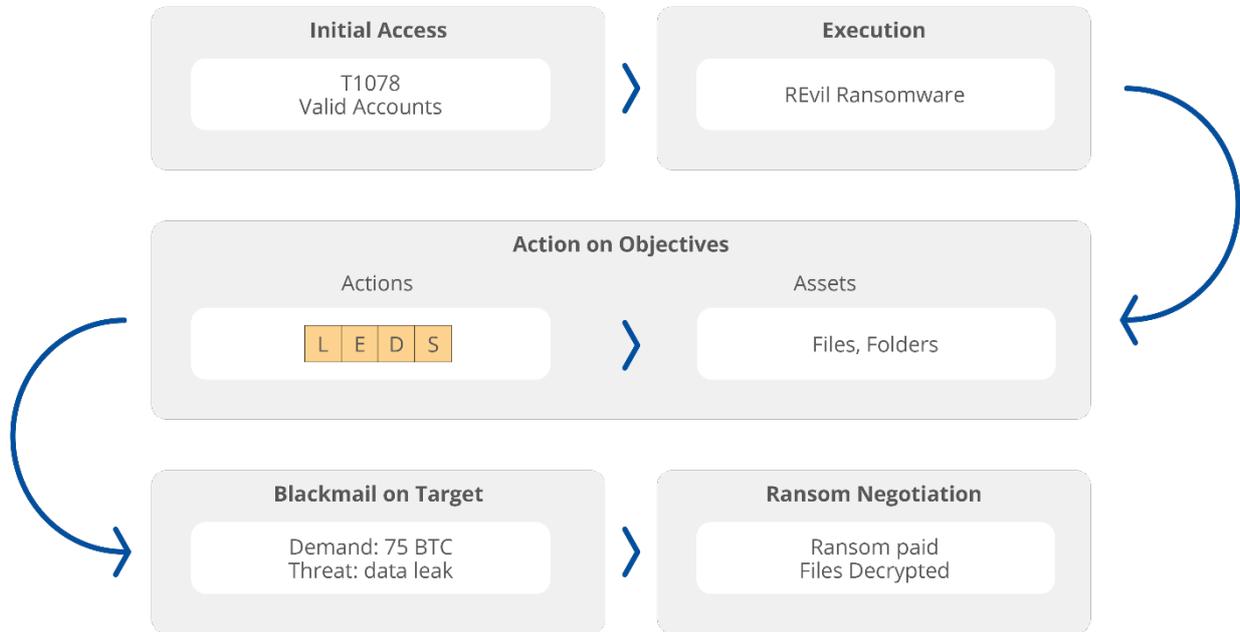
A.2 KASEYA

Kaseya VSA is a remote monitoring and management (RMM)[60] platform. Their products are installed on client workstations, endpoint management servers and managed services providers (MSPs), which are companies that provide IT services to other companies. Each MSP has a number of companies that they service and if one MSP is breached, it impacts all their clients, which explains the widespread use of ransomware.

On July 3rd, 2021, attackers gained initial access to the supplier of Kaseya VSA servers by exploiting a software vulnerability, specifically a SQL injection attack (T1190[61]) [62] [63]. The SQL attack resulted in the malicious payload by REvil being released and pushed to Kaseya customers as a hotfix. A CVE was assigned for the vulnerability introduced by the attackers: CVE-2021–30116[64].

Attackers gained initial access to Kaseya customers, MSPs, by exploiting a trusted relationship (T1199[65]) on Kaseya software; attackers could send instructions and commands to the software

---

[60] What is RMM - definition of remote monitoring and management system', Atera - RMM software | PSA & Remote Access for MSPs. https://www.atera.com/what-is-rmm/ (accessed Jul. 02, 2022)

[61] Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®'. https://attack.mitre.org/techniques/T1190/ (accessed Jul. 02, 2022).

[62] J. Allen, 'Kaseya Ransomware Attack Explained By Experts', PurpleSec, Jul. 23, 2021. https://purplesec.us/kaseya-ransomware-attack-explained/ (accessed Jul. 02, 2022)

[63] REvil Ransomware Attack on Kaseya VSA: What You Need to Know'. https://www.varonis.com/blog/revil-msp-supply-chain-attack (accessed Jul. 02, 2022).

[64] 'CVE-2021-30116'. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116 (accessed Jul. 02, 2022)

[65] 'Trusted Relationship, Technique T1199 - Enterprise | MITRE ATT&CK®'. https://attack.mitre.org/techniques/T1199/ (accessed Jul. 02, 2022)

installed on the customers. In the execution phase, the attackers deployed REvil ransomware on the target. The ransomware then proceeded to encrypt files and folders.

The blackmail component of this incident was special. Due to the impact of the attack, threat actors demanded from Kaseya and indirectly its customers, the sum of 70 million dollars in exchange for a file decryptor that would allow restoration of the availability of the affected assets in all affected systems[66]. There were also alternative demands to accommodate individual needs; 5 million dollars were demanded from individual MSPs to get a decryptor, 50,000 dollars were demanded from MSPs' customers to get a decryptor, and 40,000-45,000 dollars were demanded to decrypt specific file extensions per customer[67]. The threat actor threatened to double ransom money if there was no payment.

The result of the negotiations was that neither Kaseya nor the affected customers paid the ransom. A file decryptor was obtained, it is unknown how, and many systems were able to be restored.

Overall, the supply chain incident, shown in Figure 7, resulted in the compromise and encryption of over 50 MSPs and between 800 and 1500 companies which represents a total of 37,000 of Kaseya's clients or 0.001% of their total customer base. The ransomware demand of 70 million dollars was the biggest ransom demand as of July 23rd, 2021. The REvil ransomware encrypts files, but no data-stealing or deleting of capabilities were observed[67]. The life cycle is shown in Figure 8.
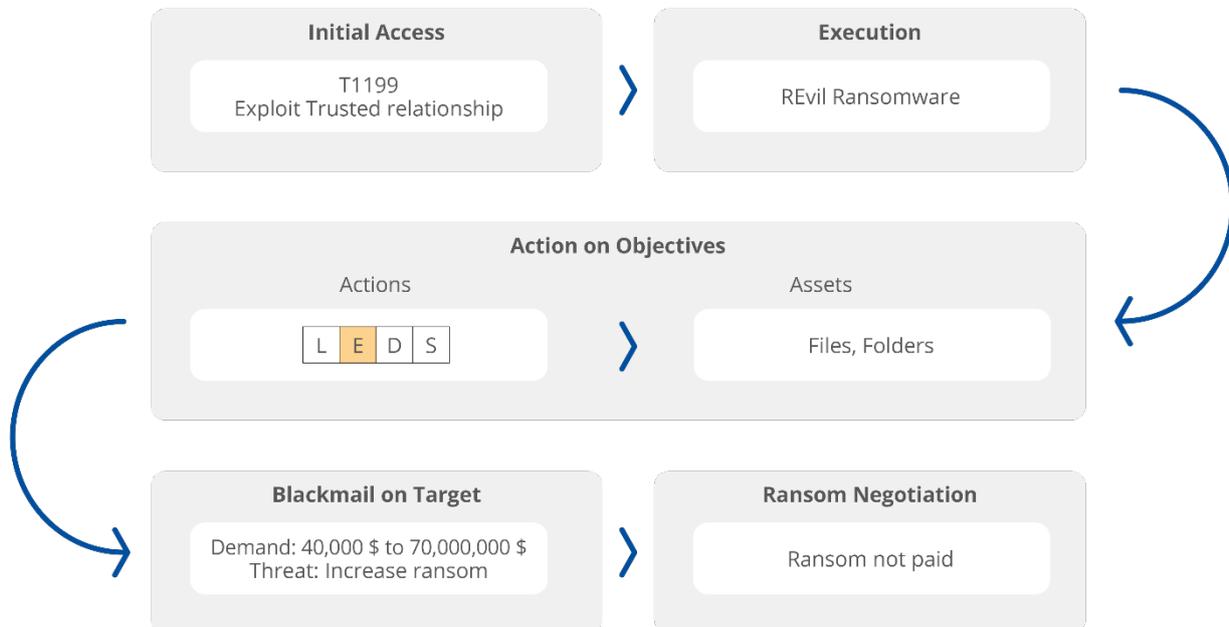
---

[66] D. Winder, '$70 Million Demanded As REvil Ransomware Attackers Claim 1 Million Systems Hit', Forbes. https://www.forbes.com/sites/daveywinder/2021/07/05/70-million-demanded-as-revil-ransomware-attackers-claim-1-million-systems-hit/ (accessed Jul. 02, 2022)
[67] 'REvil is increasing ransoms for Kaseya ransomware attack victims'. https://www.bleepingcomputer.com/news/security/revil-is-increasing-ransoms-for-kaseya-ransomware-attack-victims/ (accessed Jul. 02, 2022)

Figure 7: Diagram of Kaseya supply chain attack. The attackers deployed code to VSA instances of MSP suppliers (whether in the cloud or on-premises is still under investigation). Some MSPs, in turn, were exploited to deploy malware and ransomware to their clients.[68]
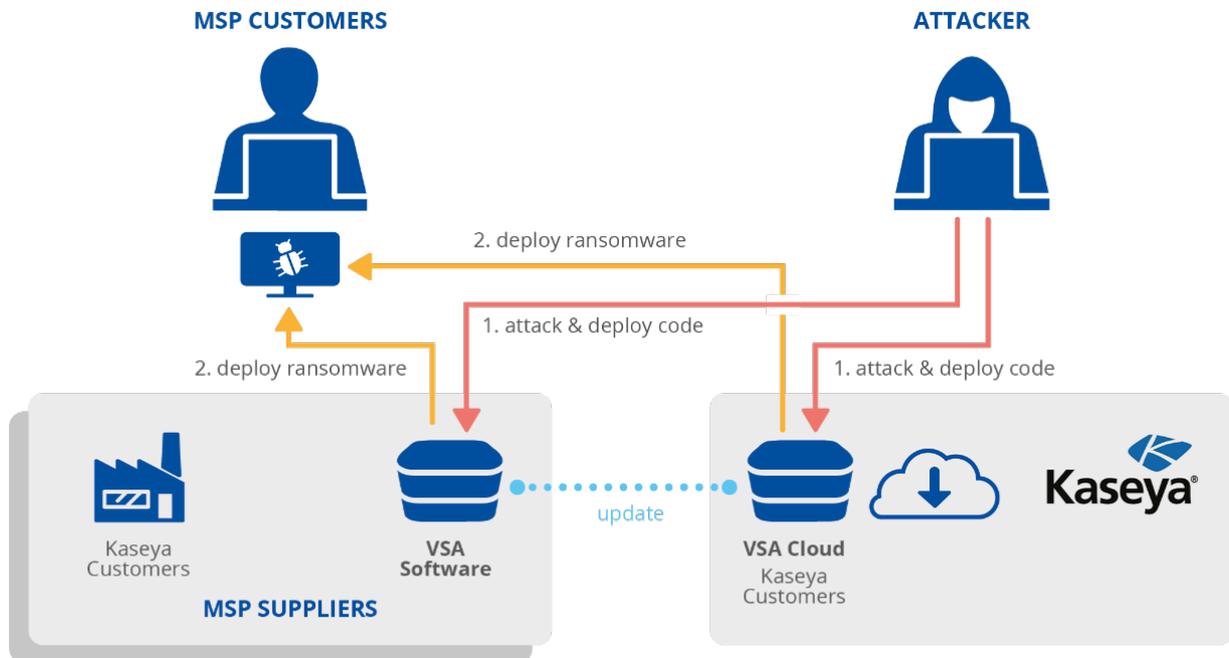
Figure 8: Life cycle of the attack against Kaseya's MSP customers in July 2021

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.

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