

# Security Navigator 2023

**Research-driven insights  
to build a safer digital society**





**Hugues Foulon**

CEO Orange Cyberdefense and  
Executive Director of Strategy,  
Security and Cybersecurity at  
**Orange Group**

Cyber security incident volumes continue to rise, but at a much slower pace. Though this war is not won, there are reasons to believe we are already winning some battles.

All is underpinned by our Core Fusion platform, enabling the identification of 99,000 potential security incidents that were investigated. Our CSIRT teams carried out 382 incident response missions to date, and our elite ethical hacking team conducted 1900 projects on demand.

Orange Cyberdefense is pleased to share once again the outcomes of a year of cybersecurity research and services provided to organizations around the world. The last few months were particularly dense in terms of macroenvironmental events, nevertheless the cyber security ecosystem emerges more vigilant and united as a result. Collaboration is strengthened as cyber threats materialize as a common, omnipresent and sprawling adversary.

No one can now deny that the state of the threat reported in these pages and the increased awareness of cybersecurity risks characterizes – beyond the uncertainty of the current environment – the era which we are entering. Cyberattacks are making headlines. The war against Ukraine is a resounding reminder that our digitized world is also the field of virtual battles. This is equally the case when hospitals are being attacked, phones and emails of major political leaders are hacked and companies are going out of business. Never has the general public been so well aware of cyber threats, and with it, the attention paid by each actor in society goes up a notch. Cybersecurity issues are now being dealt with at the highest level within Governments and company Boards. They are becoming a subject of concern for tradespeople, small business owners and the public. This fundamental and collective societal movement is necessary to reach a tipping point for change.

The combination of a growing risk and widespread awareness makes the work of cyber security ‘scouts’ - to explore, inform and support - even more critical. No actor in the cyber security community, be it in the private or public sector, is exempt from a mission that transcends individual interest, and that we define at Orange Cyberdefense as the pursuit of a safer digital society.

You will find in this report one of our contributions to this effort, based on our visibility and analysis of the current cybersecurity landscape by 2,700 experts spread across the world and our 17 SOCs, 13 CyberSOCs and CERT in 8 locations.

All is underpinned by our Core Fusion platform, enabling the identification of 99,000 potential security incidents that were investigated. Our CSIRT teams carried out 382 incident response missions to date, and our elite ethical hacking team conducted 1900 projects on demand.

Our multi-disciplinary teams help our clients fight threats effectively throughout the risk lifecycle, from anticipation to prevention to response, bringing together the best solutions on the market to meet the specific needs of each client. What we have seen among our CyberSOC customers - who are mature as they use our detection and response services - is that cyber security incident volumes continue to rise, but at a much slower pace. Though this war is not won, there are reasons to believe we are already winning some battles. Notably, the number of ransomware-related incidents decreased in the past year. But challenges remain: SMEs are particularly vulnerable, incidents originating from internal sources are a particular concern in the public sector, the manufacturing industry has the highest victim count, users are often the weakest link and attack volumes and complexity outnumber defenders.

I am therefore proud to share the Security Navigator 2023 edition with the cyber community, decision makers and general public in order to keep fighting all together. Being part of the Orange Group - one of the largest telecommunications operators globally with 263 million clients in 29 countries - puts Orange Cyberdefense in a unique ‘control tower’ position in the sector. Let’s navigate the ins and outs of cyberspace with serenity, responsibility and awareness. This report is yours. Make good use of it and let us work together to succeed in what is one of the greatest missions of our time. Thank you for your trust and happy reading!

**Hugues Foulon**

# Table of contents

- Introduction: What you need to know..... 6**
- CyberSOC statistics: This is what happened ..... 9**
  - Funnel: Alert to incident .....10
  - Types of incidents ..... 11
  - Totals ..... 11
  - General trends in detection .....12
  - VERIS Framework .....13
  - incidents and visibility .....16
  - incidents by business size.....18
  - Ransomware ..... 22
  - Cyber Extortion .....24
  - Looking at verticals..... 28
  - Professional, Scientific and Technological Services, Real Estate, Rental and Leasing ..... 28
  - Manufacturing, Healthcare, Finance and Insurance ..... 30
  - Retail and Trade, Transport and Warehousing, Accommodation and Food Services ..... 32
  - Command and Control channels..... 34
  - Conclusion..... 37
- Expert Voice Germany: Why Conti has changed incident response..... 38**
- Cyber crisis: The Ukraine war ..... 41**
  - Risk assessment..... 42
  - What you can do ..... 43
  - Attack methods..... 44
  - Just across the border: Commentary from the Orange CERT in Poland.....47
  - Conclusion..... 48
- World Watch: Stories about stories ..... 51**
  - Types of advisories ..... 52
  - LAdvisories on technology ..... 53
  - Log4j: Logging considered harmful ..... 55
  - Most featured vulnerabilities ..... 57
  - Advisories related to Cyber Extortion ..... 59
  - I spy with your phone..... 60
  - Conclusion..... 61
- Expert Voice France: Effective vulnerability management in 2023 ..... 62**
- Vulnerability data: Evolution of the weakest link ..... 65**
  - Know your weaknesses: VOC data..... 66
  - Pentesting data ..... 68
  - Real findings per asset over time..... 70
  - Vulnerabilities found per day over time.....71

- Industry comparison VOC scanning..... 72
- Industry comparison Pentesting ..... 73
- Severity ratings.....74
- Age of VOC findings.....76
- CVE published dates ..... 77
- Conclusion..... 78
- Expert Voice China: The use of deception in ICS/OT environments... 80**
- Of Malware and factories: Spotlight on Manufacturing..... 83**
  - Back to the future..... 84
  - Comparing key metrics ..... 85
  - Is the Manufacturing sector being targeted more by extortionists? ..... 86
  - Do our Manufacturing clients experience more incidents? ..... 88
  - Conclusion..... 89
- Pentesting stories and CSIRT stories..... 91**
  - CSIRT story: Of bulldozers and Ninjas ..... 92
  - CSIRT story: "Went phishing with Sharepoint (P.S. click this!)" ..... 94
  - Pentesting story: Chaining Internal Server Errors into account takeover ..... 96
  - Pentesting story: Open, Sesame ..... 98
- Expert Voice France: A security review of the Blockchain..... 100**
- The six-inch risk factor: Mobile Security..... 103**
  - Operating Systems ..... 104
  - iOS Vulnerabilities ..... 105
  - Android Vulnerabilities ..... 106
  - Mobile App Security ..... 108
  - Patches and versions..... 110
  - Conclusion..... 111
- Expert Voice South Africa:  
The Thinking Theory - a mental challenge for security leaders.....112**
- Security predictions: The only way is up!.....114**
  - An unavoidable evolution of architectures..... 116
  - Law and regulations, increasing criteria for selecting solutions..... 117
  - New prime targets..... 118
  - New old tricks..... 119
- Summary: What have we learned?..... 120**
- Contributors, sources & links..... 122**

## Introduction

# What you need to know



**Laurent Célérier**  
EVP Technology and Marketing  
Orange Cyberdefense

With the return of war in a largely Digitized Europe, especially after the COVID episode that accelerated the digital transformation of our societies, a new strategic phase is beginning. In this context, one thing is clear from the opening of this Security Navigator: more than the threat itself, it is the uncertainty that has reached an unprecedented level. It is no longer the time for isolated, one-off storms that can be avoided or dealt with. Health, geopolitical, industrial, financial and logistical crises are intertwined, making it difficult to analyze them and to predict their evolution.

In this singular context, the ability to make quick and sound decisions, despite uncertainties and financial constraints, will be a determining factor in ensuring the digital resilience of our organizations. Supporting CISOs and CIOs in their decision making is the main purpose of our Security Navigator 2023.

Our contribution is based first and foremost on the evolution of the threat that we have observed through our operational activities, on the analysis we have made of it and on the lessons we have learned. This is the core of the Security Navigator, fed by the almost 100,000 incidents investigated this year by our SOCs and CyberSOCs, by the 3 million vulnerability scans performed by our Vulnerability Operations Center (VOC), or by the 1,200 reports written by our pentesting team.

This field data, which we are happy to share with you, allows us to identify the underlying trends that are being confirmed (for example, the untenable pressure of vulnerabilities, with an average patching time that we observe to be 215 days), the technical and geographical evolutions (particularly in terms of ransomware), but also to study the scope and impact of the major events that marked the past year, whether geopolitical (war in Ukraine) or technical (Log4j crisis).

Knowing the threat also means knowing that it is constantly evolving: defending ourselves therefore means drawing all the lessons from 2022, but also admitting that we will have to face new threats in 2023. Beyond the historical data, we want to share with you testimonies, stories and reflections which, even if no situation is identical, are sources of inspiration for what the future might have in store.

This is the strength of the defense community that we must embody. We invite you to discover, throughout the pages of this Security Navigator, the stories of our CSIRT and ethical hacking teams, articles on cyber decision-making mechanisms, or our feedback on the operational management of the Ukrainian cyber crisis.

In this respect, the approach adopted by the Ukrainian government is a particularly enlightening example that should also inspire us for the years to come. Ukraine has indeed managed to avoid the cyber collapse that was predicted, by relying on the triple support of States, the private tech sector and individuals:

- First of all, the States, which provided valuable support in terms of intelligence on the threat;
- Secondly, the private sector, including of course cyber security companies, but also cloud providers who helped ensure the resilience of Ukrainian data;
- Finally, individuals, who are stakeholders in the current cyber conflicts: the warring parties are trying to unite isolated hackers around the world for their own benefit.

Without going into the realm of the offensive, this 3-layer approach can inspire us for defense strategies: it is key for each organization (1) to have the support of the state agencies of the countries in which it operates (2) to rely on trusted private cyber partners (3) to place humans at the heart of the defense system (awareness, but also mechanisms for reporting alerts).

Finally, let's mention a last approach that can help us make the right decisions tomorrow: trying to reduce the level of uncertainty. Such an objective is necessarily a long-term one and requires a reduction in the externalities and dependencies that feed uncertainty. This approach is that of sovereignty. At Orange Cyberdefense we are convinced that this is one of the trends that will structure the cyber world of tomorrow, and that we must build it today.

Whether it's sharing data, learning from best practices or learning how to control our future dependencies, we have to learn from each other to meet the cyber challenges we face with our limited resources. The effects of such an approach are already being felt: the data you are about to discover demonstrates a reduction in incidents affecting the customers we protect. While we should obviously not see this as a weakening of the threat and relax our efforts, this observation should nevertheless inspire us with hope: despite the uncertainties and constraints, victory is possible. This Security Navigator invites us to build it together: we hope you enjoy reading it!





**Carl Morris**  
Senior Security Researcher  
Orange Cyberdefense

**Diana Selck-Paulsson**  
Lead Security Researcher  
Orange Cyberdefense

## CyberSOC statistics

# This is what happened

This year was turbulent for a number of reasons. Of course the political situation has not left us untouched. The full impact of the war has yet to be determined, and we take a closer look in a separate chapter. There are some internal changes too: our analysts have started adopting a new classification system, which allows us much better insight into what has actually happened. We collected incidents from CyberSOCs all across the world and normalized the data as part of the analysis process.

Additionally for the first time we have also correlated these data sets with information obtained from vulnerability management and Penetration Testing reports, but also World Watch data and observations from across our CERT, Epidemiology Labs and other research teams to draw a more accurate picture of how we got here, and how these tendencies will likely shape the future. While some of these data sets have their own chapter in this report, we constantly consider them to validate our conclusions.

As mentioned in previous reports: when reading this it is important to keep in mind that all of these incidents are in fact attacks that were prevented and stopped. While this is reaffirmation that our clients are well protected, it is also important not to fall for what is called "survivorship bias"<sup>[1]</sup>.

### About the data

- Total of potential incidents: 99,506 (up by 5% from 94,806 in 2021)
- Out of these potential incidents, 29,291 could be confirmed as True Positive (TP) security incidents (down by 14% from 34,158)
- Period analyzed: October 2021 to September 2022
- Data sources: firewalls , directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our Core Fusion Platform

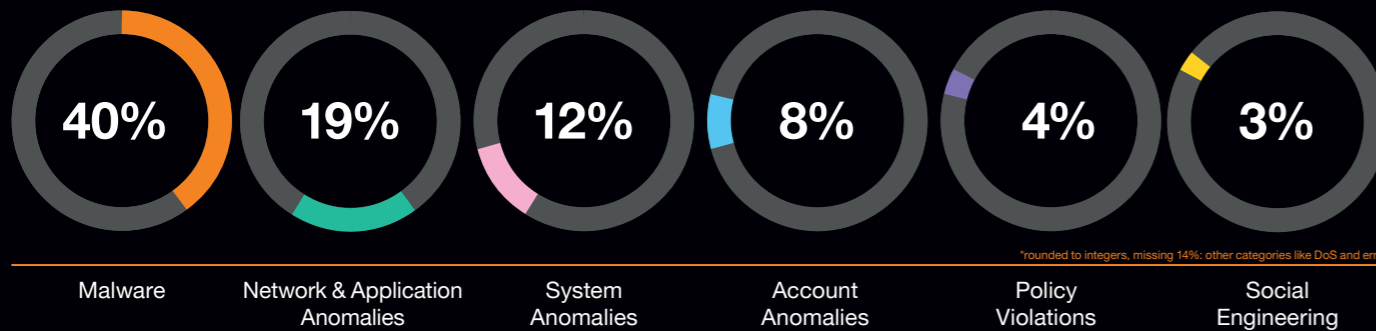


## Funnel: Alert to incident

99,506  
Potential incidents







29,291

29.43% Confirmed incidents



### Types of incidents

In 2022, we detected the following incident types:

-  **Malware** is malicious software such as ransomware.
-  **Network & Application Anomalies**, such as tunneling, IDS/IPS alerts and other attacks related to network traffic and applications.
-  **System Anomalies** are events directly related to the OS and the components around it like drivers that stop working or services that are terminated unexpectedly.
-  **Account Anomalies**, such as brute force attacks, reusing credentials, lateral movement, elevation of privileges or similar kinds of incidents.
-  **Policy Violations**, such as installing unsupported software or connecting an unauthorized device to the network.
-  **Social Engineering** is any attempt to fool users; including, but not limited to, phishing and spoofing.

### A global view

As in previous years' reports, this year we again strive to provide a global overview of what we are seeing in our incident data with the aim being to highlight trends that can also be applied to the global threat landscape. To facilitate this, a broad data set is collected from across all of the operational teams within Orange Cyberdefense which includes 17 SOCs & 13 CyberSOCs responsible for supporting our clients around the globe.

Following in the same vein as last year's Security Navigator report, we again have the luxury of utilizing a whole years' worth of data, 1st October 2021 to 30th September 2022. This will allow us to do like-for-like comparisons with last year's report, where possible and relevant. It will thus help highlight any significant changes in the threats being seen in our client base and whether there is any correlation with what is being seen in the wider landscape.

### Events, incidents, confirmed incidents

A note on terminology: We log an event that has met certain conditions and is thus considered an Indicator of Compromise, Attack or Vulnerability. An incident is when this logged event, or several events, are correlated or flagged for investigation by a human – our security analysts. An incident is considered 'confirmed' when, with help of the client or at the discretion of the analyst, we can determine that security was indeed compromised. We refer to these 'confirmed' incidents in this report as 'True Positives'. True Legitimate incidents are incidents that were raised but after consultation with the client turned out to be legitimate activity. incidents are categorized as 'False Positive' when a false alarm was raised.

### Totals

This year we are in the position to be able to do a like-for-like comparison of a full 12 months' worth of data. We are happy to say that our dataset has grown again from last year with data from **44% more clients** being included in this year's report. This relatively large growth in data only translated to an **increase of 5% in the security incidents** we handled, however. Our data shows though that the majority of this growth in client base occurred over the last 4 months. Taking into account the typically quiet summer period and the necessary onboarding processes, this relatively small growth in incidents is to be expected.

We saw an average number of 34 confirmed incidents per month and client over the past 12 months. This is a decrease from the figure of 40 we recorded for the same time period last year. This figure was brought down significantly during the last 4 months due to large client growth and the onboarding processes involved with that.

In total 99,506 incidents were recorded, all of which were investigated by human security analysts in one of our CyberSOCs. These investigations resulted in 29,291 'True Positive' security incidents being raised with our clients, 29% of all the incidents we investigated. The other incidents comprised of 10% 'True Legitimates' and 55% 'False Positives', while the remaining 6% could not be classified.



### General trends in detection

Using our traditional category classifications, Malware again takes the top spot by some way, with 40% of all confirmed incidents. This is a small increase on last year's 38%. Network & Application Anomalies was the second highest incident type, but we have seen a drop from 22% down to 19%. Although not on the scale of the 13% decrease seen last year, it still represents a fairly significant drop.

The final entry making up the trio of our top 3 identified incident types is System Anomalies, with 11.5%. This increases its overall share from the 9% recorded in last year's report. Last year's third most detected incident type, Account Anomalies, dropped down to fourth this year. As with Network & Application Anomalies there was a visibly significant decrease, this time from 13% to 8%, causing it to drop out of the top 3. Albeit in a slightly different order the top 4 incident types still remain the same as we've seen in our previous Security Navigator, although this is obviously heavily influenced by the technologies implemented and detection focus at our clients.

Despite showing increases in the report last year both Policy Violation and Social Engineering have dropped off again, this time to a share of 3.8% and 3.5% respectively.

This is not to say that either of these incident types should be taken lightly. Social Engineering is one of the most common methods used to gain initial access to a network, but these attacks by their nature cannot generally be detected purely with technical solutions. We thus have to wait until the attacker performs an action on the environment to detect the activity.

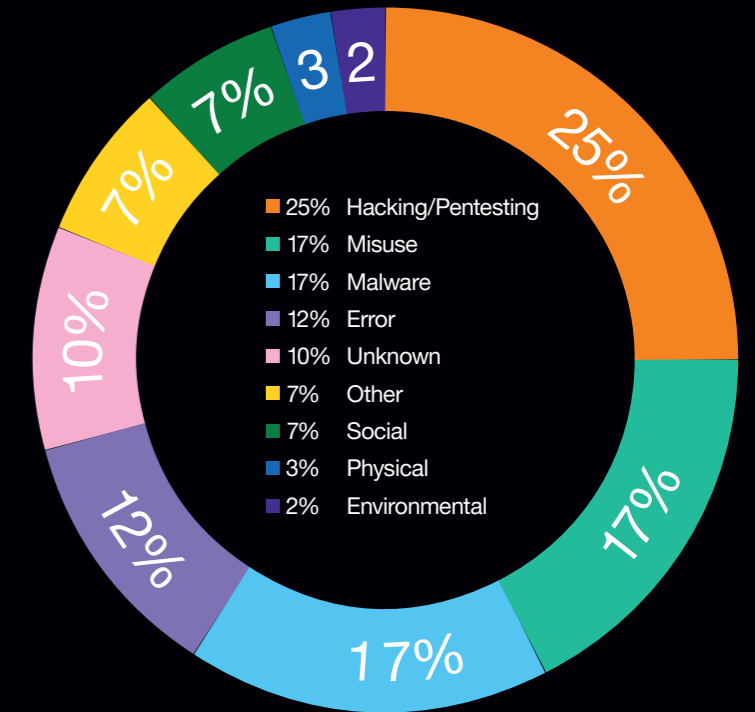
Policy Violations in turn can only be picked up and acted on if the correct levels of logging are enabled on all systems.

Just sneaking into our list of detected incident types this year is Denial of Service, albeit with only 23 detected incidents over the course of the year. All of these were detected at organizations classified as Large, where we are more likely to have appropriate monitoring in place.

### VERIS Framework

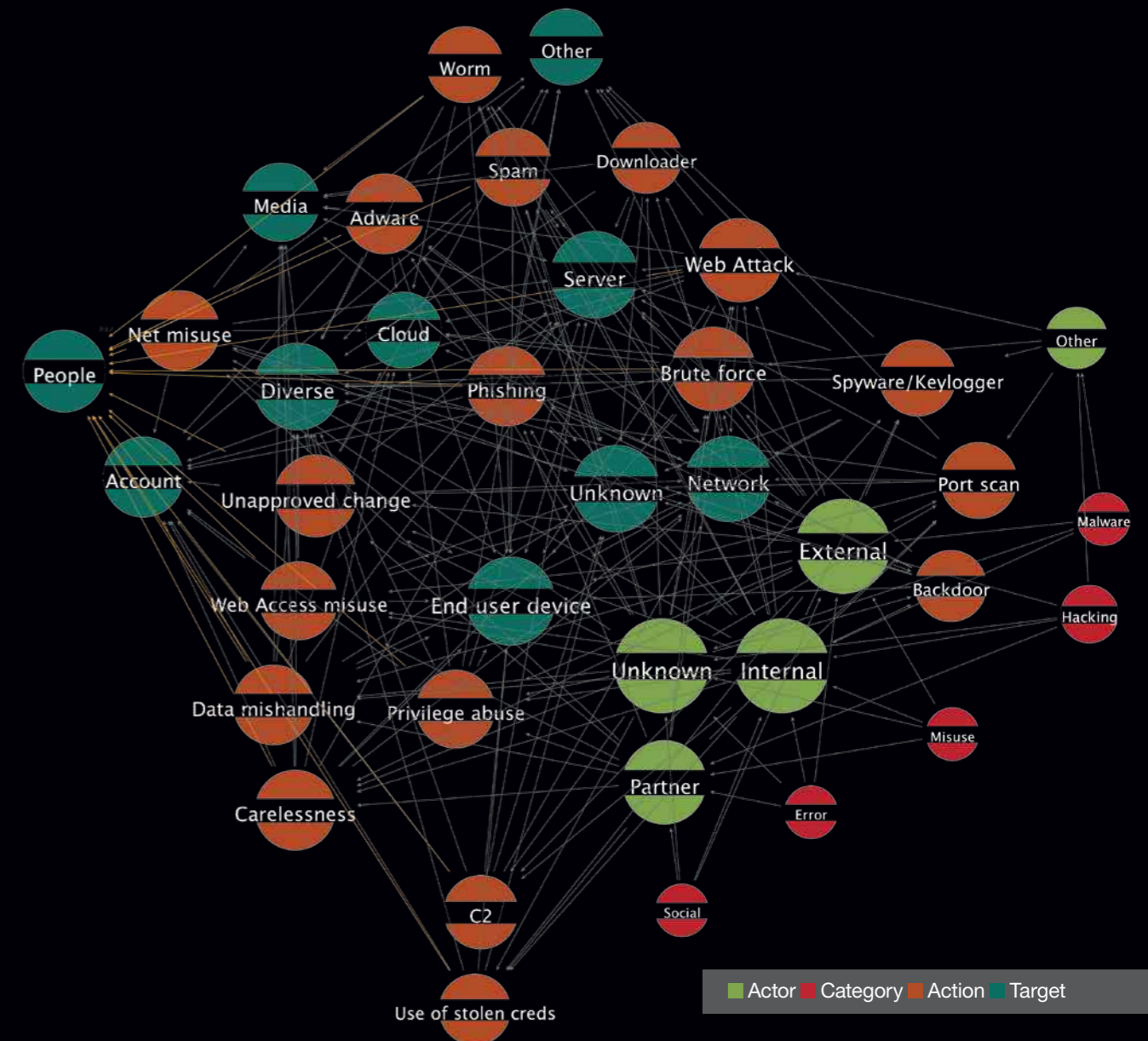
We announced in our previous report that we would be adopting the industry standard VERIS (Vocabulary for Event Recording and incident Sharing) framework for classifying our incidents.

While this change was gradually being implemented, we ran both systems of classification in parallel and hence can still provide the analysis above based on our "traditional" classification system. **26% of our verified incidents were classified with values from VERIS.** This allowed us to provide additional analysis based on this framework.



### VERIS in action: actors, targets, actions

Most common intersections of Category and VERIS Actor, Action and Asset



## VERIS Categories

The categories used in the VERIS framework are quite noticeably different from our “traditional” categorizations and consist of the following 7 primary categories:

**Malware** is any malicious software, script, or code running on a device that alters its state or function without the owner’s informed consent. Examples include viruses, worms, spyware, keyloggers, backdoors, etc.

**Hacking** is defined within VERIS as all attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms. Includes brute force, SQL injection, cryptanalysis, denial of service attacks, etc.

**Social** tactics employ deception, manipulation, intimidation, etc to exploit the human element, or users, of information assets. Includes pretexting, phishing, blackmail, threats, scams, etc.

**Misuse** is defined as the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended. Includes administrative abuse, use policy violations, use of non-approved assets, etc. These actions can be malicious or non-malicious in nature. Misuse is exclusive to parties that enjoy a degree of trust from the organization, such as insiders and partners.

**Physical** actions encompass deliberate threats that involve proximity, possession, or force. Includes theft, tampering, snooping, sabotage, local device access, assault, etc.

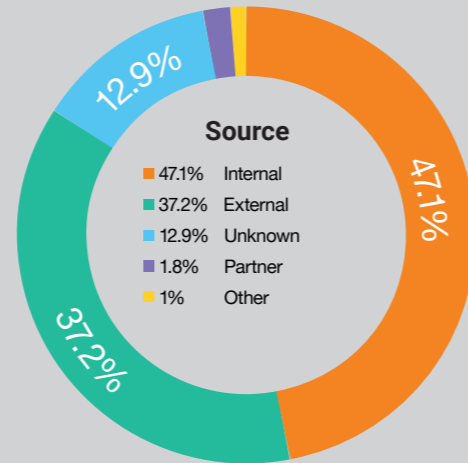
**Error** broadly encompasses anything done (or left undone) incorrectly or inadvertently. Includes omissions, misconfigurations, programming errors, trips and spills, malfunctions, etc.

**Environmental** not only includes natural events such as earthquakes and floods, but also hazards associated with the immediate environment or infrastructure in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions.

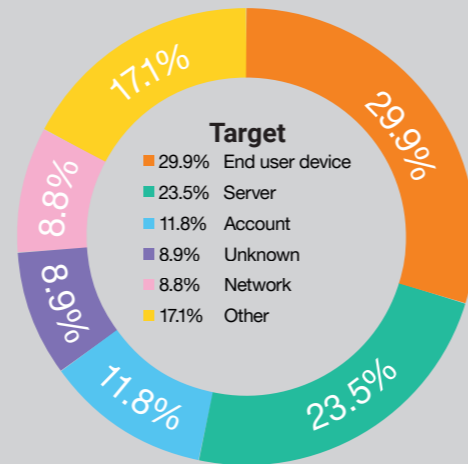
By combining the sub-action with the VERIS category, we can gain more insight into the actual cause of the incidents we have recorded. As can be seen, the top 2 falling under the Hacking/ PenTesting category are Web Attacks and Port Scans, making up almost 22% of incidents. This has some similarity to Verizon’s own DBIR 2022<sup>[2]</sup> report where their top attack vector was ‘Web Application’ which falls under the Hacking category.

The sub-action of “Unapproved hardware/software/script/ workaround”, part of the Misuse category, is the second highest combined incident type, with almost 10.5%. In our data these incidents generally involved attempts to install unauthorized or illegal/cracked software, the use of keygens, use of Tor to bypass Internet controls or the presence of potential hacking tools and scripts. This sub-action and category could also be applied to the use of shadow IT whereby employees deploy or use their own hardware, usually to bypass certain restrictions.

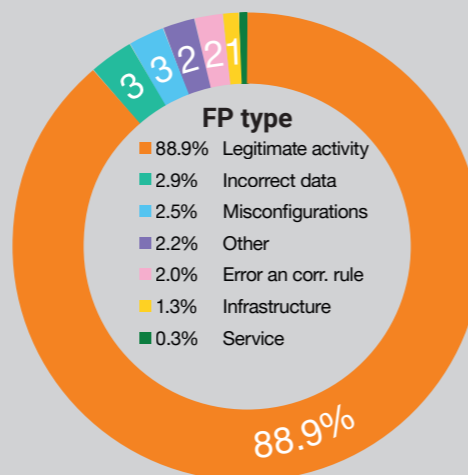
## What VERIS can tell us



~47% of incidents are caused by internal sources, not external ones.



The most targeted resource among our clients are Endpoints (~30%) and servers.



~89% of False Positives are caused by legitimate user activity.

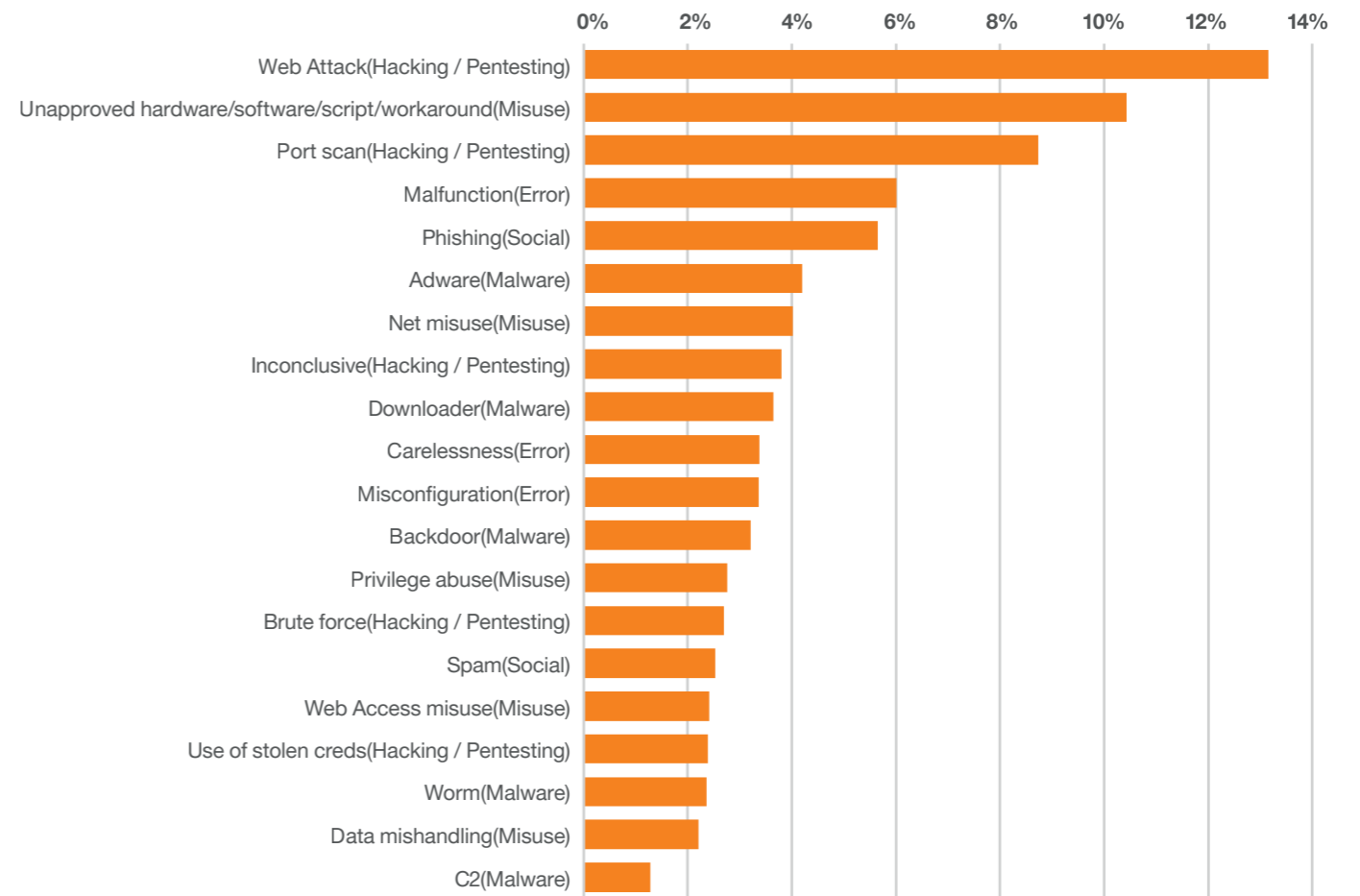
## VERIS Trends

There are a couple of categories in VERIS which can be directly mapped to our previous categorizations, for example Malware and Social. However, whereas Malware had the highest number of incident detections in our earlier analysis with 40% of all incidents, it is now joint second with only 17%. Alongside Malware, with 17% of incidents, is the Misuse category. The closest mappings we had previously would be to the Policy Violation and Account Anomalies incident types, which previously made up 12% of incidents. Whilst Misuse can be used to speak to the potential insider threat problem or a third-party abusing trust, it has to be remembered that non-malicious activity falls under this category as well.

The top incident type in our data when using the VERIS classifications was Hacking. For our purposes we have also included Penetration Testing with this category. This accounted for 25% of all confirmed incidents that were classified using the new system. Interestingly, the fourth highest number of confirmed incidents fell under the Error category. This is an area all organizations should pay close attention to, and where they can easily and relatively inexpensively apply mitigations by ensuring robust change management processes are in place for example. The costs, both financial and reputational, of unintentionally exposing data or a system to the Internet due to a simple mistake or misconfiguration can be astronomical.

## Top 20 incidents

Most observed incidents by VERIS Sub-Action & Category





## Incidents and Visibility

There are so many metrics and datapoints in security, each with their own strengths and weaknesses. But one thing almost all of them suffer from is the lack of meaningful baseline. We can observe in which Industries we report the most incidents, but relative to what? Is that a function of the volume of attempted attacks or successful attacks, or simply a function of the size of businesses in that industry or the level of visibility we have on its businesses? This problem is particularly acute in Managed Threat Detection services like our own, where we deal with an enormous variety of detection capabilities across our client base. Its surprisingly difficult to address this issue in the dataset we have.

In this year's Navigator report we attempt to clear the fog a little by presenting some analysis regarding the level of coverage our clients have in terms of detection capabilities, and how that might affect the volume and type of incidents we report.

To this end we derive a simple metric that describes the breadth and depth of detection coverage our clients in this dataset have. The 'coverage rating' scores range from 0-5 and are explained below:

### Coverage Rating Scores

- 0 No coverage
- 1 Minimal coverage
- 2 Some coverage, but less than recommended
- 3 Appropriate coverage, including all the basics
- 4 Good coverage, including the basics and more
- 5 Complete coverage

### Coverage Areas

- **Perimeter Security**  
Firewall logs, WAF Logs, IDS/IPS Logs, Email Gateway Logs, VPN / Remote Access Logs
- **Internal Security**  
AD / Authentication Logs, Firewall Logs
- **Infrastructure**  
DHCP Logs, DNS Request Logs, Web Server / Web Application Logs
- **Internet Infrastructure**  
Web Server / Web Application Logs, Web Proxy Logs
- **Network**  
Internet traffic, Internal East/West Traffic, Network Traffic Analysis (NTA)
- **Endpoint**  
Anti-virus, EP/EDR, Sysmon, MS Defender
- **Cloud, PaaS & SaaS**  
Azure - AD, Audit, KeyVault & VM, O365, Lacework and Mondoo, Palo Alto Prisma Cloud, Checkpoint Cloudguard, platforms like Adaptive Shield

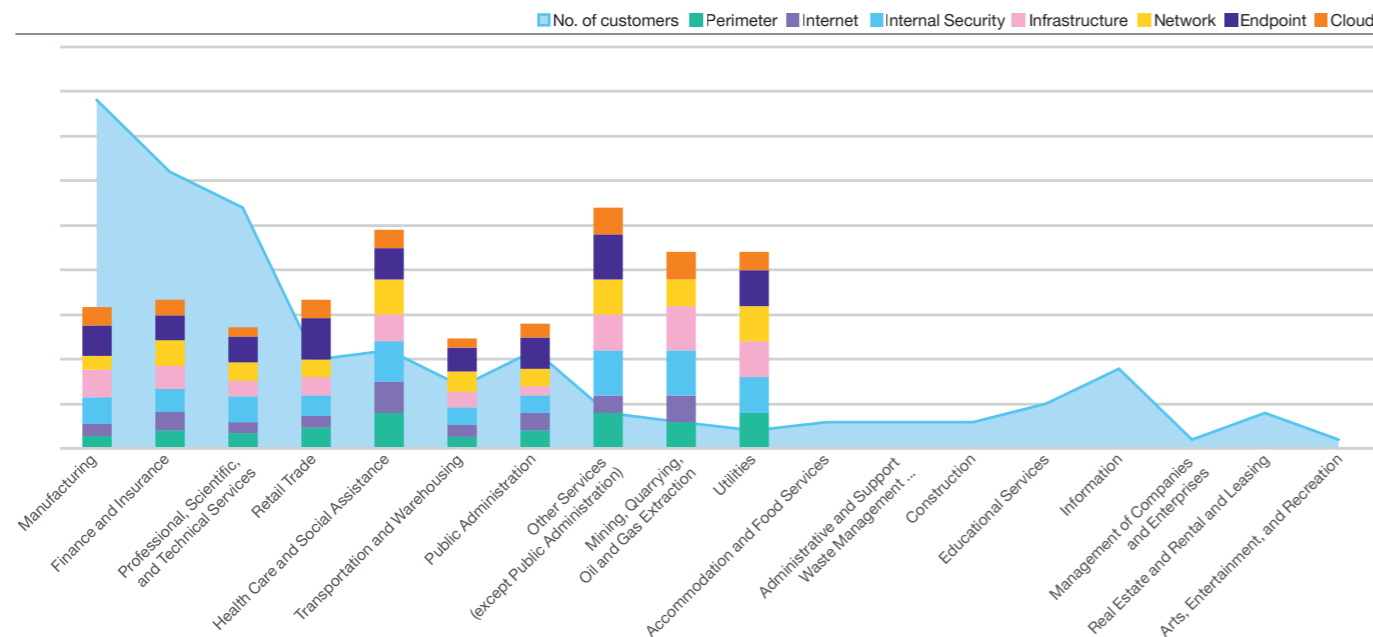
As there is no hard quantitative means of deriving the level of coverage, we rely on a manual assessment involving the people who work directly with the client. This process is imperfect and incomplete, but we believe it is a first step toward providing some essential context around our CyberSOC incident data.

## Coverage

How much visibility do we have across our client estates in each industry? We illustrate the relative scale of the assessed coverage in each industry domain below. This is a new approach, so we do not have a complete coverage assessment yet for all industries.

## Coverage by security domain per industry

How deep does our monitoring go for different industries?



## The impact of increasing coverage

With the Coverage Score as a baseline, we consider how the number of incidents (True and False Positive) changes with an increase in Assessed Coverage.

Predictably, the number of overall incidents per Client increases with the Assessed Coverage Score.

While it is safe in most cases to assume that higher coverage means more incidents, confirmed as well as noise, the actual extent of the increase depends on security maturity just as much.

This correlation between visibility and recorded incidents is intuitive, but important to remember when considering security data – ours and in general.

A review of our numbers reveals almost exactly what we'd expect: For each detection domain, the number of True Positive incidents grows with an increased level of Detection Coverage. The only exception appears to be when we've assessed the Coverage Level to be 100% - 5 points. At this level of coverage, the number of incidents starts to drop. We believe this is because of the general level of maturity of the clients with this level of coverage. The small number of clients in this group are set apart by other factors more significant than the level of coverage. The exception is in the Endpoint domain, where a greater level of coverage leads consistently to a higher number of TP as well as FP incidents being detected.

In short – you probably can't have too much Endpoint Detection.

A similar picture emerges when we consider False Positive findings by coverage score.

As a general observation, the ratio between True Positives and False Positives increases as the Coverage Score increases. This makes intuitive sense: By increasing the level of visibility we have in any domain of our environments, we increase the number of malicious incidents we detect. However, we increase the number of False Positives we have to deal with at a faster rate. More detection equals better security, but at the cost of more 'noise'.

## Industry and Business Size comparison revisited

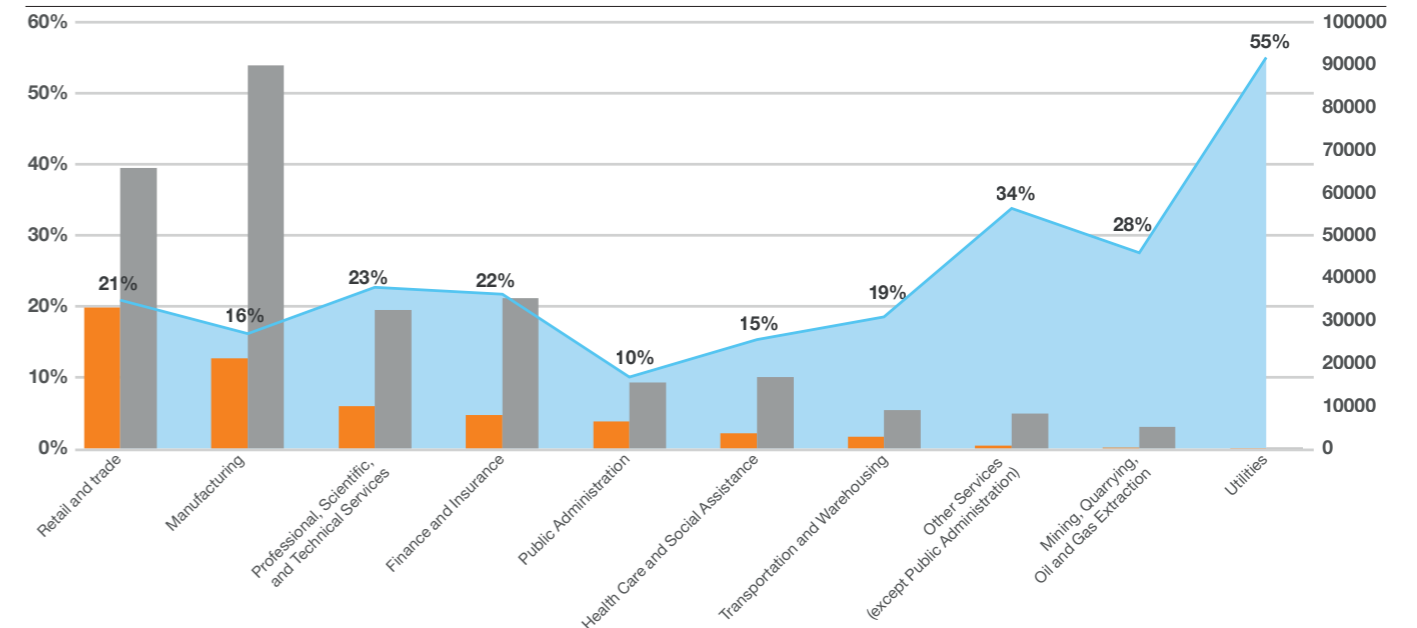
Where available, the Assessed Coverage Score can be used to review our comparison of incident levels across Industries and Business Size.

We perform a simple modification on the incident volumes to factor in the relative level of coverage: Divide the incident count by the assessed coverage score and multiply it by the maximum possible score. Put simply, the lower a client's assessed coverage score is, the more this adjustment will 'boost' the number of incidents in this comparison. For a client with the maximum possible level of coverage, we will simply reflect the actual number of incidents we observed.

Using this simple calculation we can now consider how businesses and industries compare with their relative levels of coverage taken into account.

## Incidents relative to coverage by industry

Incident count by industry when taking coverage-levels into account



# Incidents by business size

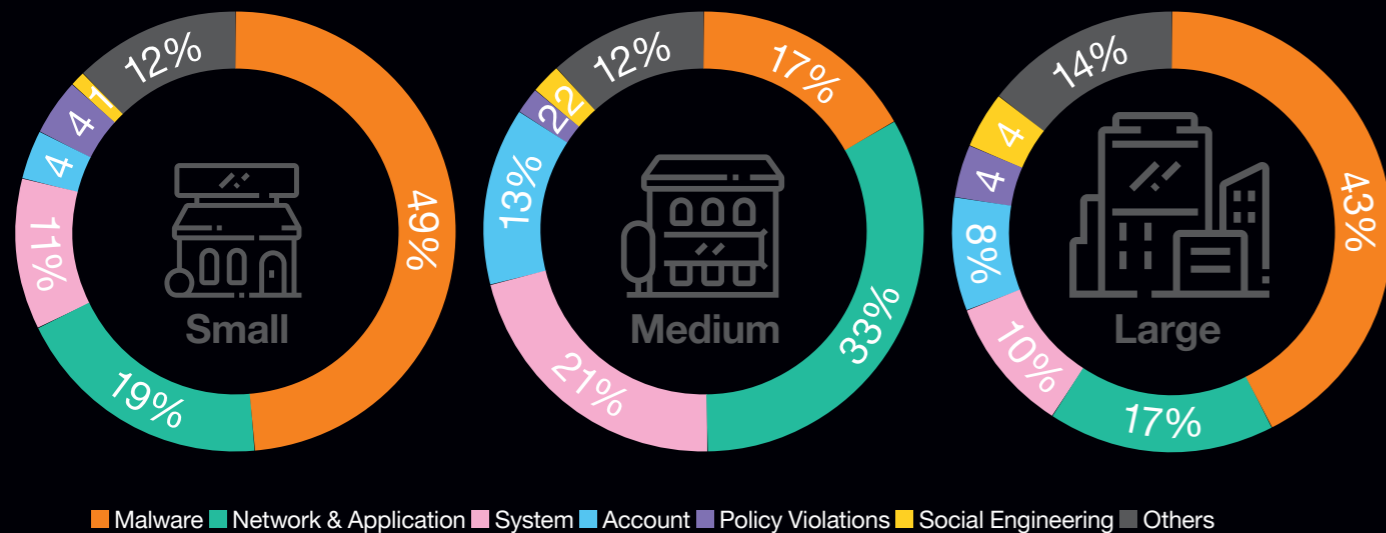
We map our detected incidents not only through classifications but also by connecting certain 'demographics' of the client. One of these is organization size.

Proportionally, we saw a 27% increase in the number of businesses that fall under the 'Small' categorisation. Both Medium & Large business sizes saw proportional decreases of 10% & 23% respectively. Overall, during the past 12 months, we have seen a growth of our client base in all three business sizes.

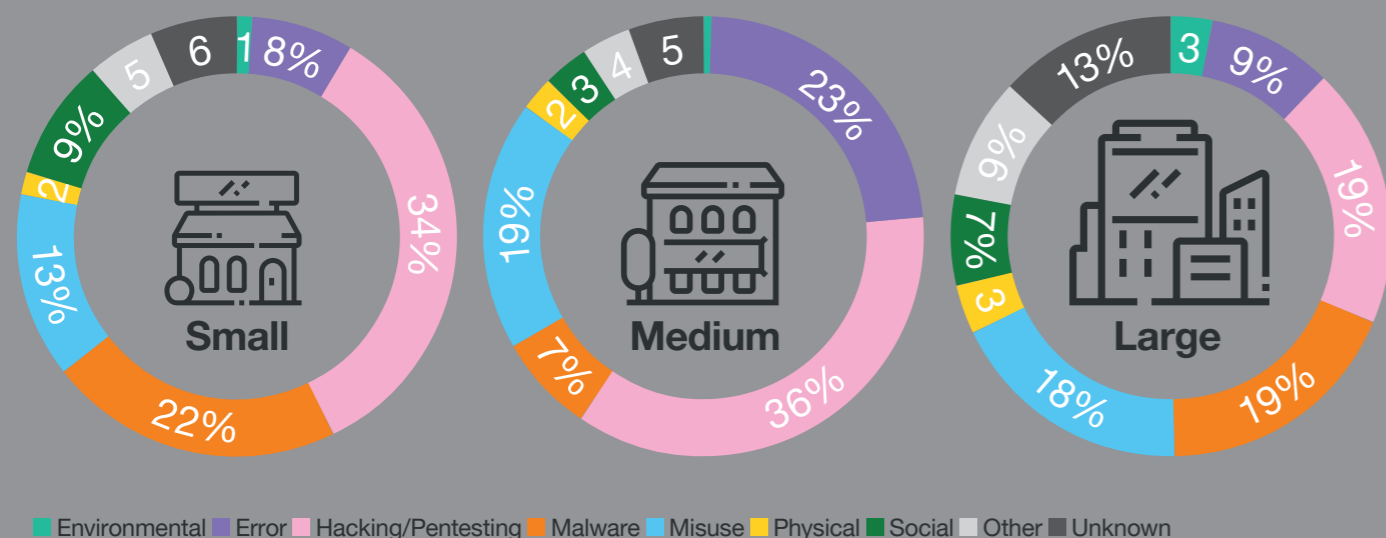
We differentiate between business sizes as the following:

- Small - Micro 1-9
- Small - Small 10-49
- Small - Medium 50-249
- Small - Large 250-999
- Medium 1000 - 9,999
- Large > 10,000

This year our data shows that Large businesses had more than 5x as many confirmed incidents than Small or Medium organizations, and almost 3x as many as Small and Medium sized organizations combined. In total Large organizations were responsible for 72% of the confirmed incident count in the past year.



## New VERIS categorization:



## Small organizations

For this year's Security Navigator 'Small' businesses (less than 1000 employees) represented 46% of all the clients, making up a total incident volume of 15.5%, or 13.9% of confirmed True Positives. Almost half (49%) of these True Positive incidents were some form of Malware - an increase on the 35% noted last year. This is a Continuation of the pattern of year-on-year increases for malware incidents (2019: 10%, 2020: 24%, 2021: 35%, 2022: 49%). We also see that, other than System Anomalies, volumes of all other incident types fell. Both Network & Application Anomalies and Account Anomalies dropped by 10% each, whilst System Anomalies jumped by around 5%.

## Medium organizations

We categorise 'Medium' size businesses to be those with an employee count of between 1,000 and 9,999. This year they represent 35% of our client- and almost 25% of all detected incidents, 13.6% of which were confirmed true positives. If we breakdown those confirmed incidents for this group of businesses, the top 3 consist of Network & Application Anomalies (33%), System Anomalies (21%) & Malware (17%). This bucks the trend we see for our 'Small' and 'Large' organizations, where Malware jumps from third placed to first for both groups. This follows a similar pattern to what we reported last year with the exception of System Anomalies, which has replaced Account Anomalies in the fourth place this year.

## Large organizations

'Large' businesses, those with more than 10,000 employees, constitute 18% of the clients represented in the report this year. However, despite having the lowest representation, they generated almost 60% of all incidents we responded to, of which 72.5% were confirmed true positives. These incidents follow a similar pattern to 'Small' organizations with the top 3 also consisting of Malware (43%), Network & Application Anomalies (17%) and System Anomalies (10%). Compared to last year, the volume of Malware incidents has remained the same while there has been a slight increase in Network & Application Anomalies, and Account Anomalies took third place from System Anomalies.

Obviously, due to their nature, it is fair to expect that 'Large' businesses will have the highest number of incidents. After all, more employees will naturally equate to more endpoints, servers and network traffic resulting in the generation of more logs and a larger attack surface. However, it is also fair to assume that they will have better protection than smaller organizations with more layers of defense in place, so it is interesting to note that the breakdown of incidents follows the same pattern as it does for the businesses we classify as 'Small'.

## What VERIS tells us

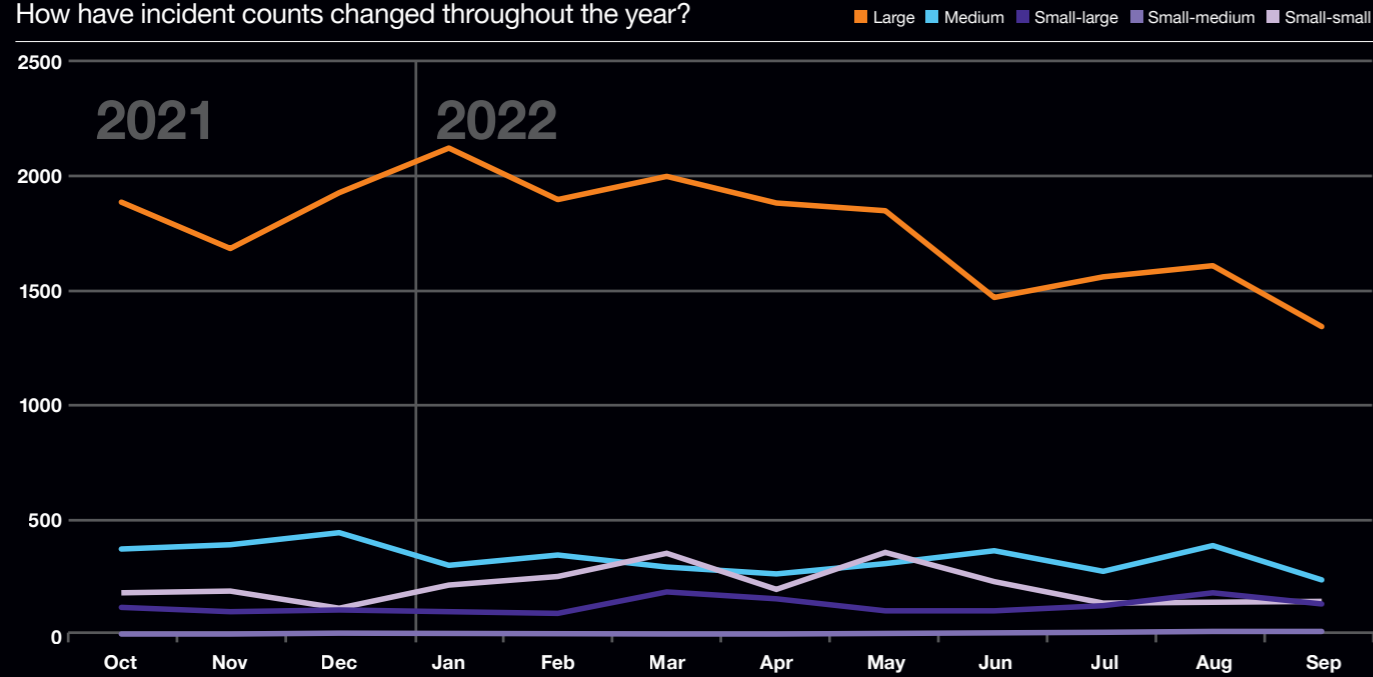
When we analyze the breakdown of categories using VERIS, the Malware category constitutes a much lower percentage of true positive incidents for all business sizes compared to our traditional categorizations. This is because the VERIS categories describe what we believe happened, while our traditional reflected how the incident was detected. Despite this difference in meaning, 'Malware' incidents remained significantly lower for 'Medium' sized businesses than their 'Small' or 'Large' counterparts. It's hard to draw any firm conclusions at this time as to why this is the case as we do not have a full 12 months' worth of VERIS data across all clients to draw on.

The most prevalent category in all business sizes, joint highest for 'Large', was Hacking/Pentesting. Due to its broad coverage, along with it including legitimate penetration testing activities, it is to be expected that this category would feature highly. Interestingly though, it made up a bigger percentage share in 'Small' and 'Medium' sized businesses, with 34% & 36% respectively than it did in 'Large' organizations that only had 19%.

Whereas the Malware & Hacking/Pentesting categories made up more than half of the confirmed incidents for 'Small' and 'Medium' sized businesses, 'Large' ones had a much more balanced distribution of incident types. Especially when you look at the top 3 incident types of Hacking, Malware/Pentesting & Misuse which were all at or around the same percentage level. One possible explanation for this is that larger businesses may have the budget and resources in place to afford a more layered approach to their defenses resulting in more places where a threat can be detected or prevented.

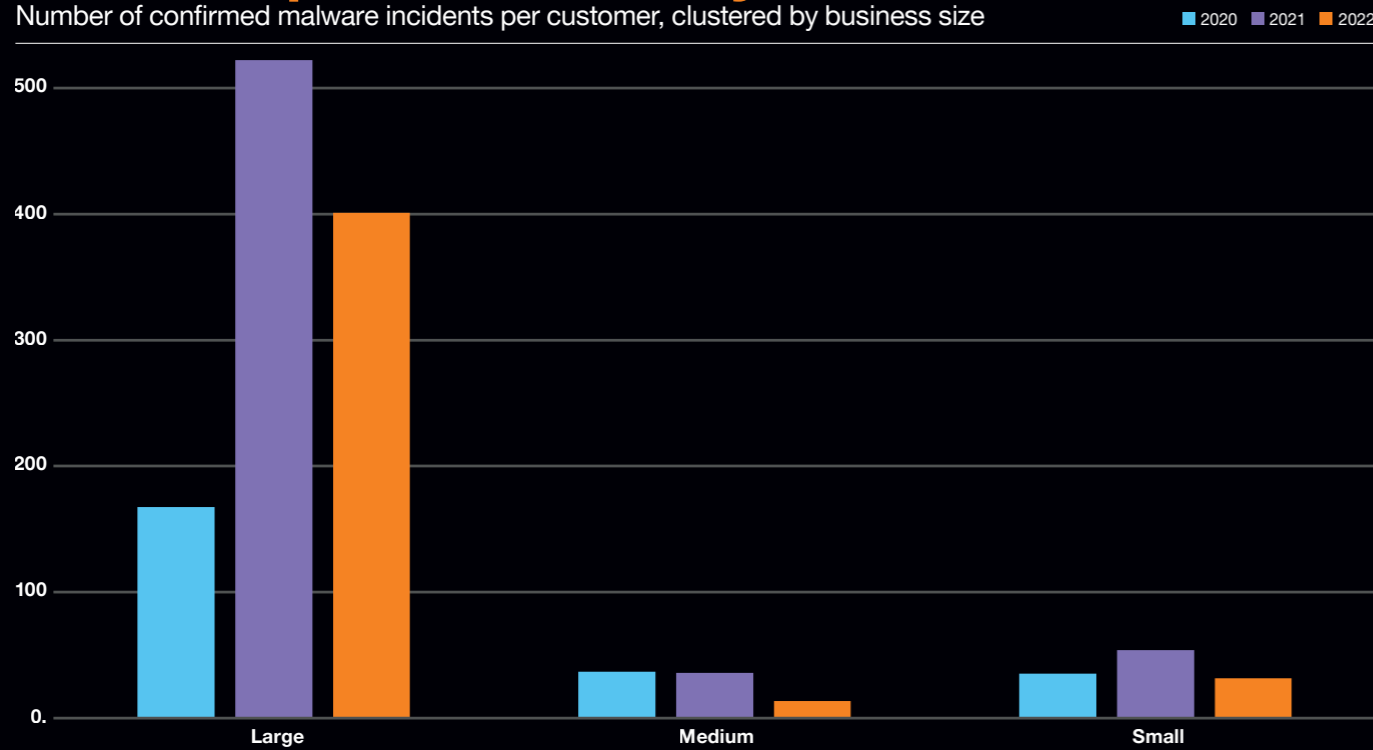
## Incidents by business size over time

How have incident counts changed throughout the year?



## Malware per customer by business size

Number of confirmed malware incidents per customer, clustered by business size



On a normalized basis Our Large clients generate about twice as many Malware incidents as their Medium-Sized counterparts. Small businesses in turn experience about half as many Malware incidents as that. This is because the number of Malware events are directly proportional to the number of endpoints.

We also note, however, that the Large businesses in the chart below have full visibility over their endpoint security events (including their EDR and native Microsoft telemetry), whereas the Small businesses have only achieved a level of 68% on average.



# Ransomware

## Background

In 2019, a ransomware group known as the ‘Maze team’ started the trend of publicly naming and shaming ransomware victims. The success of this extortion technique was recognized by other groups and has since been widely adopted.

“Double extortion” involves the use of leak websites on the dark web that are created by threat actors to publicly post sensitive data of their victims and thus apply pressure. These sites can be discovered and viewed by anyone and thus offer a perspective into the shape and volume of the crime.

Since this so-called ‘double extortion’ scheme was adopted by other threat actors, we have recorded an average of around 16 active leak sites on the dark web per month. This is 3 active leak sites less than we have seen the previous year (2021: 19). Collectively, these sites listed a victim count of 176 (in average) per month. Again, we see a decrease of 20% to last year. One reason for this is that two major threat actor groups, REvil and Conti have closed their criminal activities during this period.

## Reminder on Terminology

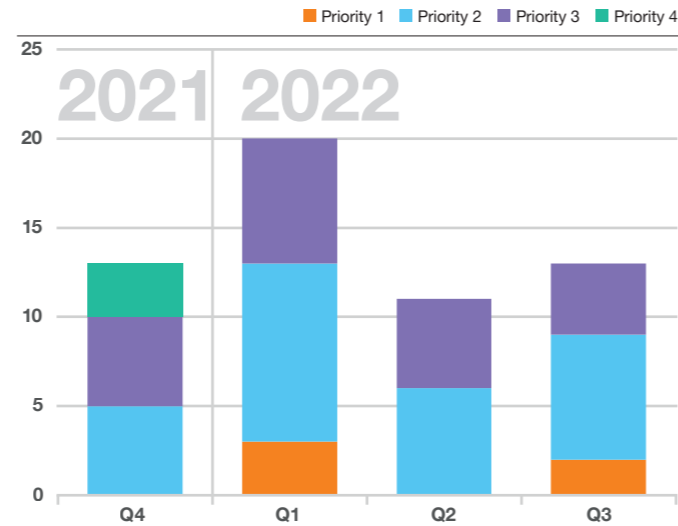
We have multiple perspectives on the ‘ransomware’ problem from our various datasets, and each perspective tells a different part of the story, so we need to be more precise with our terminology here.

We use the term ‘ransomware’ when referencing our CyberSOC data to refer to any incident that involves an attempt to encrypt data, but also any incident that can be linked to strains of ransomware or ransomware threat actors somewhere in the killchain.

For the criminal act of extorting ransom from a victim, we use the term “Cyber Extortion”, or Cy-X.

**“Cy-X is a form of computer crime in which the security of a corporate digital asset (Confidentiality, Integrity or Availability) is compromised and exploited in a threat of some form to extort a payment”.**

## Ransomware in the CyberSOC



Our CyberSOCs have not had a standard categorization for Ransomware in the past. Of the 10,700 odd True Positives categorized by the new VERIS case masks, only 29 were specifically classified as Ransomware. But we do have several specific detection sets that seek to identify ransomware via some or other means. By combining the data from these two case masks we can derive the chart above.

While we do deal with confirmed incidents related to Ransomware on a regular basis, the volume of such incidents is miniscule in context. The reason for this is simple: A successful Ransomware attack – resulting in encryption of data or some other form of extortion – is still an extraordinary event, and generally dealt with by our CSIRT teams. What the CyberSOCs deal with are early indications that a ransomware attack may be in progress. At these early stages of the attack killchain, indicators may evolve into a number of different kinds of breach if not responded to. It is hard to discern the attacker’s intent, and as the incident is (by definition) detected and responded to, the Ransomware incident that may have emerged never materializes.

## Ransomware in World Watch

The chart below illustrates the frequency with which Ransomware was referenced in our World Watch advisories.

The ransomware landscape was busy with noticeable spikes in March and April 2022. This was courtesy of the Conti chat log leaks and activity of the Lapsus\$ group combined with the war in Ukraine. This is not limited to just these as this space is rather busy.

REvil is quite the name in ransomware circles, but its activities finally attracted the ire of the US government. It felt the heat and started winding down its activities in October 2021. REvil also claimed that its infrastructure got hacked not seeming to hang around to find out who. To the surprise of many, the US and Russia announced that they were working together against REvil. In mid-January 2022 Russia said it arrested suspects possibly associated with REvil/Sodinokibi. Unfortunately, the progress was short lived. In April 2022 ransomware operations resembling REvil were spotted again.

Evil Corp, a Russian cybercriminal group known for their Dridex banking malware, was noted to have switched to using LockBit malware to encrypt victims’ data. Later, Microsoft revealed that Evil Corp was also dabbling with a USB-based malware that it said could worm or replicate.

Emotet is a dangerous and highly effective malware delivery platform that was shut down by law enforcement in early 2021. The world thought it saw the last of Emotet, but that turned out to be short lived. The group behind Conti is believed to have resurrected Emotet allowing the scourge to torment victims again.

New ransomware named Nokoyawa was discovered with possible links to Hive. At the time of discovery Nokoyawa targeted victims in South America, such as in Argentina. Analysis published about Nokoyawa notes the use of Cobalt Strike as part of the attack. Incidents involving Conti also used Cobalt Strike as part of its post exploitation activities.

Details about a new ransomware called White Rabbit were shared publicly. This is a relatively small piece of malware with similar anti-analysis tricks to those used by the Egregor ransomware.

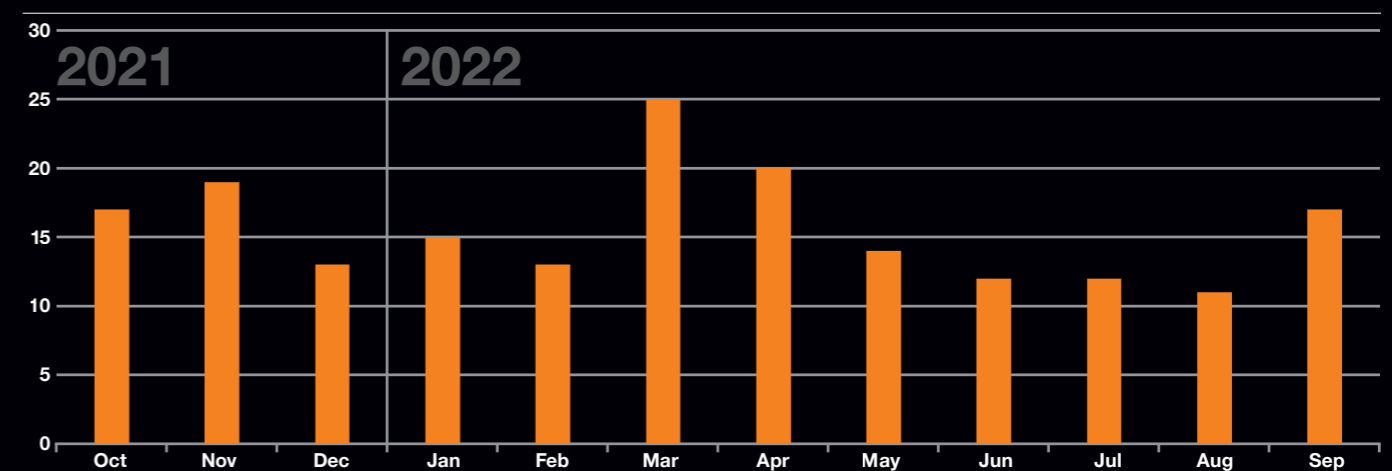
In March we saw that Hive ransomware ported its malware to the Rust programming language. At the time, this malware managed to evade detection before it was identified by a researcher.

LockBit is one of the most successful ransomware groups of 2022 when looking at number of victims listed on their leak site. LockBit announced the release of version three of their malware. The new capability allows attackers to explicitly kill certain defined processes before encryption of the data starts. LockBit has grown in the absence of other infamous groups such as Babuk, DarkSide, REvil and Conti. Ironically LockBit was possibly breached which resulted in the source code for its malware leaking. This unfortunately could lead to variants of new malware as others learn from the experience and success of the LockBit malware authors. This assumption was already tested when analysts reported that there exists overlap in code between BlackMatter and LockBit 3.0. There could be a variety of reasons for this and may not be linked to the LockBit source code leak. Malware authors are known to borrow parts from one another through splicing compiled code fragments into their own.

Black Basta was found using encryption malware that can target hypervisors such as VMware ESXi servers to encrypt the data at a higher rate. Cybereason released analysis of Black Basta ransomware stating that there are strong links to Conti, confirming what others have claimed.

Some groups, such as Vice Society, uses a variety of ransomware. Vice Society is known to have used the Zeppelin and HelloKitty malware. Vice Society is also known for quickly capitalizing on new impactful vulnerabilities such as the serious Windows printer flaws known as PrintNightmare.

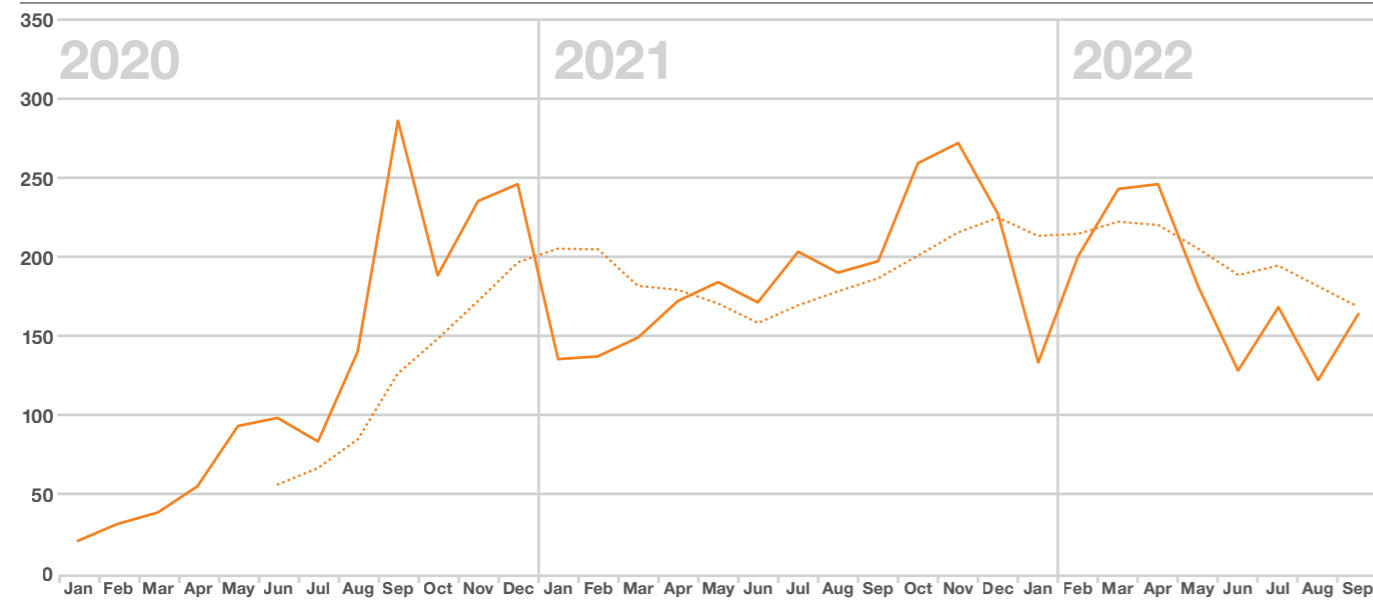
## Ransomware in World Watch Advisories



# Cyber Extortion

## Cy-X victims over time

Observable victims on leak sites



### Cy-X Threat Site Monitoring

At the beginning of 2020, we increased our research capabilities to understand the Cyber Extortion threat better. We collect data with a scraper that monitors known leak sites of double-extortion threat actors. This is an automated process and provides us with simple data points such as which threat actor group was involved, which victim suffered the attack, etc.

We then spent some time enriching the data manually each month. Here we research who the victims are in order to understand the victimology of this threat better. We also investigate as far as possible how the attack occurred. We tag the data entry with attack types, check for indications if the victim might have paid ransom and document the size of the data that was stolen. Additionally, we classify the type of data that was stolen according to the VERIS framework.

### Cy-X Country Breakdown

Large, English-speaking countries have always been the most impacted by Cyber Extortion. This is primarily because of the size of their economies. Of the 10 countries with the most recorded victims, 7 are also counted amongst the world's biggest economies as measured by 2022 nominal GDP. The bigger the economy, the more businesses, the more potential victims, the more compromised victims.

Where we see exceptions to this general rule, as for India, Japan and China, we argue it is most likely due to language and cultural 'barriers', which makes organizations headquartered in those regions harder to extort.

English speaking countries are a comfortable and familiar target to threat actors that have limited international experience and language skills. Regions like Asia, Africa, South America or the Nordics and even non-Anglophone Europe thus don't feature in our dataset as much as we'd expect them to.

This however started changing in 2021 and has Continued to do so throughout 2022.

As we show in the chart on the right, we observed a drop in US based volumes of 8% in the last 12 months, and a notable drop of 32% for victims in Canada.

In general, while there has been a notable decrease in observable victims since October 2021, we also note that the location of victims seems to be shifting – from the US and Canada, through the UK and Western Europe, and toward the rest of the world.

The number of Chinese victims has increased 182%, though they remain low in comparison to the victims observed in other regions. The second biggest increase is in the region labelled 'Other' with an increase of 148%. While this category is broad with many different countries, it does show us that the shape of the threat is changing, and almost every other country is impacted.

The number of victims in the 'Nordics' (DK, SE, NO, FI) and Middle East (AE, SA, BH, QA, TR, JO, KW, SY, LB, OM, etc) has more than doubled, though they also remain small proportionally.

Noteworthy is also that Latin America (CR, BR, CO, PR, AR, MX, CL, PE, BO, DO, EC, VE, HN, PA, PY, NI, GT, etc) has joined the top 5 of most impacted regions.

This is a trend that we have closely been following and communicating for quite some time, up to the case of Costa Rica's compromise and extortion by Conti in April 2022.

These changes accelerated during the last 6 months of our reporting period, with decreases of 34%, 33% and 20% in the UK, USA and Europe respectively, while East Asia and Southeast Asia grew by 30% and 33% over the same period.

Why is this change happening? One reason may have to do with the threat actor groups themselves.

While we generally believe that most Cy-X attacks are opportunistic rather than targeted in nature, we do see that of all Canadian victims between October 2020 and October 2021, Conti was responsible for 19%. During the last 12 months (between October 2021 and October 2022), the Conti operation shut down, significantly contributing to the reduction in victims. The threat actor 'Everest' contributed 10% of the Canadian victims for the prior 12 months period but they also recorded only a single Canadian victim during the last 12 months.

By contrast, the victim counts in the United Kingdom (another English-speaking country) increased by 21% compared to the previous 12 months. In this case the LockBit2 group – while being active during both periods – recorded 5% of U.K. victims during the first period but over 23% during the last 12 months. LockBit3 – the new version of LockBit2 – added another 5% of U.K. victims. This suggests that the LockBit threat actor group is responsible for 5x more U.K. victims in the past year than in the prior 12 months.

Threat actor targeting changes could therefore explain some of the trends we observe in country victimology.

We explore why Cy-X numbers have decreased over all in our [summary](#) at the end of this report.

As we mention elsewhere in the Navigator, for a brief period at the start of the Russian invasion of Ukraine our Polish teams noticed cybercrime levels dropping, as criminals from that region were impacted and distracted by the effects of the war. By April those numbers were increasing again. That's what we expect to happen with Cyber Extortion in the rest of the world also.

Larger economies logically experience higher levels of Cyber Extortion, but western, English-speaking countries are also a more 'familiar' target for cyber criminals, who need to grasp the language and some business practices in order to conduct a successful negotiation.

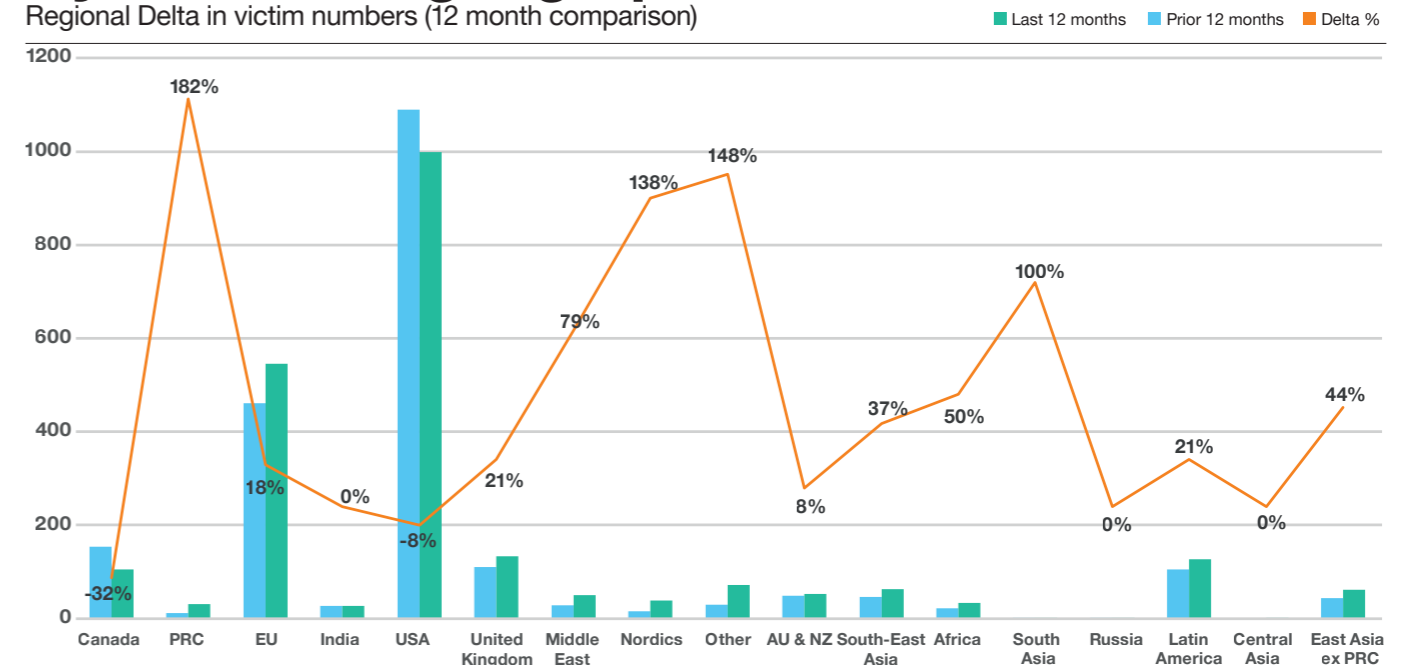
As we note in our conclusion[summary], high profile attacks against businesses in the USA have caught the attention of Intelligence Agencies, Regulators and Law Enforcement and caused concern within the cybercrime community, who dislike the high level of attention. This may be causing actors to 'hold back' on compromising or extorting victims in the USA, Canada and the UK.

Some countries may therefore be able to manage the flow of victims in their backyards, but to the extent that they succeed, we anticipate the crime will only spill over to other, smaller and non-anglophone countries.

Think of the obstacles presented to extortionists by language and business culture as a low dam wall. While the systemic factors that enable Cyber Extortion remain in place (as they have), the 'water level' will continue to rise. Even if the crime can no longer flow comfortably into the familiar, large, English speaking countries, it will still want to flow somewhere. Eventually we expect it to break its banks, overcoming the limited obstacles impeding its course, and continuing its steady flow.

## Cy-X victims: geographic shift

Regional Delta in victim numbers (12 month comparison)



### Cy-X Industry Breakdown

In considering which industries are the most impacted by the Cy-X threat, we see very similar patterns to what we have observed previously. Manufacturing remains the most impacted industry with almost the exact victim count in the past two years – bucking the trend we’re seeing elsewhere. One fifth of all victims are from Manufacturing.

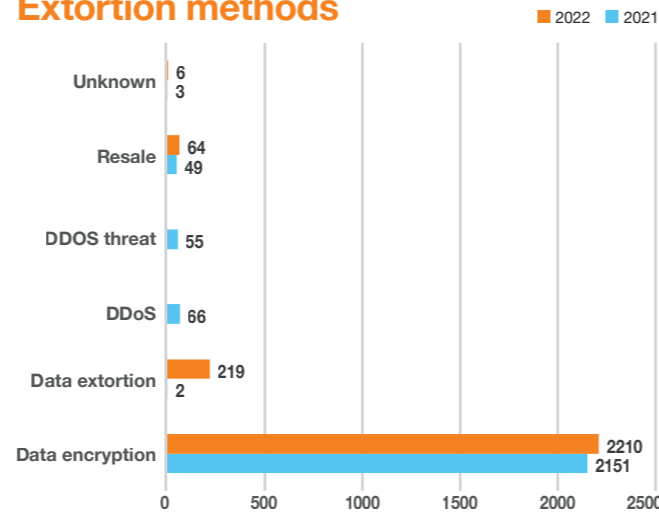
One change that we do notice for Manufacturing is in the probability that the victim has paid the threat actors. While we documented a 5% probability of payment between October 2020 and September 2021, we now see that in the past 12 months the Manufacturing sector might have paid in as many as 8% of all incidents.

We also notice a small change in extortion type, which could explain the higher probability of payment. While most incidents were classified as standard encryption in 2020/2021, in the past 12 months ‘data extortion’ incidents - involving no encryption – have increased. In cases where data was stolen with a threat of leaking, victims often pay a lower price than when they also have to buy the decryption key. Naturally, the prices are then lower and the likelihood to pay might increase. This is a trend generally observed in the threat landscape of Cy-X but seems to be also present for the Manufacturing industry.

The top 10 industries impacted by Cy-X are exactly the same as we observed last year. Only with small changes in the proportions. We Continue to believe, therefore, that the industry patterns don’t reveal any specific attacker targeting but rather that those industries most impacted seem to be particularly vulnerable in one way or another.

We can see that in 2022 data extortion has become more prevalent, while ‘traditional’ extortion by encryption has decreased.

### Extortion methods



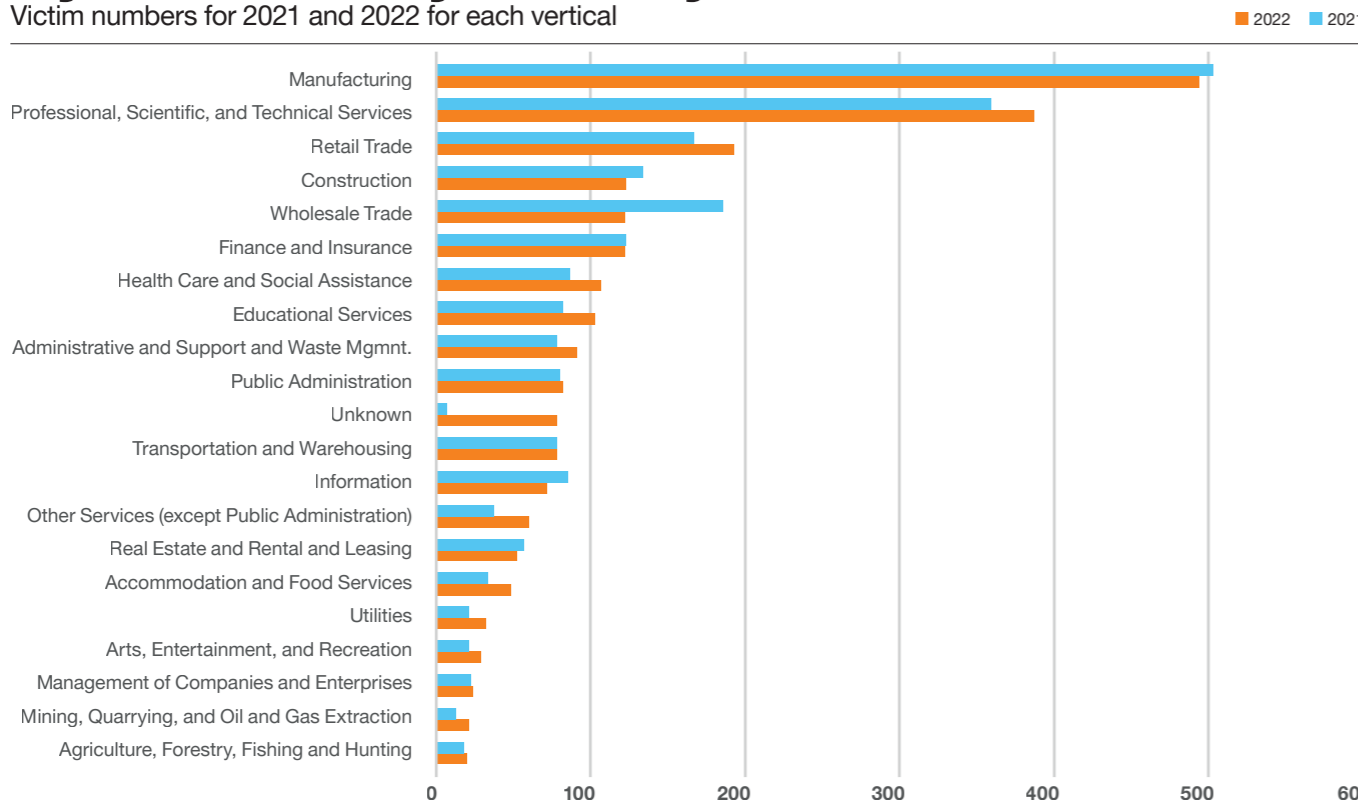
Data extortion is where threat actors do not encrypt anything, but only threaten to publish the victim’s stolen data.

As potential victims have apparently learned to defend themselves against encryption attacks by deploying backups, certain threat actors like Black Basta have started to only perform this type of extortion. We have also seen a decline in threat actors threatening or using DDoS as a method of extortion. This is likely due to the cost benefit ratio for this form of attack no longer being considered worthwhile.

The heart of this form cybercrime is extortion – an act in which the criminal takes something of value to the victim and ransoms it back – not encryption. Until the fundamental systemic factors that enable this form of crime are addressed, we should expect to see criminals Continuing to adapt and evolve new forms of extortion as victims evolve to counter each particular form.

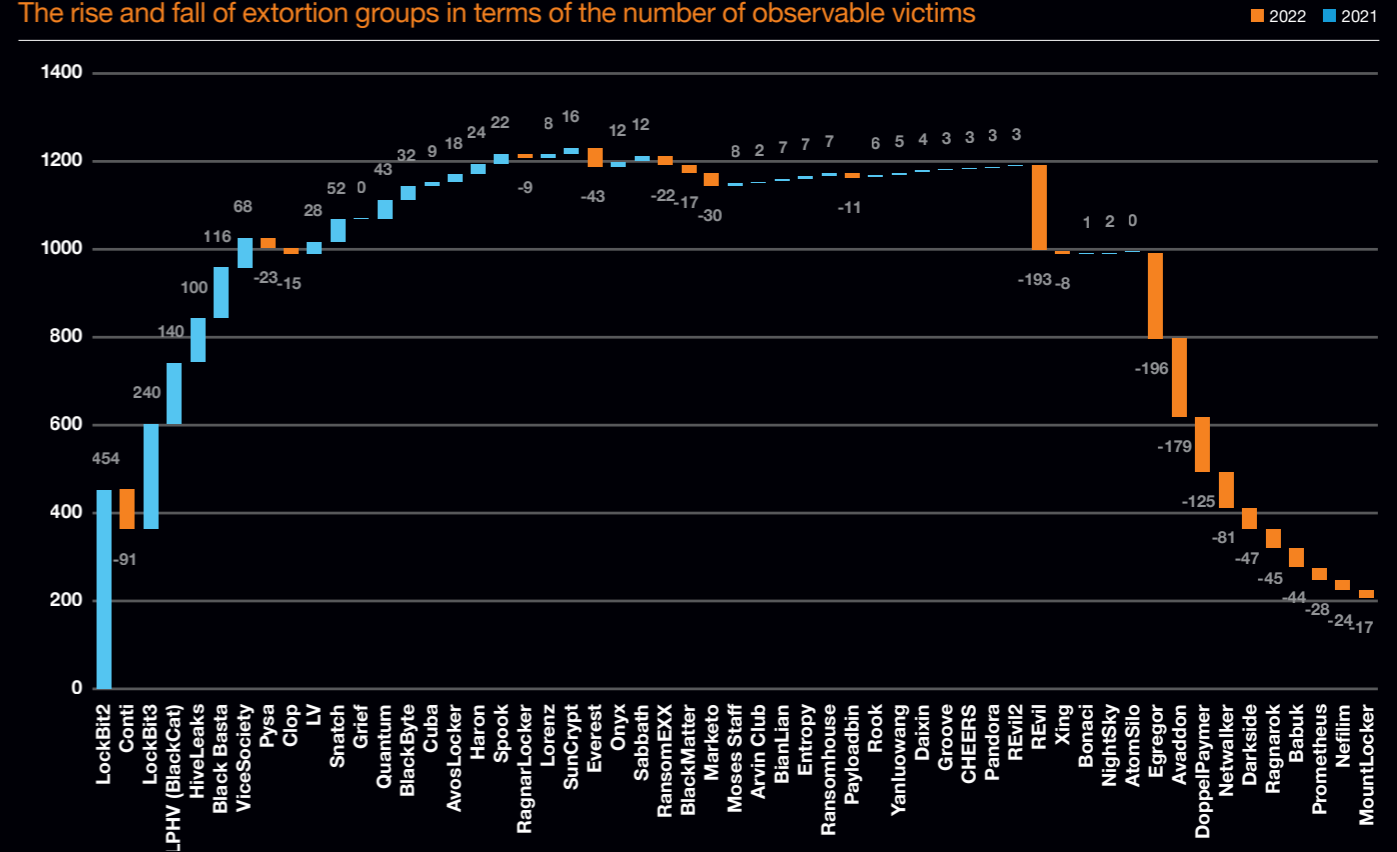
### Cy-X victims by industry

Victim numbers for 2021 and 2022 for each vertical



### Changes in victims by actor

The rise and fall of extortion groups in terms of the number of observable victims



The chart above shows increases (blue) and decreases (orange) in victim counts from last year to this year per actor. We note that some actors, like Conti, REvil, Eggor and Avaddon have essentially disappeared from our data, while others like LockBit, ALPHV and Black Basta recorded high numbers of victims in the last 12 months.

### Cy-X Threat Actors

However, after Conti disbanded in Q2 of 2022, we saw LockBit2 and LockBit3 become the biggest Cyber Extortion actors in 2022 with over 900 victims combined. Conti remains the most successful actor in our dataset.

Out of the 20 biggest actors observed in 2021, 14 were no longer in the top 20 in 2022. This shows how short the lifetime of a Cyber Extortion group truly is. We tracked 49 actors in 2021, compared to 47 in 2022. But the distribution of victims across these groups has clearly changed dramatically.

### Cy-X in World Watch

Cyber Extortion featured regularly in our World Watch advisories over the past 12 months. Most notable was the drama involving Conti.

Shortly after Russian military forces touched Ukrainian soil in February, Conti issued a statement siding with Russia. This was the start of the end for Conti. Some members of the Conti gang were offended and someone proceeded to leak internal messages from the group’s chat servers, providing fascinating insights into the dynamic of the group. Conti’s swan song might have been the final big hit on the Costa Rican government between April and May 2022.

The compromise caused severe disruptions and resulted in the newly elected president having to declare a national State of Emergency.

But other fascinating events made the news also.

The LockBit group claimed Entrust, the digital identity provider, as a victim in August 2022. A few days later LockBit reported that it was suffering a DDoS attack, leaving many to speculate if this was retaliation by a recent victim.

The Lapsus\$ group breached several large corporates including Nvidia, Samsung, Okta, IT firm Globant, Uber, and video game maker Rockstar Games. Appearing almost out of nowhere they quickly made a big impression. These high-profile scores led to the arrest of several suspects in the UK.

## Looking at verticals

The breakdown on the right shows an overview of all verticals and the threat actors considered responsible for their incidents. While we are still in the process of adopting VERIS, it does provide some insight into what kinds of actors are being encountered by each industry. Of course, these findings can be significantly shaped by the detection capabilities of each customer in the respective vertical.

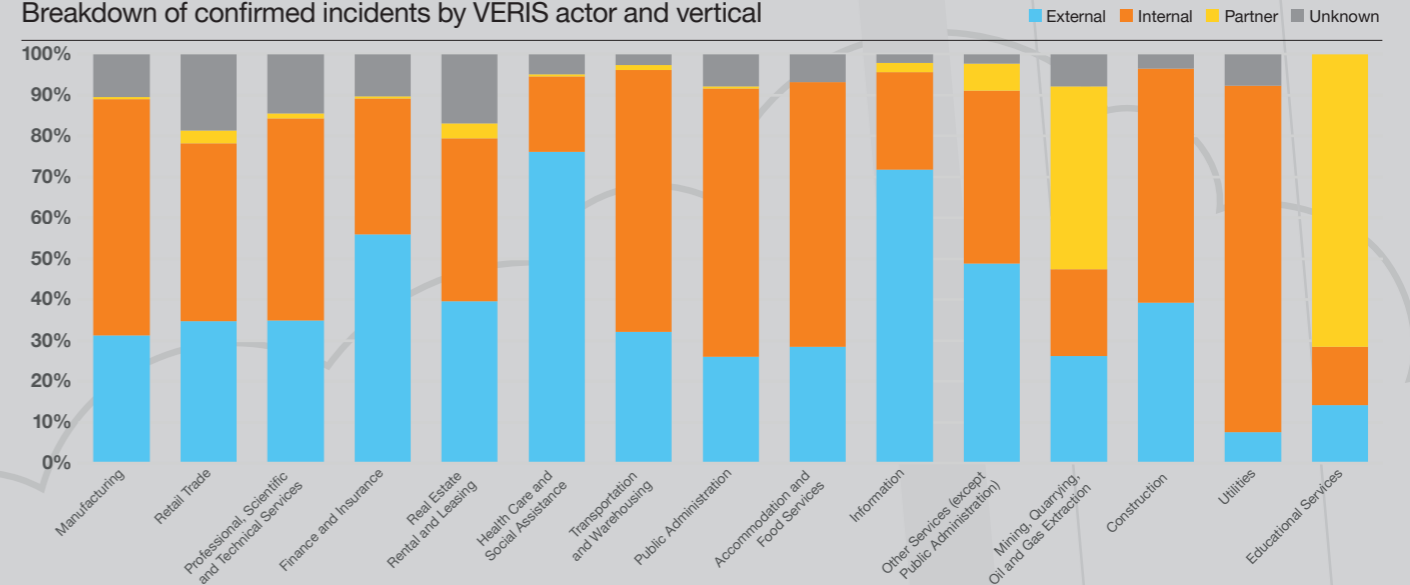
**It is somewhat remarkable how many industries seem to deal with more internal 'actors' than external ones.**

External actors typically originate outside of the organization, such as individual, malicious hackers, state-backed threat actor groups, APTs, former employees etc. Internal actors are operating from within the organization itself. These could typically be employees, consultants, interns etc. Partners are third parties, such as vendors, suppliers, outsourced IT support and the like.

**Also important to note: actions that have triggered security incidents can be malicious or non-malicious, intentional as well as unintentional.**

## Sources of incidents by industry

Breakdown of confirmed incidents by VERIS actor and vertical



### Professional, Scientific and Technological Services

This vertical is represented among the top 3 in our client base, comprising 13% of all our clients. 10% of all potential security incidents come from this vertical. Our security analysts have analyzed over 1,800 confirmed security incidents.

Network & Application Anomalies is the top incident category for this industry, with 37%, which is a very similar to last year (2021: 35%). System Anomalies represent 19%. Again very similar to last year's proportion of 20%. What sticks out is that confirmed Social Engineering incidents have reduced proportionally by over half, to 4%. Account Anomalies have also decreased proportionally, from 12% to 7% for this edition.

We observe a steady level of confirmed incidents per month for this industry, with only two exceptions in January 2022 and September 2022, where we noted small peaks. From a VERIS perspective, this vertical has mostly dealt with internal threat actors (49%).

The top 3 internal threats we recorded were 'Net misuse', 'Unapproved hardware/ software/ script/ workaround' and 'Malfunction'. External threat actors caused true positive incidents in 35% of cases, while 1,2% were attributed to 'Partners' and the rest were unattributed. The top 3 externally attributed cases for this industry were Web Attacks, Port Scan and Spam.

### Real Estate, Rental and Leasing

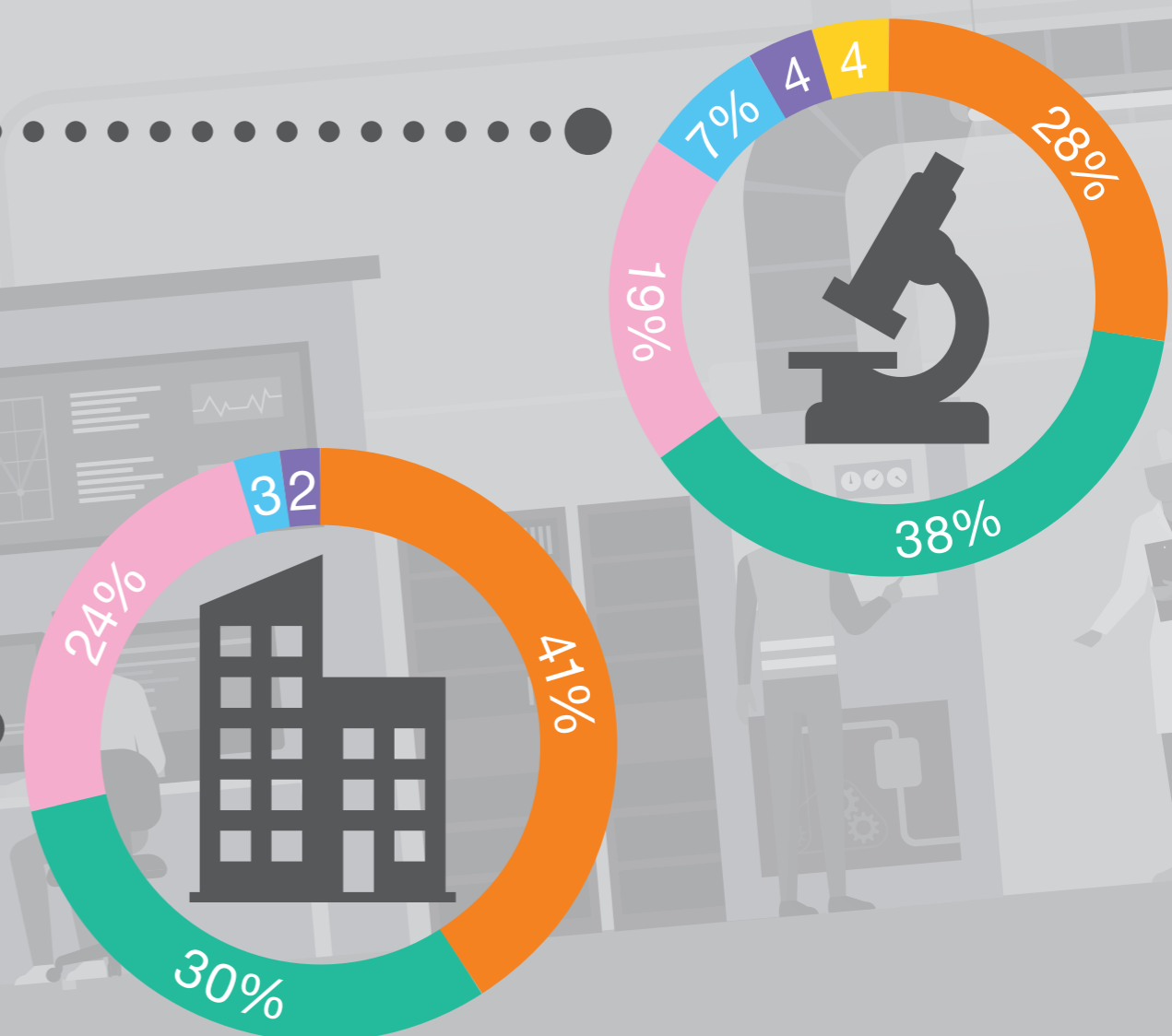
This vertical only represents 2% of our clients and equally contribute 2% of all incoming security incidents. Nevertheless, our security analysts investigated and confirmed approx. 900 security incidents.

This industry sticks out with a proportionally high true positive rate. Half of all raised incidents were confirmed to be true, 29% were classified as 'True Legitimate', only 17% were classified as 'False Positives'. The top category seen was Malware, with 41%, compared to only 16% of true positives last year. The second largest incident category is Network & Application Anomalies, with 30% (2021: 37%), followed by System Anomalies with 24% (2021: 28). Real Estate has the second highest proportion of System Anomalies after the Transport and Warehousing vertical.

However, both of these represent a small part of our overall industry distribution.

From a VERIS perspective we see an equal share of confirmed incidents being attributed to external and internal actors. These claim 39% of confirmed incidents, while 17% remain unattributed and almost 4% were caused by partners or third parties.

The most prevalent threat actions were spam, phishing and Net misuse. These were followed by Web Attacks, Malfunction, Spam (caused internally). Interestingly, in 14 security incidents, we saw that partners caused the incident. Confirmed security incidents over time show a steady increase between October 2021 and September 2022, with the peak in September 22.



Malware Network & Application System Account Policy Violations Social Engineering Others

\* Figures rounded to integers

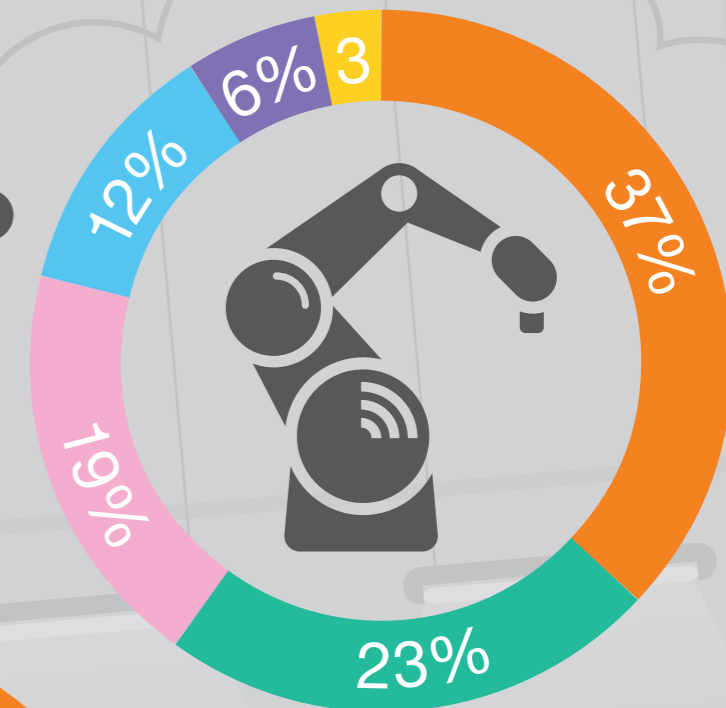
### Manufacturing

The manufacturing industry is once again the largest sector in our dataset, both in the number of clients and consequently the number of incidents recorded. Approx. 28% of all our clients are from Manufacturing. Collectively they contribute 31% of all potential incidents.

Our analysts worked on over 7,000 confirmed security incidents within the time frame. 37% were categorised as Malware-related, followed by Network & Application Anomalies with 23% and System Anomalies with 19%.

For the confirmed incidents where we have data from the VERIS framework, we observe that this industry is confronted by a larger proportion of internally-attributed incidents. 58% are internally caused, while 32% were externally caused, 1% were classified as "Partner" or third parties.

The rest were not attributed by our analysts. Where external threat actors were blamed for the incident, we observed Web Attacks, Port Scans and Phishing as the top three actions. For the incidents where the actor was classified as internal, we logged 'Unapproved hardware/ software/ script/ workaround', 'Malfunction', and 'Backdoor' as the most common actions.



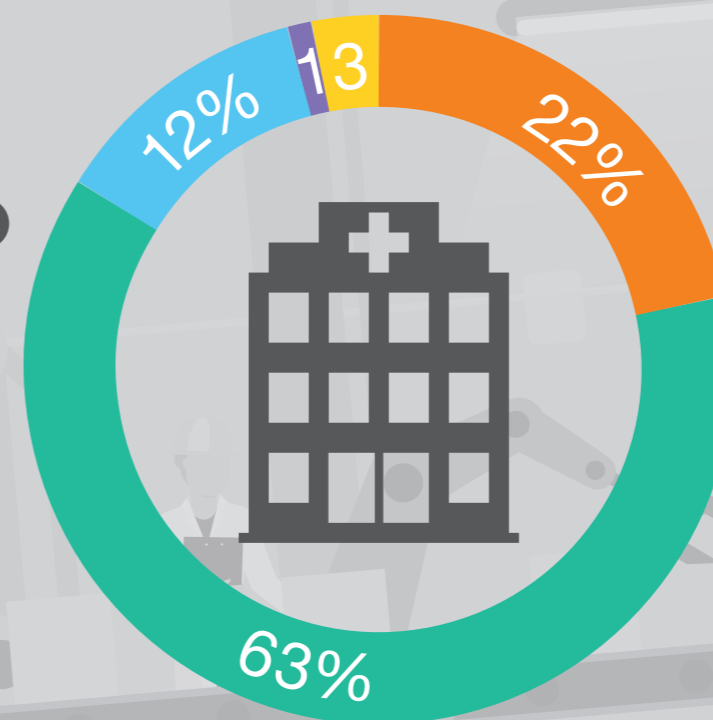
### Healthcare and Social Assistance

The healthcare sector represents 7% of the clients in our dataset and is thus our 4th-biggest industry. Like last year, healthcare ranks 7th in terms of the volume of incidents raised.

Most confirmed incidents were classified as 'Network & Application Anomalies' with 63%, followed by Malware-related incidents with 22%, and Account Anomalies, with 11%. This industry still has the highest proportion of confirmed Network-related security incidents. Social Engineering dropped from 5% of confirmed cases to 3%. From a VERIS perspective, we observe that this sector mostly encountered externally caused security incidents at 76%. 18% were internally attributed and only 0,61% were blamed on partners. This makes healthcare the sector with the highest proportion of externally caused security incidents.

Given that only a part of our incidents have been classified under VERIS, the actual number is relatively small.

Nevertheless, this finding aligns similar findings from Verizon's Data Breach and Investigations Report (DBIR) 2022<sup>[2]</sup>. Verizon also assesses that this industry has undergone a change from primarily dealing with the 'insider threat'. In recent years the industry has appeared to increase its internet attack surface and thus has also experienced more attacks and breaches by external threat actors.



### Finance and Insurance

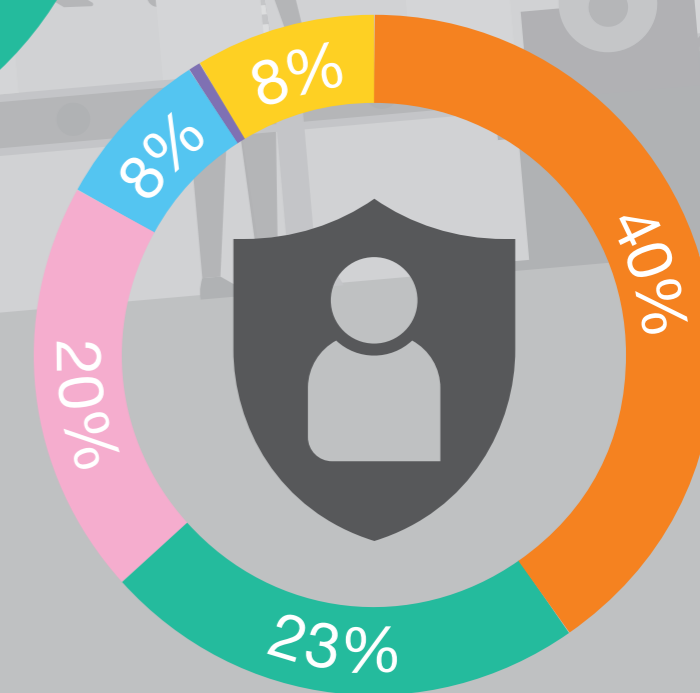
The Finance sector has gone down one spot in representation in regards to potentially seen security incidents. While last year Finance and Insurance ranked as the fourth highest, this sector has the 5th highest security incidents raised with a number of over 9,000. In our client database, we recognize that 13% of all our clients originate from this sector.

While we have seen a decline of confirmed Malware incidents last year, in this edition we are observing a much higher proportion of confirmed Malware incidents than the last two years. Confirmed Malware cases took a share of 40% while in last year's report Malware represented only 15% of all confirmed security incidents. Noteworthy though, that the number of confirmed security incidents shrank to half of what we have seen the year before.

Looking at who has caused the confirmed incidents, we registered that over half of the classified incidents were caused by an external threat actor (56%); one third was triggered by an internal threat actor (33%) and the rest was unknown to the analysts.

And lastly, as in previous years, we see one of the highest proportion of social engineering cases residing in this industry. Of all confirmed incidents, over 8% were classified as Social Engineering. In this year's report, this is only topped by the Public sector which has the highest amount of confirmed Social Engineering cases proportionally with 15%.

The top 3 incident categories for this sector this year were Malware (49%), followed by Network-related cases with 23% and System Anomalies with 20%. We see a significant change from last year's number, both in proportion of the top 3 and the categories in itself. The reason for this can be manifold, such as changes in detection capabilities, changes in client base and changes in the global threat landscape.



Malware Network & Application System Account Policy Violations Social Engineering Others

\* Figures rounded to integers



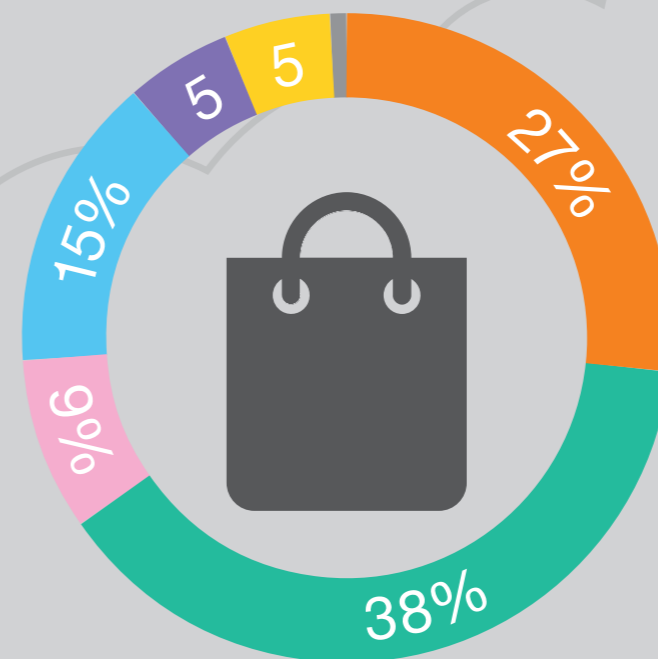
### Retail and Trade

Six percent of our clients are from the Retail sector, which generates 21% of all security incidents we processed. Retail is thus our second busiest vertical. One third of all incidents confirmed as true positives, representing over 3,500 investigations within the timeframe.

39% of confirmed incidents were Network and Application related. This is a big proportional increase from last year, when 22% of all true positives were classified as Network and Application-related. The same goes for the Malware category, where we see a small increase from the year before (2021: 23%, 2022: 27%). While Social Engineering incidents have decreased, overall, Retail is the sector with the third highest proportion of Social Engineering related cases. Like the other industries we analyze in this, Retail deals with more insider-related incidents than external.

From the portion of incidents where we have VERIS classifications, 44% were attributed to internal actors, while 35% were attributed to external threat actors. 19% percent of incidents remained unattributed, and just over 3% were blamed on partners or third parties.

The most common type of incident was the unapproved use of hardware, software, scripts and workarounds by insiders. This was followed by external incidents like phishing attacks, web attacks and the use of stolen credentials. Internal actors were further responsible for privilege misuse and misconfigurations.



### Transport and Warehousing

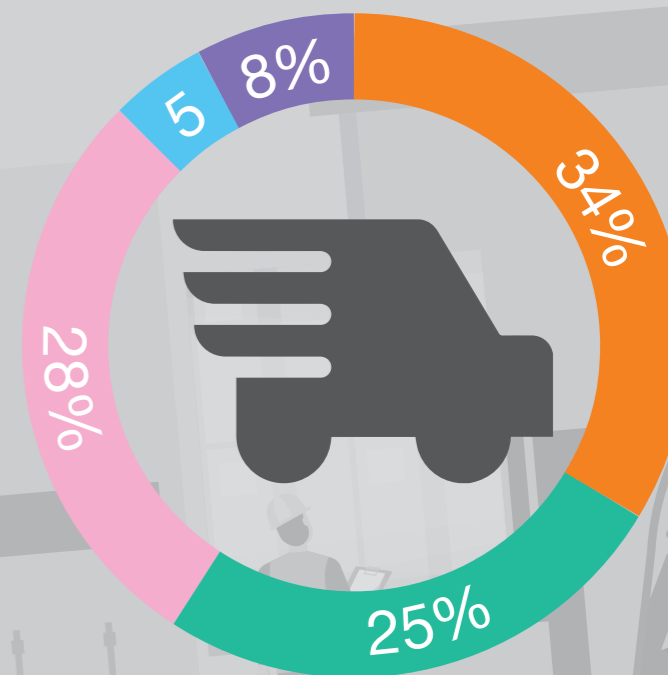
Transport and Warehousing represents 4% of our client base and generated 2% of all incidents.

One third of true positive incidents from this sector were determined to be some form of Malware, followed by 'System Anomalies' with 28% and 'Network & Application Anomalies' with 26%. Interestingly, 'Policy Violation' is the 4th largest category for this sector.

Compared to last year we observed a very similar level of confirmed Malware cases, but proportionally more Network-related incidents and a notable increase in System Anomalies (2021: 7%, 2022: 28%). 64% of all confirmed incidents that have a VERIS classification were attributed to an insider.

32% were externally caused, 3% were unattributed and 1% were blamed on partners or third parties. The major actions attributed insiders were 'Net misuse', Unapproved hardware/software/ script/ workaround' and 'Data mishandling'.

External threat actors, on the other hand, were responsible for Port scans, Web Attacks and Net misuse.

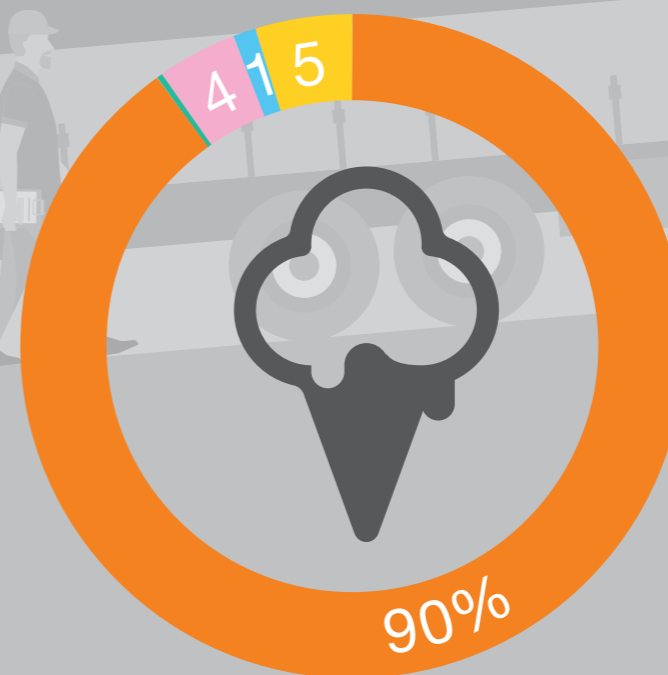


### Accommodation and Food Services

This vertical is somewhat unusual in our dataset and should be considered with caution. While only 2% of our clients originate from Accommodation and Food Services, the volume we process from it represents 10% of our incoming security incidents.

The patterns we see are thus very much shaped by the detection technologies applied. We see in this sector an over-representation of confirmed Malware incidents, representing 90% of all security incidents. This is very similar to what we saw last year. Malware was followed by Social Engineering with 5%, System Anomalies with 4% and Network related incidents at less than 1%. In over half the cases (65%), security incidents were attributed to internal actors.

These were primarily 'unapproved hardware/ software/ scripts/ workarounds' or 'Adware', or were 'inconclusive'. Externally attributed incidents constitute 28%, and include Web Attacks, Backdoors and Worms.



Malware Network & Application System Account Policy Violations Social Engineering Others

\* Figures rounded to integers

## Command and Control channels

The so-called cyber ‘Kill Chain’ describes a set of steps that an attacker will almost always traverse through in order to compromise and exploit a network. A key step in the Kill Chain is the establishment of a ‘Command & Control’(C&C) channel, which allows the attacker to surreptitiously execute commands on a compromised computer and then retrieve any outputs resulting from those commands. In the early days of computer hacking such channels were clunky, unreliable and easy to detect. They were easily lost, and difficult to scale.

### A short history of C&C

At the DEFCON hacking conference in August 1998 a legendary hacker called ‘Sir Dystic’, a member of hacker crew ‘Cult of the Dead Cow’ released a tool called ‘Back Orifice’. According to the group, the purpose of the tool was to demonstrate the lack of security in Microsoft’s Windows 9x series of operating systems. Back Orifice is a computer program ostensibly designed for ‘remote system administration’. It enables a user to control a computer running the Microsoft Windows operating system from any remote location. Although Back Orifice has legitimate purposes, such as remote administration, other factors make it suitable for illicit uses. The server can hide from cursory looks by users of the system. Since the server can be installed without user interaction, it can be distributed as the payload of a Trojan horse<sup>[3]</sup>.

Back Orifice was the predecessor to an entire new breed of remote access tools hackers would deploy to covertly control the computers they compromised.

Metasploit was created by H. D. Moore in 2003 as a portable network tool<sup>[4]</sup>. Like comparable commercial products such as Immunity’s Canvas or Core Security Technologies’ Core Impact, Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities.

In 2009, the Metasploit Project was acquired by Rapid7, a security company that provides unified vulnerability management solutions. Metasploit eventually emerged as the de facto exploit development framework that is often accompanied by third-party exploit modules that highlight the exploitability, risk and remediation of a particular bug. This modular approach – allowing the combination of any exploit with any payload – is a major advantage of the Framework and makes it a popular tool for security researchers, exploit writers, payload writers... and malicious attackers.

### Enter Cobalt Strike

Most recently a tool called ‘Cobalt Strike’ has exploded into prominence. Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”<sup>[5]</sup>. Cobalt Strike’s interactive post-exploit capabilities cover a full range of tactics, all executed within a single, integrated system. In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz.

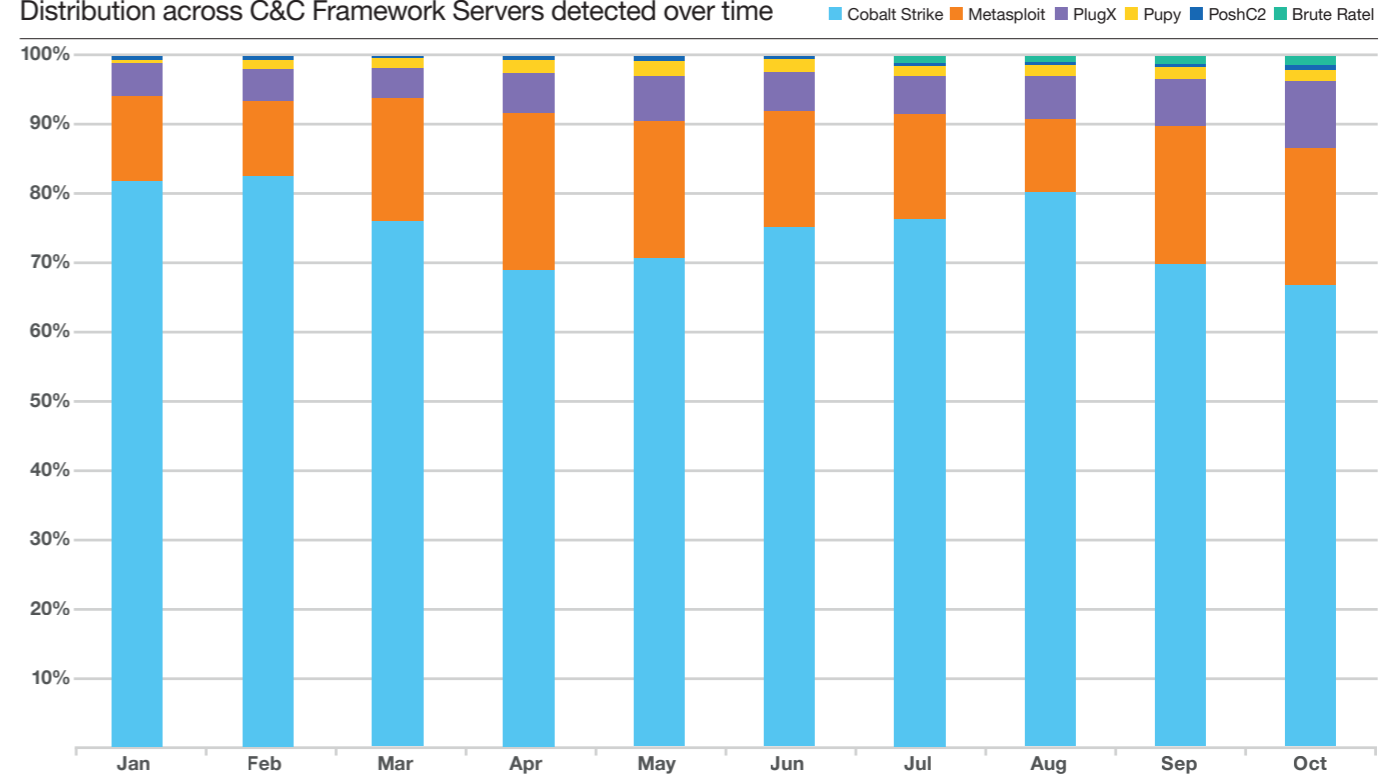
According to a 2020 report by Cisco’s ‘Talos’ research group, 66% percent of ransomware attacks during that quarter involved the deployment of Cobalt Strike. Other research teams have reported similar findings.

Pirated versions of Cobalt Strike had become a favorite tool in the arsenal of criminal hackers.

Metasploit and Cobalt Strike are still used prolifically by hackers, but there are many other C&C frameworks in daily use also. In fact, our threat detection teams track more than 20 such toolsets in common use today.

## C&C tools usage

Distribution across C&C Framework Servers detected over time



### finding the C&C in a haystack

C&C frameworks all need to ‘talk out’ of the compromised network in some way in order to establish communications with the attacker. In most cases this involves talking to a ‘server’ of some kind that acts as a kind of communications hub between the attacker and the compromised computers. Cobalt Strike, for example, calls theirs a ‘Team Server’.

In order to better protect our clients, we want to know where these servers are, so that we can detect any attempt by an internal system to reach out to them. Traffic from an internal device to a known C&C server would be a clear sign of ongoing compromise.

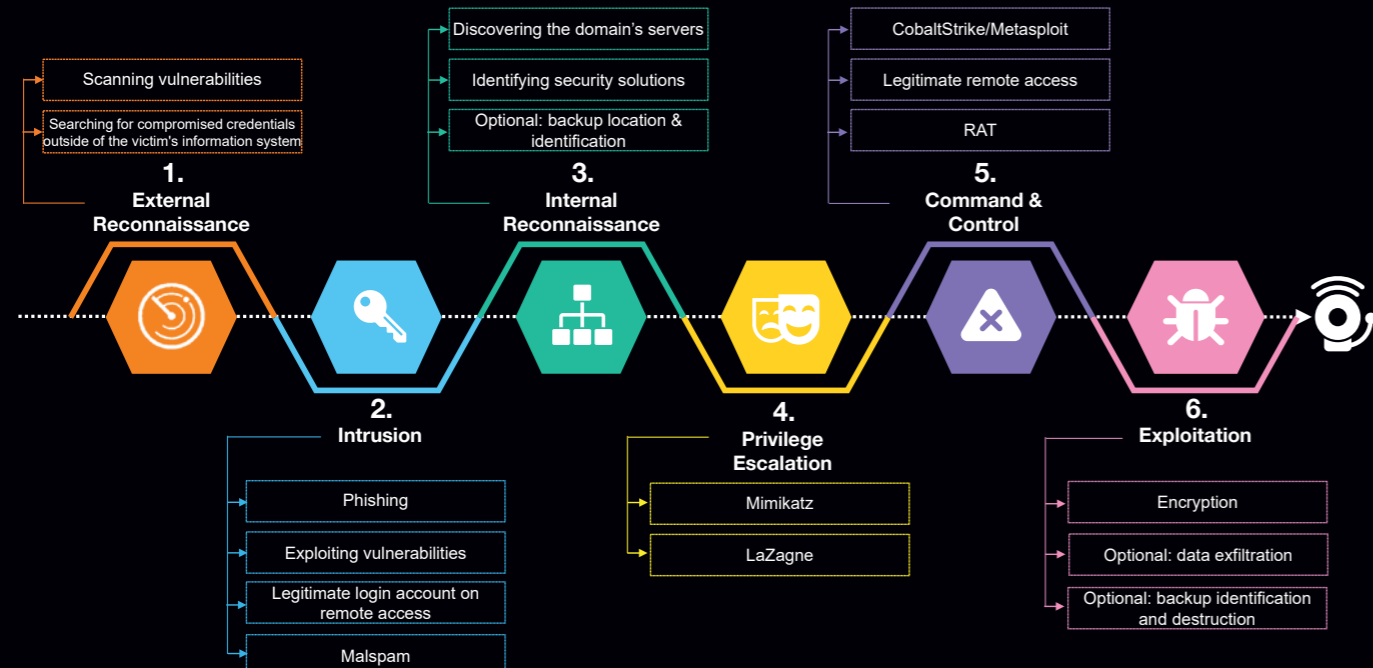
As these servers can be stood up and shut down on a whim, we keep track of them via proactive scanning. Our Advanced Intelligence & Detections Team has developed a capability that proactively searches the internet for the signatures of known C&C servers, verifies what they are, then feeds their details through into our CyberSOCs for monitoring.

Note that we only started tracking Brute Ratel in July 2022.

- Since November 2021 we have identified 806,480 such IP addresses, though IPs can be recorded more than once.
- This extraordinary data provides some interesting insight on how attacker toolsets are changing.
- C&C servers cannot all be reliably detected with active scanning.
- As other researchers have suggested, the vast majority of C&C in our dataset – 70% – are Cobalt Strike.

Where in Q4 2021 Cobalt Strike constituted 68% of all C&C servers we were able to identify, by October 2022 that proportion had dropped to 56%. During that same period the Metasploit framework has grown from 9 to almost 17%, and PlugX from 0.2 to 8%. The number of PlugX C&C servers we’ve identified has almost doubled between April and October this year. It’s not clear why this is happening, but PlugX is clearly gaining traction. An imprecise study of IP geolocations suggests that most of these servers are situated in Asia.

## The Kill Chain





## Float like a Qakbot, sting like a Bumblebee

In the last 6 months we also observed a steady increase in the size of the Bumblebee C&C ecosystem.

In the chart below we compare Bumblebee to the infamous Qakbot implant that has been active since 2007. Qakbot represents just under 1% of our dataset, while Bumblebee comes in at 0.4%. But that picture is changing also.



From this we can deduce that the Bumblebee threat actor is very active and doing well.

These changes represent a shift in tooling choice by attackers and are therefore important to take note of.

## Mi casa es su casa

Studies of this dataset allow us to make other interesting observations also, like how often IP addresses are used to host multiple different C&C frameworks.

We seldom see more than two frameworks hosted on the same server. We do see two frameworks on the same server quite frequently, however, and when we do it's almost always Cobalt Strike living alongside Metasploit. When we see a third, it's generally something more obscure. Cobalt Strike and Metasploit is the preferred combination we've observed over the last 12 months. Since these are the two most common frameworks in general, this is perhaps no surprise. Still, it's interesting to see what combinations attackers seem to prefer.

If Cobalt Strike and Metasploit are removed from this analysis, a different picture emerges. We note that 'covenant' and 'poshc2' are the C&C frameworks most frequently found together.

By proactively tracking C&C servers – a critical part of the attacker Kill Chain – we significantly improve our ability to detect compromises in progress. The data emerging from this exercise proves to offer interesting insights into how attacker behaviour is changing over time.

# Conclusion



We Continue to see Malware as a leading incident type followed by Network & Application anomalies. These two categories follow each other closely throughout with slight variations on a couple of occasions. Identifying real incidents that have business impact takes a lot of effort. Of all the incidents we dealt with approximately 29% impacted our clients in some way or form.

This year we introduced the VERIS framework to help classify the data to get a better understanding of the nature of the incidents. Although only part of the data set could benefit from this approach, we were afforded a glimpse of this higher resolution data. One noticeable improvement is that we could distinguish incidents that were caused by external threats versus those incidents caused by internal threats. This suggests that businesses are afforded the locus to potentially reduce their incident count by turning their attention to these internal transgressions.

Large and small businesses, in our data set, struggle proportionally with similar threats when looking at the data through the older data classifications lens. Using the VERIS classifications we see a different picture emerge. incidents for large businesses are more evenly distributed while incidents for small businesses are more clustered around Hacking / Pentesting and Malware categories. For Medium sized businesses Network and Application Anomalies paired with System Anomalies make for almost half of the incidents classified for true positive in this size of business. In the VERIS vernacular this translates into Hacking / Pentesting and Error categories.

The Manufacturing industry remains our biggest concern as it once again features with the most incidents dealt with as a percentage of the total. Retail and Professional Services industries round out the top three with second and third places respectively. All three struggle with internal threat problems with the Manufacturing industry struggling the most. There is good news for the Health Care and Social Assistance industry as we have seen an overall reduction in incidents for this space.

The introduction of the coverage score in this year's Navigator sets the stage to discuss the impact of a mature security approach. We noted that the more mature a business gets in terms of security coverage the harder they'll need to work as a result. There is a popular saying that goes along the way of "You cannot manage what you do not measure" however the more you measure the more you need to manage. This could be a good argument for improved continuous finetuning and ultimately scalable security solutions that can deal with the ever-increasing volume of data.

# The worst hackers out there

## Why Conti has changed incident response

**Conti was one of the biggest ransomware groups worldwide and maybe the most antisocial, too. But what makes it stand out as particularly evil even in the 'industry' of digital extortion?**

It is worth investigating this question as Ransomware has become a threat to the economic security of entire nations around the globe. Conti's ransomware attacks trigger psychological effects as well as political and economic ones. And from the perspective of an incident responder, let's try to explain why it has changed the way we think about cybercrime.

Simone Kraus, Junior Security Analyst, [Orange Cyberdefense](#)

### How has it changed the way we think?

Orange Cyberdefense initiated a project to track and document Ransomware leaks in the first quarter of 2020. We observed a 9x increase in double-extortion leaks from January 2020 to August 2021. We see that Ransomware activity was significantly rising when Conti had its peak in operations. And in addition to posing an existential threat that arises from such successful extortion attacks on a company, the psychological consequences can be devastating too and must not be underestimated.

### Blaming & shaming the victim

First, when engaging as incident responder or victim with Conti you experience that the threat actor uses elaborate psychological tricks to convince targets to pay. Technically, Conti encrypts all files after their operator has made a copy of the backups and deleted them. The targets of the Ransomware attack usually have no chance to restore any of their systems. To increase the pressure on the victims, data is stolen with the intention of leaking it if no payment is made. This is a double humiliation and can leave psychological traces that undermine the morale not only of those who have to deal with the situation but the organization in general<sup>[6]</sup>.

After the encryption, victims are informed by the attacker that their own inability led to the incident. Even worse: the operator dares to present the attack as a business relationship, which it clearly isn't. Yet Conti kindly offer their "services" as if they were not the main reason for the state of emergency. It's a twisted psychology where the cybercriminal tries to blame the victim while offering a 'helping hand' which in fact is an act of criminal extortion<sup>[7]</sup>.

### They don't just steal data; they take away the trust

Psychologically, a ransomware attack has massive consequences for the organization's employees, business partners and clients. It's a breach of trust when the incident becomes publically known, and even worse if data is published. In the long term, this can lead to a break between all actors involved, damaging the company's reputation and operations to such an extent that business does not recover from the incident<sup>[8]</sup>. People who witness such an attack on their organization will definitely change the way they think about Ransomware. It's no longer a security issue but an existential threat to the business. I've personally witnessed companies being attacked twice. It pains me to see someone going through this experience again.

#### Conti 'Support' Chat (sic)

The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your reputation. The amount at which we are ready to meet you and keep everything as collateral is \$40,000,000

I am.... speechless. Surely this is a mistake? are there extra zero's in that number by mistake?

According to the records, your revenue is more than 4billions. So it is a possible amount for you. We also made a research to throw your finance and know that you own the required amount.

i am so confused. this is a PUBLIC school district. public, meaning it is free for students to attend. You cannot possibly think we have anything close to this!

What is your position?

What do you mean?

My position is shock and horror that anyone thinks a taxpayer-funded school district could afford this kind of money!

### Conti: Criminals, Cyberterrorists and Mother Russia

Many of Conti's activities can be traced back to Russia<sup>[9]</sup>. Interestingly, some members of the group appear to be from Ukraine. Some gang members follow Russia's agenda, perceiving 'the West' as the enemy. But the relationship probably goes deeper than that<sup>[10]</sup>. Leaked chats by Conti indicate they could have former Russian soldiers in their ranks, who mentioned in their conversations that they were in Crimea in 2014<sup>[11]</sup>. In February 2022, some members declared to side with Russia in the war against Ukraine. Thereupon one affiliate leaked chats and playbooks on how the gang operates.

What followed was an abrupt end of chat communication within the gang which we can also see in our research data.

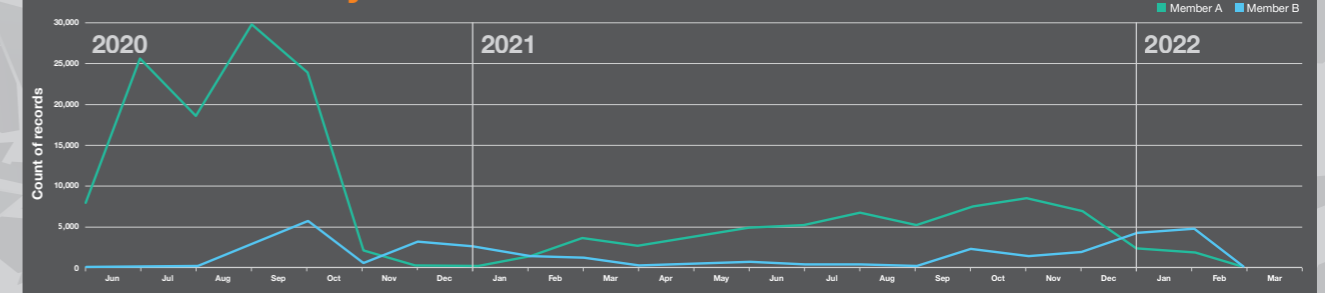
This connection might explain why Conti's operations reflect actual psychological warfare tactics, like e.g., offering their victims a 'business relationship' that in reality is brutal extortion and not business.

Indeed, Conti as a threat actor is an organized, transnational crime syndicate.

They also demonstrated their capabilities by conducting serious attacks against Costa Rica<sup>[12]</sup>. This clearly goes beyond common cyber crime. In fact, Costa Rican authorities acted decisively and declared the incident an act of war against the country<sup>[13]</sup>. And for some, Conti went too far with the attack on an entire government. There is speculation that this final attack was in part a tactic to take attention away from the gradual shutdown of its operations after the leakage of their playbooks in March 2022<sup>[14]</sup>.

But this is not the end of the story. The group merely seemed to split up. Current Ransomware attacks from groups like Royal seem to indicate former Conti members might have joined<sup>[15]</sup>.

### Conti chat activity over time



### What makes groups like Conti so dangerous to our economic security?

There is often an absence of empathy, morality, integrity or even the awareness of guilt regarding cybercrime. Researchers from the Journal of Criminal Justice concluded that cybercriminals have a cognitively dissonant world view and see very often only themselves, exploiting and manipulating others<sup>[16]</sup>. This quickly becomes a real threat to society in an environment where consequences are unlikely<sup>[17]</sup>.

As a result, attacks on our critical infrastructures are a permanent threat now. Terroristic attempts to hack our grids, hospitals, water treatment facilities or logistics are happening<sup>[18]</sup>. Cyberwarfare often precedes kinetic warfare.

In Ukraine, Russian hackers attacked media and infrastructure, days before the first shot was fired<sup>[19]</sup>.

According to the RAT (Routine Activity Theory)<sup>[20]</sup> concept, a factor that encourages crime is the absence of capable guardians<sup>[21]</sup>. This could be a security controls failure, like insufficient patch management, but it can also refer to a shortage of cyber security experts, or ordinary people with the appropriate security knowledge and awareness to shore up defenses. This doesn't mean it's the victim's fault. Yet we have seen even huge companies with the best practices implemented getting critical assets encrypted.

Virtually everyone is at permanent risk now.



### Conclusion: What could be worse?

Conti is the most wanted hacker gang, and a 10 million dollar reward has been offered for finding their members. US authorities rightfully declared them a terroristic group. They are still operating in groups like Black Basta, Blackbyte or Royal.

What are the lessons learned from analyzing groups like Conti?

Ransomware group members often strive to gain prestige with their criminal actions, an aspect that makes them particularly wicked. They have even flaunted their ill-gained wealth, posing in photos in front of luxury cars, whilst their victims bore financial and psychological costs of their acts during the pandemic lockdown. What could be worse?

CyX-threats in general should be countered in a global and more coordinated manner to halt cyber criminal groups like Conti.



**Charl van der Walt**  
Head of Security Research  
**Orange Cyberdefense**

### Cyber crisis:

## The Ukraine war

Any international conflict has far-ranging implications for the world at large, and cyberspace is no exception. Apart from the specific threats to organizations 'directly' involved in the conflict, it has the general effect of 'inflating' the risk for everyone.

While we can identify some specific actors and methods that are likely to come into play during this conflict, it is this more general inflation of the risk that most organizations should focus their attention on.

The response to this increased risk is to assume a state of general readiness while Continuing to pursue a strategy of robust defense in depth that will position us for a diversity of threats that may emerge from this conflict.

## Risk Assessment

### Threat actor

The cyber world is populated by many capable and motivated attackers. It is important that defenders do not lose sight of the overall threat landscape.

Russia is considered the primary aggressor in this conflict and cyberattacks will most likely be executed by groups or teams that are already well known to the cyber security community. These groups are referred to as Advanced Persistent Threats (APTs) or Threat Actors. Ukraine also recruited an "IT Army"<sup>[22]</sup> targeting Russian infrastructure and potentially companies doing business in and with Russia. More details on that further down.

It is however not recommended to focus on specifically named threats only. Instead, controls should be put in place and matched against specific phases of the cyber Kill Chain based on the capabilities of the business<sup>[23]</sup>. The best return on time and energy will be to put measures in place that will defend against a range of threats for any given part of the Kill Chain.

### Threat level

Information is fairly limited and there are significant intelligence gaps. We can not fully estimate how far this conflict will escalate and what risks each party is willing to take. The best approach is to be alert and ready to respond if the situation turns for the worst.

Following the Cooper color system<sup>[24]</sup>, we assign an "Alert" or orange state with the emphasis on being ready and devising plans to navigate identified threat scenarios. The implication of this state is an increased focus on the threat, thus potentially losing temporary sight of other dangers. Maintaining this state is taxing.

At this threat level we therefore recommend that organizations be aware, vigilant, and prepared to react, but without being distracted from the broader strategic priorities for building cyber resilience for their systems and businesses.

### Potential targets

Targets for cyberattacks include:

- Government institutions
- Defense & Military institutions including manufacturers
- Telecom sector & Internet traffic
- European media (propaganda)
- European & US industries invested in the region
- US, European and other governments allied with either party or imposing sanctions or other costs.

We should recall, however, that in the infamous NotPetya attack, the most damage was caused to organizations that were not even specifically targeted, but rather became collateral damage when the NotPetya worm accidentally escaped its original targeting constraints.

## Battlefield internet

The Internet is becoming more of a battlefield with a growing number of DDoS attacks, website defacements and data leaks. Possibly the most concerning activity was the Conti cyber extortion (Cy-X) syndicate announcing they were siding with Russia and would attack critical infrastructure if Russia was targeted by any cyberattacks<sup>[25]</sup>. They did later soften their tone but that didn't stop one of their own members from leaking the group's internal chat logs of the past year in an apparent act of hostility against the rest of the group<sup>[26]</sup>. Further releases could prove to be a treasure trove for security analysts as they contain Conti's source code along with a large amount of information including further chat logs, malware, victim information and their modus operandi. We currently have a team of experts analyzing the data; however, this will likely take some time due to the volume of information.

Ukrainian authorities succeeded to recruit an "IT Army", sharing guides to DDoS Russian targets. They also praised the Anonymous hacker collective for their activities. Anonymous was credited for taking the website of the state-run Russia Today TV channel down<sup>[27]</sup>. Other attacks from unknown sources resulted in more Russian TV channels being hacked to broadcast pro-Ukrainian messages and songs<sup>[28]</sup>.

Other "hacktivism" activities include the Belarusian group "Cyber Partisans" attacking the Belarusian rail network to disrupt Russian troop movements into Ukraine<sup>[29]</sup>. Another attack targeted a Ukrainian border control station with wiper malware impacting the thousands of people currently trying to flee the country because of the war<sup>[30]</sup>. A group affiliated with Anonymous claimed they had successfully attacked the control center of "Roscosmos", the Russian Space Agency, resulting in Russia losing control over its satellites<sup>[31]</sup>. Hackers calling themselves "AgainstTheWest" claimed they attacked the Russian financial institution Sberbank and would soon be leaking DNS infrastructure data, private keys for SSL, Sberbank API, CLI and SDKs<sup>[32]</sup>.

With the Russian government fully controlling the media coverage since the war started, some hacktivists have gotten creative in their attempts to let Russian citizens know what is happening. One method used has been to flood restaurant reviews with anti-war/anti-Putin messaging<sup>[33]</sup>.

Despite the controversy unfolding recently, Elon Musk became an unexpected benefactor for Ukraine early on by announcing that SpaceX's Starlink satellites had been activated for Ukraine and that more terminals were en route<sup>[34]</sup>. This could help the country maintain communications in case network infrastructure is destroyed. Some major security vendors have also decided to aid Ukraine by providing licenses, services and cloud hosting for free<sup>[35]</sup>.

We expect hacktivism and ransomware activity to continue escalating as the conflict extends, but also remain alert for direct and sophisticated state-backed activities targeting both of the primary protagonists, potentially causing collateral damage to governments and businesses worldwide.

## What you can do:

In addition, we recommend general defense-in-depth best practices for mitigating contemporary ransomware threats as a reasonable baseline for defense against a non-specific nation-grade attack:

### Identify and patch any internet-facing technologies

You should especially include Remote Access like VNC and Microsoft RDP, Secure Remote Access like VPNs, and other security technologies like Firewalls.

### Implement MFA on authentication interfaces

This step is crucial for any interfaces connected to the world wide web and can significantly reduce risk of compromise.

### Frequent backups of business-critical assets

Works best when complemented with offline backups. Test the integrity of these backups regularly by restoring critical functions.

### Endpoint protection and anti-malware

Test these solutions and identify any blind spots.

### Defense against Distributed Denial of Service (DDoS)

Implement a strategy that can protect networks and services exposed to the Internet from sustained large-scale network flooding that could cut the targeted network and services off from the Internet.

### Network Egress Filtering

Configure firewalls and other perimeter equipment to allow only the minimum of outbound traffic to the internet, especially from the DMZ and any internet-facing or critical systems. Monitor outbound traffic closely for anomalies.

### Monitor network for malicious activity

The Mitre ATT&CK Matrix is a good reference to determine if you have any blind spots in your telemetry. This can help you expand on your detection capabilities, for example monitoring any execution of common built-in system utilities<sup>[36]</sup>.

Involve incident Response teams as this can be useful to know what needs to be collected for forensic investigations.

### Continuous vulnerability management

Prioritize patches based on whether vulnerabilities have known working exploits. This is applicable to infrastructure as well as end-user software or devices.

Internet-facing services with known vulnerabilities must be patched.

### Network segmentation

Identify trust boundaries and implement tight controls for services and users that want to cross into those zones.

Least privilege concepts can also apply here.

### Least privilege

Limit services to run with only the necessary privileges to perform their functions.

Ensure staff only has access to what they require to perform their tasks.

### Threat Hunting

In-house teams should schedule time to identify scenarios for threats applicable to the organization.

## Recommendations

Our primary recommendation involves developing and priming a robust Emergency- and incident Response process, with trained people ready to execute it. If the threat level of this situation escalates further, or more specific intelligence becomes available, the key will be to enact a swift response, possibly under very adverse circumstances.

## Advice from the security scene

The French cybersecurity agency ANSSI has updated their recommendations, to include replacing any Russian cybersecurity solutions. It is anticipated they may be unable to maintain their products at the required security levels in the future. One such vendor mentioned is Kaspersky, which has tried hard to remain neutral since the conflict escalated<sup>[37]</sup>.

**Proofpoint** has released details of a phishing attack dropping a Trojan, dubbed “SunSeed” targeting a European government official working on the Ukrainian refugee’s issue. It is presumed the threat actors responsible are the Belarusian groups Ghostwriter and/or UNC1151<sup>[38]</sup>.

**ESET** researchers have reported that wiper attacks Continue to be seen with a basic worm component called “HermeticWizard”. It attempts to deploy the “HermeticWiper”<sup>[39]</sup> within a compromised local network. However, as it simply uses the SMB and VMI protocols to deploy it is not likely to be as prolific as previous worms such as EternalBlue for example. Another wiper variant, called “IsaacWiper”, has also been detected during a destructive attack on a Ukrainian government network. This variant shares no code similarities with HermeticWiper and is much less sophisticated.

## The focus is Ukraine – for now

While there is no indication that either of the above wipers has been used against any country other than Ukraine, the risk is still there that threat actors may decide to deploy them against countries or entities supporting the Ukrainian government or imposing sanctions against Russia. Remaining vigilant is therefore highly advised.

Other threats to non-Ukraine organizations going forward may well involve ransomware actors, with at least one on the famous RAMP forum recently looking for network access to companies from Ukraine but also NATO member countries.

The most impactful attack against a Western company may have been the one against KA-SAT, a satellite connection service provider used by numerous clients in Europe and operated by ViaSat (a Viacom subsidiary). The service was down due to a “cyber event”, starting in Ukraine but also affecting other European countries<sup>[40]</sup>. The breach was discovered on February 24th. This day marks the launch of the war by Russian military forces; thus, the attack might well have been carried out purposely to disrupt specific communications capabilities in Ukraine.

## Attack methods

The predicted attack methods listed below are not exhaustive but represent a range of methods from most likely – Method 1- to least likely – Method 5 – that we can expect to be deployed in this conflict.

There is also of course the persistent threat of disinformation and misinformation campaigns around this conflict, but those are beyond the scope of this document.

### Method 1 – Distributed Denial of Service (DDoS)

Denial of Service attacks can take multiple technical forms but the most common contemporary variant is the Distributed Denial of Service Attack, where multiple external systems are flooding a single victim endpoint with enough network traffic to consume all available bandwidth or resources.

- High-volume traffic intended to saturate the Internet access of targeted enterprises Service inside the network
- Bandwidth attacks combined with attacks on firewalls or IPS (Intrusion Prevention System) security infrastructure and applications
- Attacks that target a large range of business applications (HTTP, HTTPS, VoIP, DNS and SMTP).
- Perimetric defenses are ineffective against these threats.

DDoS attacks are popular for their relative ease of implementation and are commonly deployed by state actors, hackers and cybercriminals alike. Various tools and techniques, including botnets for rent, enable an attacker to generate far more traffic than an average organization can process, resulting in platforms and services becoming unavailable to genuine users. Because the source of the attack is ‘distributed’ across multiple agents, it is very difficult for the victim to manage the traffic and mitigate the attack.

Solutions are typically based on a notion of a ‘scrubbing center’. A scrubbing center is a cleaning center installed on the internet in front of an organization’s internet access, with the objective of centralizing and cleaning streams polluted by DDoS attacks before sending them to the legitimate target IP addresses.

This type of solution requires traffic to be forced towards the scrubbing center. Two deflection strategies may be considered: Diversion only if attacked – in which case, there is a delay between the time the attack is identified and when the filtering is effective – and Systematic deviation (always on mode) – in which case, the traffic is always forwarded to the scrubbing center.

### Method 2 – Phishing

The attack will involve:

- Phishing to facilitate credential theft or a Malware drop
- Attackers gaining remote access through legitimate services (VPN) or specialized malware
- Elevation of Privileges
- Lateral Movement

The most likely attack we have observed is simple but effective. In this approach, the attackers leverage spear phishing to either steal credentials or deploy malware on the endpoint.

Credential theft could be used to access services such as secure remote access or VPNs. Services relying on exposed Remote Desktop Protocol (RDP) could also be accessed using legitimate credentials.

As stated above, phishing lures could also be used to drop malware on a victim’s machine. These types of phishing attacks will include an attachment that, when opened by the recipient, will result in malware executing on the host. The absence of sufficient endpoint protection and antimalware solutions will result in the attacker having Remote Code Execution.

Gaining remote access to business infrastructure will allow the attacker to then move toward their objective. The attacker may seek to elevate their privileges or steal cached credentials that will enable the attacker to move laterally. Versions of common tools such as Mimikatz could be used to achieve this.

The attacker will propagate through the environment ultimately seeking to embed themselves in the infrastructure. Remote access trojans could be used or other specialized tooling such as the infamous Cobalt Strike framework.

### Method 3 – Exploiting known vulnerabilities

State-backed actors, including those we see active around the conflict, are adept at finding and exploiting systems that haven’t been patched for known vulnerabilities.

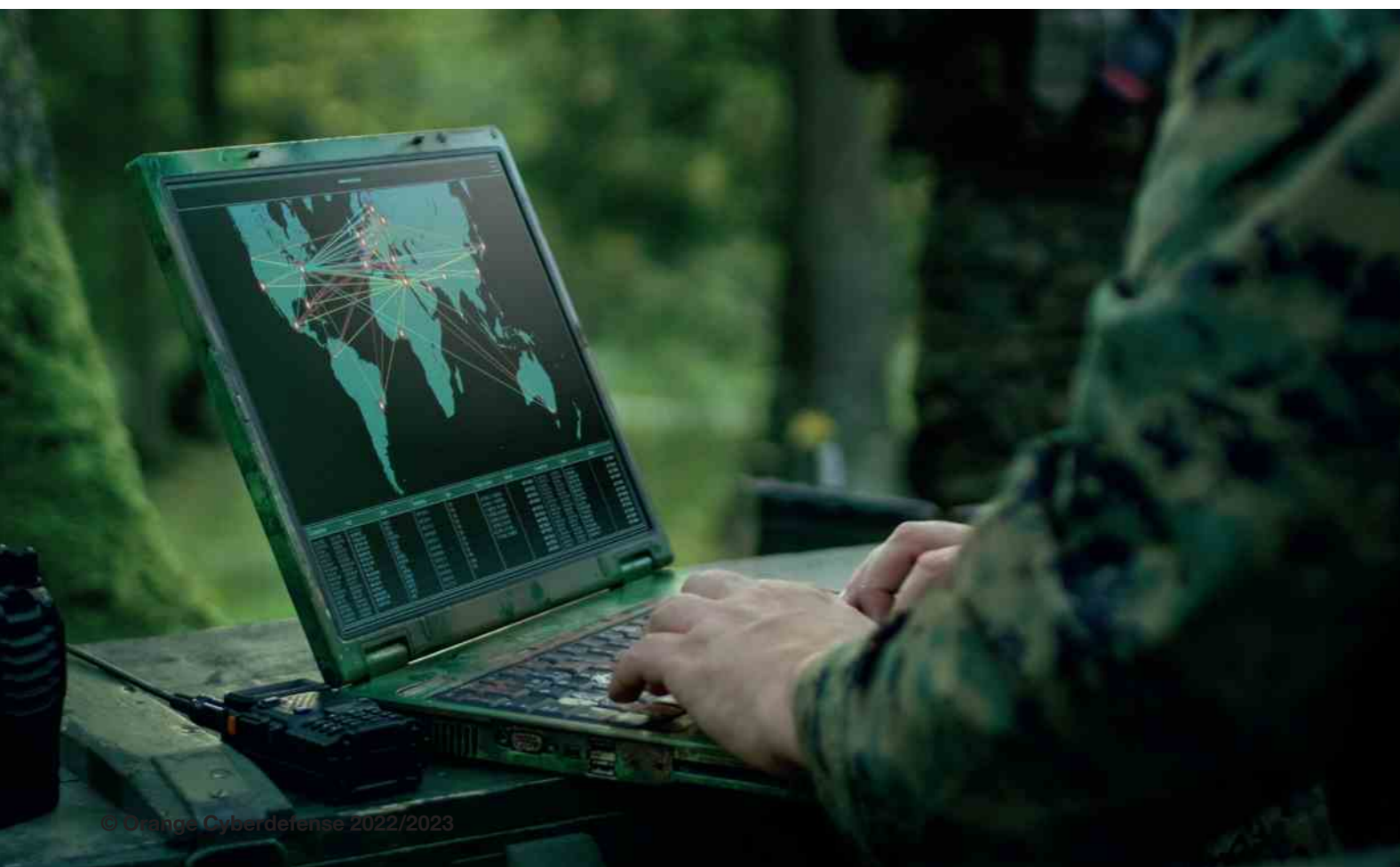
- The primary target will be systems exposed to the internet
- Remote Access platforms like RDP and VNC are frequently targeted
- Several vulnerabilities on security products like VPNs and firewalls are also actively exploited in the wild

Any internet-exposed system, including especially remote access- and security technologies, should be fully patched. The US Cybersecurity and Infrastructure Security Agency (CISA) noted in a January 11 advisory [12] that some specific vulnerabilities were commonly targeted by actors in the region.

These include:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange

Note that eliminating these specific vulnerabilities is not a substitute for general vulnerability management and attack readiness.



### Method 4 – Supply Chain Compromise

This could possibly be as follows:

- An attacker compromises supplier(s) of a target
- Pivot on to target using:
- Direct network access
- Backdoor software distributed to target
- Abuse trusted relation of the supplier for phishing

A supply chain compromise is an effective means to gain access to a target by using a trusted third party. This type of attack is more complicated and requires multiple steps to execute which could take longer. It depends on established relationships of the secondary target with the target.

Businesses such as service providers might have remote access to a client’s network as part of their service delivery process. This could be as simple as a network route that allows traffic to flow between businesses, or more evolved requiring access control. Either way, the attacker can jump from one network to another.

Another example involves compromising software or hardware that will be used by the target. The attacker plants malicious code or weakens existing components to enable hidden backdoor-access.

This kind of compromise may spill over to unintended targets. The likelihood of collateral damage increases if destructive malware was injected that indiscriminately damages systems. Though technical measures could be implemented to control the 'blast radius', that is entirely up to the attacker.

As mentioned earlier, the type of supplier compromise could involve using social engineering. It could be as simple as the attacker using the compromised victim’s email system to send a malicious email to their target. Chances are that the recipient will be caught off-guard. Attackers could also leverage that trust relationship to gather more intelligence before launching another phishing attack, increasing their chances of success.

### Method 5 – Zero-Day

An attacker can exploit unknown weaknesses in:

- Services exposed to the internet
- Service inside the network
- Browsers
- Email Clients
- Mobile Devices and Apps
- Network Equipment
- IoT Devices

Exploitation of zero-day vulnerabilities is likely available to state actors with a known history of cyber aggression. Highly resourced and well-trained teams with years of experience could have access to zero-days that they are willing to burn given the stakes. It is important to note that zero-days are discovered rather than injected.

Once found, there is little that anyone can do to stop a highly motivated and skilled attacker from exploiting an unknown vulnerability, except for acting fast once a patch is out after it was used in an attack and discovered. The type of zero-day and the nature of the affected application or device determine its potential impact.

Zero-days in internet-facing services such as email, web, or even security products (like remote access or firewalls) are particularly dangerous. Depending on the nature of this flaw, the attacker could gain access to the underlying operating systems of the host, steal sensitive information or deploy destructive Malware.

Zero-days in browsers, email clients, and messaging applications can be exploited through watering hole attacks or merely for sending a malicious message to their victim.

Fully patched mobile devices that receive regular security updates will be difficult to exploit. Mobile device exploitation is useful for surveillance, but it will likely be aimed only at specific targets as part of information gathering.

## Just across the border

A look at cyber activity in Poland from the beginning of the war in Ukraine up until now – frequency, type of attacks and general observations.

Robert Grabowski, Head of CERT, Orange Polska



### "May you live in interesting times"

That is the English expression that is claimed to be a translation of a traditional Chinese curse. And when I'm thinking of the past years and especially 2022 I'm pretty sure we could agree that these times have come. The war conflict which came so close to our borders with all the cruelty and violence also came with the whole spectrum of cybersecurity activities.



During the summer holidays we blocked over **26 thousands phishing domains** directly connected with attacks for money or sensitive data, including:

### Attacking the sellers on popular portals (like Vinted and OLX) ~45%

Using IM communicators like WhatsApp, outside the transaction platform, a scammer pretending to be a potential buyer offers the victim payment for the goods together with shipping at his own expense via a courier company. Victims are asked to enter their credit card details, which are allegedly needed to transfer the payment for the goods, on the scammer's fake website. The victim may lose all funds available on the card.

### Fake investments ~27%

Using thousands of Facebook adverts impersonating famous brands (like Tesla, Apple, Amazon etc), polish officials, celebrities and national companies, fraudsters usually phish victims to leave their data and start earning huge money with little investments. What happens next? It can be phishing with a fake advisor and persuading victims to install remote controls, mobile apps from third party websites or transferring crypto currency via legitimate apps.

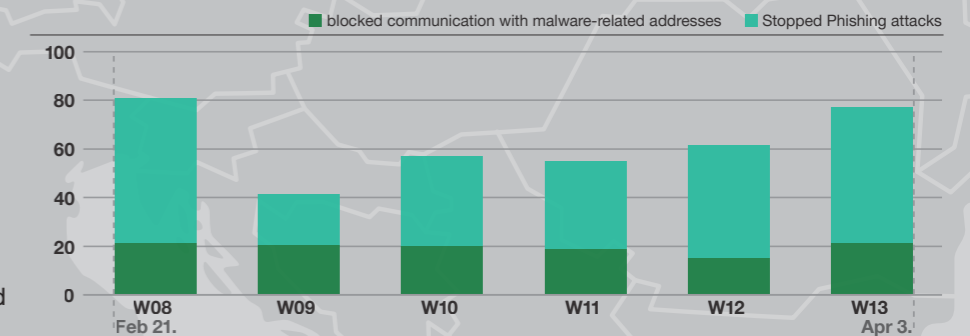
Of course the main target was Ukraine which was firstly attacked with a bunch of wipers (like HermeticWiper, IsaacWiper and CaddyWiper) and coordinated DDoS attacks. But also the world (I'm thinking of Anonymous group and others) responded to these attacks relatively quickly. Cyberwar between Russian-related groups and the rest of the world became a significant and continuous symbol of this conflict, including disinformation and propaganda. We had no choice but start to follow all these activities and also be prepared for attacks aimed at Poland.

While the network activity was constantly rising, astonishingly it turned out that the most cybercriminal activity targeting polish internet users has reduced substantially (**by about 50% for a few weeks**). It's not a secret that the majority of these attacks are performed by people from former soviet countries and it looks like they had to regroup and decide about the future of their criminal activity. And of course they came back.

In the end of February and in March we saw significant disinformation campaigns based on shock, emotions and lack of information. Disinformed people were massively blocking gas stations, ATM machines and offices. There was also panic about valid passports, sugar and other daily goods. All of this was triggered using social media, advertising campaigns and reckless people.

### Thwarted attacks on Polish clients

Frequency of common attacks during the invasion of Ukraine



## Conclusion: Not as bad as anticipated

While the number and imagination of the cybercriminals seem limitless, as CERT team we have to constantly develop our arsenal to protect users and the company. Without security enthusiasts working every day on new detection mechanisms, spreading awareness, researching methods and scenarios, reversing malwares, implementing automation and machine learning we would have lost that race long ago.



# Conclusion



The war against Ukraine has lasted for ten months at the time of writing, with clear implications to the cyber threat landscape and international economy. We have provided you with insights on what we have been observing and shared some advice on what you can do to protect your organization.

Several cyber-attacks have been observed since the beginning of the escalation of tensions. From disinformation campaigns on social networks to 'Hacktivism' and denial-of-service attacks on banking institutions and government sites.

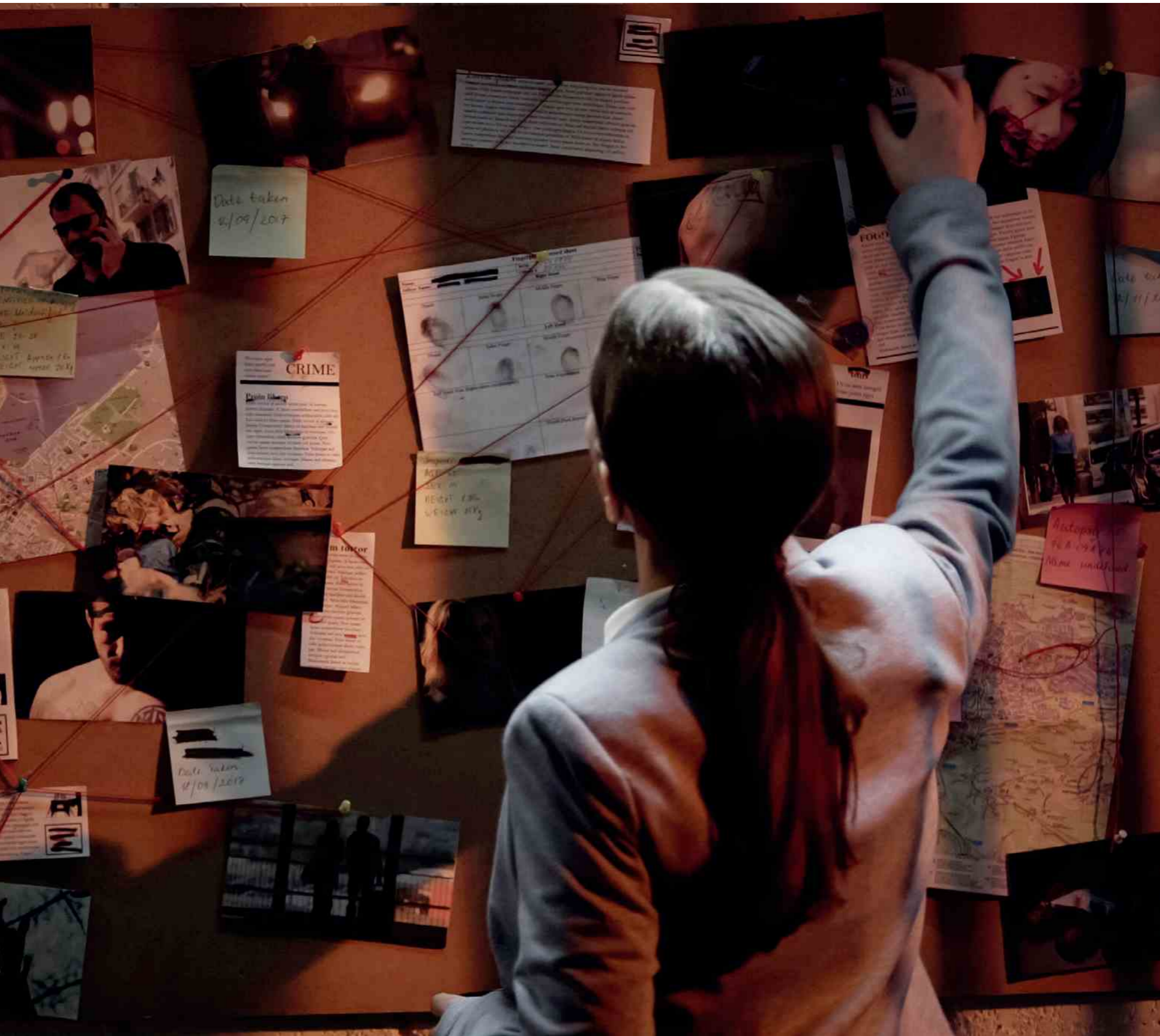
It is important for businesses to monitor the situation daily and adapt to new and relevant information as it becomes available. Businesses that have direct ties to other businesses in Ukraine and Russia need to be particularly vigilant.

At this stage the primary goal of civilian businesses and organizations should be to set up, prepare and test Cyber incident and Emergency Response capabilities. Prepare to ingest new intelligence and indicators of vulnerability, attack, or compromise from outside or inside your own organization, evaluate their potential impact and make sound risk-based decisions to respond rapidly in case of an incident affecting you or an industry peer, supplier or client.

We believe that businesses that have implemented a strong and tested response – for example to prepare for a ransomware attack – are well-positioned to deal with any cyberattack that could potentially spill over because of the war against Ukraine.

These controls will also help fend off any criminal attackers that demonstrate state-level capabilities and skills similar to those that are likely to be active in and around this conflict.





**Wicus Ross**  
Senior Security Researcher  
Orange Cyberdefense

**Joshua Sylvester**  
Security Research Intern  
Orange Cyberdefense

## World Watch

# Stories about stories

The Orange Cyberdefense Computer Emergency Response Team (CERT) produces regular advisories that we offer as part of our 'World Watch' service. This service provides analysis of vulnerabilities, threats, incidents, and other major news events that may impact our clients.

This year saw a variety of events that shaped the advisories released by the World Watch service. This forces Orange Cyberdefense to continuously review and adjust defenses based on changes we observe in the threat landscape. This intelligence-led approach allows us to enrich our services to better support our clients and offer solutions that are relevant.

We took a different approach this time in analyzing our World Watch advisories by employing the use of Natural Language Processing (NLP), which is a subset of the broader discipline that falls under Machine Learning (ML).

We used NLP as a tool to guide and shape the creation of this chapter. The usage of ML does not diminish the role or contributions of the human analyst, but in fact it boosts their abilities and highlights facets of respective stories that may have been ignored or required significant effort on the part of the analyst to discover. Using NLP helps us scale the analysis effort by automating several aspects of data classification and entity extraction.

### About the data

- This year we had a total of 553 World Watch messages
- 249 were unique messages, followed up with 304 additional commentaries and analysis on these unique reports
- 229 distinct CVEs were commented on, of which 50 CVEs featured more than once
- Data was gathered from October 2021 up to and including September 2022
- Data sources: Analysis produced by CERT and Security Research Centre (SRC).

### From artificial to real intelligence

We took a modest approach and created three models. Two models are used for classification of text and the third model is used to extract entities of interest from text.

Our first NLP model is used to categorise or classify text into four themes that we were interested in and this model we named our 'thematic model'. The thematic model can classify text as either Vulnerability, Ransom, Mobile, or Threat. The model was unable to cleanly identify any breaches and we subsequently were forced to exclude that category. A further challenge with breaches is to extract additional information such as victim and the type of impact.

The second model, in ML parlance is referred to as a Named Entity Recognition (NER) model, and is used to identify entities such as vendors, applications, operating systems, malware, and other interesting terms. We named this model the 'NER model', for the lack of a better name.

The thematic model was created using text and news articles that were already labelled matching our four categories or themes. Similarly, the NER model was created using an existing set of labelled text in the form of the NIST National Vulnerability Database (NVD) Common Vulnerability Enumerations (CVE) data. We used CVE data from the last 12 years to build the NER model.

The CVE data is especially rich in metadata as it contains a Common Platform Enumeration (CPE) dictionary as well as a Common Weakness Enumeration (CWE) classification for the vulnerability being described.

The CPE data allows us to create the NER model to identify vendor names, application names, and operating system names. This model also can extract possible entities that could be malware.

The purpose of the third NLP model is to classify text into one of the possible 10 CWE pillars and which we refer to as the CWE model. A CWE pillar is the highest weakness or flaw category. There are several subcategories of types of vulnerabilities such as memory buffer overflows, SQL Injection, Cross-site scripting (XSS) etc., but ultimately any vulnerability can be classified under one of the 10 pillars. For now, we settled on only looking at the overarching 10 main categories to improve accuracy.

As with any tool we need to realize its limitations and its pit falls. We mentioned 'improving accuracy' of the models and this is something to note. ML models can yield results that, if taken at face value, could mislead or result in false claims. To put this in more technical terms one must consider the False Positive rate or the True Negative rate. There is also a bias hidden in the model that can shape the results.

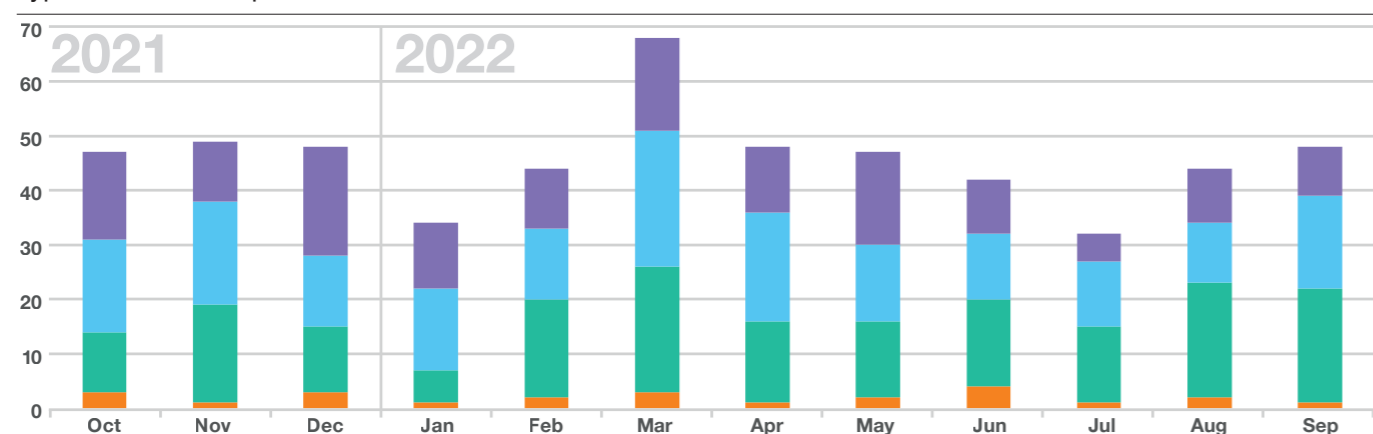
The accuracy of the 'thematic model' was 88.64%, which might seem high but ideally you want this as close as possible to 100%. The CWE model reached an accuracy of 84.92% and was relatively accurate when classifying vulnerabilities associated with CWE pillars 'Improper Neutralization' and 'Improper Control of a Resource Through its Lifetime'. This was due the fact that 73.4% of the data in the training set were examples for these two CWE pillars. The balance of the training data, 26.6%, was used to train the remaining 8 CWE pillars and is most likely the reason for the low accuracy for these CWE pillars.

The NER model was constructed using an auto labelling approach and achieved an accuracy of 96%. Auto labelling means we used the metadata present in the NVD CVE data to annotate the vulnerability text by giving hints to the training model. Some examples include patterns such as CVE IDs and others include version numbers.

Machine Learning is a fast-growing field with new techniques and methodologies discovered frequently. The correct usage of ML can lead to gains in productivity and scale that would never have been possible before. This means we can respond quickly to new information and make better decisions.

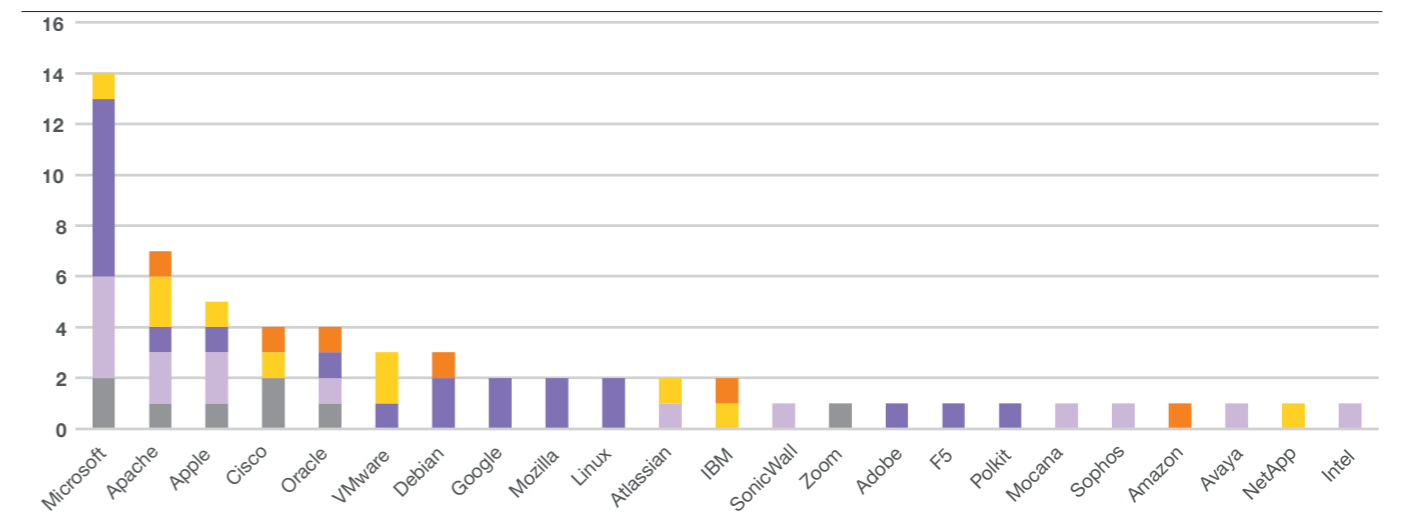
## World Watch Advisories

Types of advisories published over time



## Advisories by technology

Vendors and technologies addressed in Advisories, including criticality



### Changes a foot

We published 553 World Watch advisories for the period October 2021 up to and including September 2022. This consists of 249 unique advisories, followed by 304 additional commentary and analysis on these unique World Watch reports.

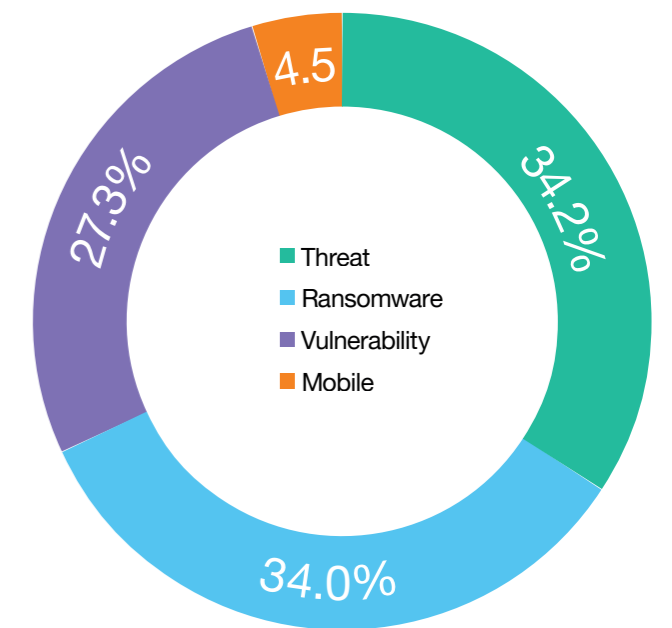
This year we changed the categories or themes to track Vulnerabilities, Threats, Ransomware, and news, incidents or vulnerabilities related to mobile devices. We are interested in tracking news or incidents relating to Ransomware and decided to create a separate category from the Threat category. Similarly, the Mobile category was created with the intent to track news and events relating to this category independent from the Vulnerability category and the Threat category.

The Threat category also includes several news items or events relating to the war in Ukraine, with an eye on how these events may spill over into cyber space. The category labelled "Threat" is a broad category and includes threats such as APTs, malware, and possibly breaches. The NLP model had a difficult time to identify a breach with an acceptable level of accuracy. The NER machine learning model also did not have the ability to extract features such as victims and nature of the impact. As a result, there will be little to no information shared about any breaches.

### Vulnerabilities

Although several vulnerabilities have been reported by vendors that are severe in nature, we have only issued one World Watch advisory that we considered critical. This was for the Log4j vulnerability, CVE-2021-44228 as well as the three related CVEs, known as Log4Shell that were made public back in December 2021. These vulnerabilities feature rather prominently in other World Watch updates, and we will touch on those further in the chapter as well as in other parts of this report.

### Proportion of advisory types



There was spill over of two other vulnerabilities, CVE-2021-38647 and CVE-2021-36970, that we rated as critical for the previous reporting period. The first of these two vulnerabilities, CVE-2021-38647, is known as OMIGOD and impacts the Azure Linux VMs. Vendors that depended on the Microsoft Azure Linux VM were impacted by this serious vulnerability. The second tracked vulnerability, CVE-2021-36970, is related to the Windows Print Spooler flaws known as PrintNightmare, for which Microsoft released multiple patches between June and October 2021.

## Third-party software supply chain complexities

Modern software can have many different dependent libraries. These libraries are code written by other people. Reusing the code make sense, especially for libraries that are written well. Developers and quality assurance teams save time as they do not have to reinvent the wheel and verify that the new wheel design and implementation performs within parameters, just like that other vendors wheel. Unfortunately, people make mistakes and popular libraries may contain latent defects or flaws that could be exploited. We tracked several news and vulnerability announcements that fit this scenario.

Apache, more formally known as the Apache Software Foundation (ASF), features quite prominently in this year's list of vulnerable vendors. ASF oversees several open-source projects that are used by many other vendors. The most notable vulnerability under the ASF banner is courtesy of the Log4j Java library that provides a fast, extensible, and rich logging capability. Any solution built on Java in the last 10 plus years is likely to use Log4j in some form or fashion. By extension of that logic then any serious vulnerability in Log4j is thus automatically inherited by the vendors building applications on top of this open-source library. In our dataset this includes examples of Oracle, Cisco, IBM, Amazon, and others. Several patches were issued by ASF to fully address the flaw, to the frustration of many since this resulted in quite a waste of effort for those patching systems using the library.

Continuing this theme, a vulnerability named Spring4Shell, not to be confused with Log4Shell, emerged in late March 2022. The nature of the flaw was very reminiscent to but distinct from Log4Shell. The Spring4Shell vulnerability set is tracked as CVE-2022-22963, CVE-2022-22965 and CVE-2022-22950. A very specific setup is required to trigger Spring4Shell, unlike Log4Shell which was much more ubiquitous. These vulnerabilities were discovered when Sophos patched a serious security vulnerability found in the Sophos Firewall user interface. Spring4Shell also impacted for example Cisco's Edge Intelligence and Data Center Network Manager. Many other vendors had to scramble to determine if their products were vulnerable due to using this popular Java application framework.

The Mozilla Network Security Services (NSS) cryptographic library contained a heap overflow vulnerability, CVE-2021-43527, that can be triggered when verifying digital signatures. This impacted LibreOffice, Apache OpenOffice, the mod\_nss SSL module for the Apache Web Server, Red Hat Directory Server, Red Hat Certificate System, SUSE Linux Enterprise Server, and others.

PolKit, an open-source policy management component, contained a serious flaw tracked as CVE-2021-4034 that affected Linux distributions such as Fedora, Ubuntu, and others. This flaw affected PolKit versions stretching back as far as 2009. Later the same year, about nine months after we reported the vulnerability in January 2022, we reported that malware was targeting IoT devices and exploiting this vulnerability to elevate privileges on compromised devices.

It would be unfair to single out open-source software to illustrate the point. An example of closed source software dependencies come in the form of Mocana NanoSSL, a subsidiary of DigiCert. Armis released research about several vulnerabilities related to flaws in this library, dubbed TLStrom 2. This impacted Aruba and Avaya switches, and some APC Smart-UPSs. One of vulnerabilities in this library is tracked as CVE-2022-23677 and could result in remote takeover of a vulnerable system over the network.

The examples given here are limited to components used in software that physically reside on premises or on devices we use, but what about the cloud? Earlier in the chapter we mentioned the Azure Linux VM vulnerability called OMIGOD that impacted those that built their solutions on top of existing virtual machine images. The OMIGOD vulnerability reminds us that we must keep track of components in software as well as the aggregate that make up runtime environments such as cloud VM images and containers built by others.

One could argue that vendors could be more transparent about the composition of the products they provide. This is already true for large corporates and governments that require much more transparency as part of their procurement processes. The idea of a Software Bill of Materials (SBOM) is nothing new, but this is still a major challenge especially for legacy solutions. Ideally any new solution must be able to provide a complete list of software components giving risk officers the ability to assess likely exposure when new vulnerabilities are announced or when due diligence is required.

Technology monocultures, such as Microsoft, may help ease this headache, but that may introduce other considerations like being at the mercy of that vendor's pricing models and geopolitical allegiances. Security monocultures may suffer from bigger shocks when easily exploitable vulnerabilities are present such as EternalBlue (CVE-2017-0144). The SolarWinds incident also reminded us that software can be tainted in ways that we would not expect forcing more rigor into our security architectures.



## Log4j: Logging considered harmful

Logging is an important part of monitoring applications and systems, especially to debug if something goes awry. For the most part logging is a mundane and boring background process. That was until a series of flaws were discovered in the popular open-source Log4j Java logging component.

There were four vulnerabilities named Log4Shell and tracked as CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832 that caused major pain for many IT and security teams. Three of the vulnerabilities could result in possible Remote Code Execution, but CVE-2021-45105 that could result in a local denial of service condition.

The nature of the Log4j flaws were such that the vulnerable systems could be compromised simply because a developer decided to log information the application received from an external source. Depending on the application, one could trigger the vulnerability by typing in malicious text into a web application field. The flaw as not limited to just web applications, but any Java application that could take user input and log that value. In some cases, the vulnerability could lead to arbitrary code execution on the host, but also in some cases creative attackers could leak runtime and environment variables such as API keys, credentials, etc, if present.

This Log4j flaw was possible due to the rich templating capabilities intentionally designed for the Log4j component. This allowed the developer to have a flexible way to interact with the library through special text values that Log4j will interpret and perform certain actions, almost like basic macros.

Java can, as part of its design, send code over the network that could result in code execution on the side being invoked or on the receiving end. The technical term for this is serialization.

This feature was abused because Log4j supported the 'Remote Method Invocation' or RMI capability through its templating feature. This feature was enabled by default for some systems.

Many believe that something like the Log4Shell vulnerability could possibly rear its ugly head, soon.

The chart below illustrates the volume of confirmed incidents involving Log4J raised by our CyberSOCs over time.

**We raised 118 incidents related to Log4J between December 2021 and September 2022. Most of them were raised in December '21, when the issue first 'broke'.**

Four of these incidents were rated 'Priority 1' – our highest level of priority – two in December, one in April and one (surprisingly) in August 2022.

**84% of these incidents were raised due the detection of relevant Indicators from our Datalake Threat Intelligence platform.**

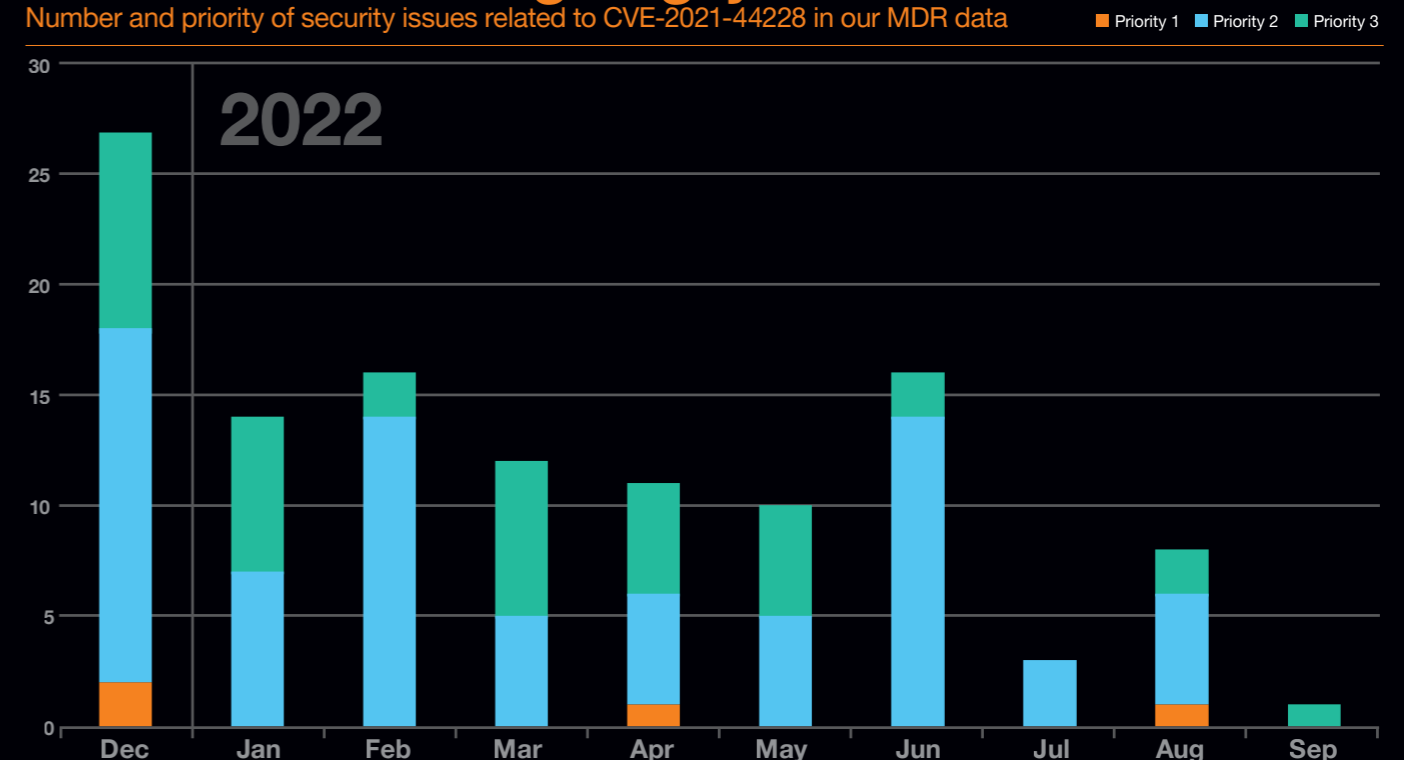
The rest of the attacks were detected through a variety of techniques, including manual Threat Hunting operations.

**CVE-2021-44228 – Log4J** – was the only CVE identified across all our datasets: Word Watch, Vulnerability Scanning and Penetration Testing data.

- **World Watch:** Ranked 1st of 229 CVE. Mentioned 8 times.
- **VOC:** Ranked 9,013 of 21,026 CVE. Reported on 6 unique hosts
- Ranked 7th in our **Penetration Testing** data. Reported in just 1 penetration test

## Incidents involving Log4j over time

Number and priority of security issues related to CVE-2021-44228 in our MDR data



## Security debt

Debt, as a financial concept, means that a choice is made, consciously or unintentionally, to borrow from another party to gain something without having the means now to pay out of your own pocket. That what was borrowed must be returned and in many cases with interest for the period that elapsed.

In the context of good software development practices that means decisions made by the developers and designers should be able to account for little to no flaws. Anytime a design or implementation choice is made at the expense of reviewing it for flaws or defects we accumulate 'security debt'. As coders and designers defer the discovery and correction of a potential flaw to the future, so do they delay the associated costs to the future. This could be a conscious practical decision that is not born out of malice. There might not have been enough time to make a deadline and addressing the flaw now will result in a missed opportunity. Similarly, a flaw can be introduced unintentionally or accidentally. In either case the possible cost, should a security incident arise due to the flaw, will be for the users of this software.

Security debt, like real financial debt, accrues interest by compounding impact. Log4j demonstrated how an obscure library could find itself into so many corporate products. With every deployment and solution that implicitly use Log4j, businesses inadvertently invited risk into their business. This is repeated for every other business or organisation implicitly using this software. Before we know it the exposure of this flaw is beyond what we could imagine and remediating this flaw will cost a considerable amount collectively. If a business chooses not to remediate the flaw out of choice or because they are not aware of it, then the future cost of an incident will potentially exceed the immediate cost of fixing the flaw now. There is an inherent risk in anything, some can be managed, and others may need to be dealt with when they occur. The trick is to find the balance between both.

## Security debt as seen from the raw NLP tags

Named Entities Recognition Value	Named Entities Recognition Label
CVE-2007-4559	CVE ID
Released	Update
Tarfile	Application
Attack	Relevant term
path traversal	Relevant term
Overwrite	Relevant term
arbitrary files	Relevant term
Allows	Relevant term
Application	Relevant term

## Zero-day dread

A zero-day vulnerability is something every attacker, or red teamer, dream of and that defenders dread. Any modern security architecture should, ideally, be designed such that incidents resulting from unpatched vulnerabilities, zero-day or not, can be detected and contained.

The number of vulnerabilities in systems will increase and it's only a matter of time before a system degenerates into the unpatched status. The reality is that vendors struggle to identify vulnerabilities or to even issue patches fast enough after they have been disclosed.

The PrintNightmare vulnerability (CVE-2021-34527) saga started in June 2021 when researchers leaked information about this before Microsoft could issue a patch.

Microsoft finally said it fixed the flaw in September 2021, but users still reported printer and network issues because of the fix.

Atlassian Confluence suffered from a serious unauthenticated Remote Code Execution vulnerability, CVE-2022-26134, that was disclosed early resulting in the vulnerability turning into a zero-day. Proof-of-concept code was circulating allowing anyone to exploit unpatched Confluence servers over the internet.

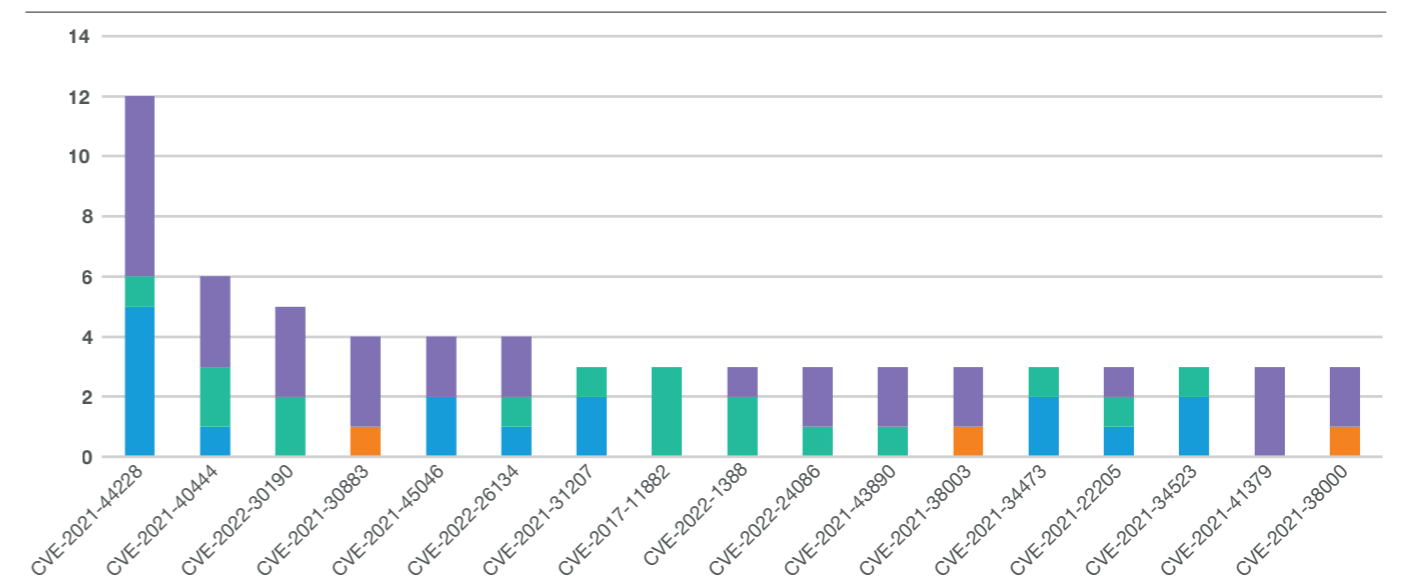
Apple made a conscious decision to stagger fixes for a serious vulnerability, CVE-2021-30883, across different versions of its mobile operating system.

The flaw was first patched in the newly launched iOS 15 operating system, and two weeks later in iOS 14. This meant that users wanting to be safe had to upgrade to a new operating system and possibly having to deal with teething problems. This flaw impacted Apple iPhones, iPads, iPod Touch, Watch, and Macs and could allow an attacker to execute arbitrary code with the highest level of permission.

Vendors will take time to fix security vulnerabilities and often users must still perform validation to ensure these patches do not introduce instability, as in the case of the PrintNightmare patches. Deploying fixes takes time and creates a window of opportunity for attackers to sneak in. Delaying the investment in good security architecture that can detect and contain a breach is looking increasingly like a poor decision.

## Most featured vulnerabilities

Vulnerabilities featuring in 3 or more World Watch advisories across all themes



## The unpopular contest

World Watch advisories included at least 229 distinct CVEs, of which 50 CVEs featured more than once. Two Remote Code Execution flaws in Microsoft products made the podium for most discussed, namely a flaw impacting Microsoft’s MSHTML (CVE-2021-40444) and a flaw in Microsoft’s Windows Support Diagnostic Tool or MSDT (CVE-2021-43890).

If anyone was handing out prizes for most talked about vulnerability this year, then Log4j will be the winner by a long shot. We reported on at least six known incidents where attackers used Log4j to deploy ransomware or breach a network.

Three of the ransomware incidents that mentioned the Log4j flaw were linked to groups strongly affiliated with governments such as the North Korea (Lazarus), China (APT10), and Iran (APT35). Even a new ransomware named ‘Night Sky’ allegedly exploited the Log4j flaw to extort its victims.

Microsoft Exchange vulnerabilities named ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) featured due to Continued exploitation as did ProxyLogon (CVE-2021-26855 and CVE-2021-27065), another set of Microsoft Exchange vulnerabilities, which goes hand in hand with ProxyShell.

The GitLab vulnerability (CVE-2021-22205) is particularly worrisome given the threat of a software supply chain compromise. GitLab is used by software development teams to manage source code and other activities relating to the development pipeline. If an attacker were to gain access to a GitLab host then they could steal proprietary information, steal authentication access tokens, or taint the software or build process with a type of backdoor.

Finally, we are reminded of how relevant older vulnerabilities can be. The infamous Equation Editor vulnerability, CVE-2017-11882, found in the similarly named Microsoft Office Equation Editor component was problematic back in 2017 and 2018. Attackers with roots in Asia targeted a telecommunication company in South Asia according to research by Fortinet<sup>[41]</sup>, as well as various companies in Eastern Europe according to another report by Kaspersky<sup>[42]</sup>. The likely vector here is social engineering as this type of vulnerability requires the victim to open a tainted Office document. One wonders why old vulnerabilities remain relevant. Is it because old software is still actively used, and unfortunately remains unpatched?

Application	CVE	Type
Microsoft MSHTML	CVE-2021-40444	Remote Code Execution
Microsoft Windows Support Diagnostic Tool	CVE-2022-30190	Remote Code Execution
Microsoft Exchange	CVE-2021-31207	Path Traversal
Microsoft Exchange	CVE-2021-34473	Remote Code Execution
Microsoft Exchange	CVE-2021-34523	Privilege Elevation
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
Microsoft Exchange	CVE-2021-27065	Remote Code Execution
Microsoft Office	CVE-2017-11882	Remote Code Execution
Microsoft Windows AppX Installer	CVE-2021-43890	*No info available*
Microsoft Windows Installer	CVE-2021-41379	Privilege Elevation
Apache Log4j	CVE-2021-44228	Remote Code Execution
Apache Log4j	CVE-2021-45046	Remote Code Execution
Google Chrome	CVE-2021-38003	Out-of-bounds Write
Google Chrome	CVE-2021-38000	Improper Input Validation
Atlassian Confluence	CVE-2022-26134	Remote Code Execution
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Apple iOS/iPadOS/WatchOS/macOS	CVE-2021-30883	Remote Code Execution
Adobe Commerce / Magento	CVE-2022-24086	Improper Input Validation
F5 Big-IP	CVE-2022-1388	Missing Authentication

## In the name of evil

Security professionals that perform network and system penetration testing require tooling to perform their tasks, much like any other profession. The cyber security professional’s toolbox is rich with a large variety of tooling that could be considered malicious. Communities and business have emerged that bundle the proverbial ‘Swiss army knife’ of hacking tools with operating systems such as the pervasive Kali Linux. In many cases this is done under the legitimate banner of education and security research.

As the level of sophistication or need grows certain types of tools are required. Creating these kinds of tools are time consuming and challenging, thus it is the perfect opportunity for any entrepreneur to stake their claim in this space. Enter ‘adversarial emulation’ tooling. Adversarial emulation tools are intended to assist with legitimate consulting engagements where a business hires a security professional to attempt to breach the client’s network within a goal-oriented exercise using techniques associated with a special calibre of attacker in mind.

Cobalt Strike is such a tool and offers a malleable platform that enables the user to perform tasks that can emulate techniques and procedures normally in the league of advanced attackers. In the right hands this tool is limited only by the experience and imagination of its operator.

Unfortunately, it’s not that easy to limit who has access to offensive tools such as Cobalt Strike, which is a common problem not just limited to cyber space and manifests in the physical world also.

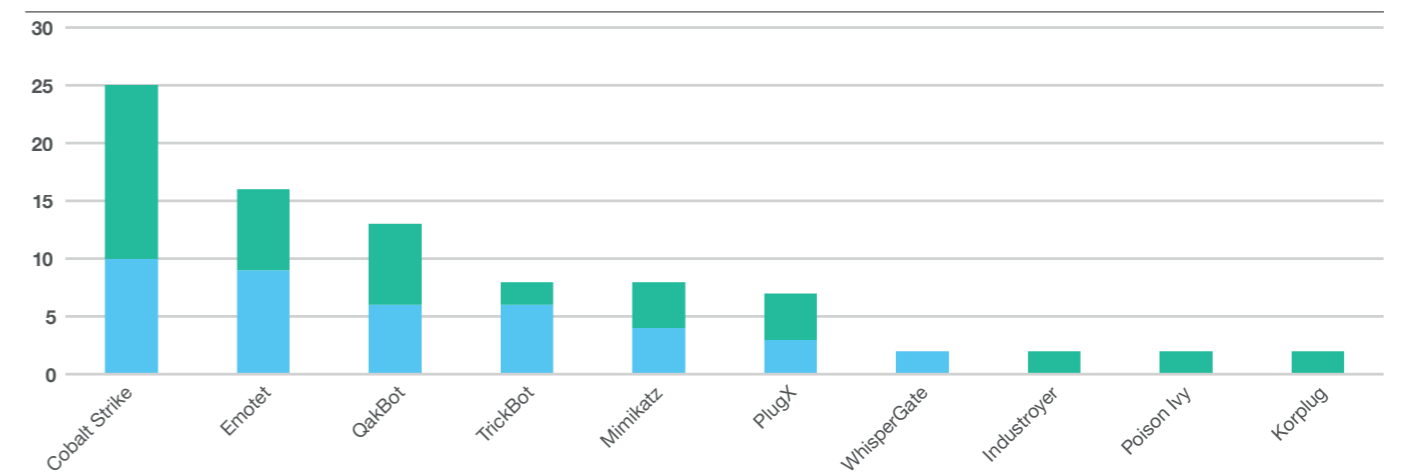
We found that Cobalt Strike was discussed more frequently than threats such as Emotet, QakBot, or Trickbot. At least 9 other malware types were mentioned in the same distinct advisory across the Ransomware and Threat category as Cobalt Strike.

Malware such as Trickbot or Emotet is typically used by attackers to get a foot in the door using phishing, for example, to drop other malware that inevitably results in a Cobalt Strike beacon or payload being injected into the breached environment. This allows the attacker to build a beachhead into its victim’s infrastructure enabling the attacker to perform espionage, pivot to other networks, or turn the extortion screws on in the form of ransomware.

It is unfortunate that a tool such as Cobalt Strike is getting such a bad reputation, but we expect other similar tools such as Brute Ratel C4 to become as prominent. Limiting or prohibiting these tools will not cause the other threats to disappear as something else will just appear in its stead. We specifically cover Cobalt Strike in our [CyberSOC chapter](#).

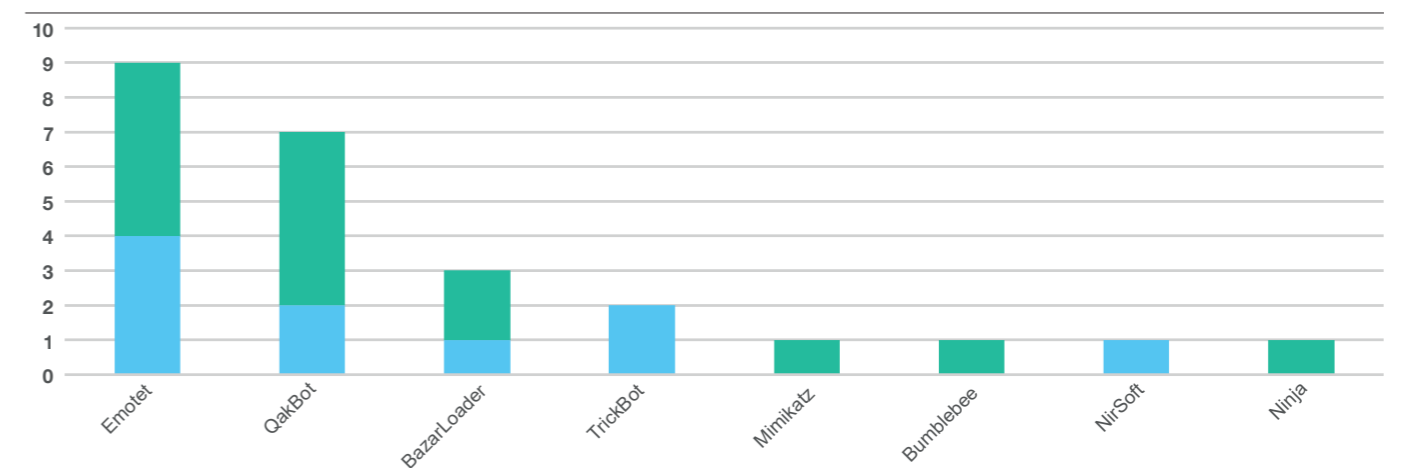
## Advisories on ‘Ransomware’ and ‘Threat’

Malware found by NLP under the Ransomware and Threat theme (more than one occurrence)



## Advisories on ‘Malware’ and ‘Cobalt Strike’

Malware found by NLP in combination with Cobalt Strike



## I spy with your phone

The modern mobile phone is a unique platform with Google and Apple investing heavily in developing new features to keep its user base engaged. As with any system there are flaws and over time these flaws will be exploited. This is not necessarily because of poor security, in fact mobile security architecture is arguably much better than that found in normal PCs. The complexity of hardware security elements and the usage of cryptography is eye-watering. The fact that entertainment services and financial service providers trust certain mobile device manufacturers is because of their security architecture.

Mobile phones are packed with several capabilities that, when turned against a target, results in a highly effective surveillance platform. A highly specialized market exists that offers access and tracking of targeted mobile devices. This is all made possible through exploitation of vulnerabilities in the operating systems of the mobile devices or in some cases by targeting vulnerabilities in mobile applications. In concept very similar to how PCs can be targeted illustrating that some ground truths are transferable across platforms.

There existed a vulnerability, CVE-2021-38000, in Google Chrome that could allow an attacker, if exploited successfully, to load any URL the attacker wanted. The flaw impacted Google Chrome on Linux as well as Chrome running on Android and was patched in late 2021. In Q2 of 2022 we learned that Cytrox's Predator mobile phone spyware has the capability to exploit this vulnerability, among others such as CVE-2021-1048 that allows for local privilege escalation.

RCS Labs S.p.A has a spyware product called Hermit that can target both Android and iOS devices. The iOS version of Hermit allegedly makes use of known vulnerabilities shared by jailbreaking enthusiasts such as CVE-2022-30883 that allows for arbitrary code execution at kernel level. This type of vulnerability can then be used to pivot onto other areas of the compromised device, leading to information exfiltration and surveillance activities.

Citizen Lab has been doing great work in highlighting and dissecting the mobile spyware market.

Citizen Lab shared details of an exploit developed by the NSO Group for its Pegasus spyware that was used against European politicians. The vulnerability targets the iMessage application that is part of the Apple iOS mobile operating system. Members from the Google Project Zero team later published an excellent in-depth analysis of the exploit named FORCEDENTRY developed by NSO Group. The analysis revealed an intricate and highly sophisticated exploit that made one marvel at the level of technical expertise involved in crafting such elaborate exploits. The FORCEDENTRY exploit is effectively a Turing-complete virtual machine disguised as an image that circumvented a security feature of Apple's mobile devices called the 'BlastDoor' sandbox. Unfortunately, the flaw that FORCEDENTRY exploited was due to a design choice that allowed the exploit to trigger before BlastDoor could be effective.

Some governments do not squirm to spend millions of dollars on procuring the services of these spyware vendors in the name of protecting their citizens and interest.

Running endpoint protection on mobile devices is an option but is somewhat limited as it requires active monitoring of network traffic and requires access to parts of the device to infer malicious behaviour. This is due to the security architecture of these devices. Traditional anti-malware on Windows runs inside a special space of the operating system that gives it access to process information and file system handles. This allows the monitoring software to get better fidelity on the type of local activity. Mobile vendors can opt to provide a similar anti-malware friendly API, but this new feature increases the attack surface for malware. There is also a strong argument against such a feature to protect privacy.

Adding more features to systems tends to weaken their security posture in the long run. To improve the security of a system we need to remove features to the point where only the useful features remain, but that kite will not fly.

More information can be found in the [Mobile Security chapter](#).

## Conclusion

In the science fiction novel Dune, by Frank Herbert, at one point the protagonist chants "I must not fear. Fear is the mind-killer. Fear is the little-death that brings total obliteration. I will face my fear. I will permit it to pass over me and through me. And when it has gone past I will turn the inner eye to see its path. Where the fear has gone there will be nothing. Only I will remain."

As dramatic as this may be, it is rather striking how close the title was of two blogs by Kieman McGowan and Phillip Kristoffersen respectively. The authors of these blogs titled "Complexity is the mind-killer" share their thoughts on software design and implementation decisions. McGowan and Kristoffersen highlight that one needs to select the simplest solution that can get the job done but allow yourself enough room to maneuver if you need to adapt.

Likewise, IT and cyber security teams need to find the right balance to administrate systems, manage configurations, and meet the demands of compliance that ensure their organization can operate in a seemingly chaotic and dangerous cyber space. Complexity in solutions combined with the opaqueness in their composition will lead to mistakes and make it so much more difficult to determine if the latest serious vulnerability is present in a system.

Marc Andreessen of the VC firm Andreessen-Horowitz is famous for saying "software is eating the world". By this we now know that software is defining how we live, work, and govern. Try doing business, apply for a government service, or gain access to healthcare without having to interact with software along the way. Some modern refrigerators have more software than you can shake a stick at. At every point and turn along this path there are cyber security risks that need to be managed.

Clients will become more demanding of their vendors and service providers to provide quick turnaround and a transparent response when new serious vulnerabilities are announced. Tighter service level agreements will govern response times and types of assurance. Ultimately, procurement processes and due diligence processes will become much more onerous for the parties involved unless there exists a mechanism that can answer the pressing questions with reduced effort.

asset Management will become more and more important and should extend beyond operating systems and hardware and into the cloud. Teams will need to understand what each feature and each access permission published by cloud infrastructure is for and whether it is used.

Attacks against mobile devices do happen, but from what we saw these are limited to the surveillance industry for now. The architecture of modern mobile phones is good in that it forces attackers to spend quite a bit of resources to get near their targets. It is also worth noting the importance of mobile phones to the bottom line it fills for manufacturers as it is in their interest to protect these platforms. Similarly, it is in your business' interest to ensure that mobile devices are managed according to general best practices as these devices are integrated heavily into our professional lives.

Ultimately simplifying systems and reducing the attack surface is a long-term strategy that tackles fundamental cyber security problems at its root as an attacker cannot exploit something that is not there. Medium term strategies include understanding your environment and ensuring that it can be adapted to meet the demands of business while managing the associated risks. This will involve getting vendors onboard to agree to an acceptable approach for dealing with cyber security incidents and provide feedback when serious vulnerabilities are reported. The day-to-day fight will not change and will still require judicious vulnerability management combined with rigorous monitoring and detection methodologies to identify and isolate threats. A robust and disciplined response is needed when threats are detected inside your infrastructure. Stay ahead of them by following an intelligence-led approach.



# Patch where it hurts

## Effective vulnerability management in 2023

Good vulnerability management is not about being fast enough in patching all potential breaches. It's about focusing on the real risk using vulnerability prioritization to correct the most significant flaws and reduce the company's attack surface the most.

Company data and threat intelligence need to be correlated and automated. This is essential to enable internal teams focus their remediation efforts. Suitable technologies can take the shape of a global Vulnerability Intelligence Platform. Such a platform can help to prioritize vulnerabilities using a risk score and let companies focus on their real organizational risk.

**Mélanie Pilpré**, Product Manager, **Orange Cyberdefense**



Based on these facts we understand that there is no point in patching every vulnerability. Instead, we should focus on those that pose a real risk based on the threat landscape and the organizational context.

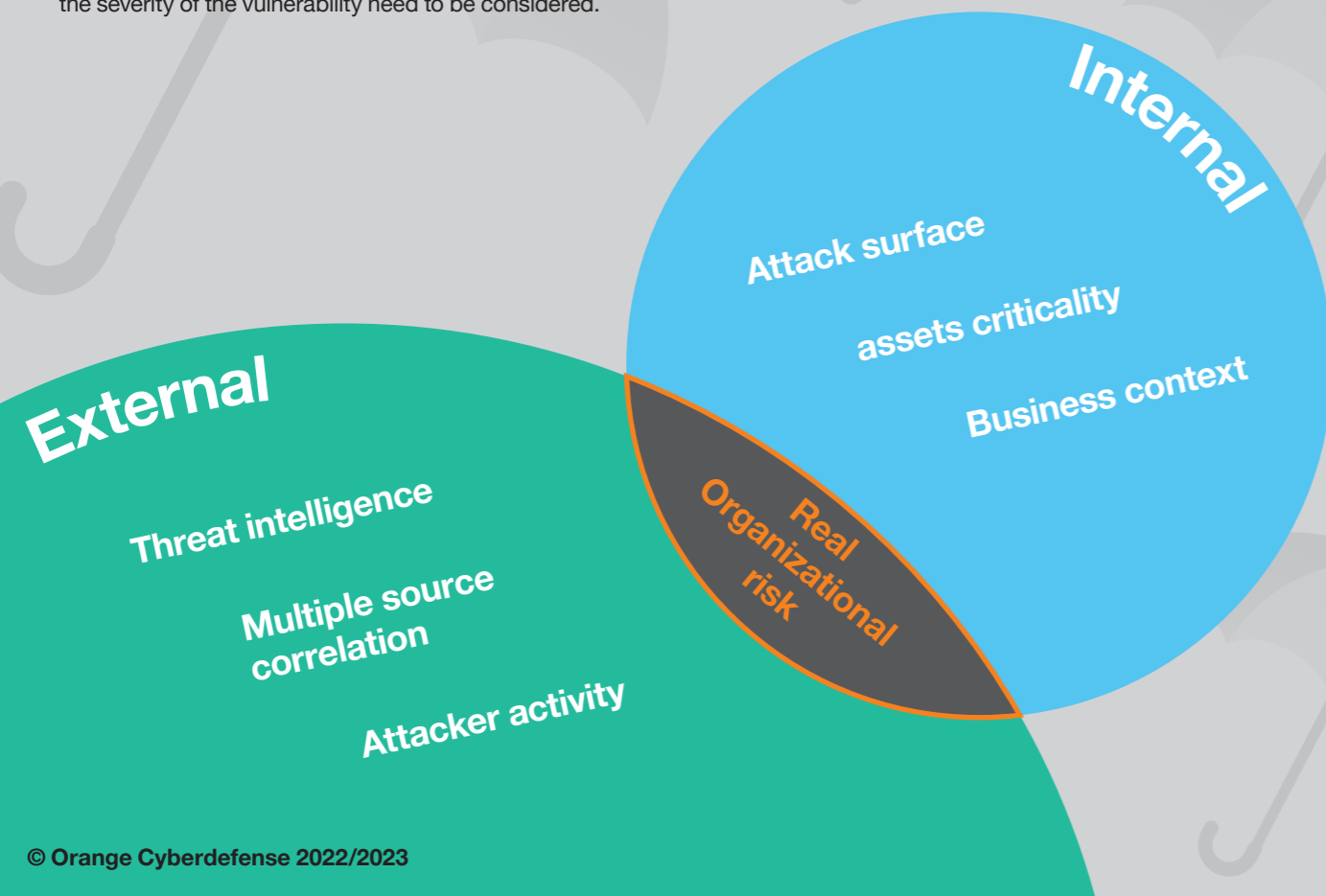
### The concept of risk-based vulnerability management

The objective is to focus on the most critical assets and the assets having a higher risk to be targeted by threat actors. To approach a risk-based vulnerability management program we need to consider two environments, which are outlined in the graphic below.

### Getting started

Three facts to have in mind before establishing an effective vulnerability management program:

1. The number of discovered vulnerabilities increases every year. An average of 50 new vulnerabilities are discovered every day so we can easily understand that it's **impossible to patch them all**.
2. Only some vulnerabilities are actively exploited and represent a very high risk to all organizations. Around 6% of all vulnerabilities are ever exploited in the wild<sup>(49)</sup>: we need to reduce the burden and focus on the real risk.
3. The same vulnerability can have a completely different impact on the business and on the infrastructure of two distinct companies, so both the business exposure and the severity of the vulnerability need to be considered.



### The internal environment

The Clients' landscape represents the internal environment. Companies' networks are growing and diversifying and so is their attack surface. The attack surface represents all components of the information system which can be reached by hackers. Having a clear and up-to-date view of your information system and of your attack surface is the very first step. It is also important to consider the business context. In effect, companies can be a greater target depending on their business sector due to specific data and documents they possess (intellectual property, classified defense...). The last key element to consider is the unique context of the company, individually. The objective is to classify assets according to their criticality and to highlight the most important ones. For instance: assets that if not available would cause an important disruption to business continuity, or highly confidential assets that if accessible would make the organization liable to multiple lawsuits.

### The external environment

The threat landscape represents the external environment. This data isn't accessible from the internal network. Organizations need to have the human and financial resources to find and manage this information.

Alternatively, this activity can be externalized to professionals who will monitor the threat landscape on the organization's behalf.

Knowing the vulnerabilities which are actively exploited is a must since they represent a higher risk for a company. These actively exploited vulnerabilities can be followed thanks to threat intelligence capabilities combined with vulnerability data. To have the most efficient results, it's even better to multiply the threat intelligence sources and correlate them. Understanding attacker activity is also valuable since it helps anticipating potential threats. For instance: intelligence concerning a new zero-day or a new ransomware attack can be actioned on a timely basis, to prevent a security incident.

Combining and understanding both environments will help organizations define their real risk, and pin-point more efficiently where preventative and remediation actions should be deployed.

There is no need to apply hundreds of patches but rather ten of them, selected ones, that will drastically reduce an organization's attack surface.

## Patch smarter, not harder!

There are five key steps to implement a risk-based vulnerability management program:



**Identification:** Identify all your assets to discover your attack surface: a discovery scan can help having a first overview. Then launch regular scans on your internal and external environments and share the results to the Vulnerability Intelligence Platform.



**Contextualization:** Configure your business context as well as the criticality of your assets in the Vulnerability Intelligence Platform. The scanning results will then be contextualized with a specific risk scoring per asset.



**Enrichment:** The scan results need to be enriched using additional sources provided by the Vulnerability Intelligence Platform, such as threat intelligence and attacker activity that will help to prioritize considering the threat landscape.



**Remediation:** Thanks to the risk scoring given per vulnerability, which can be matched with threat intelligence criteria like "easily exploitable", "exploited in wild" or "widely exploited" for instance, prioritizing remediation effectively is much easier.



**Evaluation:** Monitor and measure the progress of your vulnerability management program using KPIs and customized dashboards and reports. It's a continuous improvement process!





**Charl van der Walt**  
Head of Security Research  
Orange Cyberdefense

## A history of vulnerabilities

# Evolution of the weakest link

In previous versions of the Navigator report, and indeed in other parts of this report, we have focused on what we see the attacker doing. It's important that we remain realistic about what perspective we're holding. For example, our CyberSOC data allows us to consider what we're detecting on our client networks. Cyber Extortion data allows us to consider the victims of ransomware who have refused to pay out immediately.

For this year's Navigator, for the first time, we're assuming a brand-new perspective: Vulnerability. This perspective allows us to consider the problem from a different point of view. Rather than look at the threat, or the impact of security failures, we now look at one of the key causes, namely unpatched, poorly coded or misconfigured computer systems. In almost every attack, regardless the origin or the outcome, there is a computer vulnerability of some kind involved.

## Know your weaknesses

To move toward a better understanding of the scope and shape of the vulnerabilities our clients must deal with, we leverage two new datasets for the first time this year:

1. **Vulnerability Scans:** Our VOC service performs continuous (semi) automated scans of client assets to identify known vulnerabilities that have not been patched or mitigated.
2. **Penetration Tests:** To gain a much more 'real world' view on how well their IT systems resist a targeted attack by a skilled hacker, clients will engage our team of over 200 Ethical Hackers to conduct controlled emulation of an attacker by a real adversary.

This being the first year that we examine data from these two services, neither dataset is perfect. Nevertheless, both datasets hold valuable intelligence, and viewed together they provide some invaluable insights. In this chapter we will look at the data from these two services separately and, where sensible, together.

## Vulnerability scanning data

For the analysis of the vulnerabilities on our client's internal and internet platforms, web applications and cloud systems were scanned.

This is a managed service in which identified assets are scanned by one or more engines on a prescribed basis to collect patch and vulnerability information. The findings are reviewed and moderated by our specialist analysts, who also provide remediation guidance and other support to our clients.

As of the end of 2019 our teams have been gradually porting our clients worldwide onto a single, centralized reporting platform. As the data on this platform has grown and matured we are now in the position to perform an analysis on the data it contains.

For the purposes of this report, we considered 41 distinct clients whose service and datasets can be considered comparable and consistent. These clients have all been scanned on a semi-regular basis between October 2019 and October 2022, resulting in 6,877 distinct vulnerabilities being reported across 38,809 unique 'assets'.

We should note that the number of Clients and the number of assets in this dataset have not been consistent over time. This is of course because we have onboarded and offboarded Clients and assets onto the platform during the year.

Vulnerability Scans are performed automatically or semi-automatically by a variety of Scanning Engines, which may vary from client to client.

These include:

- Qualys
- Qualys Web Application Scanner
- Nessus
- Nexpose
- Netsparker
- Custom Scanners

Each finding is assigned a unique name and number, which allows us to differentiate between them. A finding will also include a Port Number, Risk Rating (Information to Critical), a CVSS<sup>[4]</sup> Score (0-10), CVE reference where appropriate and some other supporting detail.

We consider a Unique asset to be the combination of Client, Name, IP Address and asset Type (e.g. host or web application).

For the geeks amongst our readers, we should note that by these two sets of definitions the same Vulnerability could be reported on the same asset, but on different Ports. This is common, for example, with Web Servers that may run on Port 80 and Port 443. We feel this provides an unreleastic view and thus chose to count the same issue reported on two or more ports as the same finding.

To account for this we can further define a 'Unique finding' as the combination of:

- Client
- asset
- IP
- HostType &
- Name of finding

**Considered on this basis, this study contains 2,079,031 unique findings.**

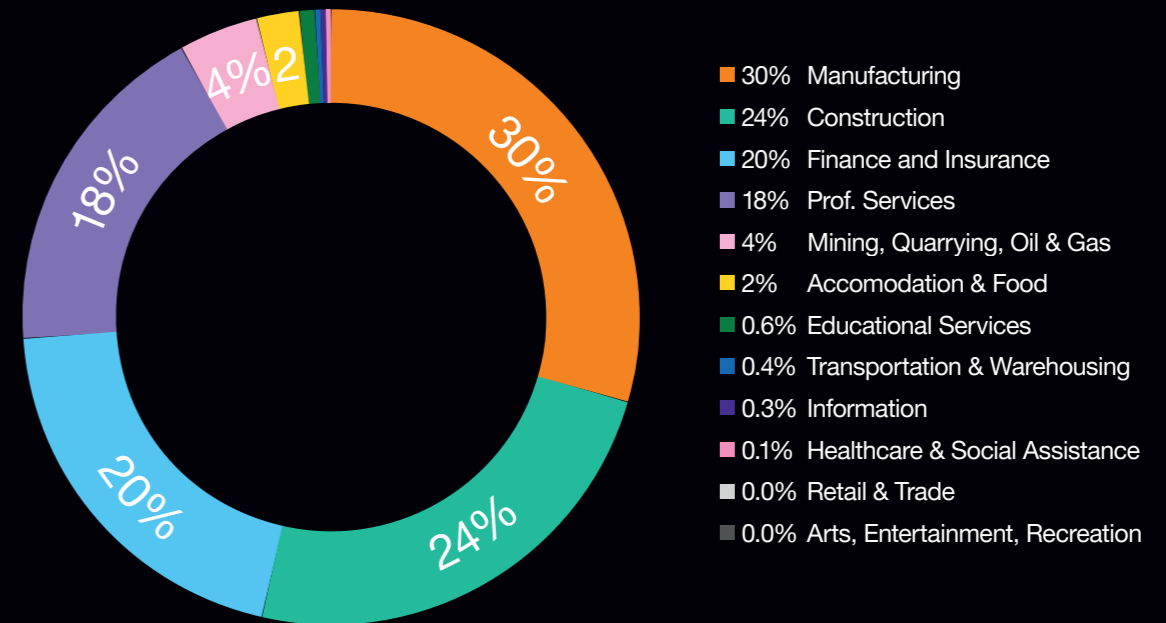
As the data we are reporting on is derived from the reporting platform we use for our Managed Vulnerability Scanning service "Managed Vulnerability Intelligence [identify]", we must note that our Analysts may review the findings reported by the Scanning Engines and reclassify them if they are considered to be inaccurate or inappropriate in some way, or work with the Client to consider and track appropriate remediations.

We note that some findings are not relevant and exclude these from some of our analysis, particularly 'False Positive' and 'Duplicates'. It is also meaningful to differentiate between 'Active' and 'Potential' vulnerabilities in specific analyzes.

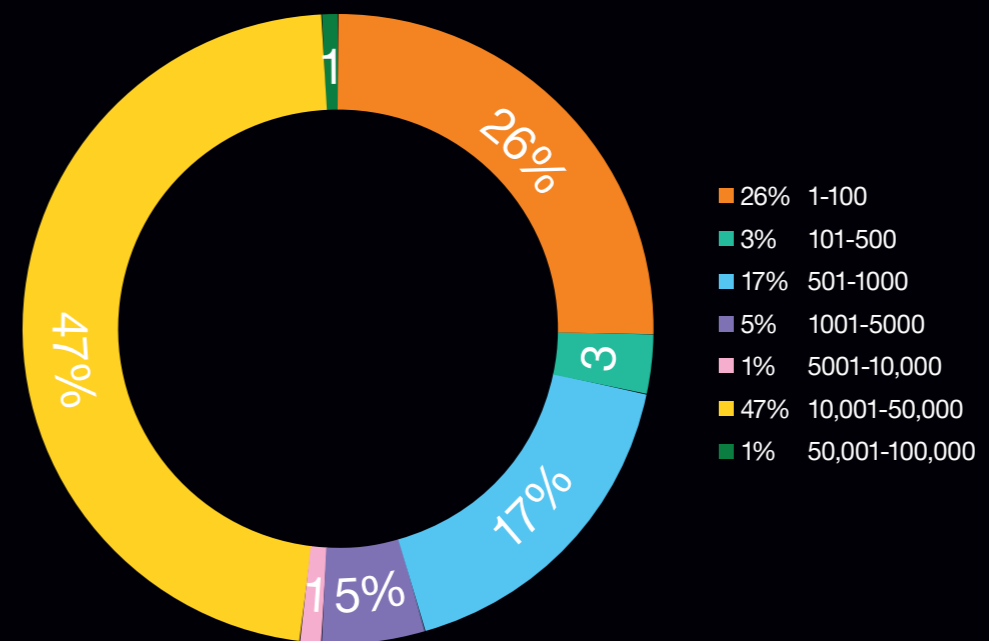
**Interestingly, only 1% of the findings in this dataset were marked as False Positive.**

By combining the definitions and principles above, we can define a final metric – Unique finding Per asset. **To allow for a simple, normalized comparison of findings across Time, Industry, Scanner and the like, we consider the number of unique findings, divided by unique assets, to derive a simple finding per asset, which allows for normalized comparisons across different segments of our data.**

## Distinct assets being scanned by Industry



## Distinct assets being scanned by Client Employee count



We should note that not all Vulnerabilities are considered equally severe, so findings are assigned a Severity Score ranging from 'Informational' to 'Critical'.

We note that a large quantity of all the findings are tagged 'Informational', and therefore provide information about the target, or the scanning process, but not about vulnerabilities on the target. Much of our analysis will therefore exclude this portion of the findings.

## Penetration Testing Data

A Penetration Test is a contracted exercise in which a team of skilled and highly-trained 'Ethical Hackers' is tasked with emulating the activities of a real attacker in order to assess the security of a system, identify vulnerabilities, and derive opportunities to improve its security posture.

Like Vulnerability Scanning, this exercise involves finding and reporting Vulnerabilities in the target systems, and has a similar goal. But the process is very different. The tester will also seek to identify known vulnerabilities (often those with CVE numbers assigned to them) but will then also attempt to leverage those vulnerabilities to gain access to a target system, identify valuable resources that could be compromised or pivot from there to attack other systems in range. Penetration Testing is usually very targeted, performed within a set of constraints agreed with the client that will include the targets in scope, the time available, the location and privileges of the attacker, and sometimes specific goals or 'objectives' the tester should seek to achieve. Each test is performed by one or more specific Ethical Hackers who then also writes up a report by hand explaining what was done, what was achieved, what that implies and what could be done to improve security posture.

The 'findings' of a Penetration Test report are therefore only a small element of the overall output, but they contain elements similar to the findings of a vulnerability scan and can be analyzed in a similar way, and even compared to some extent.

**Our global Penetration Testing team comprises more than 200 Ethical Hackers in 10 countries.**

As reports are a boutique product – hand-written by the tester and customized to meet the client's specific requirement - they do not lend themselves readily to quantitative analysis. For the purpose of this study, therefore, we have developed a basic Machine Learning capability that is able to extract data from these human-readable reports, quantify specific elements (like findings and their assigned Severity) and even extract key entities, like CVE numbers, technologies involved, etc.

## The most popular types of tests in this subset of projects are as follows:

Test type	Proportion of the tests	Type
WebApp	30%	Attack on a custom web-based application.
External	25%	An attack on the internet-facing systems from the internet
Internal	15%	An attack on internal systems by an attacker originating from the internal network, or who has already breached the perimeter
Application Security	11.5%	Attack against a stand-alone application
Mobile	7%	Attack against a mobile phone application
Red Team	2.8%	A targeted attack where the tester has a specific objective and very limited constraints.
API	2.5%	Attack against a web API

**We collected, anonymized and enriched 1,424 such Penetration Test reports from January 2018 to October 2022.**

Of course, such an 'algorithm' is only modestly good at getting to the 'heart' of the Ethical Hackers true message to the client, and this is only a fraction of the all the projects performed by our teams over that period, but we opted to select a subset of reports with similar attributes like language, style, categorizations etc, to make for a meaningful analysis. We plan to extend this scope for future releases of the Navigator.

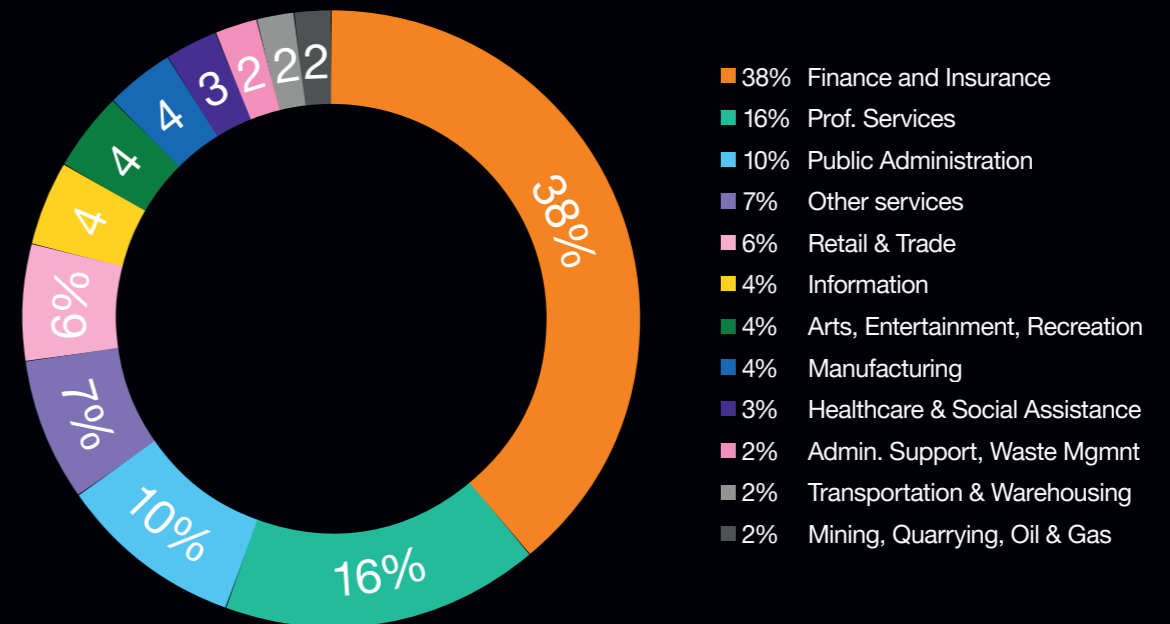
A reasonable cross-section of industries is represented in this dataset, but there is a clear weighting toward industries that are highly regulated or otherwise more conscious of security for some reason.

Finance and Insurance is the dominant industry across this dataset, but it can be seen that businesses in other industries in this dataset are also increasingly engaging us for tests. 'Professional, Scientific and Technical' is a big industry that has gradually become better represented, as has 'Information' and 'Public Administration'. The amount of testing for other industries varies over time.

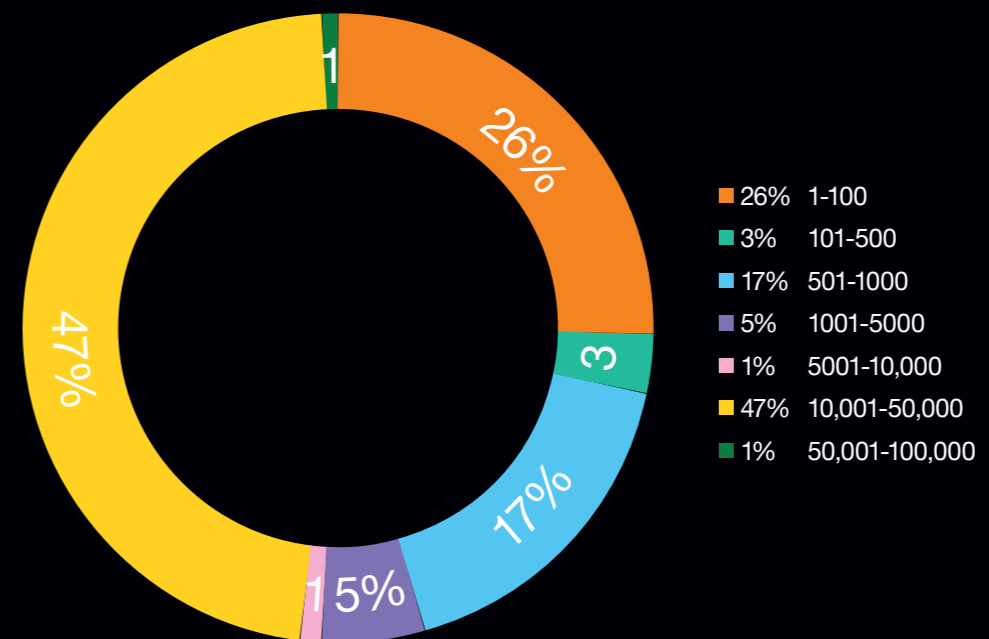
As the number of clients and the number of tests performed will vary dramatically from industry to industry, we consider not only the number of clients or projects, but the amount of time invested into projects. Eventually, we consider time-invested as a baseline in this manner to allow us to perform normalized comparisons across the dataset.

**54% of the Clients in this dataset engaged us for just one test during the period. A further 40% engaged us between 2 and 10 times, while 6% of clients in this dataset engaged us over 10 times during the period.**

## Assets scanned by Industry



## Assets scanned by Client Employee count



As the number of clients and the number of tests performed will vary dramatically, we consider not only the number of clients or projects, but the amount of time invested into projects in our analysis. We consider time-invested as a baseline in this manner to allow us to perform normalized comparisons across the dataset. To achieve this we add up the CVSS score assigned to each finding in a Test, and divide it by the number of testing days invested in that test, to derive a normalized 'CVSS Per Day' metric, which we can use to compare different segments of the dataset.



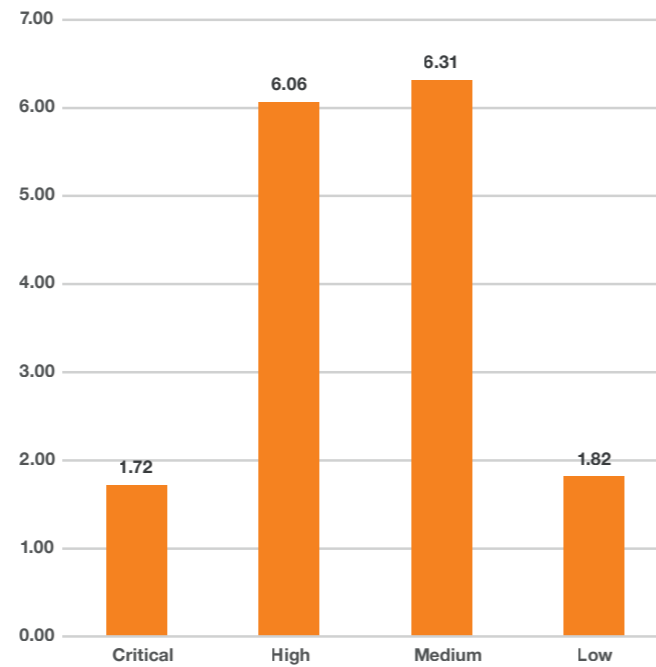
### Vulnerability Scanning findings

In order to consider finding volumes in a meaningful way, we consider the spread of 'Unique findings' as defined above across various segments of our dataset.

The chart on the right illustrates the number of 'Real' findings (excluding False Positives and Informational) we report per Unique Asset. Ignoring 'Informational' findings, false positives and duplicates, we report an average of 16 Findings per Asset. The distribution across severities displayed in the chart is largely intuitive, although it is somewhat surprising that the majority of findings are classified as 'Medium' or 'High' severity.

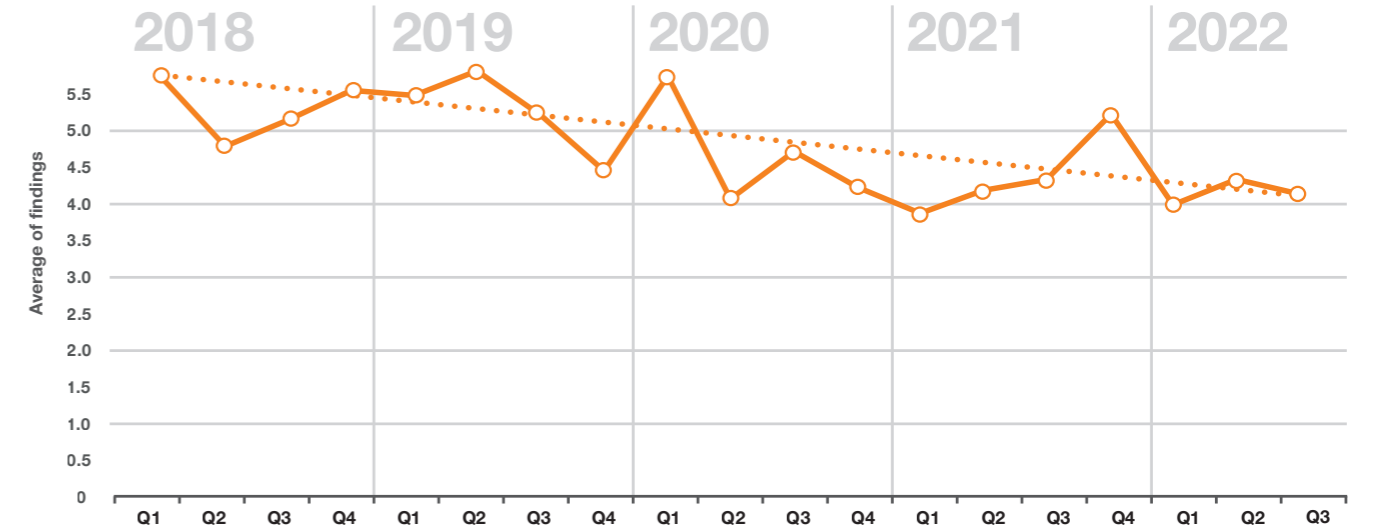
It also appears that the number of findings grows at a rate similar or even higher than the growth in number of assets.

There is too much variation and too little time reflected in this data to arrive at any firm conclusions on that matter, however.



### Vulnerabilities found per day over time

CVSS score of found issues per project day in Pentesting



### Penetration testing findings

For first time clients, from the beginning of 2018 to August 2022, there has been a 55% decrease in the (combined) volume and severity our testers are reporting for each day of work performed.

But it doesn't seem unreasonable to assert that our testers – arguably among the best in the world – are having to work a little harder to report serious issues within their client base.

Our testers also need to work harder to report 'Serious' findings – ranked High or Critical – that would indicate that our team reported significant security weakness while testing.

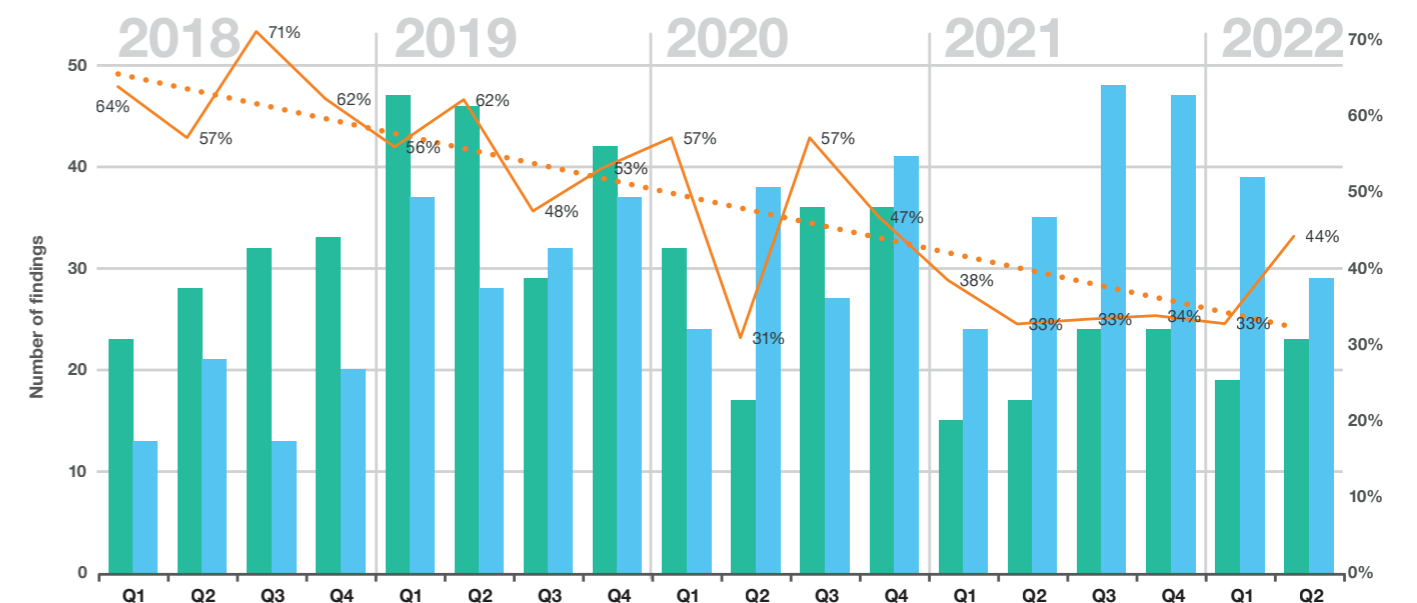
Put differently – and expanding now to our full dataset of all tests in 2022 – our testers would have to work 8 hours 47 minutes to achieve the same results they would have managed in 8 hours at the start of 2018 – an increase in effort of 10%.

On average over the last 4 years our qualified Ethical Hackers reported a Confirmed Serious (High or Critical finding) for every 7.7 days spent testing. The average time spent across all tests is 9 days.

There are many variables that impact the result we see above, many of which are invisible to us in the data.

### Critical vs. non-critical findings over time

Proportion of penetration test results in different criticalities



### Industry comparison: VOC scanning

In the charts below we consider the number of findings per asset for the different Industries and business sizes represented in our dataset. For this comparison we restrict ourselves to only consider 'hosts' (as opposed to web assets) and only the standard network scanners – Qualys and Nessus. This is to allow for a more objective comparison across all the industries in our dataset.

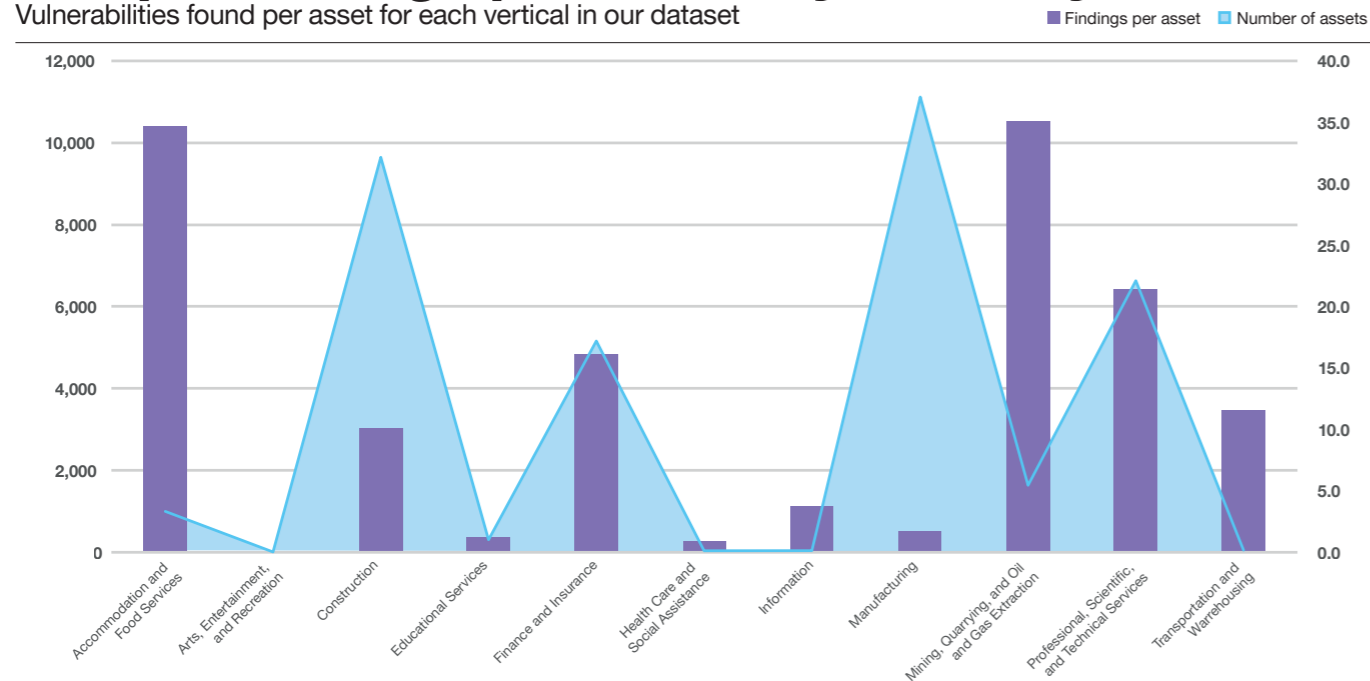
Industries for which we have low asset counts in this dataset can probably be ignored for the purpose of this comparison. But for the 4 biggest sectors, where we have in excess of 4,000 assets each to examine, the variation in finding volumes is considerable.

The maximum age of findings in the view below serves as much as an indication of how long clients from that Industry have been present in our dataset as anything else, while the average age is a better proxy for how well clients are doing at addressing the issues we report. Industries with high maximums and low averages would therefore be doing the best, high maximum and high average... the 'worst'. Industries with very low maximum ages have probably not been in the dataset for very long and should therefore perhaps not be included in comparisons on this metric.

**However these Industries are compared, the finding Age is a concerning metric.**

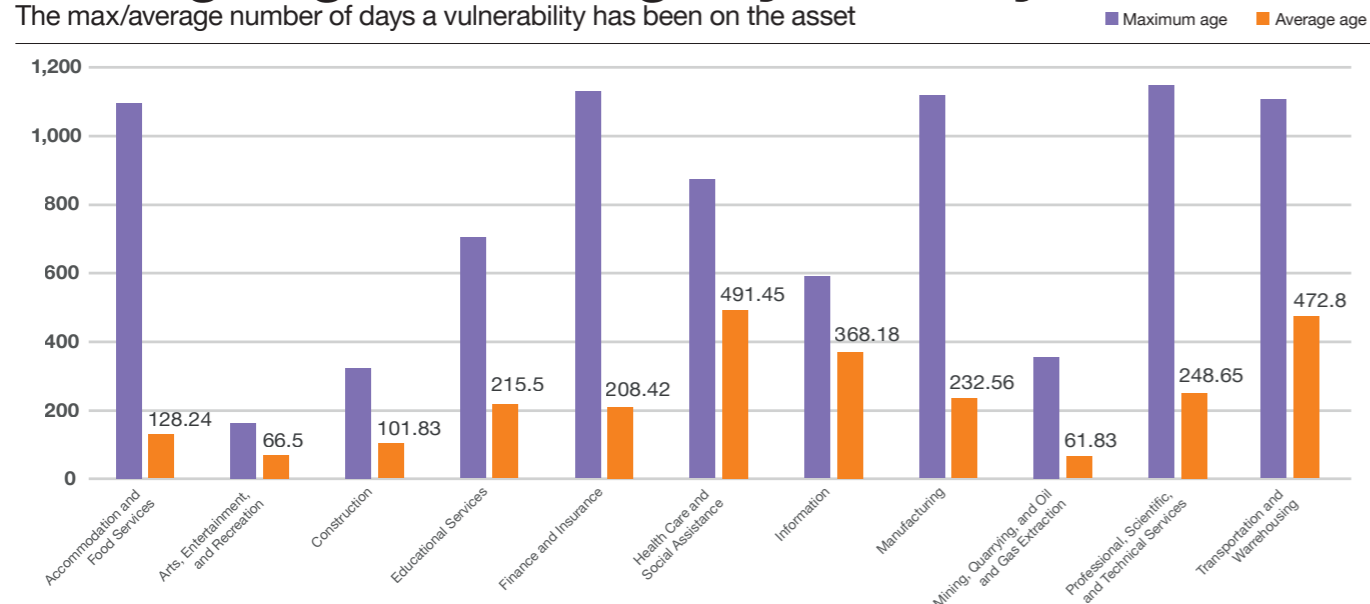
## Unique findings per asset by industry

Vulnerabilities found per asset for each vertical in our dataset



## Average age of findings by industry

The max/average number of days a vulnerability has been on the asset



### Industry comparison: Pentesting

There is a reasonable distribution of Industries represented in our Penetration Testing dataset, but the types of tests and durations vary considerably. There are also several variables that are not visible to us in this dataset. To compensate for this somewhat, we limit our comparison to include only clients for which we performed the three most common forms of test – Internal, External and Web Application.

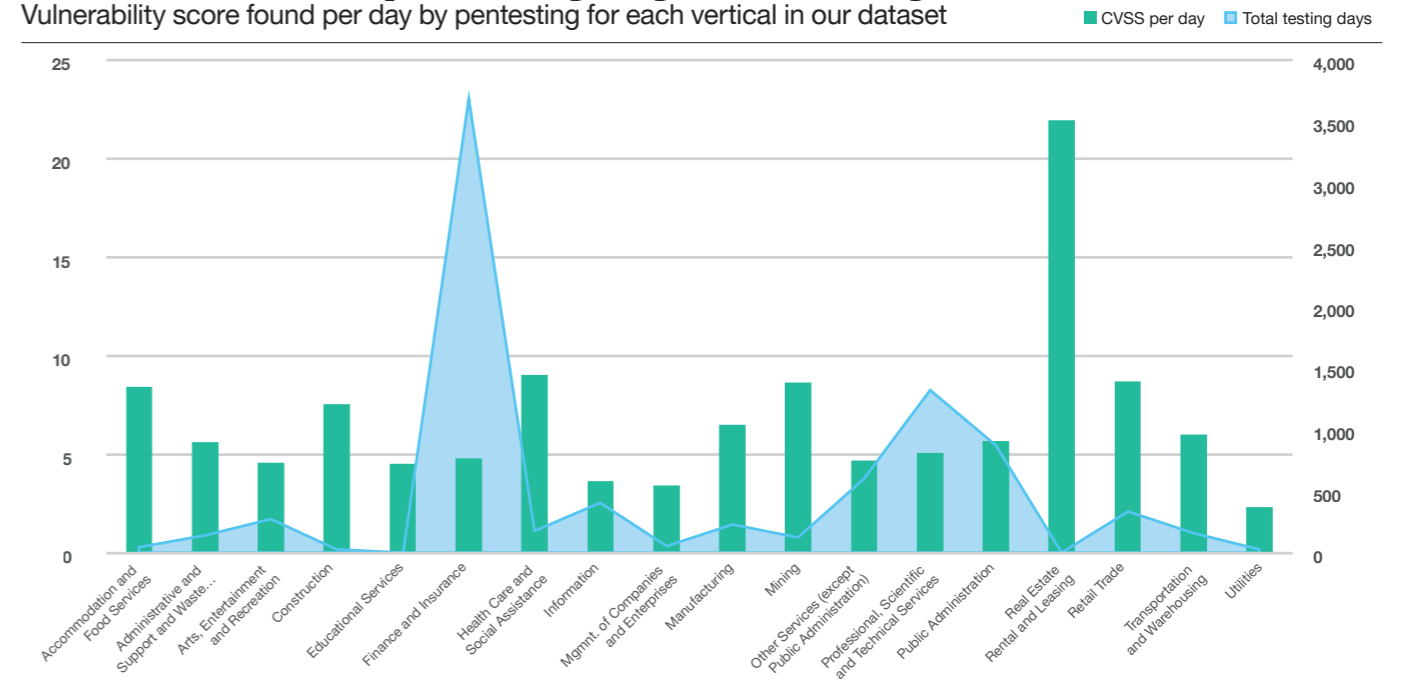
Given this level of variability, it is difficult to draw any conclusions about the relative Vulnerability Management posture across industries. What stands out rather, is the apparent inverse correlation between CVSS<sup>[44]</sup> Per Day score and the total number of testing days for each industry: the more testing is done in an industry, the less we appear to find.

This is certainly the case for the stand-out industries in this dataset – Real Estate, Healthcare, Mining, Administrative and Retail. Industries that do a lot of testing with us on the other hand – Finance and Insurance in particular – tend to deal with fewer findings.

The relative levels of Penetration Test findings across Industries do therefore tell us something about the level of security for those Industries, but only in so much that more 'mature' Industries - which test more and more often – are likely to be better at Vulnerability Management overall.

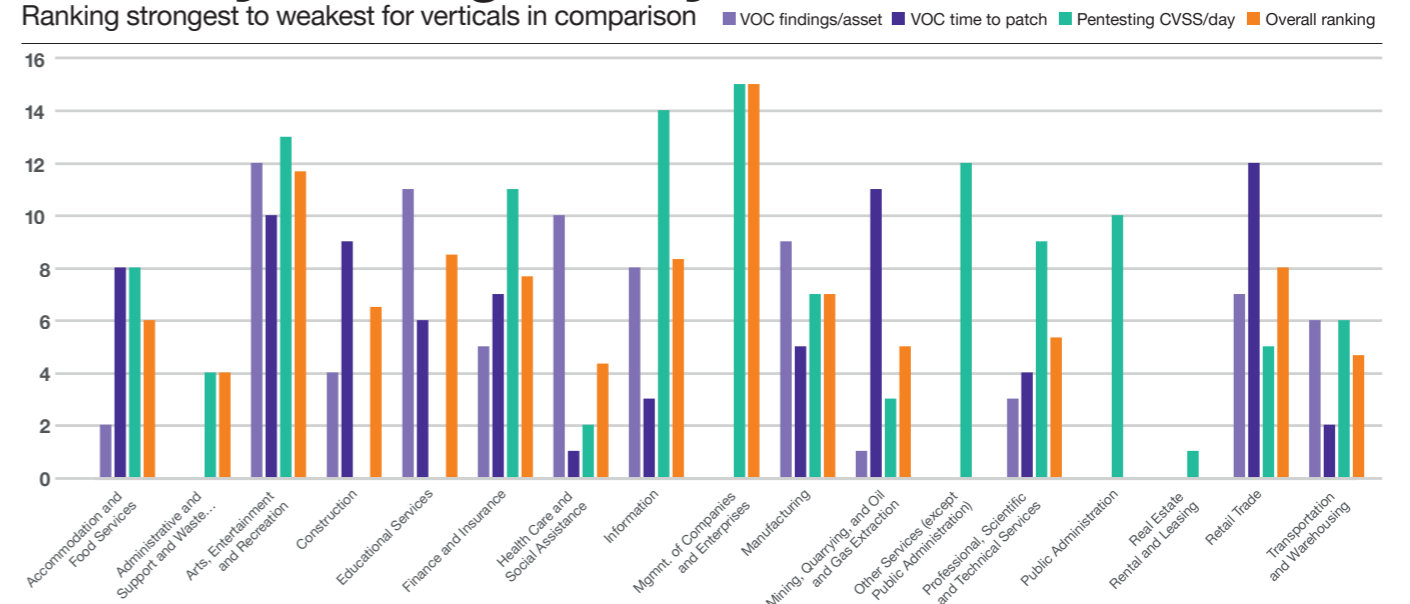
## CVSS score per day by industry

Vulnerability score found per day by pentesting for each vertical in our dataset



## Industry ranking for key metrics

Ranking strongest to weakest for verticals in comparison



### Scoring vulnerabilities

The Common Vulnerability Scoring System (CVSS) is a public framework for rating the severity of security vulnerabilities in software. It is application and vendor neutral, enabling an organization to score its IT vulnerabilities across a wide range of software products – from operating systems and databases to web applications – using the same scoring framework.

**A CVSS score can be between 0.0 and 10.0, with 10.0 being the most severe.**

Like most providers, we use CVSS across our services as a standardized means of assigning severity scores to vulnerabilities.

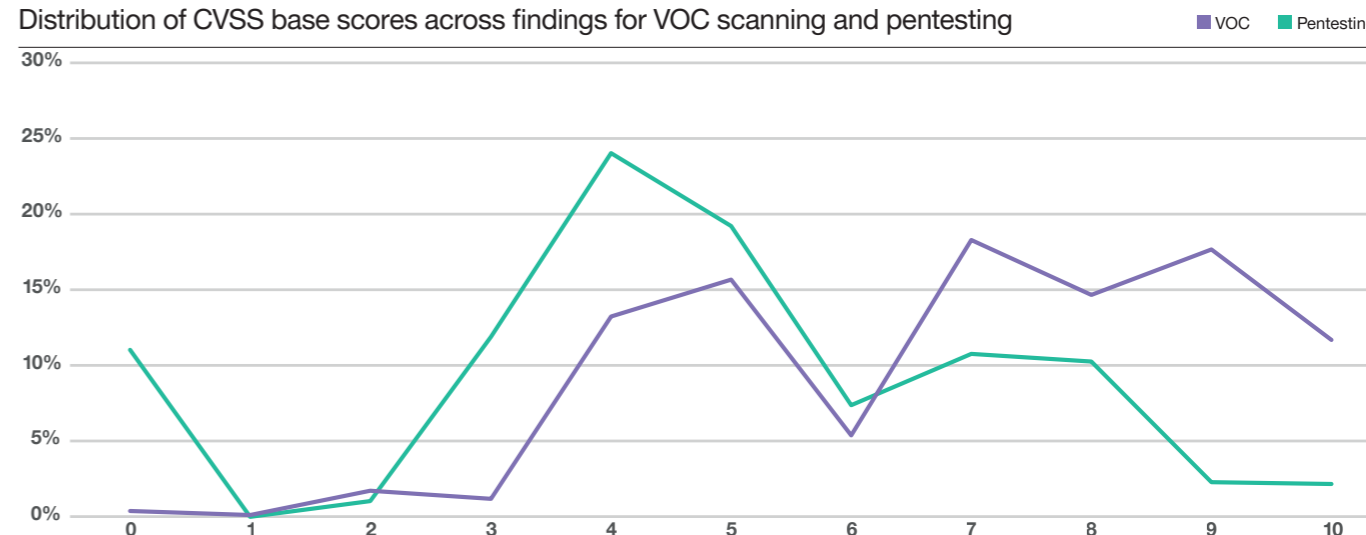
In our VOC scanning services the CVSS score assigned to a finding is generally hard coded into the vulnerabilities database used by the scanner, and therefore assigned automatically to the finding.

In our Penetration Testing services on the other hand, the score is very deliberately decided and assigned by a skilled and experienced analyst. One would expect the CVSS Score assigned to vary depending on the type of target and the starting point of the attacker, and indeed it does.

It is interesting also to consider how the distribution of assigned CVSS scores compares across the two datasets – Vulnerability Scanning and Penetration Testing. We use a rounded CVSS score to simplify this comparison.

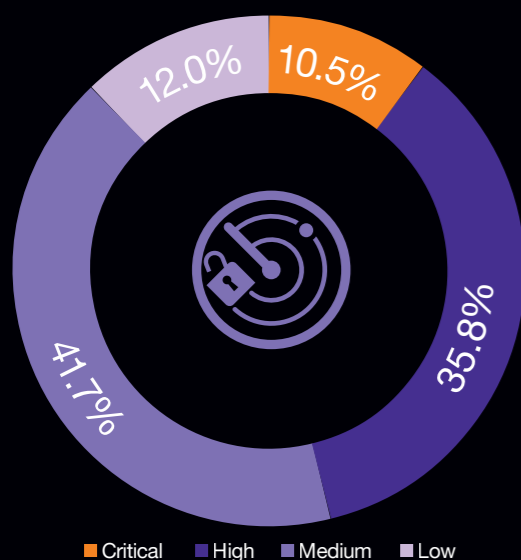
### CVSS Base Scores

Distribution of CVSS base scores across findings for VOC scanning and pentesting



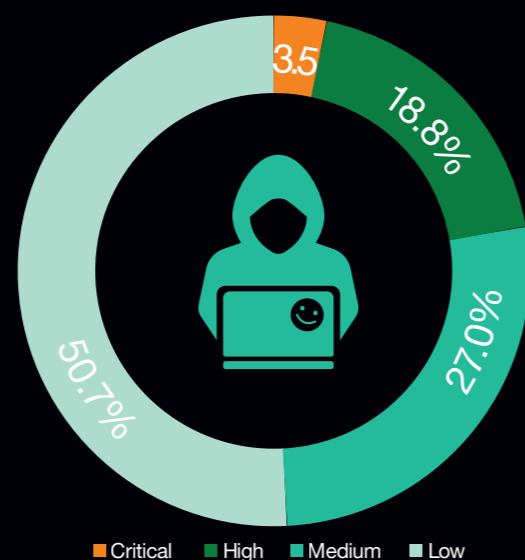
### Severity ratings across unique findings

Severity of VOC scanning and Pentesting findings in comparison (excluding Informational)



#### Severity: VOC scanning

46% of confirmed vulnerabilities reported on client assets would be considered Critical or High Severity



#### Severity: Pentesting

22% of confirmed vulnerabilities reported on client assets would be considered Critical or High Severity

A glance at these two charts reveals that CVSS scores assigned to findings across these two services is largely similar in the middle, but differs considerably at the edges. Somewhat surprisingly, we observe that:

- The most commonly assigned CVSS scores across both services range between 3 and 4 (Low/Medium).
- Almost no findings are assigned a Score below 3. We see more 0-level findings in our Penetration Testing data, but that is probably because these findings are removed from the Scanning data when we exclude the 'Informational' findings.
- As a proportion we observe more High and Critical findings in our Scanning data than in our Penetration Testing data. Almost 12% of Scanning findings are assigned a score of 10, compared to 2.2% of Penetration Test findings.

Intuitively we would have expected to see a greater weighting toward higher CVSS scores in our Penetration Testing service, but on consideration it makes sense that the scope of Penetration Testing is generally more tightly defined, and that analysts are likely to be more judicious in their assignment of scores.

**In short, we consider the Penetration Testing findings to be a better reflection of the vulnerability state of the systems we assess.**

1. In our pentesting the majority of findings have a CVSS score of 4 or 5 (Medium)
2. We almost never report a finding with a low CVSS Score of 2 in any kind of Test
3. In 'Internal' tests, where the tester starts inside the security perimeter, the majority of findings are rated CVSS 8 (High) and we report 42% more findings with a CVSS of 10 (Critical) than with a CVSS of 0 (None)
4. For 'External' tests, where the tester approaches from outside the security perimeter, the number of findings with a CVSS score above 5 drops off steeply. Still, over 20% of findings from this perspective are reported with a CVSS of 7 or more (High and Critical)
5. For 'Mobile Application' tests, 36% of findings have a CVSS of 4 (Medium). Yet over 10% of findings reported still have a CVSS of 7 or above (High and Critical)
6. 'Red Team' tests leave ethical hackers more leeway to pursue a specific target. Almost 30% of findings are assigned a CVSS of 8 (High). Unsurprisingly 18% of Red Team Assessment findings are assigned a high ranking of 9 or 10.

### Age of VOC findings

Vulnerability Scans are performed on a recurring basis, which provides us the opportunity to examine the difference between when a scan was performed on an asset, and when a given finding on that asset was reported. We can call that the finding 'Age'. If the findings first reported are not addressed, they will occur in more scans over time with increasing Age, and so we can track how the Age of reported findings changes over time.

As the chart below clearly illustrates, the majority of real findings in our dataset, across all Severity levels, are between 75 and 225 days old. There is a second 'peak' at around 300 days, which we suspect has more to do with the age of the data in the dataset and can therefore be ignored. Finally, there is a fascinating 'bump' at around 1,000 days, which we believe represents the 'long tail' of findings in the dataset that will simply never be addressed.

75% of the findings in the 1000-days 'bump' are Medium Severity, but 16% are classified as High or Critical Severity.

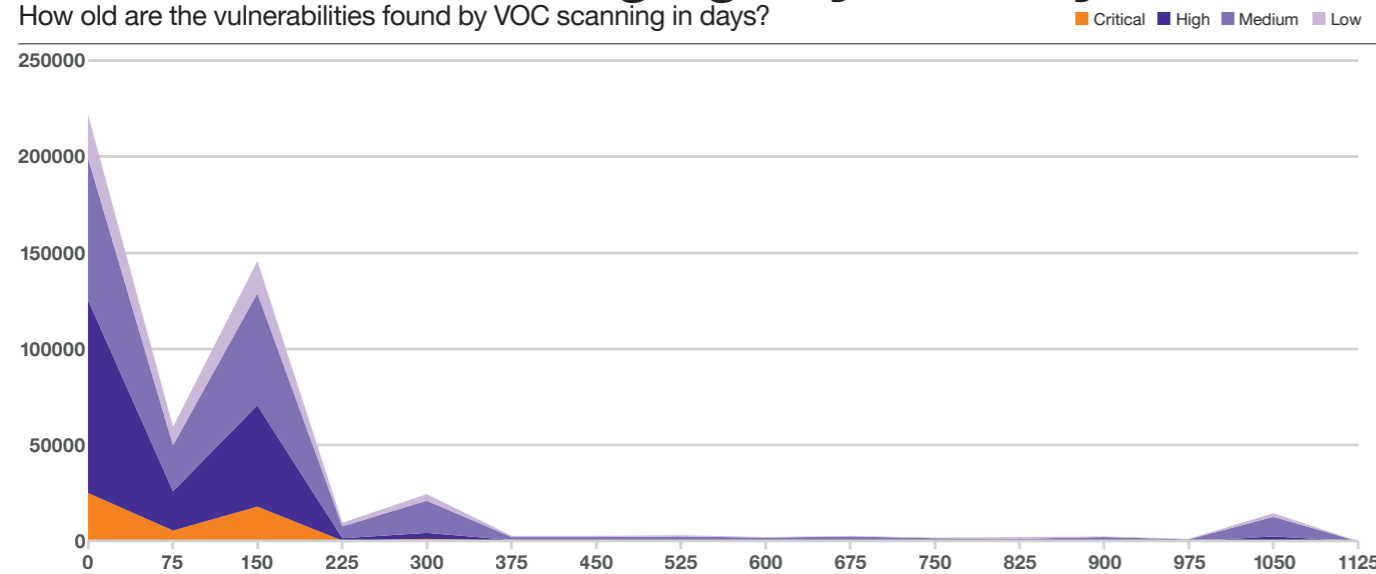
The Average Age of findings in our dataset is impacted as much by changes in our Client and assets set as any external factor, as can be seen in the high degree of variation. Yet, there is a clear increase in the Average Age of findings of 341% from 63 to 215 days over the 24 months since we've been onboarding clients onto this platform.

Roughly grouping confirmed findings from our Vulnerability Scan data by 'Age Group' reveals the following:

- Only 28% of all Findings are addressed in under 30 days
- 72% all Findings take 30 days or more to patch
- 52% of all Findings take 90 days or more to patch.
- The average age of findings is 215 days

### Distribution of finding age by severity

How old are the vulnerabilities found by VOC scanning in days?



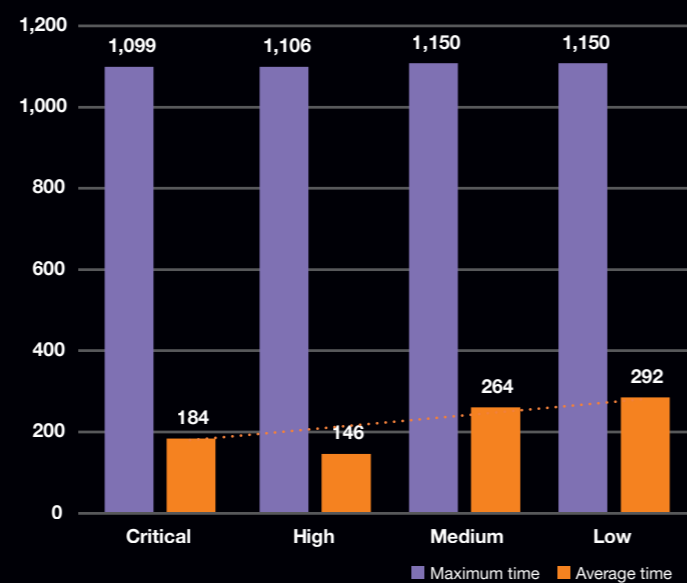
### Average/max age of findings by severity

Taking a closer look at the readings of average vs. maximum time for different ratings of criticality we end up with the chart on the right.

Even Critical Vulnerabilities are taking around 6 months on average to resolve, but that is encouragingly at least 36% faster than the time for low severity issues.

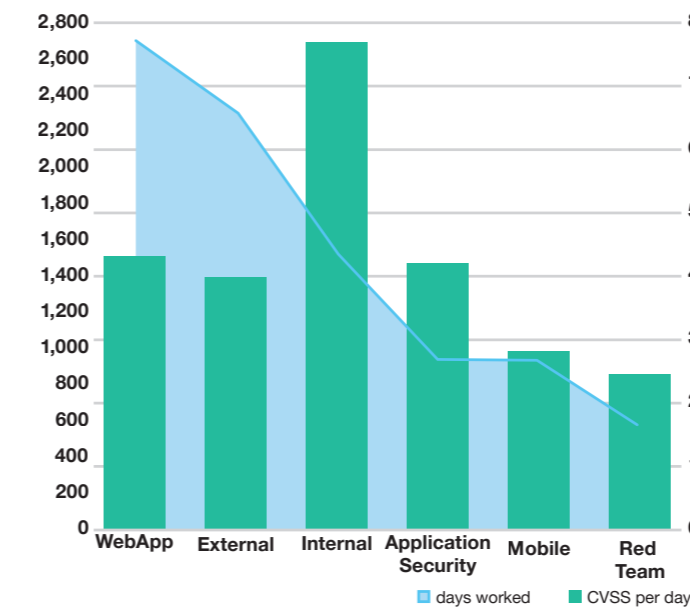
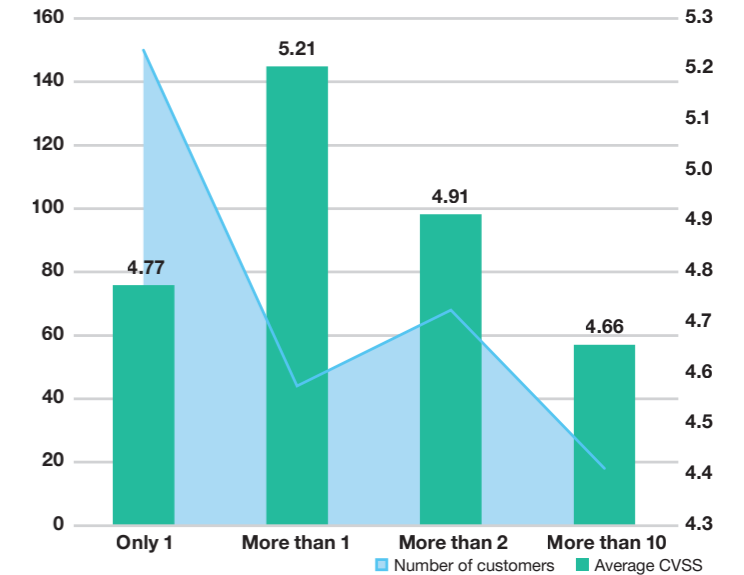
While our conclusion of critical issues being resolved faster stands for the average mitigation time, the maximum time is consistently high regardless of criticality.

We will have to watch this metric more as the dataset grows in the future.



### Score change when multiple assessments are conducted

As Penetration Tests are not repeated in the same way as vulnerability scans, we cannot directly track simple metrics like 'Time to Patch'. As a proxy, however, we can consider the difference in findings between clients who perform frequent tests with us, and those that only perform one test.

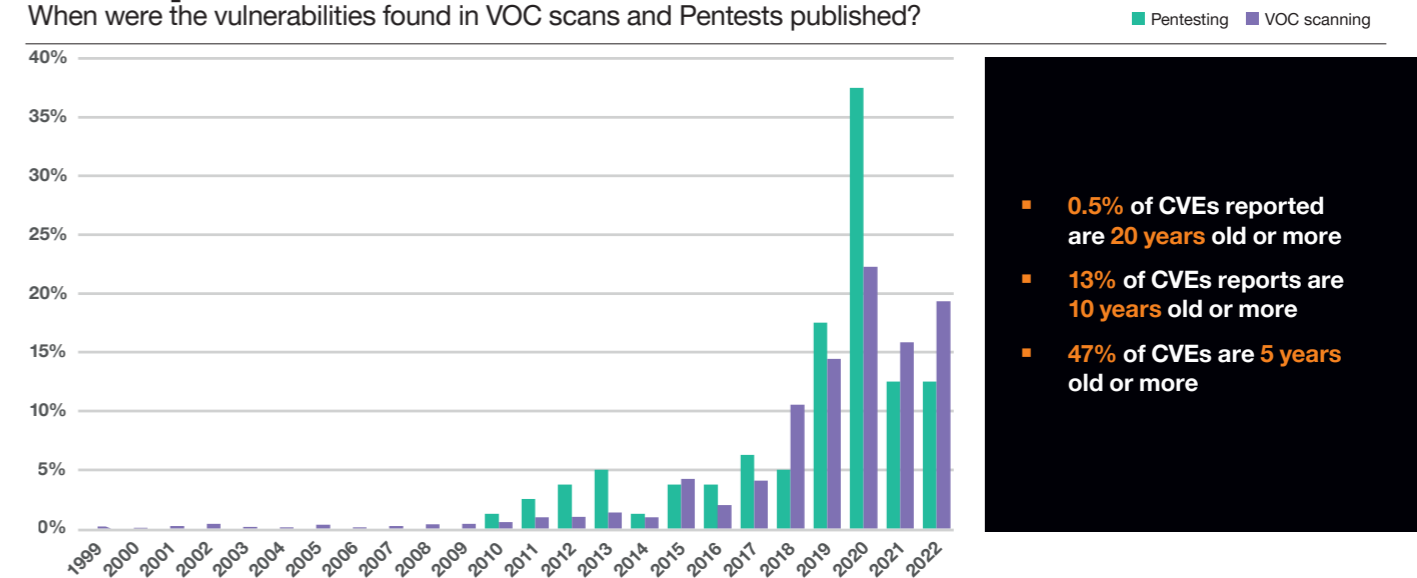


### CVSS by test-type

- Internal Assessments produce the Highest CVSS score per day worked, but an Average CVSS Score per finding below Red Team and ATM (Automated Teller Machine) Assessments.
- ATM (Automated Teller Machine) assessments produce the highest Average CVSS score per finding, but 3rd highest CVSS per Day, behind Internal and Cloud Assessment
- Cloud Assessments produce the 3rd highest CVSS Per Day score, but with an Average CVSS per finding of only 4 (Medium).
- Web Application Assessments and External Assessment produce a similar Average CVSS per finding, but Web Application Assessment produce a slightly higher total CVSS per day of testing.

### CVE published dates

When were the vulnerabilities found in VOC scans and Pentests published?



- 0.5% of CVEs reported are 20 years old or more
- 13% of CVEs reports are 10 years old or more
- 47% of CVEs are 5 years old or more

# Conclusion



**More than 22 vulnerabilities with assigned CVEs are published each day. With an average CVSS score above 7 (High Severity), each of these disclosed vulnerabilities is a significant datapoint that affects our risk equations and our real exposure to threats.**

Vulnerability Scanning and Penetration Testing are mechanisms we use to make sense of the vulnerabilities that may impact our security posture, understand their potential impact, prioritize and take appropriate action. These two assessment exercises are different in approach, but use similar language and serve a similar purpose.

This year we are including an analysis of datasets from both services in the Navigator. This is the first time we are attempting this, and our data is still far from perfect. It will improve as we mature and extend our datasets over time, but in the meantime the data we have is already offering significant insights. Two apparently contradictory perspectives emerge. Together they offer a succinct summary of the state of security as it stands today.

On the one hand, we note that the volume and severity vulnerabilities we report grows faster than the number of assets in our environments. Put simply, the size of the vulnerabilities problem appears to grow faster than the size of our technology estates.

And organizations already struggle to manage the vulnerabilities we know about. On average it is taking our clients 215 days to patch a vulnerability. This is a little lower for Critical Vulnerabilities – it appears these are patched 36% faster than 'Low' severity issues. But the picture is still grim: 72% of all findings take 30 days or more to patch, 57% take 90 days or more.

Our pentesting teams are still discovering vulnerabilities that were first identified in 2010, and our scanning teams encounter issues that date back to 1999! Indeed 47% of CVEs are 5 years old or more. 13% are as old as 10 years or more.

22% of confirmed vulnerabilities reported by our Pentesting Teams would be considered Critical or High Severity. On average over the last 4 years our qualified Ethical Hackers reported a Confirmed Serious (High or Critical finding) for every 7.7 days spent testing. We report these kinds of significant security weaknesses in over 49% of all the tests we perform.

**But there is an apparent silver lining.** We can assess the amount of effort required by our Penetration Testing teams to discover serious issues on their engagements. There are many variables in this assessment, some observation bias as well in terms of the kinds of clients who engage us for these tests, but within that uncertainty there is a hopeful pattern to be seen:

**The proportion of tests with 'Serious' findings by just under 9% from the beginning to the end of our dataset.** For first time clients, from the beginning of 2018 to August 2022, there has been a 55% decrease in the (combined) volume and severity our testers are reporting for each day of work performed.

**For our full dataset of all tests - in 2022 our testers would have to work 8 hours 47 minutes to achieve the same results they would have managed in 8 hours at the start of 2018 – an increase in effort of 10%.**

There are many variables that impact the result we see above, many of which are invisible to us in the data. But it doesn't seem unreasonably optimistic to assert that our testers – arguably among the best in the world – are having to work a little harder to successfully breach their clients.



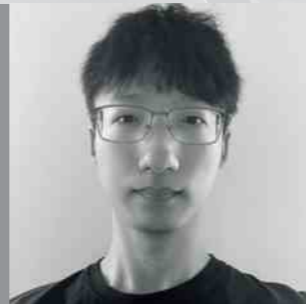


# Honey pot factory

## The use of deception in ICS/OT environments

With the rapid increase of attacks on industrial control systems (ICS) in the past few years, the importance of cybersecurity for operational technology (OT) is consistently growing. Deception is an effective option to improve threat detection and response capabilities. However, ICS security differs from traditional IT security in several ways. While deception technology for defensive use like honeypots has progressed, there are still challenges due to fundamental differences like the protocols used. This article is intended to detail the progress and challenges when deception technology transits from traditional IT security to ICS security.

Thomas Zhang, Security Analyst, [Orange Cyberdefense](#)



### The value of deception: taking back the initiative

Deception technology is an active security defense method that detects malicious activities effectively. On one hand, this strategy constructs an environment of false information and simulations to mislead an adversary's judgment, making unsuspecting attackers fall into a trap to waste their time and energy, increasing the complexity and uncertainty of the intrusion.

At the same time, the defenders can collect more comprehensive attack logs, deploy countermeasures, trace the source of attackers and monitor their attack behaviors. Recording everything to research the tactics, techniques, and procedures (TTP) an attacker uses is of great help for security analysts. Deception techniques can give defenders back the initiative.

With some deception applications, for instance honeypots, the operating environment and configuration can be simulated, thus luring the attacker to penetrate the fake target. By this means, defenders will be able to grab the payloads the attackers drop and get information about the attacker's hosts or even web browser by javascript in web applications. What's more, it is possible to know the attacker's social media accounts by JSONP Hijacking as well as countering the attacker through 'honeyfiles.' It can be predicted that deception technology will be more mature and widely used in the coming years.

Recently, the integration of information technology and industrial production has been accelerating with the rapid development of the Industrial Internet and intelligent manufacturing. The connection of massive industrial networks and equipment to IT technology will inevitably lead to increasing security risks in this field.

### Production at risk

Frequent security incidents such as ransomware, data breaches, and advanced persistent threats seriously affect industrial enterprises' production and business operations and threaten the security of the digital society. Generally, these systems are prone to be weak and exploited easily by the attacker due to their simple architecture, which uses low processing power and memory. It is challenging to protect ICS from malicious activities as the components of ICS are unlikely to take any updates or patches due to their simple architecture. Installing endpoint protection agents is complex – if possible at all. Considering these challenges, deception can be an essential part of the security approach.



**Conpot** is an open-source low-interactive honeypot that supports various industrial protocols, including IEC 60870-5-104, Building Automation and Control Network (BACnet), Modbus, s7comm, and other protocols such as HTTP, SNMP and TFTP. It is designed to be easy to deploy, modify and extend. The Conpot and Conpot-based honeypot are among the most popular ICS deception applications that have been used by researchers.



**XPOT** is a software-based high-interactive PLC honeypot which can run programs. It simulates Siemens S7-300 series PLCs and allows the attacker to compile, interpret and load PLC programs onto XPOT. XPOT supports S7comm and SNMP protocols and is the first high-interactive PLC honeypot. Since it is software-based, it is very scalable and enables large decoy or sensor networks. XPOT can be connected to a simulated industrial process in order to make adversaries' experiences comprehensive.



**CryPLH** is a high-interactive and virtual Smart-Grid ICS honeypot simulating Siemens Simatic S7-300 PLC. It runs on a Linux-based host and uses MiniWeb HTTP servers to simulate HTTP(S), a Python script to simulate Step 7 ISO-TSAP protocol and a custom SNMP implementation. CryPLH's interaction ability is gradually increasing from the simulation of ICS protocols to ICS environments.

With the development of cybersecurity technology, deception has been applied in various circumstances like the web, databases, mobile apps, and IoT. Deception technology has been embodied in some ICS honeypot applications in the OT field. For instance, ICS honeypots like Conpot, XPOT, and CryPLH can simulate the Modbus, S7, IEC-104, DNP3 and other protocols.

Accordingly, deception technology like the honeypot applications above can make up for the low efficiency of detection systems for unknown threats and can play an important role in ensuring the safety of industrial control networks. These applications can help detect cyber attacks on industrial control systems and display a general risk trend. The actual OT vulnerabilities exploited by the attackers can be caught and sent to the security analyst, thus leading to timely patches and intelligence. In addition to this, it is possible to get a prompt alert e.g. before a ransomware breaks out and avoid massive losses and a stop in production.

### Challenges

This is not a 'silver bullet' however. In comparison to the sophisticated deception available in traditional IT security, deception in ICS still faces some challenges.

First and foremost, there are numerous kinds of industrial control devices as well as protocols, and many protocols are proprietary. It is almost impossible to have a deception technology that can be applied to all industrial control devices. Therefore, honeypots and other applications often need to be customized for the emulation of different protocols, which brings a relatively high threshold for implementation in some environments.



The second problem is that pure virtual industrial control honeypots still have limited simulation capabilities, making them susceptible to hacker identification. The current development and application of purely virtual ICS honeypots only allows the underlying simulation of industrial control protocols, and most of them have been open source, easy to be found by search engines such as Shodan or Zoomeye. Collecting adequate attack data and improving ICS honeypots' simulation capabilities is still challenging for security researchers.

Last but not least, high-interaction industrial control honeypots consume considerable resources and have high maintenance costs. Honeypots often require the introduction of physical systems or equipment in order to build a real-run simulation environment. However, industrial control systems and equipment are costly, hard to reuse, and challenging to maintain. Even seemingly similar ICS devices are often remarkably diverse in terms of functionality, protocols and instructions.



### Is it worth it?



Based on the above discussion, deception technology for ICS should be considered for integration with new technology. The ability to simulate and interact with a simulated environment strengthens defense technology. Moreover, the attack log captured by the deception application is of great value. Analyzed through AI or Big data, helps to get an in-depth understanding of ICS field intelligence.

To summarize, deception technology plays a vital role in the rapid development of ICS network security and improves intelligence as well as the ability of defend. However, the technology is still facing challenges and needs a breakthrough.



**Charl van der Walt**  
Head of Security Research  
**Orange Cyberdefense**

## Of Malware and factories Spotlight on Manufacturing

In our 2022 Navigator it was noted that the Manufacturing Industry appeared to be over-represented in our dataset of Cyber Extortion victims, when compared with the general size of that industry.

We posited at the time that this did not suggest a deliberate targeting decision by attackers, but may rather be because of the 'general level of vulnerability of businesses in that sector'.

Manufacturing was also the most represented Industry in our dataset – contributing with more incidents than any other sector in our 2022 dataset.

Manufacturing is once again very prominent in our 2023 dataset. It is still the most impacted industry in our Cyber Extortion dataset, as tracked by monitoring double-extortion leak sites. Indeed, this sector has represented more than 20% of all victims since we started observing the leak sites at the start of 2020.

Let's take a closer look and examine some possible explanations. And debunk them.

## Back to the future

The manufacturing industry is also once again the most represented sector in our CyberSOC incident data, both in the number of clients and consequently in the number of incident volume.

Approximately 28% of all our clients are from Manufacturing, contributing with an overall share of 31% of all potential incidents. We have the highest level of ‘visibility’ (detection in place) for our clients in the Manufacturing sector, followed by ‘Finance and Insurance’ and ‘Professional, Scientific, and Technical Services’.

We note that 58% of incidents this industry deals with are internally caused, while 32% were externally caused, 1% was classified as “Partner” or 3rd parties. When external threat actors had caused the security incident, we observed the top 3 threat actions were Web Attacks, Port Scanning and Phishing.

**Manufacturing ranks 7<sup>th</sup> of all industries when considering the level of findings reported per day by our Ethical Hacking teams.**

These two observations made us curious: What is it about the Manufacturing sector that causes it to stand out in this way?

Several questions present themselves, which we will attempt to examine here:

1. What part does Operation Technology play?
2. Are businesses in Manufacturing more vulnerable?
3. Is the Manufacturing sector being deliberately targeted more?
4. Do our Manufacturing clients experience more incidents?

We aim to use insights from all our datasets to consider these question, including:

- Double Extortion Leak Sites;
- CyberSOC incidents
- Penetration Testing and
- Vulnerability Scanning.

## What part does OT play?

Another tempting assumption to make is that businesses in the Manufacturing sector are compromised more often because they have mission critical plants, systems and processes that rely on notoriously insecure Operational Technology (OT) or Internet of Things (IoT) systems that are attractive to target and easy to compromise. One could argue further that plants and factories can often not afford to be disrupted or shut down and that Manufacturing is therefore a soft target for extortionists.

Yet once again we don’t see these theories supported in our data.

There are of course several examples of industrial processes being hobbled by cyber-attacks:

- October 26, 2021: Attack on National Iranian Oil Products Distribution Company (NIOPDC)
- January 29, 2022: Attack against Oiltanking Deutschland and German mineral oil trade company Mabanaf
- June 27, 2022: Three Iranian Steel factories sabotaged by cyber attack

The attack against US Energy giant Colonial Pipeline was probably the most notable recent example of a successful attack against an industrial facility.

In July this year US intelligence agencies even warned of a hacking toolset dubbed ‘Pipedream’ that is designed target specific Industrial Control Systems. But it is not clear to us if or when these tools have ever been encountered in the wild. Indeed, apart from the infamous Stuxnet attack from 2010, one struggles to recall a single cyber security incident that involved the specific compromise an OT system.

The attack against Colonial Pipeline involved the compromised backend administrative systems and not Operational Technology, and this is still the case for most reported incidents at industrial facilities.

Furthermore, according to the logic of perspective we discussed above, if businesses in the Manufacturing sector were so much more willing to pay the ransom that they are considered a ‘soft target’, then one might expect to see such business featuring on the ‘name and shame’ leak site less often, not more.

Once again much of the truth is not fully revealed in the data, but we see no reason to believe that Manufacturing businesses are being targeted or compromised more because they use insecure Operational Technology.

Operational Technology is of course surrounded by traditional IT systems, like ERP and Programming Workstations that run well know applications and Operating Systems and could very easily be caught up in even the least sophisticated ransomware attack. To examine this possibility we consider the next question:

## Are businesses in the Manufacturing sector more vulnerable to attack?

To examine this question we reach again for two datasets already referenced elsewhere in this report – a set of 3 million vulnerability scan findings, and a sample of 1,400 Ethical Hacking reports.

Refer to the relevant sections this report for a detailed analysis of these datasets.

As detailed in those sections of our report, those datasets allow us to derive three metrics that facilitate somewhat normalized comparisons across the industries in our client base:

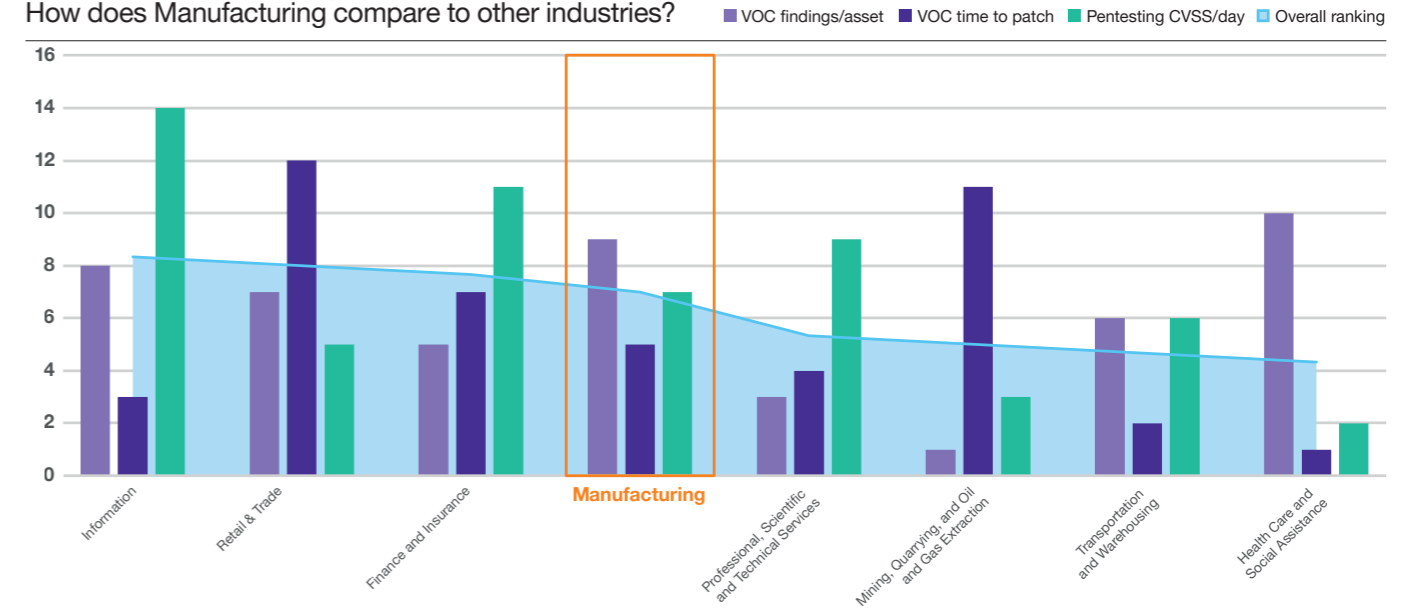
**Vulnerability SOC (VOC) scanning findings per asset, time to patch, Pentest findings per day of testing.**

If we rank Industries for their performance on each of those metrics and sort from worst to best, then our clients in the Manufacturing sector arrives in 5th place out of 12 comparable industries.

The chart on the right shows the overall “ranking” of our Manufacturing clients out of comparable industries.

## Comparing key metrics

How does Manufacturing compare to other industries?



### Let's take a closer look at how Manufacturing performs in comparison to other verticals.

In the table we consider the number of findings per asset for the different industries represented in our dataset across different business sizes. For this comparison we rank industries from 'weakest' to 'strongest', from 1 to 15. In other words, the ranked 1 would be considered the least 'secure', while the industry ranked 15 would be considered the most 'secure'.

Metric	Manufacturing	Average	Ranking (out of 15)
VOC unique findings/asset	1.7	16.2	9
Time to patch (average)	232 days	215	5
Days to patch (critical)	435 days	178	2
Days to patch (high)	211 days	136	3
Days to patch (medium)	150 days	262	9
Pentesting CVSS per day	4.81	3.61	7

### VOC unique findings/asset

On this metric there were three other industries that performed better than Manufacturing.

While we have a comparatively high number of assets from Manufacturing clients in our scanning dataset, we report far fewer findings per asset than the average across all industries. Almost 10 times fewer, in fact.

### Time to patch

On this metric seven other industries ranked better than Manufacturing. The average age of all findings for this industry is 419 days, which is a concerning number and worse than recorded for eight other industries in this dataset.

### Pentesting findings

Our pentesters spent about twice as much time testing in other industries (on average) than in Manufacturing. Still, our dataset represents a total of 235 days of testing for clients in the Manufacturing sector.

CVSS<sup>[44]</sup> is a global standard for reporting the severity of a vulnerability. To perform normalized comparisons across different segments of our dataset, we use the metric ‘CVSS Per Day’, for which we simply add up the CVSS score assigned to findings and divide that total by the number of days spent on that test.

Using this metric, we observe that the average CVSS Per Day for all the tests we conducted for the Manufacturing sector was 4.81, compared to 3.61 on average for clients in all other sectors in the dataset – 33% higher.

Overall, we rank the Manufacturing sector as seventh or eighth weakest of all industries from a vulnerability point of view.

**These rankings are not a perfect metric, and we don't have the data to make general assertions about security for an entire industry, but there certainly does not appear to be anything in this data to explain why we observe so many more incidents for this sector.**



### Is the Manufacturing sector being targeted more by extortionists?

We use the North American Industry Classification System – NAICS - classification system when categorizing our clients, and the victims in our Cyber Extortion dataset.

This grouping system is very broad and includes multiple sub-categories, which are not able to track in our data. We should note therefore that ‘Manufacturing’ does not only mean businesses that run factories, but rather any businesses broadly associated with the manufacturing ecosystem.

A consideration of double-extortion victim counts per industry reveals a very interesting pattern: Of the 10 industries with the most recorded victims in the dataset, 7 are also counted amongst the biggest industries by entity count.

The chart below lists the number of victims we observed when monitoring a set of leak sites during the period of October 2021-September 2022.

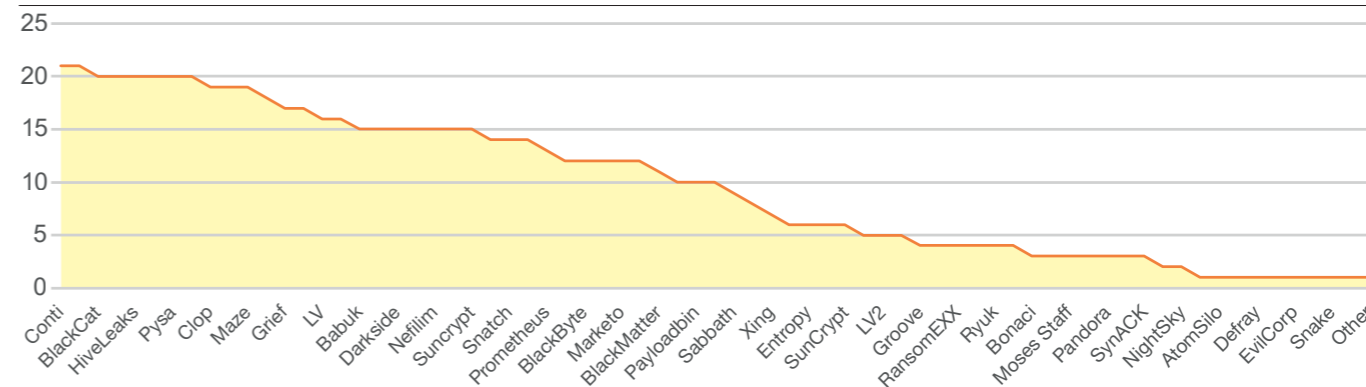
### Cy-X data: a question of perspective

We should note carefully, however, that the data we analyze here to draw our conclusions about Cyber Extortion is derived from observing and documenting double-extortion leak sites. These represent the very last stage of a ransom incident, where the environment has already been compromised, the data stolen and encrypted, and ransom demand sent. We must assume that many victims pay quickly upon receiving the demand, and therefore never appear on the leak site. We also know that many actors don’t use such observable sites at all.

It may thus be that the patterns and trends we see from the leak sites are good proxy for the patterns and trends of the attacks themselves. But it could also be that the shape of victims who end up on the leak sites are influenced by other factors entirely. For example, while our immediate impulse may be to deduce from the numbers that Manufacturing is attacked often, the real explanation for the numbers may be that Manufacturing is attacked no more often than any other sector, but pays less readily, and therefore appears on the leak sites more frequently.

## Victim Industry counts

Cy-X leak threat victimology: number of industries targeted by actors



As a general rule, therefore, we posit that the number of victims in a given industry is merely a function of the number of businesses in that sector.

The victim’s industry is generally not a strong predictor of suitability as a victim of Cyber Extortion. Rather, more victims are simply recorded in industries with more entities and therefore more potential victims.

But 3 industries that are counted among the ten biggest in terms of business size, but not counted among the top 10 in terms of the victim count are:

- Other Services (except Public Administration): 2nd biggest industry, 14th victim ranking
- Real Estate and Rental and Leasing: 7th biggest industry, 13th victim ranking
- Accommodation and Food Services: 8th biggest industry, 15th victim ranking

This observation leads us to deduce that Manufacturing as an industry is indeed being targeted more than other industries.

Yet we see very little evidence that threat actors are systematically singling out specific industries for targeting. The chart above, by way of example, visualizes the number of different industries in the victim lists of major Cyber Extortion actors we’ve been tracking. As the chart clearly illustrates, most threat actors have several different industries in their victim lists, and only 5 criminal groups have less than three. Moreover, if we consider the spread of actors that have reported victims from Manufacturing, we note an almost identical distribution to what we see in the dataset overall.

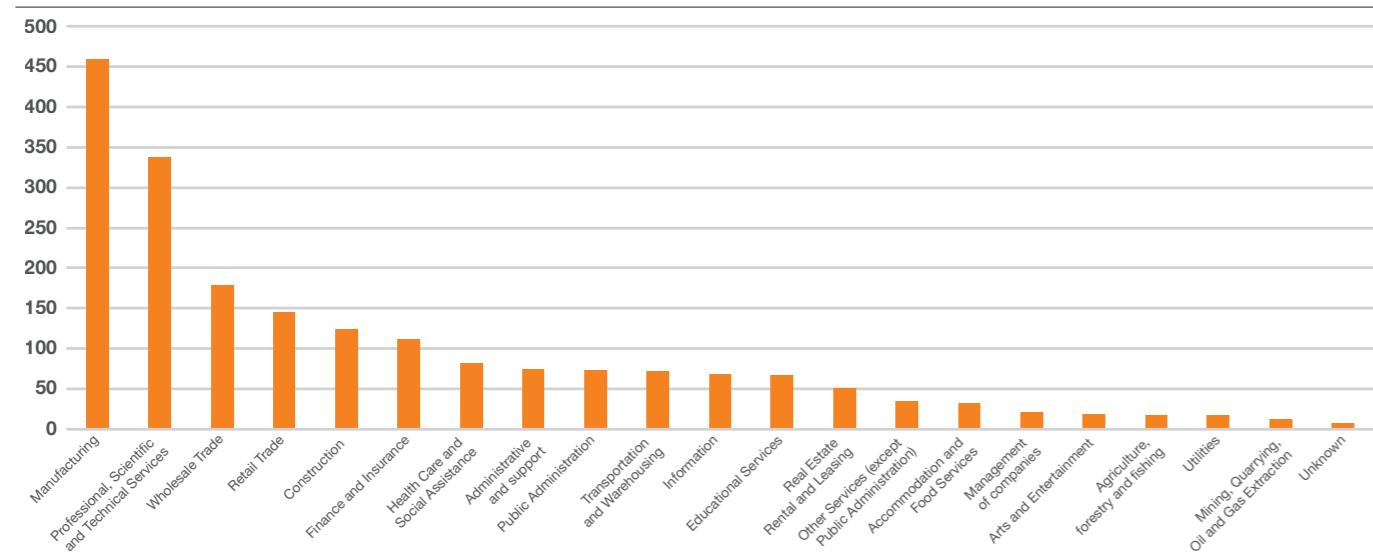
Another theory might be that victims in the Manufacturing industry are considered more willing to pay the ransom. But we see no evidence to support that in our data either. As the chart below illustrates, we see the most victims in Manufacturing, but victims from this industry who get listed on leak sites seem only the 5th most willing to pay.

Our dataset offers a limited perspective here, however. A lot happens ‘behind the scenes’ and is invisible to us.

**The Manufacturing industry is another exception to our general rule. The sector ranks 12th in terms of the number of business entities included, but 1st by a significant margin in terms of the number of Cy-X victims we recorded.**

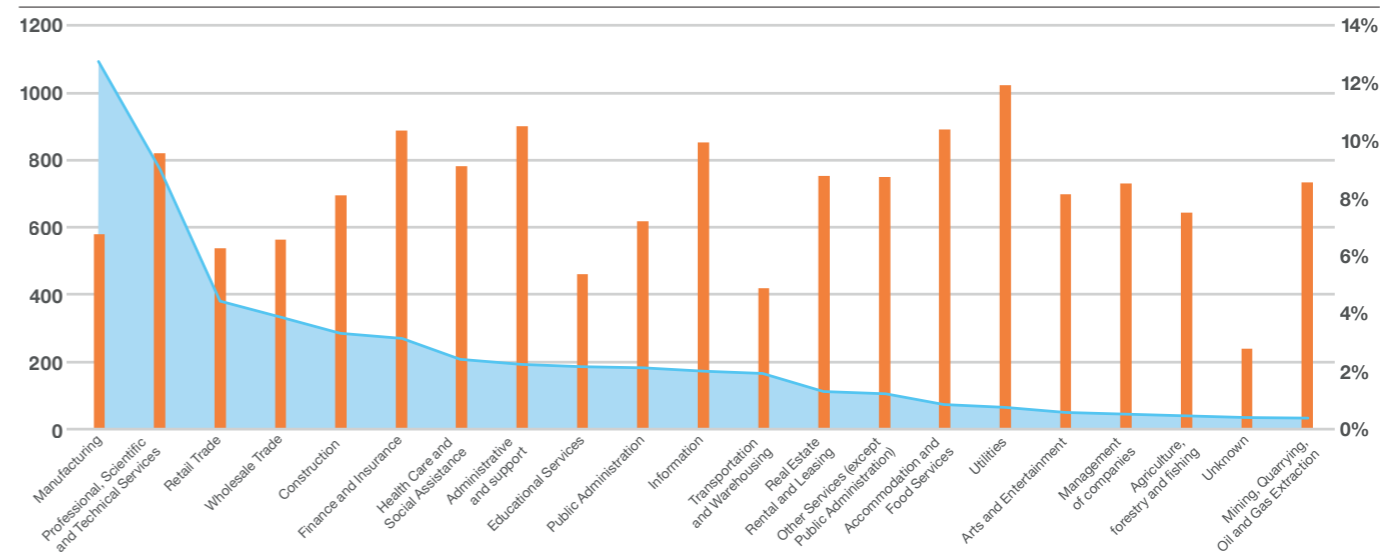
## Cyber Extortion by Industry 2022

Cy-X leak threat victimology by number of threats



## Willingness to pay ransom

Victim Count and apparent willingness to pay ransom by industry



## Do our Manufacturing clients experience more incidents?

As we've noted elsewhere, the Manufacturing industry once again generates the highest number of incidents as a percentage of the total in our CyberSOC dataset. 31% of all incidents are generated for the 28% of our clients that are from this sector.

Seen in conjunction with the high number of Cyber Extortion victims from the Manufacturing sector, this high proportion of CyberSOC incidents seems telling. The incident data lacks context, however. Without a baseline to represent the number and size of these clients and some measure of how much of their estates we are monitoring, it's very difficult to draw any conclusion from them.

To establish a baseline by which clients and industries can be compared, we assign clients a 'Coverage Score' between 0 and 5 in 8 different 'domains' of Threat Detection, account for a maximum total detection score of 40.

We perform a simple modification on the incident volumes to factor in the relative level of coverage: Divide the incident count by the assessed coverage score and multiply it by the maximum possible score. Put simply, the lower a client's assessed coverage score is, the more this adjustment will 'boost' the number of incidents in this comparison. For a client with the maximum possible level of coverage, we will simply reflect the actual number of incidents we observed.

Using this simple calculation we can now consider how businesses and industries compare with their relative levels of coverage taken into account.

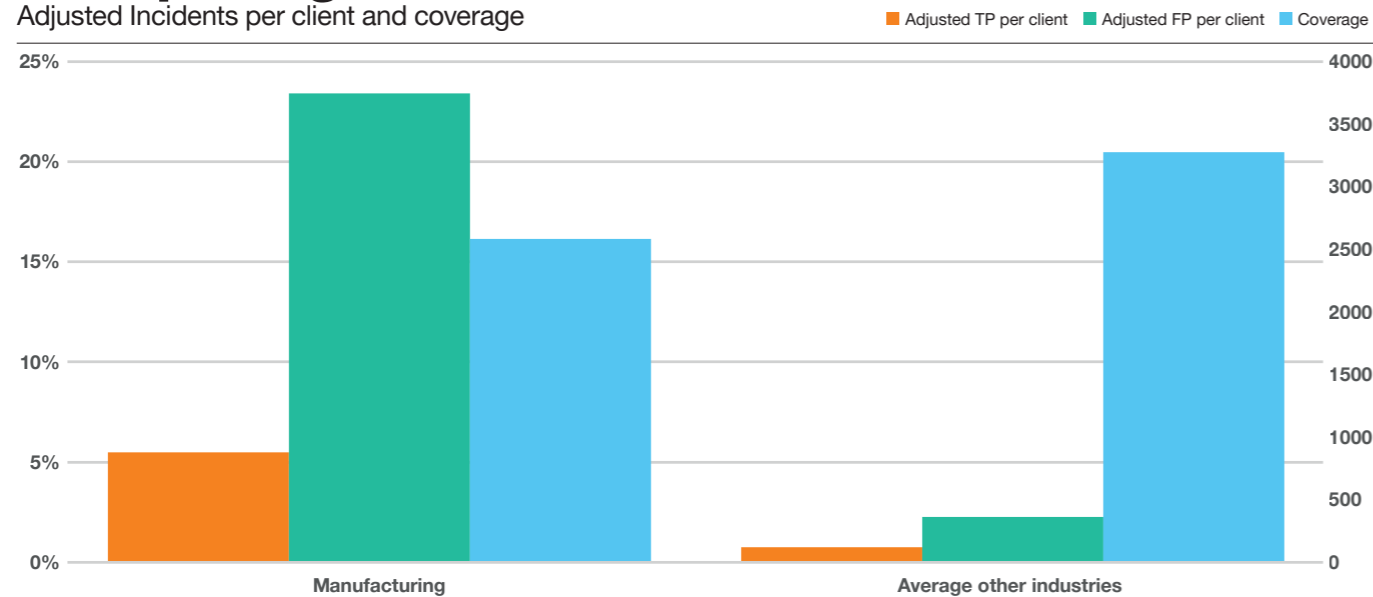
Manufacturing ranks 3rd out of 10 industries on this metric.

As the chart below illustrates, we estimate that we have about 16% of the 'visibility' we'd like to have across our clients in Manufacturing, compared with 20% across clients in all other Industries. If we adjust the True Positive and False Positive incidents as described above, we still see more than seven times as many incidents per client from Manufacturing than the average for all industries.

In a similar comparison, limited only to Perimeter Security Coverage, and only Medium Sized business, Manufacturing ranks 1st with the most incidents per Client out of seven comparable Industries.

## Comparing incident count

Adjusted Incidents per client and coverage



# Conclusion



There's a formal theory of crime (Routine Activity Theory) that describes a 'Suitable Victim', alongside a 'Motivated Offender' and the lack of 'Capable Guardians' as the three elements that usually converge in time and space for a crime to occur. Discussions of RAT<sup>[45]</sup> suggest that there are simple routine choices that can make a potential victim less vulnerable<sup>[46]</sup>. Improving routine practices to reduce technology vulnerability should thus render a potential victim less likely to be affected by this crime.

**Basic security hygiene practices** like risk assessment, patching and secure configuration. We ruled out a massive impact of OT security vulnerabilities, and therefore focus on patching of regular IT systems. We note that our scanning teams assess a large number of targets but report relatively few vulnerabilities per asset for the regular IT used by this industry. Eight other industries performed worse than Manufacturing in our assessment. But we also note that the average age of all findings for this industry is 232 days, which places Manufacturing 5th worst of all industries in this dataset. From the perspective of our Penetration Testing Teams, only 6 out of 15 Industries ranked worse than Manufacturing. Overall, we rank the Manufacturing sector as 5th or 6th weakest of all industries from a vulnerability point of view.

Researchers also suggest there are four further variables that would make a victim more 'suitable', namely: Value, Inertia, Visibility, and Access (VIVA)<sup>[47]</sup>. We summarize our considerations regarding the Manufacturing Industry through the lens of these variables.

**'Value'** refers to the potential financial gain or increase in status an offender might attain from undertaking the criminal activity. In the case of Cyber Extortion, what's stolen is something that is of value to the victim; not the criminal. It might be the case that Manufacturing businesses have more to lose than other industries, which makes them more vulnerable to extortion. As we noted, however, we did not observe businesses in this industry being more likely to pay than others, which seems to suggest this is not the case.

**'Inertia'** refers to the relative difficulty of moving or transporting a stolen object or asset. In the digital space 'inertia' would describe controls like encryption, DRM or traps that make it more expensive or riskier for an attacker to exploit a stolen asset. We have no reason to believe that this would be different for Manufacturing, so we rule this out from our comparison.

**'Visibility'** affects suitability in that items left in clear view are more likely to be stolen. In digital we argue that 'visibility' would translate to internet attack surface, including exposed IP addresses, web applications and email addresses. We have 13 'external' or internet tests for Manufacturing in our Penetration Testing dataset. Measured on 'CVSS per Day', Manufacturing ranks 6th worst out of 14 Industries. We thus have no reason to believe that our Manufacturing clients are dramatically more 'visible' than clients in other industries.

**'Access'** considers whether a victim or place can be easily accessed by an Offender. In the digital space we think of 'Access' as being about detection and response. And indeed our CyberSOC data does suggest that our Manufacturing clients are experiencing a high volume of incidents relative to the level of coverage they have – ranking 3rd after the 'Retail' and 'Public Administration' sectors. But this high volume of CyberSOC incidents could also be read to suggest that our Manufacturing clients are detecting and disrupting more attacks, thus limiting 'access' for would-be attackers.

The question of why we consistently record such a high proportion of victims from the Manufacturing industry is not readily answered with the data we have. We believe that in the end it comes down to high levels of vulnerability, best reflected in our Penetration Testing, and findings Age data. Our theory is that attackers are mostly opportunistic. Rather than singling industries out, they compromise businesses that are vulnerable. The clients represented in our datasets have engaged with us for Vulnerability Assessment or Managed Detection, and therefore represent the most 'mature' in that industry. We can deduce therefore that on average businesses in this sector would benchmark worse in terms of vulnerabilities. Whether the high number of victims we observe on attacker leaks sites is a direct reflection of the high number of overall victims in this sector, or the skewed reflection of an industry that refuses to concede to initial ransom demands, is not yet clear. What does appear likely, however, is that vulnerability is the primary factor that determines which businesses get compromised and extorted.



**Robinson Delaugerre**  
CSIRT Investigations Manager  
Orange Cyberdefense

## Pentesting and CSIRT stories

# Network on fire

### What to do when cyber is in flames

The year 2022 was synonymous with an inferno for the entire globe. A constant battle against stubborn flames, sparing no one, not even an increasingly combustible computer world.

When your house burns you call the fire fighters. In IT however, not all fires are visible. So what to do when it's not your server room that is on fire, but the files stored on those servers?

In IT you need to spot the early signs of fire in a different way. The spark of ignition is more treacherous and secluded than ever before. As Pierre Corneille suggests, "The fire that seems to be out, often sleeps under the ashes". The objective of an incident response team is to be prepared to thoroughly extinguish a fire down to the slightest ember, through rigorous training and experience, combining confidence building and efficiency improvement.

Even the best preparation does not mean that you will always avoid the flashover. Attackers are witty. A few left-over vulnerabilities, like traces of virtual gasoline left in your network, will be sufficient. As the fire spreads, it's invaluable to have CSIRT experts by your side for fire-fighting. They will help to extinguish the flames before your network burns to the ground.

The following stories are true, and relate the experience gained by our Pentesting and CSIRT teams, both in the preparation and anticipation of the fire, and in its suppression.

## CSIRT story: Of bulldozers and Ninjas

It all seemed straightforward: the client got in touch one Thursday to say that a relatively small part of their network had been attacked by ransomware and had been completely encrypted. The client had already done some basic cyber hygiene and had segmented their network, so only 40-50 servers had been affected. But taking a closer look, there was something much more sinister going on.

Thomas Eeles, CSIRT Manager, **Orange Cyberdefense**



### 1 A bit of weekend work

Our initial response was to do what we always do: dive in and look at the problem. It soon became apparent that we were dealing with pretty 'noisy' attackers.

They weren't attempting to hide what they were doing, and there wasn't anything sophisticated about their actions. In fact, they were using off-the-shelf tools. After a review of the situation, we thought we'd have it all sorted by Sunday.



### 2 Just about to wrap things up when...

The cleanup was going well, and we soon had everything back under control. We were just a couple of hours from closing the case when we noticed something odd. It looked like a piece of software an IT team would use, except it didn't tally with what the client managed on a daily basis. We investigated further and realized that the client had been attacked twice: the 'noisy' attackers and an unrelated and much more sophisticated outfit.



### 4 From hunter to prey in one e-mail? Not with us!

While they may have been taking their time, clearly, these attackers were watching the client. They emailed about a week into our investigation to say they knew we had found them. The note also said they'd stolen several terabytes of data, and the client needed to pay up, or the load would be dumped onto the Dark Web.



### 3 Low and slow

How had no one noticed the other intrusion? Because they had been much more methodical. While the first team got in and started causing havoc immediately, the second wave of attackers had been on the network for about twelve months, dipping in and out. It was low, slow, and technical compared to the group we had initially dealt with. They were biding their time, collecting more and more data from the network, using existing software (such as PowerShell) to blend in. This was why none of the client's endpoint detection and response (EDR) or automated detection and response (ADR) tools picked anything up.



### 5 A complete lockdown

To prevent the release of what was critical company information and save the client from having to pay the ransom, we had to lock everything down. The client's logs didn't go back far enough for us to understand the extent of the attack, so we had to assume that absolutely everything was compromised.



### 6 Sicilian Defense

We deployed our preferred state of the art EDR solution across 3,500 endpoints, started monitoring all IP addresses, implemented multi-factor authentication, and effectively locked down the network until we knew we had kicked the attackers out.

It took three weeks to clear everything out, restore the data and resecure the client's network; slightly more than the four days we initially expected.

## Lessons learned:

These two attacks were significant disruptions to the client's operations. While they were unrelated, it was only because of the first noisy attackers that we were even looking at the network. Due to the technical sophistication of the second attack and how much of the activity looked commonplace, most scanning tools would miss it.

It's an excellent example of where companies can have some basics in place - like EDR and network segmentation - but can still miss things.

That would be our one big takeaway: any organization should ensure they have all the basics sorted, no matter how insignificant they think they are. That way, they will be protected from 90% of the attacks that will come their way (the dumb, brute force, paid-for access), and so they'll know that any untoward activity will need more investigation.



## CSIRT story: "Went phishing with Sharepoint (P.S. click this!)"

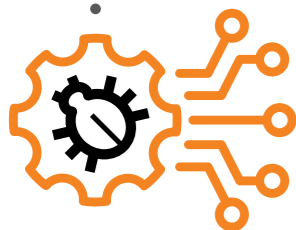
As cyber education levels improve, we'd hope to see a reduction in the number of successful social engineering and phishing attacks. But as often happens in cyber security, a new threat emerges as soon as businesses have come up with a solution. And with it comes fresh, almost existential questions we all must answer. Namely, who can you trust if you can't trust your colleagues?

John Askew, CSIRT Analyst, Orange Cyberdefense



### 1 A standard attack

Business email compromise is one of the most common attacks we help our clients deal with. It's not hard to see why. Everyone has an email account, which links to the outside world for even the most insular and walled-off teams. Most of the time, bad actors get in by brute-forcing the account password or sending a phishing email with a fake login to see a document.



### 2 Once they're in, they're in

The attacks we help deal with tend to follow a similar pattern. Once attackers have login details, they'll look around and see what's going on: how the individual in question works, what sort of contact they have with other departments, and what their access levels are like.



### 3 Using little phish to catch big phish

If the account in question isn't that interesting, the attackers will try to pivot to something like a decision-maker or a finance team. Someone that handles invoices would be a good target. Making that jump, however, requires a bit of work because people with more responsibility often have more advanced security measures. This is where we're seeing attackers taking an internal phishing trip.



### 4 Reeling them in

The attacker will send a phishing email to the preferred target via the account they've already accessed. They upload a phishing document to an internal file sharing site such as One Drive or Sharepoint, which automatically generates a message containing a link to the file that's shared with the target. As the attacker's phishing document isn't attached to the email, the technique can circumvent traditional phishing detection, looking legitimate to the new target as it comes from a Microsoft account. Once that file has been shared, the attacker has the chance to capture the relevant login details.



### 5 Playing in a new pond

Now that our attackers are in an account with more opportunities, they'll start to see what they can exploit. They might look for overdue payments or reissue invoices with new bank details. We've encountered instances where attackers have used the new account to take over conversations and slowly remove participants until only the primary target remains, with no one knowing something bad is happening. Plus, by setting up inbox rules, the account owner doesn't see these exchanges. They'll remain in place so long as their invoices are being paid, often suspicion isn't even raised until complaints about unpaid invoices are raised by third parties.

## Lessons learned:

How do you combat this sort of attack? We always look at getting the basics right. It doesn't matter how tight our client's corporate security is. One person that doesn't have a decent password or multi-factor authentication (MFA) and doesn't interrogate strange or unexpected messages with attachments is a threat. They're gifting attackers an opening they can exploit.

When we're brought in to investigate these attacks, we make sure that passwords have been reset and MFA is implemented across all users. We then look at policies, processes, and levels of understanding across the organization. Without the right tools and culture, these attacks will keep happening.

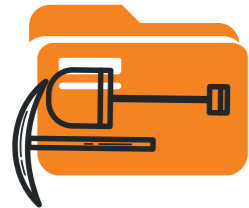




## Pentesting story: Chaining Internal Server Errors into account takeover

In most cases, error pages don't say much when looking at them with human eyes. Error 404: "looks like this page is lost in eternity". Error 403, "You shall not pass". Error 500, "Oops, looks like you broke something". We all encountered them before. But what if that 500 page is more than just "breaking something" and suddenly becomes an entry point for stealing your account?

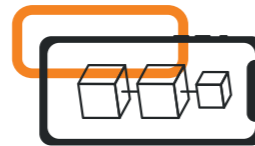
Bram Ruttens, Ethical Hacker, Orange Cyberdefense



### 1 Discovering the session

By digging deeper into the source code of a random page in the client's web application, a debug JavaScript function could be found that was disclosing the user account's session cookie, as a regular string. A dream scenario for every hacker! Let's just steal it with a simple regex & cross-site scripting, right?

Unfortunately, it wasn't as simple as that.



### 4 Bypassing CSP via Google Analytics

Another problem appeared, Content Security Policy. Good for them, their policy was strong and didn't allow exfiltration via XSS, directly. Being a hacker teaches you quickly enough that getting access "directly" often only works when movie hackers try to hack the Pentagon. Therefore, we chose the "indirect" way.

Their CSP did allow Google Analytics, since they tracked their users via a tracking pixel. Well, we did exactly the same. We set up our own pixel that leaked the session string via a specific parameter that allows to send arbitrary data.



### 3 Bypassing Cloudflare's WAF signatures

Okay, we have XSS, but we also have a WAF. Lucky for us, Twitter's infosec community is friendly enough to provide us with a 2-year old bypass for Cloudflare's XSS filtering.

We adapted it, and it worked. First problem solved!



### 5 Some JavaScript Magic

Since everything was in place, the only thing we had to do was craft our final payload, containing the Cloudflare bypass and the CSP bypass and the user's session token. Thanks to JavaScript, the mighty full-stack language, we quickly came up with a neatly packed solution that we could send to a victim as a simple URL.



### 6 Thanks for all the cookies!

We simulated the attack by creating a new account and an incognito browser.

The malicious URL was pasted in the browser, and TING TING! Google Analytics' Dashboard alerted us that a very kind user sent us their session token via an unknown tracking pixel.



### 2 Cross-site scripting as exfiltrator

We discovered that when the application can't handle specific user input, it returned an error page with status code 500. That specific page that was presented had an interesting URL parameter that allowed untrusted user input.

You guessed it, XSS!

## Lessons learned:

Protecting a custom web application can be tough, but with the right methodology and mindset, the vast majority of currently known bugs can be prevented.

Also as an end-user, using a web application can be challenging. Trackers constantly trying to follow your browsing behavior, your digital footprint, etc.

Some important points to keep in mind for both developers and end-users:

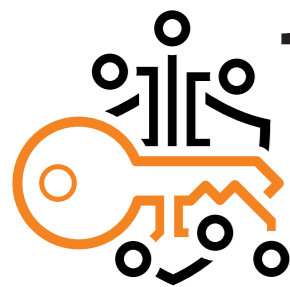
- Make SDLC and awareness part of your development procedure
- Never store session cookies at insecure places
- Never trust user input
- Don't take 3rd-party security solutions for granted



## Pentesting story: Open, sesame!

Initial analysis of the client makes it clear their physical security is managed by a large international vendor. The vendor claims the network of the client is “air-gapped” and no communication is possible to the outside world. The Dutch ethical hacking team is asked to assess the physical security environment of the vendor on-site. Carte blanche ‘please open the gate(s) for me’.

**Thijs Vos**, Security Specialist, **Orange Cyberdefense**  
**Bart van Bodegom**, Security Specialist, **Orange Cyberdefense**



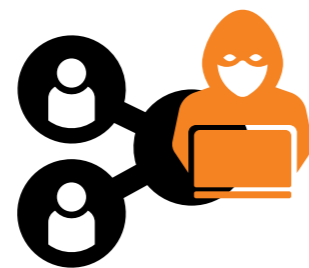
### 1 Physical security: check...

The client's premises are closed off with fences and gates which can be opened via the control room with the right permissions. Permissions are assigned based on the role each of the vendor's employees has. For example, front-office security employees can make badges with a certain number of privileges on them. If access is needed to more secure parts of the terrain, a supervisor must approve this.



### 2 ...but: be my guest!

During the assessment, we found a way into the guest area in the building. Due to unaware personnel and monitoring we were able to find a network patch in the security network. The network doesn't provide an IP-address via DHCP, so we chose a random IP in the range and assigned it to our devices.



### 3 If it happens in our network it's OK I guess...

So, no Network Access Control (NAC) was in place and after the initial foothold in the network we found there was little to no segmentation. It was practically a “flat network”. Security personnel was only capable to interact with the ‘control room’ software from specific client workstations. These workstations were patched and up to date. But the lack of NLA on RDP for some servers gave us insight in some usernames which we could use to successfully test some weak passwords.



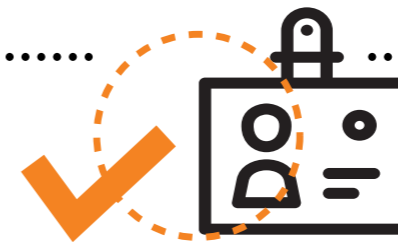
### 4 Access granted (by ourselves)

Due to the lack of awareness about digital security, operators were given local administrator rights for the workstations. With these rights we could enable RDP remotely so we could interactively logon to the client workstations with the ‘control room’ software.

We could now control the rights our physical cards had.

### 5 Your home is my castle!

Wouldn't it be cool if we didn't need these rights but could just control door access through the ‘main panel’ digitally? So, we managed to take over some accounts and eventually got ‘Domain Admin’ rights. From now on it was just a matter of time. A couple of hours later we managed to locate the system with the main controller software. This system was used by the supervisor and gave us the control over every gate and door of the building without them knowing we did.



### 6 Let us open the door for you....

We asked the supervisor to go to a door and didn't say anything till he got there. The card reader showed a red light when he tried to use his card.

The supervisor contacted us, he was standing in front of the door and we remotely opened it.

## Lessons learned:

The lessons learned from this assessment are very clear: you can have as good physical security as you want, but when an outsider or even an insider threat gets access to a network patch, the network is quite open. Some key takeaways:

- Correctly implemented Network Access Control could have prevented this breach.
- Segmentation and filtering between the segments would have helped to create some barriers when trying to access systems involved with physical security.
- Host-based firewalling and hardening of systems should be best practices.
- Personnel can be a weakness or a strength in terms of security. Awareness is key to make it the latter.
- Monitoring, at least of the most critical systems, is a requirement.



# Securing the Web 3.0

## A security review of the Blockchain

orange™

According to many experts, "Web 3" could be the future of the Internet and of access to information. After a "Web 1" made of static web pages and a "Web 2" characterized by the rise of web applications, enabling user contributions but controlled by large companies, the "Web 3" aims to be decentralized, collaborative and to give back control to its users.

**Benjamin Thomas**, Security Consultant, **Orange Cyberdefense**  
**Corentin Aulagnier**, Security Consultant, **Orange Cyberdefense**  
 Special thanks to **Julien Meniszez!**



### Introducing the Blockchain

This notion is made possible by Blockchain, a technology that allows individuals or companies to exchange data or property rights, directly in peer-to-peer, without any controlling entity, in a decentralized way.

Instead of being controlled by a single centralized authority that is the sole judge of the reliability of information, this infrastructure is controlled by all participants, without a trusted third party, via cryptographic algorithms.

Each participant in the network verifies the work of the others in real time automatically, making it possible for the first time to carry out transactions and data exchanges in a decentralized manner while maintaining confidence in the process and in the reliability of the data. The data is verifiable by all participants in an open ledger and is deemed tamper-proof.

### Looking closer

In practice, on public blockchains, anyone can host a network node and participate in its security. This is usually done through the installation of a software client on a computer or a server, either on-premise or at a Cloud Provider. Some blockchains also have a compiler and a virtualization layer, allowing developers to run "smart-contracts": simple immutable computer programs that work according to the same principles of decentralization as the rest of the network and allow the advent of Web 3.

This technology became mainstream with the appearance of digital assets, commonly known as "cryptocurrencies" since 2017. Often simply seen as new means of exchange, digital assets also are one of the key elements of security and governance of public blockchains and Web3.

Beyond digital assets, the great revolution of blockchain lies in the "trustless" nature of these networks: no one has to know or trust each other to make the network secure. Security is then ensured by cryptography, decentralized governance and incentive mechanisms.

### Breaking the chain

Although considered unbreakable, repeated hacks targeting this technology have cost the industry several billion dollars and destroyed the myth of the Blockchain's flawless security.

In fact, Chainalysis counts more than \$3 billion in stolen digital assets in 2021, with a growth of more than 500% compared to 2020<sup>[48]</sup>.

Part of these attacks can be explained by the potentially larger attack surface implied by the use of a Blockchain.

Although most attacks targeting Web 3 are specifically aimed at smart-contracts, this is not the only attack vector used by attackers. Attacks targeting design flaws in application design, private key management and the Web3 human-to-machine interface (or "wallet"), are also common and can have disastrous consequences.

The public nature of blockchains greatly simplifies the attackers' job as they can access the source code of applications and use it without constraint before attacking the application.

In addition, the interconnections between each decentralized application make it possible to carry out supply chain attacks, which threatens the integrity of a secure application by attacking interconnected third-party applications.

Other less frequently mentioned risks can also affect Web3 security, such as:

- The use of new, unfamiliar programming languages representing a risk of new vulnerabilities,
- Blockchain nodes hosted in public clouds tend to centralize these networks and make them dependent on a handful of companies or on a state,
- The centralization around a limited number of software clients reinforces the risk of software bugs that would impact the entire network.

### End-to-end security consideration

It is important to consider security by design, from end-to-end. Part of this security is common to all information systems, such as:

- Securing the information system infrastructure that hosts the Blockchain (Cloud or On-Premise),
- Cryptographic signature algorithms and hash functions,
- Management of private keys,
- Identity and Access Management (IAM),
- Monitoring,
- Front-end security and web vulnerability management,
- Application Programming Interface (API) security,
- Training and awareness, for developers, businesses and managers,
- Resilience, Continuity and disaster recovery, crisis management,
- Security governance and management,
- Data protection,
- Regulatory implications.

But unlike Web2, the use of Blockchain for Web3 introduces new specificities that are important to understand and secure. These specificities are present from the start of a project with the choice of the Blockchain, the consensus algorithm or the virtualization environment to be used, or in the choice of parameters such as fault tolerance and crypto-economy. We can also list other specificities such as the management of the network nodes (security related to the authentication of the nodes, RPC communication, administration access and software clients), and the security of the end-user's wallets.

### Focus on smart contract security

Smart contracts remain the most targeted specificity of Web3 by hackers, due to their exploitability and the high possible return on investment for attackers.

As in conventional programs, attacks on smart-contracts usually exploit known vulnerabilities. These vulnerabilities can be found in design flaws or in the source code of the application, usually written in recent languages (such as Solidity, Vyper, Archetype, Rust or Cairo). It is therefore necessary to ensure a good level of secure development training for developers and to ensure that the applications can evolve against obsolescence.

As anyone can retrieve the source code of a smart-contract on a public Blockchain network, it is important to ensure a maximum level of security before the program is released.

This can be achieved by auditing the smart-contract security. Searching for vulnerabilities, using formal methods, auditing the quality of the code and libraries, static and dynamic analysis, manual and automated, the smart-contract audit is the essential step in the process of deploying an application on the Web3.



### A short history of attacks

Targeted application	Stolen amount	Year	Attack vector used
Ronin Network <sup>[49]</sup>	\$ 614M	2021	Phishing, Private keys management
Poly Network <sup>[50]</sup>	\$ 611M	2021	Smart-contract vulnerability
Nomad <sup>[51]</sup>	\$ 190M	2022	Smart-contract vulnerability
Wormhole <sup>[52]</sup>	\$ 326M	2022	Smart-contract vulnerability
Beanstalk	\$ 182M	2022	Design flaw

### Conclusion: The foundations are built now!

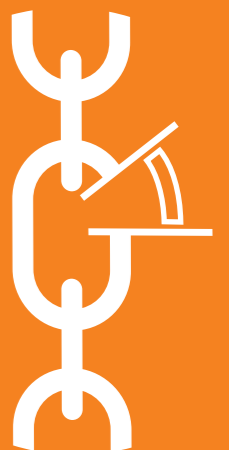
Far from the corporations that control Web2, Web3 promises a sovereign future in which users would be at the core of the system.

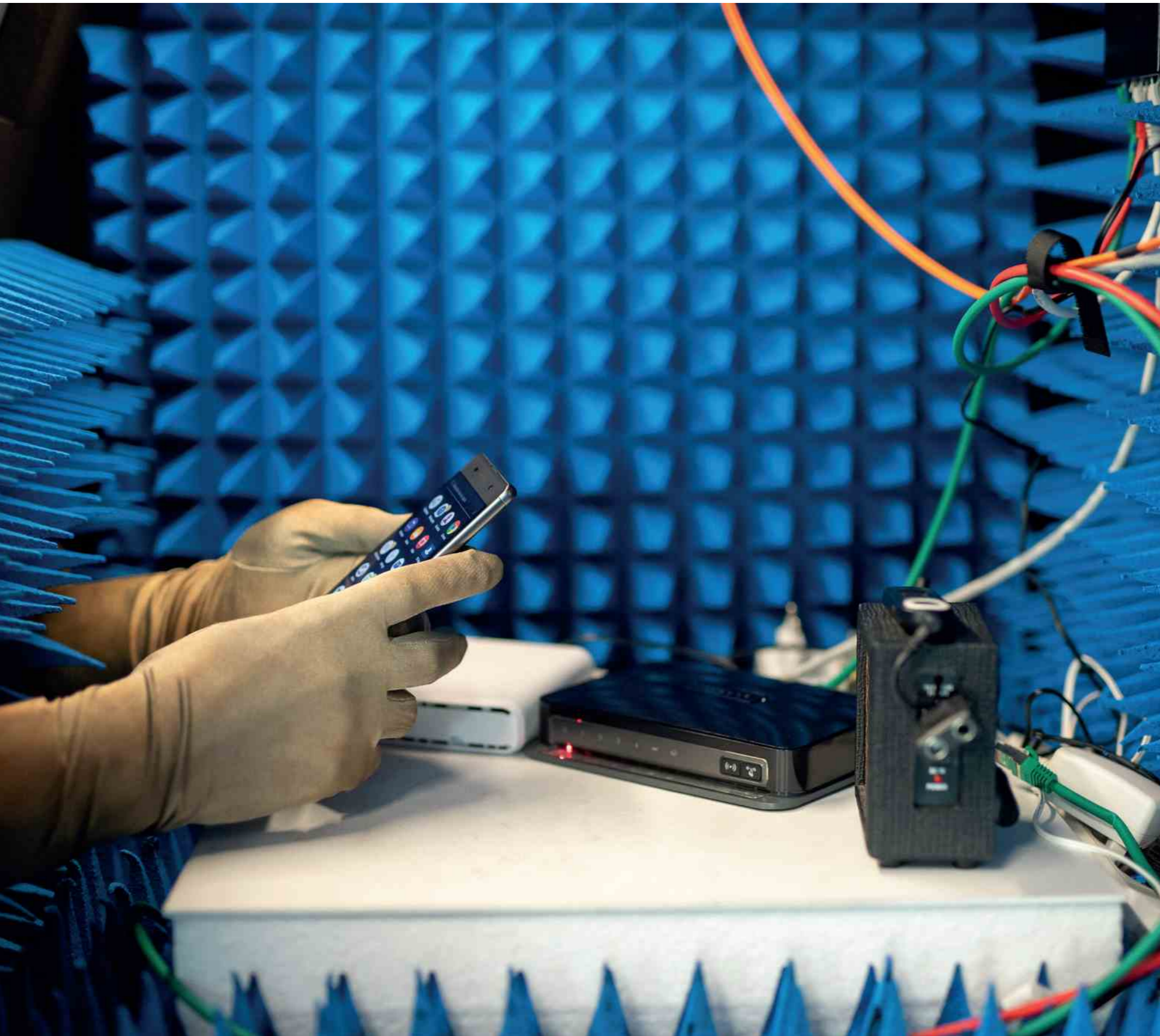
Today used by avant-gardists, Web3 could tomorrow secure data for billions of people, companies and institutions. This could expand the profiles and motivations of attackers as well as the impact of an attack. The emergence of new technologies such as quantum computing must also be considered today to ensure sustainable security in the Web3.

The constant evolution of this technology allows the emergence of new concepts that contribute to the development of future Web3 applications. Zero-knowledge proofs, rollups, modularity, subnetworks, multi-tenancy, all recent concepts that add an additional layer of complexity to this technology and for which security must also be considered.

In order to avoid building the future of the Web on weak foundations, it is important to consider Web 3 security from end-to-end.

This will be a fundamental part of enabling a safer digital society.





**Joshua Sylvester**  
Security Research Intern  
Orange Cyberdefense

**Charl van der Walt**  
Head of Security Research  
Orange Cyberdefense

## The six-inch risk factor: Mobile Security

In the 2022 Navigator we commented on the apparent increase in vulnerabilities, exploits and attacks against mobile phones, and particularly iOS.

It was noted that considerable efforts – and substantial amounts of money – were invested in finding and exploiting vulnerabilities in mobile phones. As was seen in the past, we concluded that at some point it was likely, if not inevitable that such capacities, once created, would leak from the realm of government espionage to the world of the common criminal.

We had, for the first time, observed an increase in advisories on mobile platforms and their vulnerabilities, particularly Android and Apple's iOS.

As we note in the 'World Watch' section of this year's Navigator, attacks of this kind against mobile phones Continue to make headlines. Concerns about remote exploits to control mobile phones raise questions about the security posture of mobile devices, and especially our ability to patch them in response to new vulnerabilities. This is especially critical keeping in mind the role mobile devices play in modern communication and concepts like Two-Factor Authentication (2FA).

In this chapter we therefore dedicate some space to consider the questions of vulnerabilities and threats against mobile phones, and how these may differ across platforms.

## Data

To glean some understanding of the mobile security situation, we reference three distinct datasets:

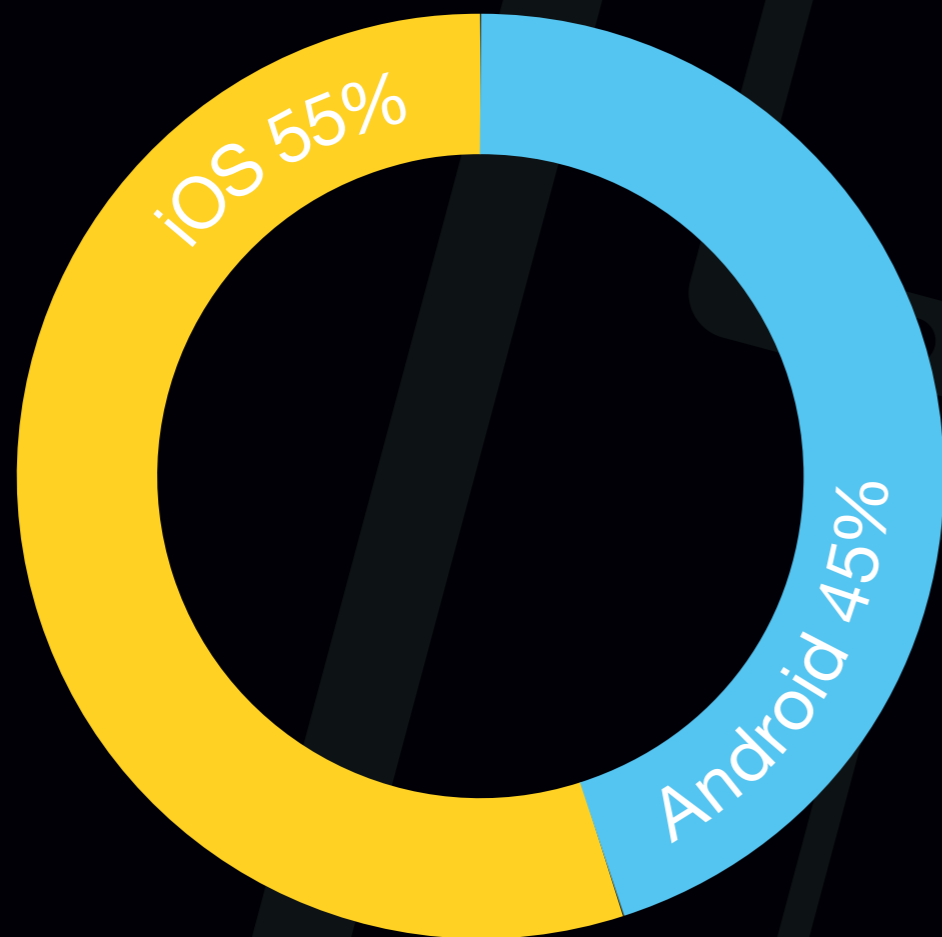
- Web server logs from Orange group portalsOK, containing over 60 million User Agents that were collected from September 2021 till September 2022.
- An excerpt of 96 Penetration Tests performed by our Ethical Hacking teams against mobile phone applications (apps) between January 2018 and October 2022.
- Malicious apps in app stores from Meta and Human Security

## Vulnerabilities in Mobile Operating Systems

Vulnerabilities within the mobile space are becoming a cause for concern, with organizations like the NSO Group providing exploits to governments to allow tracking of individuals. Less individuals. Less sophisticated Threat Actors using mobile exploits to gain information is also becoming a more common occurrence<sup>[53]</sup>.

## Operating Systems

Within our dataset an average of 55% of the users over time were on iOS while 45% were on Android. These figures are derived by examining the User Agents presented by web browsers to major web properties belonging to the Orange Group.



## iOS Vulnerabilities

To examine the response from Apple when a vulnerability is disclosed and the user base that is affected, we use the example of CVE-2022-22587. This vulnerability allows an attacker to run arbitrary commands at the kernel level due to a memory corruption issue. This vulnerability affects all iOS versions excluding 15.3 and higher. The exploit was reportedly used in the wild, but we have no information about who used it or when.

In the graph above we can see that CVE-2022-22587 vulnerability was discovered on the 1st of January 2022. At the time 99.25% of all Apple users collected in the dataset would be considered vulnerable to the exploit<sup>[54]</sup>.

The time between the discovery and the patch on the 26 January was 25 days. Although this vulnerability was apparently exploited in the wild it was only in the public domain for 25 days before Apple released a patch.

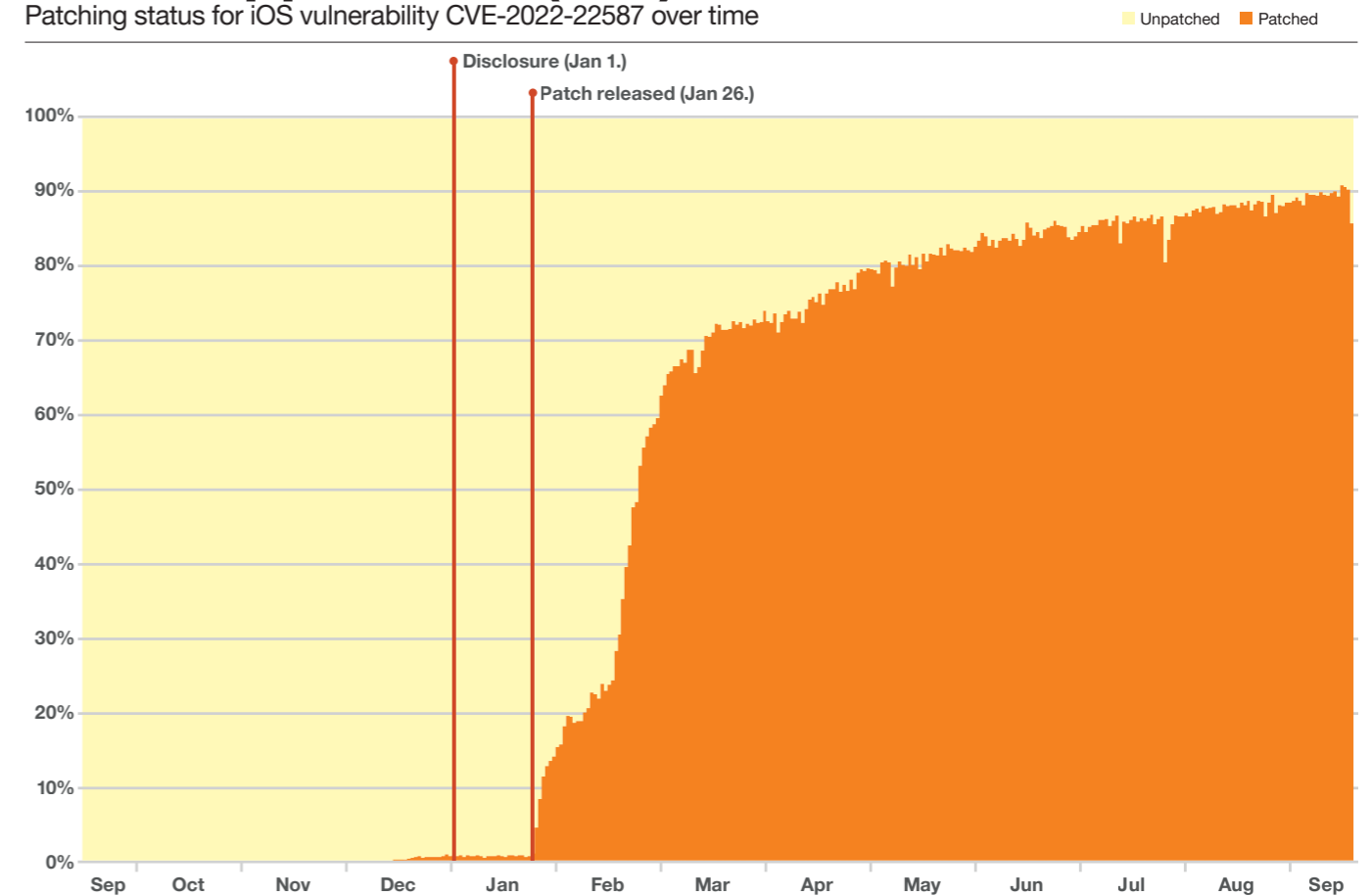
- From the time of the patch to the point where 50% of users were protected, was 31 days.
- The time for 70% of users to be patched from the release date was 51 days.
- And for 90% of the population to be patched took 224 days.

This suggests strongly that patch coverage for Apple iOS is logarithmic, with many users initially updating when the patch is released, but patch adoption slowing over time.

**Eventually adoption seems to trail off completely with 10% of devices left vulnerable after many months of the patch being available. We consider it likely that these users will probably never patch.**

## Patch application (iOS)

Patching status for iOS vulnerability CVE-2022-22587 over time



## Android Vulnerabilities

To examine the response and user base action when a vulnerability is disclosed in Android devices, Samsung phones will be used as an example. This is done to compensate for the difference in how Android handles versioning compared to Apple. From Android 9 on, the user-agent field in the browser component lack adequate fidelity to determine the exact version number. This is unlike Apple's mobile devices that provide the exact version number. Security versions are also named separately and are therefore invisible to us in this dataset. We were able to find specific examples of Samsung phones having received no patch for a major Android version, which is why we chose to focus on this vendor for the purpose of this exercise.

CVE-2022-22292 is an Android OS vulnerability that allows an untrusted application to run arbitrary code. The vulnerability is present in Android versions 9 through to 12, but a patch was made available for version 10, 11, and 12. Knowing this, we can observe the number of devices that would be considered vulnerable before and after the patch was released. We assume (somewhat unrealistically) for our purposes here all devices were actually updated when the patch was released, as the Android version numbers do not actually convey this detailed information.

In the graph below we can see that CVE-2022-22292 vulnerability was disclosed on Nov. 27 2021. At that time, 83.4% of devices in our dataset would be considered vulnerable to the exploit.

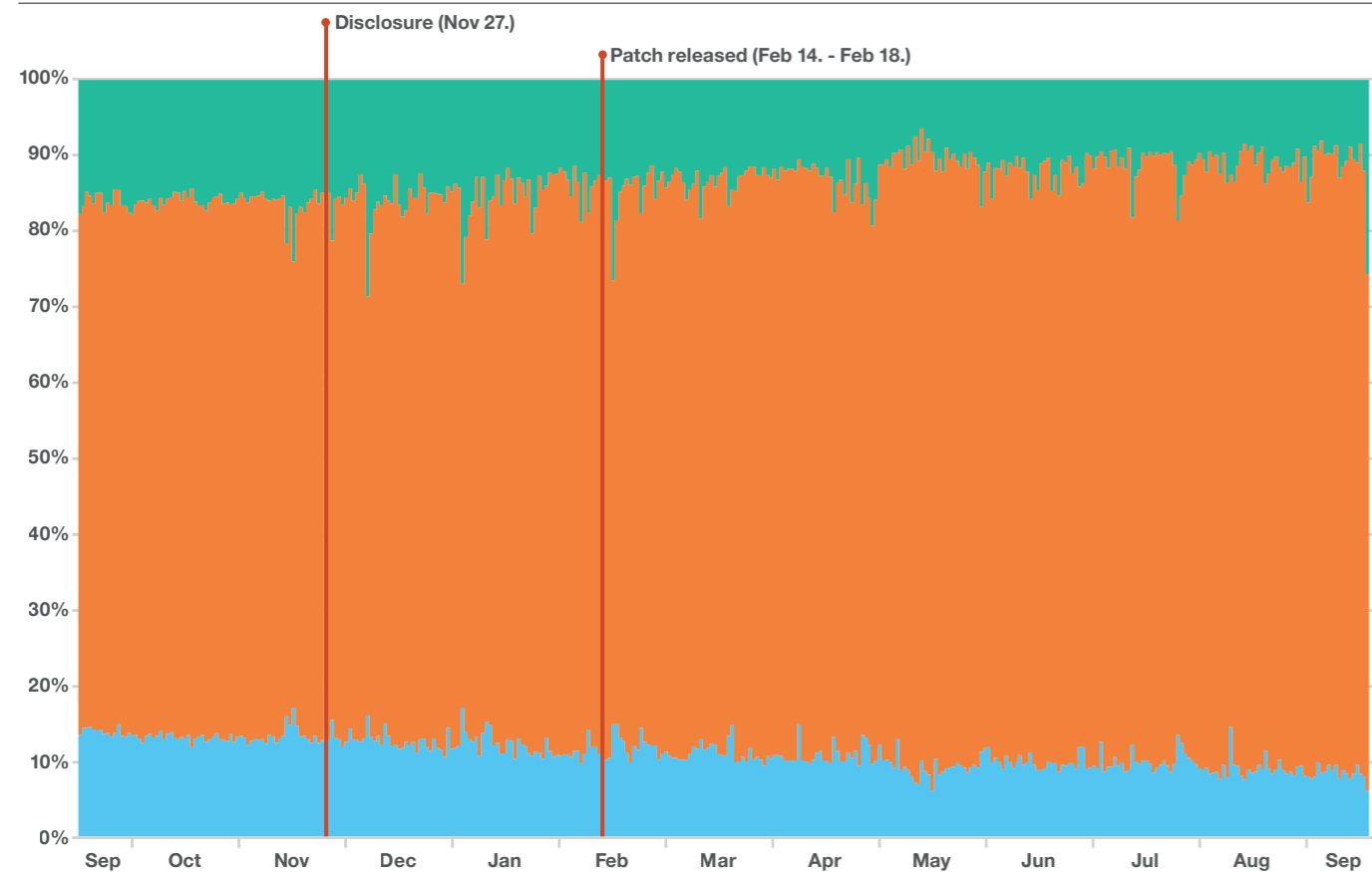
This proportion is lower than the 99.25% of Apple devices considered vulnerable when CVE-2022-22587 was disclosed due to some devices being on such old versions they were fortuitously not affected. This meant that 16.6% of devices were not vulnerable at the time, despite actually not being up to date.

The patch was released 83 days after it was disclosed to Samsung. This is longer than it took in the Apple example we presented above, but Apple's vulnerability was publicly disclosed whereas this one was privately disclosed to Samsung themselves, thus arguably reducing the urgency from Samsung's point of view.

This patch released by Samsung left 10.4% still exposed to vulnerability due to support being dropped for Android 9. This percentage gradually reduces in our dataset over time. But as with the Apple case, a long tail remains and seems likely to persist for some time to come.

## Version status (Android)

Distribution of Android vulnerable and not vulnerable to CVE-2022-22292



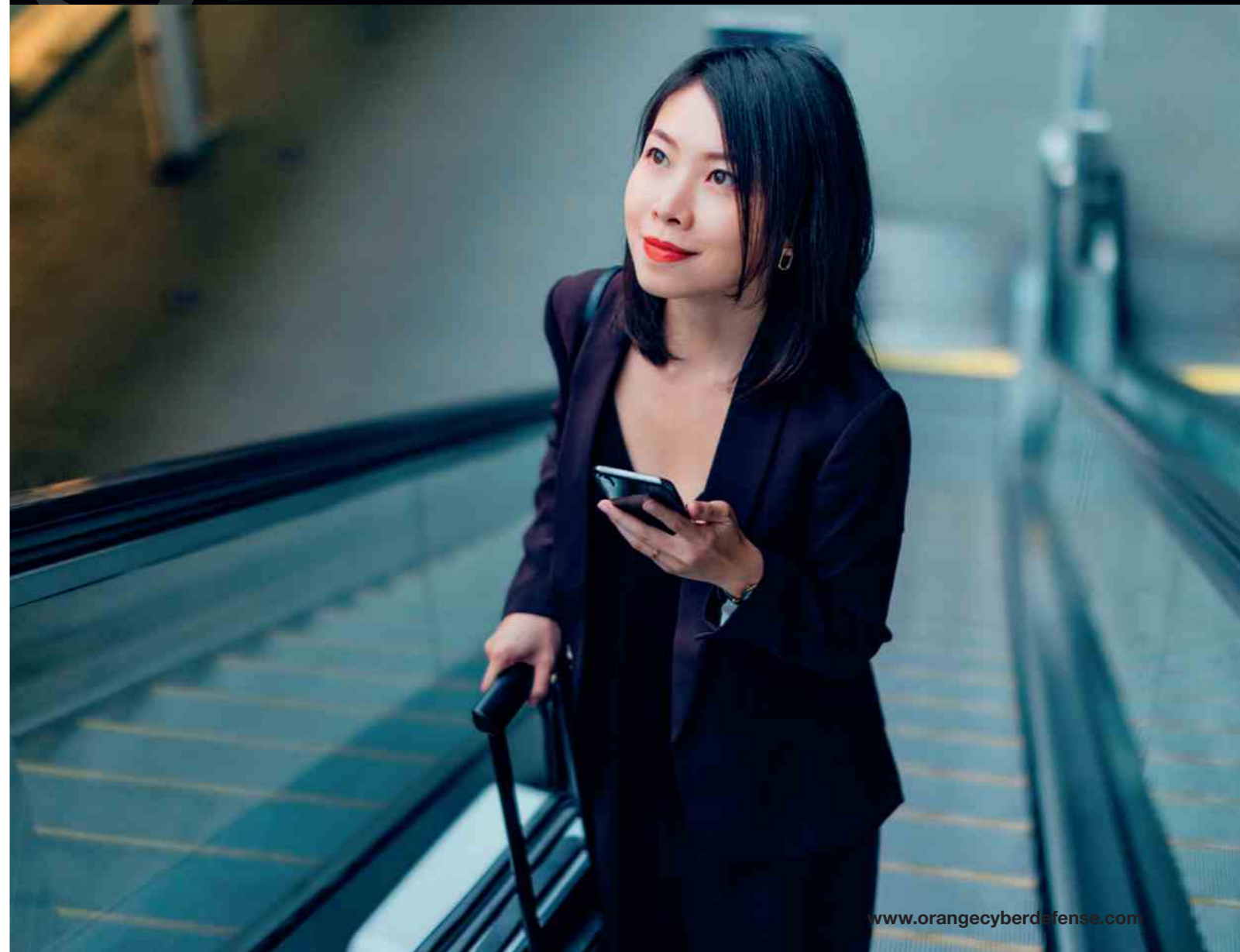
## Discussion

Both iOS and Android have their fair share of vulnerabilities with 547 vulnerabilities discovered for Android in the year 2021 but only 357 for iOS. 79% of the Android vulnerabilities were considered to have a low attack complexity (meaning that it is trivial to exploit them), compared to just 24% of iOS. However, 18 of the Android vulnerabilities received a critical CVSS<sup>[44]</sup> score, whereas 45 received a critical CVSS score for iOS<sup>[55]</sup>.

This suggests that Android has more exploits than iOS that are easier to exploit but that not as many would have had a severe impact. Apple iOS appears harder to compromise but the rewards for doing so are arguably larger. This can be seen in the real world with endless headlines about Android exploits being used in the wild by multiple threat actors compared to headlines where iOS is generally exploited by those players in the mobile surveillance space.

From the two vulnerabilities discussed above, it seems clear that a higher proportion of iPhone users are at risk of being vulnerable when a security issued is disclosed, due to the homogeneous nature of the ecosystem. Users migrate to a new version quickly, however, with 70% updating within 51 days of the patch being released.

The Android ecosystem on the other hand is much more fragmented compared to Apple, with more devices reporting older versions. This has the effect of devices being vulnerable to more old exploits, while also being less vulnerable to new exploits.



## Mobile App Security

Mobile users need to be concerned about vulnerabilities in their device's Operating System, but they also need to consider the security of mobile applications themselves.

We analyzed 96 Security Assessments performed against mobile phone applications between January 2018 and October 2022.

**93% of security issues reported on the Apps we assessed were ranked as Low or Medium severity. 6% were High and 1% were Critical. A mobile App takes 9.7 days on average to assess, and we reported 'Serious' (High or Critical) findings in 24 of the 96 Apps – 28%.**

The Severity assigned to findings, expressed as CVSS score, is similar for Mobile App assessments as for all other tests that we perform. The majority of findings are rated 4 or 5 (Medium), but a greater percentage are rated 4 for Mobile Apps than for other assessments.

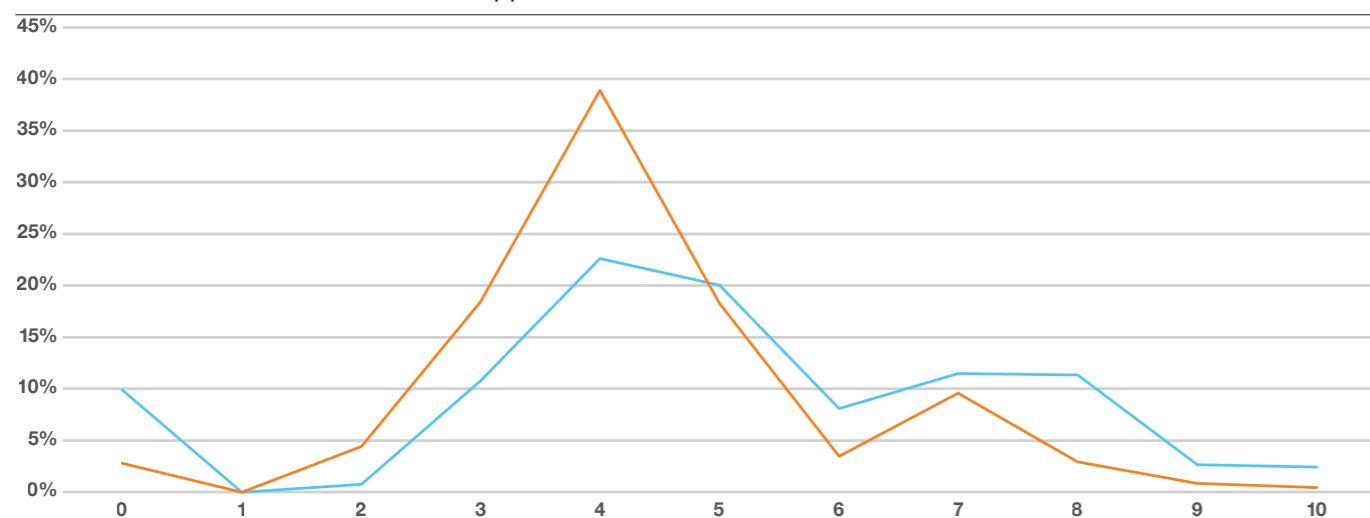
Mobile App assessments contain fewer findings rated at 6. After CVSS 7 (High) the number of findings in App assessments drops of faster than in other test types. For example, 2.4% of findings are rated 10 in other assessments, while for Mobile Apps that proportion is only 0.4%.

Finally, a summary comparing mobile apps, typical desktop applications, and 'thin' web applications reveals that our testers must work harder to report findings in mobile apps than in the desktop and web application space.

This is not to say that there aren't vulnerabilities in mobile apps – as our data and recent history demonstrate – only that these risks are no worse in the mobile space than elsewhere. The strict security models common on modern mobile platforms also help to mitigate the impact on a user should a particular app be compromised.

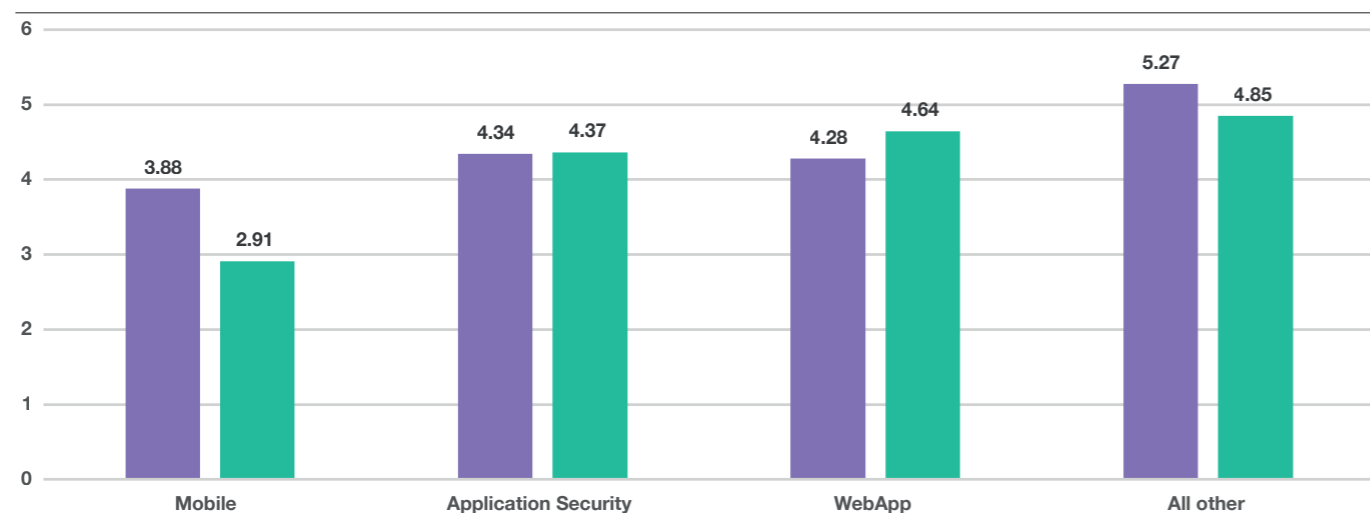
## Vulnerability score of mobile apps

Distribution of CVSS scores for mobile app assessments vs all other tests



## Vulnerabilities in comparison

Comparing mobile apps, typical desktop application, and 'thin' web applications



## Open-Source vs Closed-Source

The comparison between open source and proprietary software security is a popular debate that extends to mobile device security and vulnerability management also.

In Android's case, the open-source nature of the base Operating System theoretically allows experts to proactively evaluate the code, identify bugs and suggest improvements. The argument is that this allows more vulnerabilities to be found and fixed. The downside to this approach is that more vulnerabilities are made public, as the large volume of Kernel vulnerabilities found in Linux seems to suggest. This also means more Proof of Concept exploits will be released into the wild where threat actors can copy and weaponize them.

Apple's closed-source design makes finding exploits more difficult, which in turn arguably makes the platform more secure. If a threat actor does discover a vulnerability, however, it may go undetected for a longer time. As our data above suggests, moreover, the homogenous nature of the iOS ecosystem means that a greater proportion of Apple users will be vulnerable to a new exploit at given time.

'Security' is not a simple term to define, and a 'security comparison' is even more difficult to achieve. This simple comparison between iOS and Android security patching clearly illustrates this point. There is no simple answer to the question of which platform is more vulnerable, and much will depend on what perspective one takes.

For the overall ecosystem, Apple's homogenous approach appears successful at reducing the total level of risk across the community. For individual users, the flexibility offered by Android provides the option of separating from the herd. For businesses, the question may come down to something else entirely.

## App Marketplace

Both Apple and Android have their respective application marketplaces - the 'Apple App Store' and 'Google Play'. The App Store offers 2.2 million apps, compared to Google Play's 2.7 million. Both marketplaces have security measures in place to limit the user's exposure to malicious apps.

These include reviewing apps before they are put on the app stores and sandboxing applications so they cannot reach resources they are not supposed to.

In 2022 eight times more malicious apps were on the Google Play store than on the Apple App Store - 781% This could be due to many factors<sup>[56][57]</sup>.

The first is simply that more malicious apps are submitted to the Google Play store which means more will slip through the net and end up in the trusted public domain. Since Android has more low complexity vulnerabilities, it enables more people to exploit these vulnerabilities and try their luck getting listed on the Google Play store. There are also more exploits ready-made to add to an Android app. Our own Pentesting team developed Kwetza, a research tool that allows testers to add a Meterpreter payload to an APK file. It could also be argued that Google's Play Store review mechanisms is not as good as the Apple App Store.

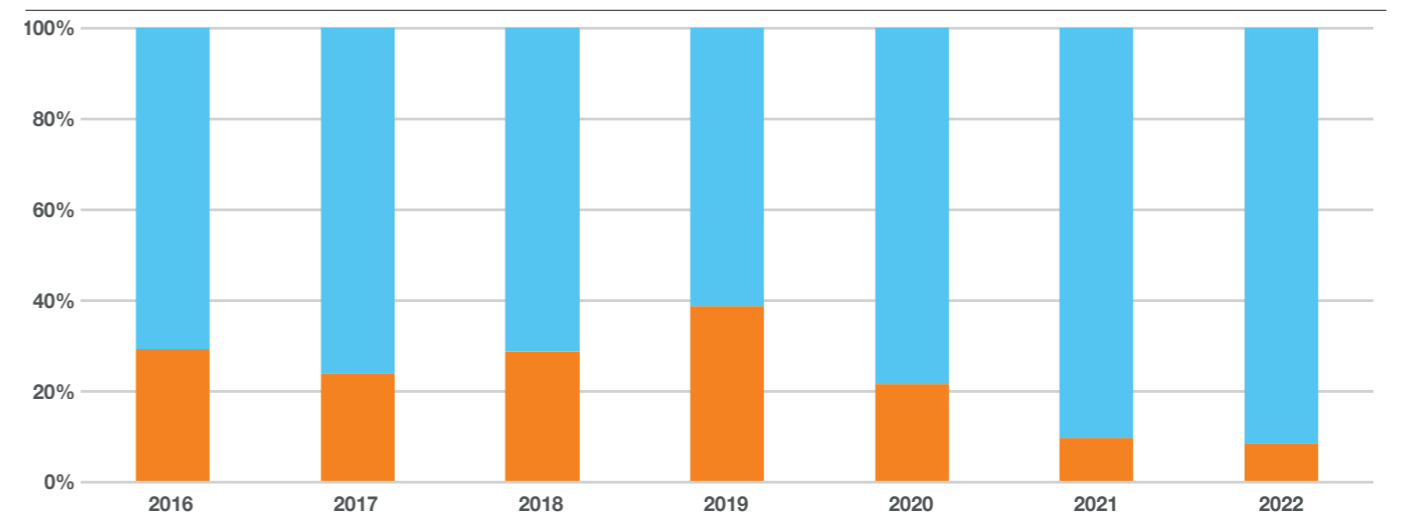
On top of this, of course, there is the issue of unofficial app stores in the Android space, which fall completely beyond Google's ability to regulate.

Although even apps that are top of their categories can turn out to be malware in the Google Play store (such as DxCleaner, which had over 5 million downloads before being taken off the store), Android additionally allows users to download untrusted apps which adds fuel to the fire. Allowing the option to install apps that are not on the official app store is great for users. But potentially insecure or manipulated apps can vastly increase the attack surface.

Data collected from VirusTotal, focusing on Android apps, shows that a high percentage of the apps submitted were malicious. The overall trend is however that the number of malicious apps as a percentage of the submitted apps overall is decreasing. We saw a similar number of apps submitted each year except for 2022 where in August the number of apps submitted rose substantially, this could be caused by a few factors such as their partnership with Google and a VirusTotal mobile app which submits potentially malicious apps from the user's phone.

## Malicious apps detected by VirusTotal

Proportion of apps classified as malicious and non-malicious by VirusTotal over time



### Patches and versions

Patching is becoming as important in the mobile device space as for traditional desktops and servers. As new vulnerabilities are discovered, it becomes a cat and mouse game to fix the issues before they can be exploited. But in the mobile space this is only possible when the user plays along. If users choose not to update their device, or if the device is too old to update, they remain at risk. We have commented on the homogeneity of iOS already, but the picture becomes even more clear when considering all iOS versions over time as see below. Each colour on the chart represents a different version of iOS, and the 'waves' of adoption as new versions are released is clear to see.

Indeed, iOS has become even more homogenous over the course of this year, possibly because they released fewer updates.

At the end of this year, it was taking only two weeks on average for 60% for iOS users to adopt a new version when it is released . Only 10% - 20% of iOS users stay in the long tail and did not update.

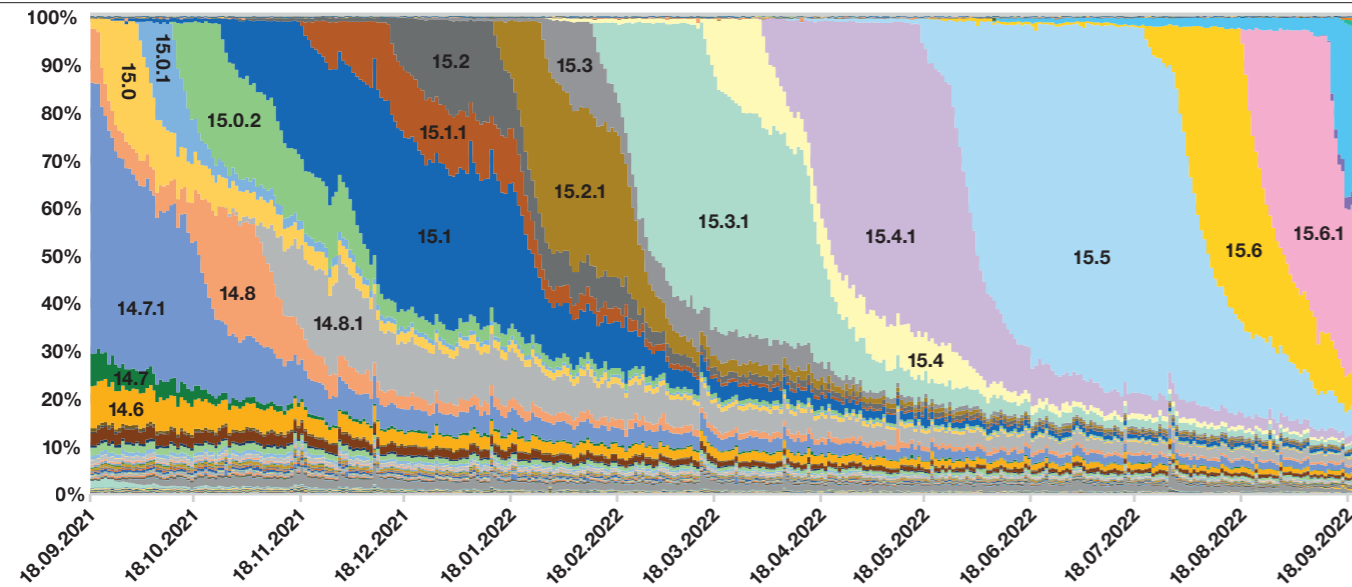
In data on Android, by comparison, over an 8-month period only 30% of users transitioned to the new major version, Android 13. The most common explanation for this has to do with how Android versions trickle down to end users through each individual vendor and sometimes even mobile carriers, who must tweak and approve changes. This leaves many users stuck on older versions until the new version is made ready for their phone. For Android, the long tail of users not updating to the newest 3 versions is 20%-30% throughout the year, which is significantly higher than for iOS.

This diffusion of responsibility for patching across the Android ecosystem creates the comparatively flat pattern of updates we see below.

## Distribution of iOS versions

How present are different versions of iOS and how fast are updates applied?

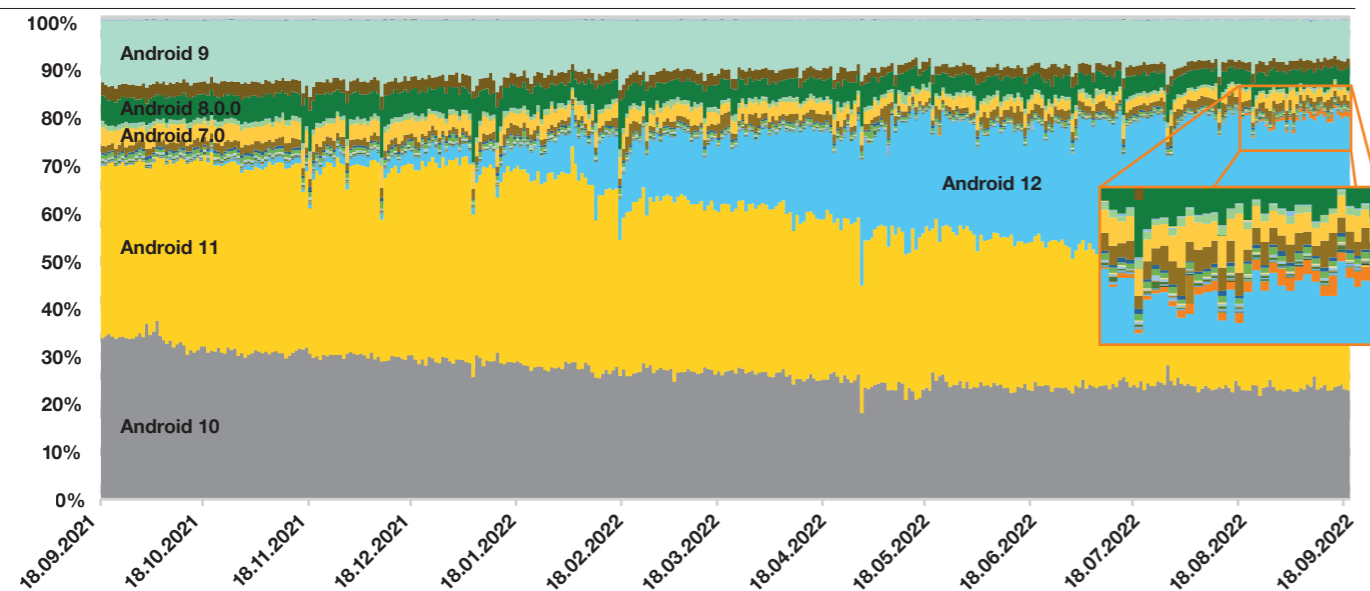
16.1 (current) 16.0.1 16.0 15.7



## Distribution of Android versions

How present are different versions of Android and how fast are updates applied?

13 (current) 12.0.2 12.0 11.1



# Conclusion

Mobile device security is probably not the most pressing concern for most of our readers from enterprise environments, and neither should it be. There is a gradual shift in temperature, however, the issue of mobile is gradually finding its way onto corporate risk registers.

The mobile threat landscape basically comprises of four major threats:

1. Direct or physical access to an individual device, for example by Law Enforcement, a jealous partner, or a criminal who has stolen the instrument.
2. Malicious applications containing exploits and backdoors that are distributed via legitimate marketplaces or on private repositories
3. Vulnerabilities in legitimate applications that can be exploited to compromise sensitive data, or the device itself.
4. Vulnerabilities that allow for Remote Code Execution with or without engaging the user.

The second and third in this set are appropriately the most prevalent at present. Our data suggests that around 30% of the apps we assess for our clients contain issues we classify as "serious". Combined with issues in API and security mistakes made by platform providers, mobile apps represent a significant risk for the privacy of our data.

The final issue of vulnerabilities in mobile Operating Systems is slowly but surely drawing more attention, and this issue is the primary focus of this chapter.

A comparison between the two major mobile OSs proves not to be trivial, however, and will likely surface strong biases of perspective. Our readers are encouraged to start considering this debate early, in order to prepare for a likely future in which the vulnerability management of corporate mobile phones does become a basic security requirement.



# The Thinking Theory

## A mental challenge for security leaders

In an always-on, interconnected world, security leaders are tasked with the daunting challenge of safeguarding businesses against a wide range of risks. They must be able to identify potential threats, assess the impact of those threats, and develop plans to mitigate their impact either actively or in advance. To do this effectively, you must be able to think critically about the challenges you face in your role as a security leader and make decisions that could ultimately change the fate of your organisation. The ability to review and improve your critical thinking is therefore a key skills requirement in today's leadership realm.

Ulrich Swart, Training Manager & Technical Team Leader, [Orange Cyberdefense](#)



### Think about thinking

Have you ever thought about thinking... I mean, "really thought" about why you think a certain way or why based on your thought processing you did something in a different way?

On a daily basis it is estimated that we make close to 35,000 semi-cognitive decisions, 122 of which will be informed decisions that result from us consciously thinking about them. As a security leader the choices you make or the conclusions you draw won't just result in an unsatisfying meal for the day, it could have an effect on the security of thousands.

It is therefore important for us as security leaders to assess our thinking theory, how we approach cognitive processes and eventually make decisions or complete actions. This is where metacognition\* comes in.

### Think like a leader

Security leaders are constantly making decisions that could have serious implications. It's important that they are able to reflect on their decision-making process. Being a good leader also means that you should be able to grow yourself. Metacognition can help leaders identify any biases or errors in their thinking and make necessary corrections.

It can also help security leaders become better problem-solvers. By being aware of your own cognitive processes, you can learn to identify patterns and come up with creative solutions to complex problems.

As a security leader, you should start paying attention to your own thought processes. Reflect on your decisions and see if there's anything you can do to improve.

### Improving your thinking theory

#### Explore the unknowns

Do some self-reflection to find your own weaknesses. You don't know what you don't know. So you need to become aware of your own knowledge gaps and know when to rely on others or outside sources to assist you with your approaches.

#### Understand the knowns

Regularly review past experiences you've had and how you've dealt with them. Understand and trust your approaches that worked in the past. Don't fix something when it is not broken. So if your approach worked in comparable situations, reapply!

#### Challenge yourself

Ask yourself the hard questions in order to grow your thinking methods. Challenge your past thinking and the resultant decisions. Assess what went well and what didn't and understand how you could have changed your mental approach to modify the outcome.

#### Define mental goals

Consider potential mental obstacles you might face and set yourself some goals to prepare for them. You'll find yourself in the right mindset to approach obstacles once you've trained your mind on overcoming them.

#### Prepare your thoughts

Where possible mentally prepare for upcoming scenarios. Define a mental action plan you could draw on when the time comes to increase your thinking capacity and mental well-being.

#### Monitor performance

Check-in with yourself in the midst of a situation. Determining if things are going according to plan allows you to actively reflect and modify your approaches before an outcome has been solidified.

#### Ask for feedback

Rely on others to provide you with insights and improvement areas. Once you've gotten feedback actually do something about it. Others' approaches and thinking methodologies could grow your own approaches to the next level.

There is also a set of questions you can ask yourself in order to improve **metacognition** in the three stages of thinking. Consider the following:



#### Planning

This stage is usual in preparation for a situation or before a strategic planning session. The outcome of this stage of thinking will determine your mental action plan.

#### Ask yourself:

- Have I approached a similar situation in the past?
- What do I want to achieve?
- What should I approach first?



#### Monitoring

This stage is when you are in the middle of a situation or planning task. The outcome of this stage will provide you with a mental check-in to gauge where you are.

#### Ask yourself:

- Am I approaching this the right way?
- Is there anything I can do differently?
- Who can I ask for help or feedback?



#### Evaluating

This stage should come after dealing with a situation or task. The outcome of this stage should give you mental feedback and approaches to re-approach situations in the future.

#### Ask yourself:

- What worked well and why?
- What could I have done better?
- Can I apply this approach in future situations?

**TLDR:** There is a number of ways to challenge and improve your thinking theory. You should always strive to become a better leader and a better version of yourself. This is all possible through an increase of metacognition.

Three challenges you should make part of your leadership toolset:

**Challenge 1: Regularly review your thoughts** - Apply metacognition approaches to assess your thought processes and iron out flawed, delayed, biased thinking. Actively practice your improved thinking approaches in order to form new mental pathways.

**Challenge 2: Enhance your approach** - Allow others to challenge your thinking. Mentors, peers and team members are the best tools to enhance your mental processes. Ask for feedback or allow people around you to challenge your approaches, learn from them and action it.

**Challenge 3: Keep on learning** - Never stop growing your knowledge. The more you know the easier it becomes to approach scenarios and situations. Learn new skills, delve into case studies, listen to peers and network with those you look up to. Everyday should be seen as an opportunity to learn.

Hopefully these challenges will help keeping you busy and growing your cognitive approaches. At the end of the day your thoughts control you but you control your thoughts. So make the best of adjusting your thoughts to serve you well.



\* **Metacognition** is defined as "thinking about thinking". It involves being aware of your own cognitive processes and using that self-awareness to improve the way you think. In other words, it's a way of reflecting on your own thought processes and making adjustments accordingly.



**José Araujo**  
Global CTO  
Orange Cyberdefense

## Security predictions

# The only way is up!

The present influences the future as the past has influenced us!

When I was asked to lend myself to the exercise of predictions, this is the phrase that came to mind: What should we be prepared for?

I share with you some elements that I think must be in the mind of any CISO, not for the future, but right now to prepare for it. These elements cover different parts of the business.

- The best approach to build a secured information system
- The notion of trust and all the legal issues that come with it
- Three critical areas that need specific focus as they will become a frequent target for attacks
- Three themes that an organization must consider in anticipating its future

I therefore invite you to take the time to take a deep-dive into these subjects!



## An unavoidable evolution of architectures

### Let's go back a bit

Sixty years ago, it was already possible to submit jobs to a remote computer to execute them on a time-sharing principle. Resources were rented and shared reducing the costs.

The 2000s brought us cloud computing. This model is changing the way IT is managed and consumed and from a security point of view, the perimeter security model is completely obsolete in the cloud.

Until 2019, organizations had not massively adopted these technologies for many reasons. Moving legacy systems and applications to the cloud can be complex and expensive. Furthermore, it requires a change from the very traditional way to think about security that was inherited from the fortified castles of old.

In a fortress there is a moat and walls to cross, the ramparts, which act as a filter. Well sheltered, internal activities were consequently considered healthy. The outside didn't matter and, when firewalls were correctly configured, the internal assets (data and computers) were considered safe. Internally, no real protection was deployed.

### Where we are today

Cloud is no more an option. Maybe the question will come up again one day, but the COVID-19 pandemic successfully challenged the way we are working.

Users are everywhere and demand to have access to the latest solutions and technologies.

This includes business software, collaborative and classic office tools or services like videoconferencing. Data usage has increased, boosting bandwidth demand and the need to rely on robust architectures.

We are currently in an in-between stage.

Existing security components remain key components of any security policy, but they are no longer enough. The notion of perimeter security is insufficient when employees are mobile, and more and more services are hosted outside the company's own data centers.

### Where are we going

It is necessary to change the way we think about cybersecurity. The key is to reduce the implicit trust granted to users and data flows.

#### Zero Trust is the future.

But Zero Trust, misunderstood or poorly implemented, is likely to increase vulnerabilities. In particular, the use of new and numerous software solutions multiplies the risk of loss of control compared to physical solutions. It can increase the risk of configuration errors, or the presence of vulnerabilities exploited by attackers.

The adoption of a Zero Trust model and the associated architecture in no way replace the control of endpoints used to access resources and services. It is necessary to continue to apply the principles of risk management.

The transformation to a Zero Trust model must be gradual and controlled to ensure the protection of data and assets.



## Law and regulations, increasing criteria for selecting solutions



Europe woke up and a fundamental movement is launched. The legal framework has evolved in recent years, starting in some countries, and is considered at the European level now. Privacy problems are addressed and more recently, cybersecurity and economic issues as well, resulting in new regulations and initiatives.

### The evolution of the legal framework

In France, the national cybersecurity agency (ANSSI) revised its cybersecurity certification and labeling program (SecNumCloudv3.2) to include both data localization requirements and protections against the extraterritorial reach of foreign laws. Other countries are considering the same kind of program and ENISA is currently working on the "Cloud Services Scheme". Although it is too early to draw conclusions on their work, it is likely that these aspects will have to be taken into consideration in the foreseeable future.

### The evolution of positions

In the beginning, large industrial players were reluctant, but they are now joining the movement. Several initiatives are emerging, attempting to provide sufficient levels of guarantees in terms of security and immunity. Hyperscalers are starting to propose their own offers. Some of them allow the client to choose where they want to store their data. Others are offering mechanisms to ensure data is accessible only with client authorization, supported by the principle of "bring your own key".

These approaches have the same weakness: the cloud provider is still operating the service. A certain level of security is obtained on the data at rest or in transit. However, data protection during treatment remains a risk.

**New solutions and services are being born, relying on the same technologies as available today but fully operated by an independent company, immune to extraterritorial laws, by design.**

### Trust in terms of technology

The increasing threat requires us to reconsider how trust is obtained. It is necessary to find the delicate balance between the protection obtained from security solutions and the trust put on employees, subcontractors, and solution providers. It also includes the legal frameworks that can apply.

### The delicate definition of sovereignty

Sovereignty is a political concept. It is generally defined as the capacity, for a government, to make laws and free itself from the power of others to interfere.

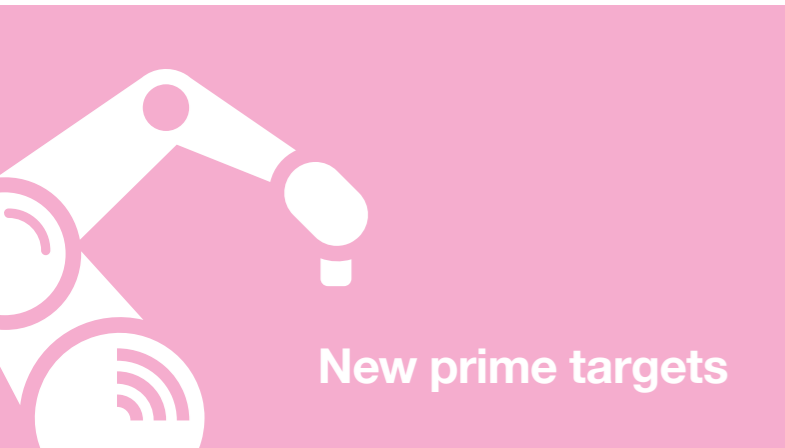
For an organization, the challenge is to have guarantees on the data for which it is responsible, in front of the laws of the countries where they are stored, and also in front of any applicable extraterritorial laws. They may be applicable for many reasons and the origin of the company providing the service may only be one of them.

**The future is made of this search for trust considering sovereignty issues.**

### A recent awareness

The United States of America are the best example of countries that have always been considering this risk. Their governmental institutions have the capability to rely exclusively on national solutions and providers. An easy task due to the vast number of digital and cybersecurity companies present in their territory.





### A matter of objectives

The two main motivations of cybercriminals are money and access to information. Microsoft Windows was the main targeted system because a discovered vulnerability exploitable in millions of systems increases the return on investment for attackers.

There are other motivations. Some attackers want to destroy systems or have enough impact to destabilize a company or society for political or wider economic reasons. This is the case of hackers or sponsored state attacks.

**There will be an increase of attacks against specific information systems for non-monetary gains.**

### Mobile devices: a gold mine

The grey market is interesting to observe in order to understand how precious some targets are. Some actors in this market are proposing to buy vulnerabilities which would allow an attacker to penetrate a user's mobile device with zero interaction from the victim. The proposed price varies from one platform to the other, but they can pay up to \$2.5 million for the most efficient ones.

More than 1.5 billion smartphones are sold in the world every year and are used for all kinds of purposes, including payment, multi-factor authentication and professional communications.

**Smartphones will remain a prime target and attacks will most likely increase further.**

### Industrial systems

A few decades ago, critical infrastructures operated in isolation. They had little resemblance to IT systems, running proprietary control protocols and using specialized hardware and software. They are now more complex and interconnected. A failure or an attack on one of them can, cascade into a devastating chain reaction. Because of their design and their life cycle, most systems still utilize outdated components featuring known vulnerabilities.

Numerous attacks have been detected against these systems with the potential to have an impact on the real world. Cyberattacks against critical infrastructures are more likely to target industrial control systems than to steal data. The recent war against Ukraine highlighted the risks on these infrastructures. Such kinds of targets have the potential for global impact, posing a threat to the entire population. **Attacks against these critical and essential systems will likely increase.**

### Internet of things and embedded systems

In the same way as for industrial systems, connected devices pose a particular challenge in terms of security. Permanently connected by design, they typically have low computing capability and are often located in areas where applying good security practices is a challenge. Manufacturers of such devices must handle data very carefully as it can contain personal or sensitive information. This is the reason that pushed the European Commission to recently define new rules governing the cybersecurity of all network-connected devices sold in the EU, The Cyber Resilience Act.

Almost simultaneously, the new UNECE Regulation 155 and 156 have been adopted and require respectively to implement a cybersecurity management system and a software update management system for the automotive sector.

**These various regulations will push manufacturers to become compliant. Yet there is little doubt that these platforms will remain attractive targets for attackers or increasingly become so in the future.**



### New old tricks

### Business almost as usual

Ransomware attacks have been in the spotlight over the past few years due to their ever-increasing impact and number. However, over the past few months, there has been a significant drop in these attacks worldwide.

Better understanding of cybercriminals' methods and ecosystem, in addition to better organization and collaboration amongst law enforcement agencies, had a positive impact in the fight against attackers. The geopolitical context and cryptocurrency fluctuations were also an explanation for this decrease. It is unlikely that this type of threat will drop off the top 3 cyber threats though. As previously said, the main motivation of cybercriminals remains the pursuit of profit, and ransomware attacks remain one of the most lucrative approaches. As a reminder, the methodology has evolved over time:

- Extortion was initially based on encryption of the user's data to demand a ransom in exchange for the decryption key.
- Attackers have imagined a solution to increase their profits. Before encrypting everything, they exfiltrate the sensitive data from the victim's system giving them additional leverage to collect payments. This data is used to add pressure to the victim and, when the ransom is not paid, it is often published in public forums.
- More recently, triple extortion appears. Attackers can directly contact the identified suppliers or clients to demand a ransom to not publish their data. To add pressure, they are using distributed denial of service attacks or phone calls against these targets.

**Ransom demands are not about to stop, and this type of attack will continue to thrive.**

### Cyber insurance

There are huge debates over the legality of paying ransoms to criminals.

Most of the public authorities involved in the fight against cyber crime are blaming insurers for encouraging the increase in ransomware cyberattacks by agreeing to pay ransoms. They generally call for an end to this practice. Paying ransom is not an offense currently in most countries. When the insurance provider pays, this is seen as a transfer of risk. Furthermore, if insurers automatically reimburse the costs of restoring data, the cost of claims will explode, and insurance rates will likely follow suit.

**It is therefore to be expected that the discussion will continue on how to insure cyber risks, what are the consequences and which payments should or should not be legal.**

### Cybersecurity during an M&A

The impact of a cyberattack can be so severe that 60% of SMEs close within 6 months after being hacked<sup>[58]</sup>. It is important to understand the risk exposure of a company even during mergers and acquisitions (M&A). Several aspects should be evaluated, including its level of maturity and preparedness but also previous security issues and data breaches. Conducting such kinds of assessment is a challenge today, but it will become more structured and embedded as an essential step in any decision-making process.

**Cybersecurity is becoming a subject of concern at Board level, and becoming a criterion in evaluating M&A opportunities.**



## Report summary

# What have we learned?



**Sara Puigvert**  
EVP Global Operations  
Orange Cyberdefense

This year certainly held a lot of surprises.

In a perceived state of permanent crisis it is important to avoid paralysis when facing problems.

On the contrary, we think it is even more important to recognize and value good news.

Looking closer at the data in this report, we can find quite such positive trends.

Let's start with the subject of vulnerabilities.

Agreed, we still see that a lot of "disclosed vulnerabilities" are generally not patched very fast, even if a patch is available. But we also see that the time taken for patching critical weak spots has tendentially gone down, and likely will continue to do so as more businesses endorse risk-based patching strategies.

Our Ethical Hackers still breach our customers' security set-ups, but they are taking longer and must work harder to successfully do so.

The incident count per customer has decreased too, from 40 to 34. True, our customers are well protected and how sustainable that is, while our client base constantly changes and grows, remains to be seen. But it still is good news.

And lastly, let's look at the impact of the war in Ukraine and Log4j vulnerability: everyone in the cyber landscape was seeking cover in preparation of the big storm, the ultimate cyber-Tsunami. These events did have an impact, but now that the dust has somewhat settled, we can conclude: the impact could have been far worse.

In fact, reading the report from our CERT colleagues in Poland, quite the opposite happened. While hacktivist activities worldwide increased, we have not yet seen any devastating collateral damage being done outside the direct parties in conflict. There was no second Wannacry, no NotPetya running wild, destroying thousands of businesses around the globe.

We believe that these changes can be explained by a combination of factors.

For one, targeted subjects are becoming less vulnerable. Massive efforts have been underway, especially in North America, the UK and Western Europe, to improve the security posture of businesses. It may be that these efforts are paying off.

The brand image of the Conti group became viewed as 'toxic' within the cybercrime community after their internal chats were leaked to the public following their decision to publicly side with Russia in the war against Ukraine. Eventually a series of setbacks led the group to dissolve, with a temporary impact on victim numbers. Unfortunately, although without surprise, Conti's affiliates moved swiftly to other existing RaaS (i.e. Lockbit or newer ones as BlackBasta, BalckByte, Royal, ...)

High profile attacks in the USA have caught the attention of Intelligence Agencies, Regulators and Law Enforcement in the USA and caused concern within the cybercrime community, who dislike the level high level of attention. This may be causing actors to 'hold back' on compromising or extorting victims in the USA and Canada.

Regulators have been making life difficult for cryptocurrency service providers known to be popular with extortion actors. In September 2021, for example, the US Treasury's Office of Foreign Assets Control (OFAC) announced that the cryptocurrency exchange Suex has been added to the Specially Designated Nationals and Blocked Persons (SDN) List, thereby prohibiting Americans from doing business with the company. Restricting such 'nefarious' players may be making Cyber Extortion more difficult to monetize.

Other coordinated Law Enforcement/FBI interventions, like the successful dismantlement of the infrastructure supporting the Raccoon Infostealer, may be having an impact as well.

Cyber Insurance is becoming more difficult to access. It has been common to see threat actors refer to the victim's cyber insurance policy. Offenders have also been observed arguing that the extortion demands would be covered by an insurance policy. In the report "The state of ransomware 2020", Sophos states that for 94 per cent of incidents where a ransom is paid, payment was covered by insurance.

Although growing cybercrime levels drove waves of new and bigger claims, the cyber insurance industry has been pushing back, however. It may be that without access to ready sources for ransom payment, criminals are finding it harder to make money.

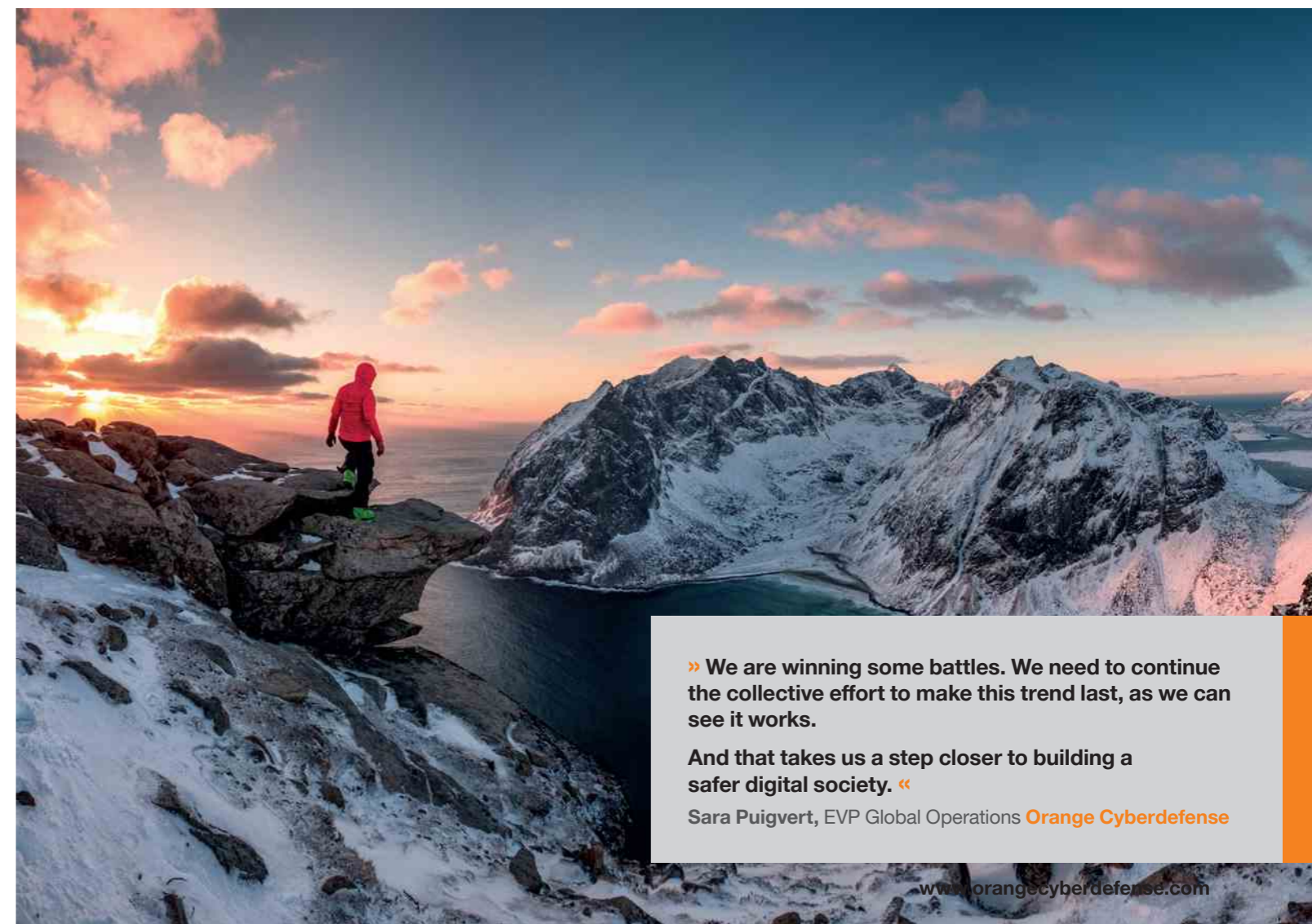
As we mention in our section regarding Ukraine, we notice that cybercriminal activity targeting Polish internet users reduced substantially (by about 50% for a few weeks) from the start of the war. It's no secret that most of these attacks are performed by people from former CIS countries, and it looks like these groups may have been distracted in one way or another by the impact of the war.

They did return to "business" eventually, but we have not seen anything beyond of what has become the new normal.

So, what does that mean for our cyber security? Security is still a moving target, a constant chase. Did we get any closer? Have we found our silver bullet? Unfortunately not. However, it means that we are in fact seeing the result of hard work, ongoing dedication and a strong will to become more mature in our digital life and workspace. It means that politics, law enforcement and economic powers have recognized the problem and collectively started to counteract. And it means that the actions we have taken are yielding a result.

We are winning some battles. We need to continue the collective effort to make this trend last, as we can see it works.

And that takes us a step closer to building a safer digital society.



» We are winning some battles. We need to continue the collective effort to make this trend last, as we can see it works.

And that takes us a step closer to building a safer digital society. «

Sara Puigvert, EVP Global Operations **Orange Cyberdefense**

## Contributors, sources & links

# Sources

This report could not have been created without the hard work of many researchers, journalists and organizations around the world. We've gratefully used their online publications for reference or context.

## Sources/links

- [1] [https://en.wikipedia.org/wiki/Survivorship\\_bias](https://en.wikipedia.org/wiki/Survivorship_bias)
- [2] <https://www.verizon.com/business/resources/reports/dbir/>
- [3] [https://en.wikipedia.org/wiki/Back\\_Orifice](https://en.wikipedia.org/wiki/Back_Orifice)
- [4] [https://en.wikipedia.org/wiki/Metasploit\\_Project](https://en.wikipedia.org/wiki/Metasploit_Project)
- [5] <https://attack.mitre.org/software/S0154/>
- [6] <https://www.orange cyberdefense.com/za/blog/threat/cyber-extortion-cy-x-the-actors-and-the-victims>
- [7] <https://www.orange cyberdefense.com/global/blog/do-ransomware-threat-actors-know-that-their-activities-are-criminal>
- [8] <https://www.bbc.com/news/technology-56933733>
- [9] <https://www.reuters.com/technology/russia-based-ransomware-group-Conti-issues-warning-kremlin-foes-2022-02-25/>
- [10] <https://www.wired.com/story/Conti-ransomware-russia/>
- [11] <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/strategic-corruption-cybercrime-connection/>
- [12] <https://www.siliconrepublic.com/enterprise/costa-rica-cyberattack-explainer-Conti-ransomware-group>
- [13] <https://www.worldpoliticsreview.com/in-costa-rica-ransomware-attack-takes-aim-at-the-government/>
- [14] <https://flashpoint.io/blog/history-of-Conti-ransomware/>
- [15] <https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/>
- [16] <https://www.sciencedirect.com/science/article/abs/pii/S0047235217301897>
- [17] <https://cms.law/en/int/publication/ransomware-attack-can-we-negotiate-with-cybercriminals>
- [18] <https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/>
- [19] <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>
- [20] [https://en.wikipedia.org/wiki/Routine\\_activity\\_theory](https://en.wikipedia.org/wiki/Routine_activity_theory)
- [21] <https://www.orange cyberdefense.com/global/blog/threat/inside-the-criminal-mind-applying-criminology-theories-to-cy-x>
- [22] <https://www.zdnet.com/article/ukraine-is-building-an-it-army-of-volunteers-something-thats-never-been-tried-before/>
- [23] Lockheed Martin, "The Cyber Kill Chain," [Online]. Available: [www.lockheedmartin.com/en-us/capabilities/cyber/cyber-Kill Chain.html](http://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-Kill Chain.html)
- [24] K. T, "The Cooper color code and threat assessment," SoftRep, [Online]. Available: [sofrep.com/news/the-cooper-color-code-and-threat-assessment/](http://sofrep.com/news/the-cooper-color-code-and-threat-assessment/)
- [25] <https://heimdalsecurity.com/blog/is-Conti-ransomware-siding-with-russia/>
- [26] <https://www.bleepingcomputer.com/news/security/Conti-ransoms-internal-chats-leaked-after-siding-with-russia/>
- [27] <https://www.bbc.com/news/technology-60784526>
- [28] <https://www.infosecurity-magazine.com/news/hackers-russian-tv-schedules/>
- [29] <https://www.washingtonpost.com/politics/2022/05/13/cyber-attack-hack-russia-putin-ukraine-belarus/>
- [30] <https://cybernews.com/news/cyberattack-on-ukrainian-border-control-slows-refugee-crossing/>
- [31] <https://www.businessinsider.in/tech/news/anonymous-hacking-group-has-broken-into-a-russian-space-website-and-leaked-files-belonging-to-its-space-agency-roscoms/articleshow/89985696.cms>
- [32] <https://securityaffairs.co/wordpress/128576/hackivism/anonymous-causes-damages-to-russia.html>
- [33] <https://www.businessinsider.in/tech/news/Google-and-tripadvisor-disable-restaurant-reviews-in-russia-after-they-were-flooded-with-protests-against-the-ukraine-invasion/articleshow/89973737.cms>
- [34] <https://www.france24.com/en/live-news/20220227-musk-activates-starlink-internet-service-in-ukraine>
- [35] <https://www.csoonline.com/article/3651685/how-security-vendors-are-aiding-ukraine.html>
- [36] Mitre, "Matrix – Enterprise | Mitre ATT&CK," [Online]. Available: [attack.mitre.org/matrices/enterprise/](http://attack.mitre.org/matrices/enterprise/). [Accessed 31 January 2022].
- [37] <https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/>
- [38] <https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails>
- [39] <https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/>
- [40] <https://www.bleepingcomputer.com/news/security/viasat-shares-details-on-ka-sat-satellite-service-cyberattack/>
- [41] <https://www.fortinet.com/blog/threat-research/pivnoxy-and-chinoxy-puppeteer-analysis>
- [42] <https://ics-cert.kaspersky.com/publications/reports/2022/08/08/targeted-attack-on-industrial-enterprises-and-public-institutions/#lkyvqfi875ftflu9>
- [43] [https://website.kennasecurity.com/wp-content/uploads/2020/12/Prioritization\\_to\\_Prediction\\_Volume\\_6\\_\\_\\_Attacker\\_Defender\\_Divide.pdf](https://website.kennasecurity.com/wp-content/uploads/2020/12/Prioritization_to_Prediction_Volume_6___Attacker_Defender_Divide.pdf)
- [44] [back to P66] [back to P73] [back to P85] [back to P107] The Common Vulnerability Scoring System (CVSS) is a public framework for rating the severity of security vulnerabilities in software. It is application and vendor neutral, enabling an organization to score its IT vulnerabilities across a wide range of software products – from operating systems and databases to web applications – using the same scoring framework.
- [45] Lawrence E. Cohen and Marcus Felson.1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44 (August), 588-608. <https://doi.org/10.2307/2094589>
- [46] Billy Henson.2020. Routine Activities. In: T.J. Holt, A.M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime*.
- [47] Majid Yar. 2005. The novelty of 'cybercrime': An assessment in light of Routine Activity Theory. *European Journal of Criminology*, 2, 4, 407-427. <https://doi.org/10.1177%2F147737080556056>
- [48] Chainalysis 2022 crypto crime report : <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>
- [49] Ronin network attack : <https://www.theverge.com/2022/7/6/23196713/axie-infinity-ronin-blockchain-hack-phishing-linkedin-job-offer>, <https://halborn.com/explained-the-ronin-hack-march-2022/>
- [50] Poly network attack : <https://www.theblock.co/post/114045/at-least-611-million-stolen-in-massive-cross-chain-hack>, <https://www.businessinsider.in/investment/news/biggest-crypto-hacks-of-2021-over-4-billion-stolen/slidelist/88560280.cms>
- [51] Nomad bridge attack : <https://zerion.io/blog/nomad-bridge-hack/>, <https://medium.com/nomad-xyz-blog/nomad-bridge-hack-root-cause-analysis-875ad2e5aacd>
- [52] Wormhole attack : <https://decrypt.co/91899/hacker-steals-320-million-solana-ethereum-bridge-wormhole>, <https://halborn.com/explained-the-wormhole-hack-february-2022/>
- [53] <https://www.bitdefender.com/blog/labs/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android>
- [54] <https://securityaffairs.co/wordpress/127240/hacking/apple-fixed-two-zero-day-2022.html>
- [55] <https://www.humansecurity.com/learn/blog/poseidons-offspring-charybdis-and-scylla>
- [56] <https://www.bleepingcomputer.com/news/security/2021-mobile-security-android-more-vulnerabilities-ios-more-zero-days/>
- [57] <https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps/>
- [58] <https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses>

### Disclaimer

Orange Cyberdefense makes this report available on an “as-is” basis with no guarantees of completeness, accuracy, usefulness or timeliness. The information contained in this report is general in nature. Opinions and conclusions presented reflect judgment at the time of publication and may change at any time. Orange Cyberdefense assumes no responsibility or liability for errors, omissions or for the results obtained from the use of the information. If you have specific security concerns, please contact Orange Cyberdefense via <https://orangecyberdefense.com/global/contact/> for more detailed analysis and security consulting services.

**Very special thanks**  
**to all cyber hunters,**  
**analysts and engineers**  
**in our VOCs, SOCs,**  
**CyberSOCS, to our Ethical**  
**Hackers and Incident**  
**responders.**

**These are your stories.**



# Why Orange Cyberdefense?

**Orange Cyberdefense** is the expert cyber security business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe.

As the leading security services provider, we strive to build a safer digital society.

Our Global footprint with a European anchorage enables us to meet local requirements and international standards, ensure data protection and privacy for our clients as well as for our employees. We embed security into Orange Business Services' solutions for multinationals worldwide.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 13 CyberSOCs and 8 CERTs distributed across the world as well as sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our clients throughout the entire threat lifecycle.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats. We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our clients to invest their resources where they have most impact, and actively contribute to the cyber security community.

Our experts regularly publish white papers, articles and tools on cyber security which are widely recognized and used throughout the industry and featured at global conferences including Infosec, RSA, 44Con, BlackHat and DefCon.

We believe strongly that technology alone is not a solution. We wrap elite cyber security talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio. It is the expertise and experience of our multi-disciplined people that enable our deep understanding of the landscape in which we operate.

[www.orange cyberdefense.com](http://www.orange cyberdefense.com)

Twitter: @OrangeCyberDef