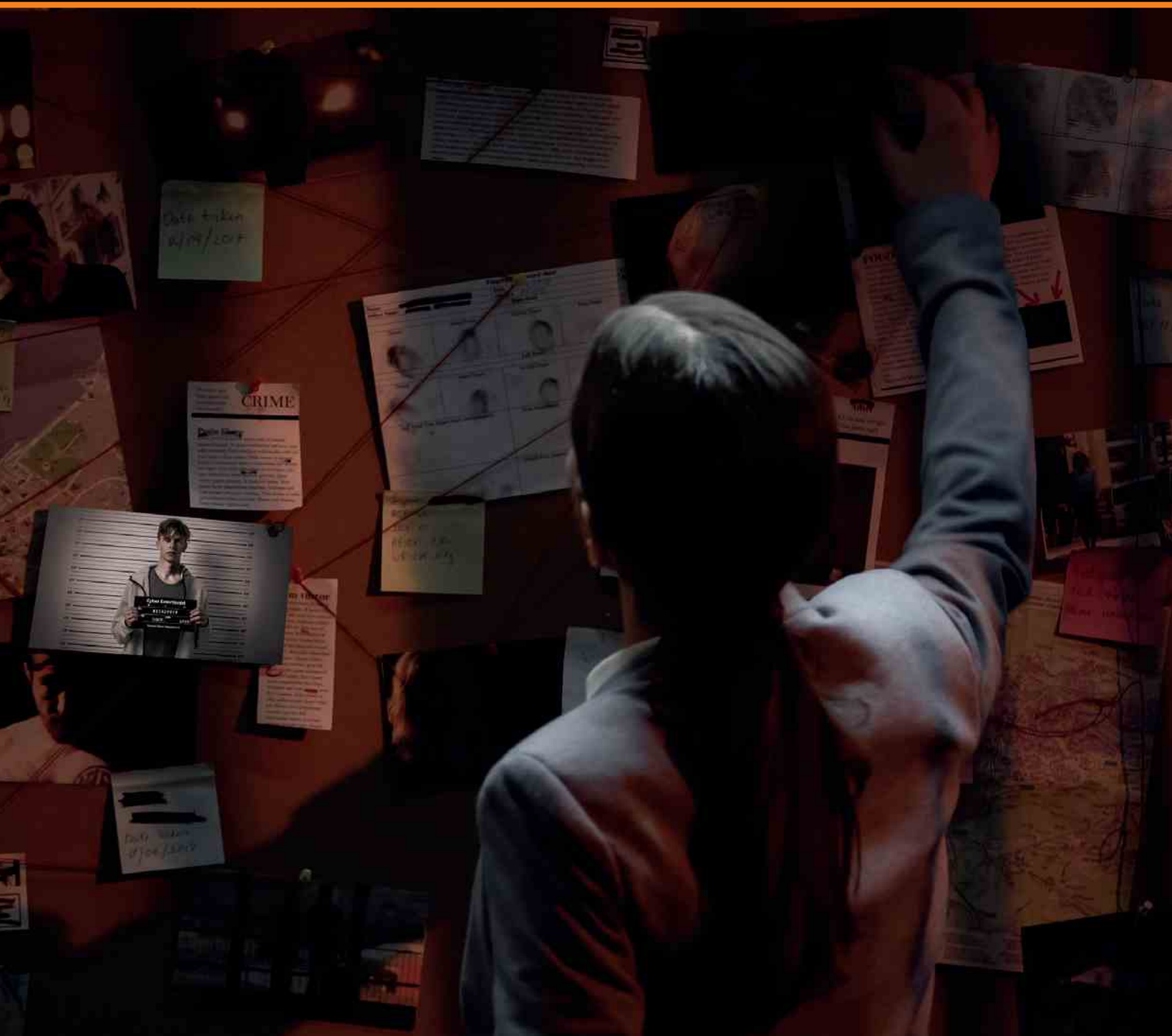
Orange
Cyberdefense

Cy-Xplorer 2023

When bits turn to blackmail: navigating the ecosystem of cyber extortion and ransomware



Authors

Diana Selck-Paulsson
Lead Security Researcher
Orange Cyberdefense

Vincent Hinderer
Cyber Threat Intelligence Team Leader
Orange Cyberdefense

Co-authors

Charl van der Walt
Head of Security Research

Carl Morris
Senior Lead Security Researcher

Wicus Ross
Senior Security Researcher

Mael Sarp
Cyber Threat Intelligence Analyst

Marine Pichon
Cyber Threat Intelligence Analyst

Tristan Marcelin
Junior Security Analyst

Table of Contents

Executive Summary **4**
Key findings **5**
1 Introduction **6**
Methodology 8
2 Threat actors **10**
Tracking re-brands and affiliation over time 14
The case of Conti 16
The rise of new actors in 2022 17
3 Did Russia's invasion impact the cyber extortion ecosystem and their choice of victims? **18**
Before the war 20
War disrupts 20
NATO countries 21
Nordic countries 22
5 Deep dive into the Tactics, Techniques, and Procedures (TTPs) **24**
Initial access 26
Intel471's data exploring the Initial Access Listings landscape 29
First stage payloads 30
Encryption payloads 31
A view from the CSIRT 32
Observed extortion techniques in 2022 33
6 Who are the victims of cyber extortion? **34**
Geographic distribution 36
France 38
The Nordics 38
Other countries & regions 39
Australia & New Zealand, Benelux, Europe 39
Latin America, USA & Canada, South-East Asia, United Kingdom 40
Industry distribution 42
Sub-Industries: Finance, Prof. Services, Manufacturing, Education 42
A difficult choice to make – too big, too small, too political, too poor 48
7. Disrupting Cy-X **50**
Law enforcement activities 52
8. Outlook to 2023 ..... **56**
9. Report summary **60**
Appendices **62**

Executive summary

State of cyber extortion

Cyber extortion (Cy-X) attacks have become increasingly prevalent in recent years, posing a significant threat to organizations of all sizes and industries. These attacks involve threat actors gaining unauthorized access to a victim organization's IT network and data, then threatening to publish, encrypt, or destroy the data unless a ransom is paid. They can take various forms, including ransomware attacks, where attackers encrypt a victim's data and demand a ransom to provide the decryption key, or distributed denial of service (DDoS) attacks, where they flood a victim's website or network with traffic to disrupt their operations until a ransom is paid.

In response, many organizations are turning to threat intelligence as a critical tool to understand the threat landscape to then identify their vulnerabilities and increase their security posture. By gathering, analyzing, and sharing information about potential or existing cybersecurity threats to their critical assets, they can anticipate and mitigate these threats proactively, rather than reacting to them after the damage is done.

This report provides organizations with an overview of the trends and patterns observed in the cybercriminal ecosystem in 2022. It highlights key findings and insights, including changes in the type and frequency of cyber extortion activities, the impact of geopolitical tensions on cybercrime, and the evolving techniques used by threat actors. To compile it, Orange Cyberdefense collected and analyzed data from 2,110 victims of Cy-X attacks across the globe.

- Overall, the findings show a fluctuation in the number of victims across different countries and industries, with cyber extortion activities expanding to new regions. The number of Cy-X victims fell by 8% compared to previous years, but we anticipate this to be a temporary drop and the number of attacks to increase in the first half of 2023.
- The US and Canada, which have been among the most heavily impacted by Cy-X historically, experienced the greatest decline in the number of victims. Whereas there was an increase in the number of Cy-X victims in the Nordics, Southeast Asia, and Latin America.
- Across the industries, the number of Cy-X victims in the Manufacturing, Professional Services, and Retail Trade industries declined. However, this decrease was offset by an increase in the number of victims in other sectors, including Utilities, Educational Services, and finance and insurance.
- While threat actors previously prioritized larger organizations, last year the number of victims was almost equal across large, medium, and small organizations. Although large and small organizations were slightly more affected than medium-sized.

As Cy-X attacks continue to rise, it's important to understand the underlying trends and geopolitical pressures that contribute to these activities. Threat actors are constantly adapting their tactics to evade detection and exploit vulnerabilities, making it essential for organizations to stay informed and prepared.

The underground marketplaces of the cybercrime ecosystem also offer a wide variety of services, information, and tools to threat actors. Among them, credentials are highly valued as they provide access to systems without the need for identifying vulnerabilities. Phishing attacks and credential brute force are still prevalent, while both old and new vulnerabilities are exploited if they prove to be reliable and effective. Additionally, there has been a resurgence in the use of Search Engine Optimization (SEO) abuse as a social engineering technique to exploit victims.

Cy-X activities were notably affected by the war in Ukraine. Although, it only resulted in a temporary slowdown, providing threat actors with an opportunity to regroup and resume their attacks. But as many countries have taken a firm stance on either side of the conflict, which resulted in heightened geopolitical tensions, publicly declaring allegiance to one side or the other may have attracted the attention of attackers who are opposed to that position.

While the collaboration between law enforcement agencies worldwide has sometimes been successful in disrupting cybercrime, threat actors have a ruthless and determined mindset which means that despite facing increased security measures, they are continually evolving their tactics to circumvent police actions and restrictions.

Overall, having a strong understanding of the current threat landscape, allows you to anticipate potential threats to your organization and take proactive measures to protect your critical assets and enhance your cybersecurity posture.

General trends:

- Over 2,100 organizations globally were publicly referenced as a victim of Cy-X in 2022 (with many more still unknown).
- LockBit has dominated the Cy-X criminal ecosystem in 2022, accounting for almost half of all victims (800+ victim organizations from 60+ different countries).
- In 2022, we monitored 69 active threat actor groups, 38 of which operated a leak site on the dark web to extort their victims.
- The decrease in the number of Cy-X victims could be attributed to the war in Ukraine and its indirect implications (financial sanctions for instance), and we expect to see an increase in Q1 2023.
- From 2021 to 2022, we observed 16 Cy-X actors undergo transformations, 19 of them were identified as new players, indicating that they were not related to existing groups.
- We have seen positive developments in law enforcement agencies and governments taking action to disrupt the Cy-X criminal ecosystem, including arrests of criminals, infrastructure takedowns, money seizures, international sanctions, development of decryptors for victims, and "hack back" activities.

Victimology (Country/Industry/Business size):

- Businesses from 96 different countries were impacted by Cy-X in 2022. That means half (49%) of all countries in the world have been victimized by Cy-X (and those are only the countries we know about).
- There has been a notable shift in the geographic distribution of Cy-X victims.
- We saw a decrease in the U.S. (-21%), Canada (-28%) and Europe (-2%).
- The biggest increase was in the Southeast Asia region (+42%), the Nordics (+40%) and Latin America (+32%).
- Countries are typically targeted based on opportunity, and the number of victims within a country is primarily determined by the number of registered organizations in that country.
- 50% of the victims impacted by Cy-X belong to the top 30 countries with the most businesses.
- The top three industries/verticals that were impacted the most in 2022 showed a considerable decline compared to 2021: Manufacturing (-39%), Professional Services (-25%), Retail Trade (-11%)
- Instead, in 2022 we saw more victims from the Utilities sector (+51%), Educational Services (+41%), finance and insurance sector (+11%) and healthcare sector (+5%).
- A deeper examination shows that within Manufacturing, food Manufacturing, fabricated metal product Manufacturing and chemical Manufacturing were impacted the most.
- Organizations of all sizes were almost impacted equally. Although, large and small organizations have been targeted slightly more than medium-sized.
- Victim organizations' ransom demand is usually calculated based on their publicly listed annual revenue.
- A prominent victim (due to being in a critical sector or having major brand recognition) may attract more attention from cybercriminals.

TTPs:

- Phishing remains the top initial attack vector, closely followed by exploiting vulnerabilities and bruteforcing open RDP.
- On average, cybercriminals are capable of leveraging vulnerabilities within 29 days of disclosure.
- SEO poisoning has been used more often by cybercriminals since Q3 2022.
- Each stage of an attack relies heavily on a component of cybercrime-as-a-service, and very few cybercriminals are now responsible for the entire attack chain.
- Encryption can happen in between 4,5 and 7 minutes.
- In 2022, some of the malicious encryption code developed by the groups we monitor, and the gangs' own Operational Security, exhibited significant flaws.

Ukraine war:

The war in Ukraine has influenced the Cy-X criminal landscape to some degree, as the Conti group's alignment with Russia has instilled a political dilemma in an ecosystem typically driven by financial incentives.

Our investigation into whether NATO member countries were more affected since the war did not find any supporting evidence. Instead, we found that non-NATO countries were impacted more frequently in this period, including Brazil, Australia, Switzerland, Thailand, and Taiwan.

Overall, in 2022, 74% of the Cy-X victims were from NATO countries, while 26% were situated in non-NATO countries.

We also examined whether Finland and Sweden have been more affected by cybercrime since their official applications to join NATO. While we noticed an increase in victims from these two countries, the number of victims is still relatively small and may not be statistically significant. However, we anticipate there will be consequences led by Russia following Finland's successful NATO membership application.

In conclusion, the war and its outcomes have affected the Cy-X ecosystem similarly to other aspects of cyberspace, as cyber has become a tool of war.

Introduction: Understanding cyber extortion

Anatomy of a digital crime scene

We recorded 2,110 victim organizations of Cy-X leak sites on the dark web in 2022. We define Cy-X as a form of computer crime in which the security of a digital asset (Confidentiality, Integrity or Availability) is compromised and exploited in a threat of some form to extort payment.

As part of our research, we observed a slight decrease in the number of Cy-X victims in 2022 compared to previous years, whereas in Q1 2023 there now appears to be a significant increase. The reason for this is still unknown, however, one potential explanation could be the ongoing war in Ukraine and its indirect implications such as economic sanctions. We will explore the potential impact of the war on the Cy-X ecosystem in a later chapter. Another reason could be the fast-moving cybercrime ecosystem. While several criminal operations were shut down during 2022, new ones quickly opened and took their place.


POLICE LINE DO NOT CROSS
POLICE LI

Orange Cyberdefense has been collecting victim data from leak sites since January 2020. During this time, we collected data from over 6,500 organizations that have fallen victim to cyber extortionists. It is worth mentioning that the numbers we have collected are consistent with the information available on other publicly available reports. However, those numbers are not the full picture. The victims we observed on dark web leak sites are only a portion of the entire attack chain. This data does not disclose the victims who have been breached but have not been publicly identified by a threat actor in a double-extortion scheme. Nor does it include organizations that have chosen to pay the ransom for economic reasons and, as a result, do not appear on leak sites.

Furthermore, not all threat groups maintain a leak site, and despite our efforts to monitor their tactics, techniques, and procedures, these groups are not included in our overall victim count. This means that there is a significant number of unreported victims, commonly referred to as the "dark number". This dark number represents the number of victims that we cannot see. Like an iceberg, there is much more hidden beneath the surface.

Methodology

We scrape the dark web to monitor the cyber extortion threats and document victim organizations being publicly named and shamed on those sites. Additionally, Orange Cyberdefense monitors relevant cyber extortion operations on a daily basis.

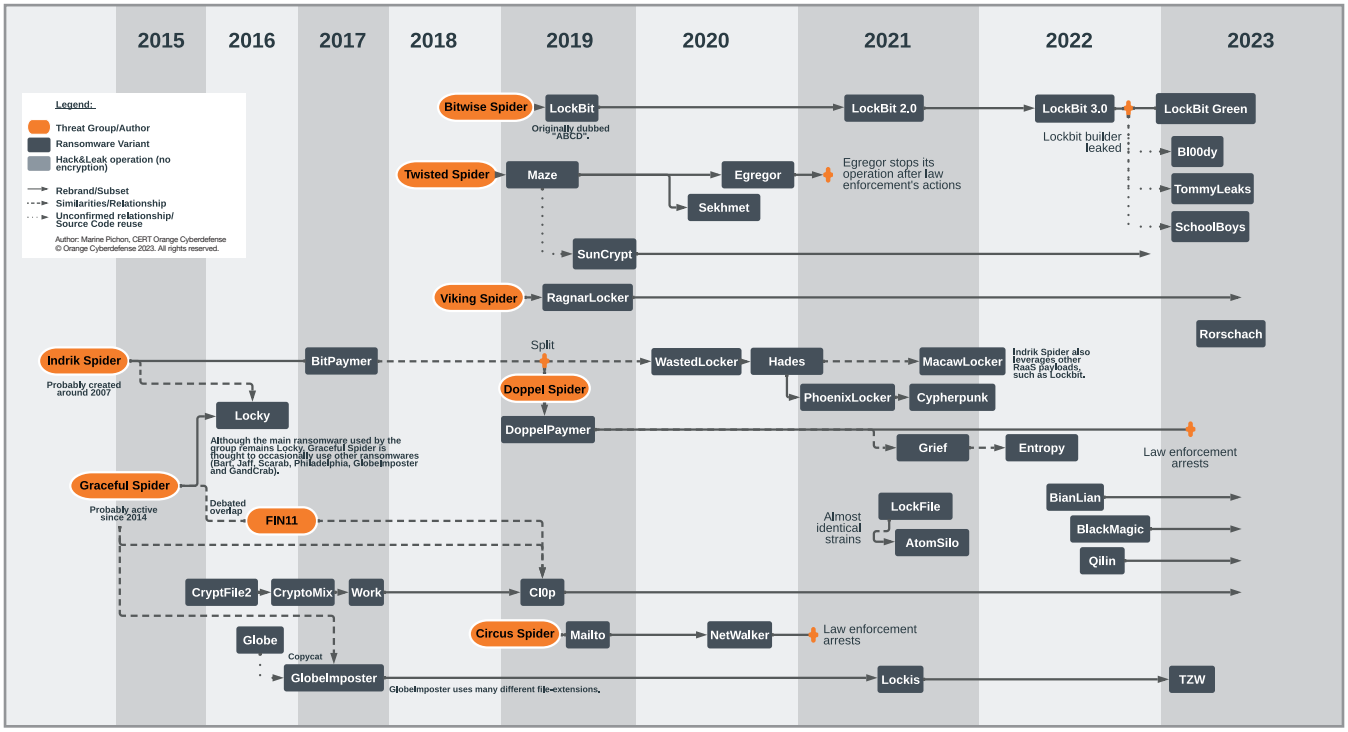
Since December 2022, our cyber threat intelligence (CTI) analysts have been working on a graphical map of the ransomware ecosystem.

It is frequently updated to track the fast-changing developments of the various threat actors (ransomware and data extortion gangs) including their relationships and attempts to “rebrand” into new operations.

On top of collecting the activity (victim count, threat actor group/variant, time stamp) we study the victim organizations to document which country they are headquartered in, which sector and sub-industry they belong to and which business size category (by employee count) they are in. Additionally, we look at the leak itself and document how much data was stolen, what type of data was stolen and if the leak is still online or if it has been removed since its first appearance. This could potentially mean that threat actors and victims have come to an agreement.

And lastly, over the past years, we have increased our efforts to use as many well-established data classification frameworks as possible. While this is a tough nut to crack in our industry, we strive to use classifications that can be re-used and applied by others without further mapping into yet another classification system. For our industry classification, we use NAICS code 2022[1]. For the business size classification, we use the OECD as a framework[2]. For any incident and event description, as well as country codes of victim organizations, we use VERIS[3].

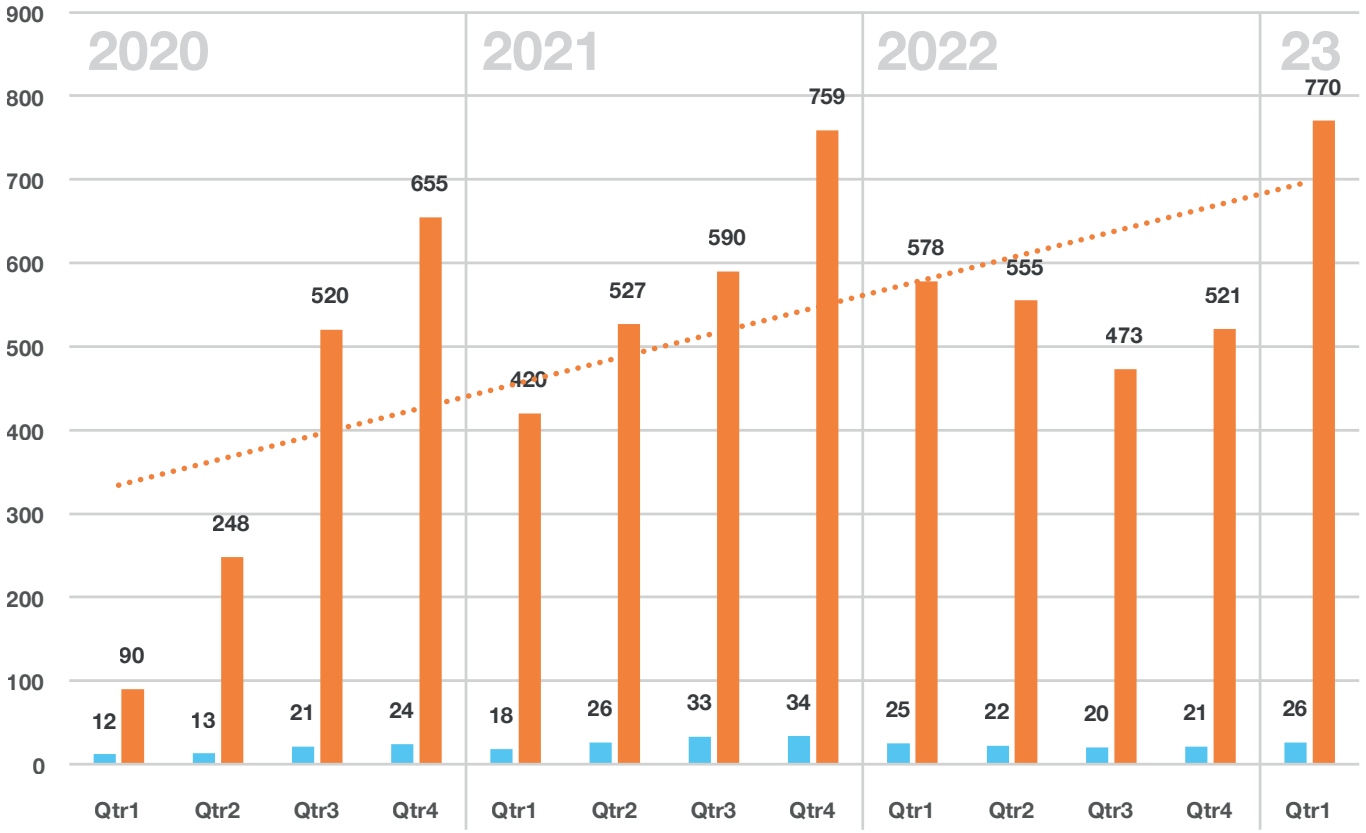
All these efforts result in a victim database of 6,707 victims that were publicly exposed on Cy-X leak sites between 2020 and 2023 (Q1), by 88 unique threat actors, as outlined above.



- **The latest PDF version of this map is publicly released on GitHub.**

Cy-X victims over time

Observable victims on leak sites and distinct actors



Criminal groups involved in Cy-X

Threat Actors

Most of the data charts in this report are based on threat actor groups with a leak site.

A list of other threat actor groups that we are considering for this report can be found in Appendix A. We tracked 69 different Cy-X threat actors in 2022 (38 with a leak site), for which we recorded:

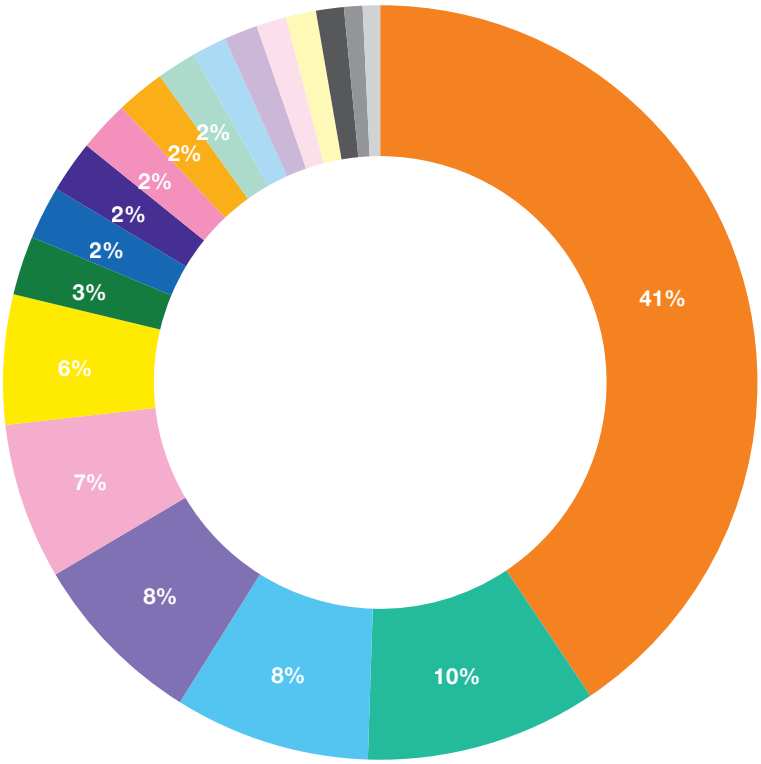
- Whether they run as a Ransomware-as-a-Service (RaaS) operation.
- If they were active in 2022.
- Whether or not they 'only' exfiltrate data to extort money or encrypt and execute other extortion techniques also.

In 2022, we collected the victim data of 38 different groups with leak sites that victimized organizations around the world.


4'9"
4'6"
4'3"
4'0"
3'9"
3'6"

Cy-X Threat Actors 2022

Threat Actors that operate leak sites observed in 2022



- 41% LockBit2 & 3
- 10% ALPHV (BlackCat)
- 8% Black Basta
- 8% Conti
- 7% HiveLeaks
- 6% ViceSociety
- 3% Royal
- 2% Quantum
- 2% Snatch
- 2% LV
- 2% Cuba
- 2% RagnarLocker
- 1% Clop
- 1% BlackByte
- 1% BianLian
- 1% Lorenz
- 1% AvosLocker
- 1% Play
- 1% SunCrypt

The threat actor responsible for the most recorded leaks is LockBit. In mid-2022, LockBit2.0 re-branded to LockBit3.0 and together these two malware families have victimized over 800 organizations from over 60 different countries. LockBit still hold the lead in 2023 and are followed by ALPHV (a.k.a. BlackCat) with an even number of 200 victims for 2022. BlackCat began shaming victim organizations in November 2021, and at the time of writing this report is still active. Thirdly, BlackBasta has victimized 169 organizations since April 2022 and continues to do so at the time of writing.

The threat actors at position four and five are a good example of operations that were forced to close. As some readers might be aware, Conti had been drawing a lot of (un-) wanted attention shortly after the war against Ukraine began. After it publicly announced being pro-Russia, Conti suffered an internal leak from a presumed disgruntled Ukrainian member, which eventually lead to the end of their criminal activities under the Conti name.

Although the event may have been externally influenced, Conti chose to exit under this brand itself. The threat actor group called 'Hive' on the other hand was compromised and shut down by US law enforcement in January 2023, which we will dive into more specifically in chapter 7 "Disrupting Cy-X".

Both the examples above show how abruptly groups close operations. But others are consistently eager to fill up the space. We will talk more about this phenomenon of 're-branding' in the next chapter.

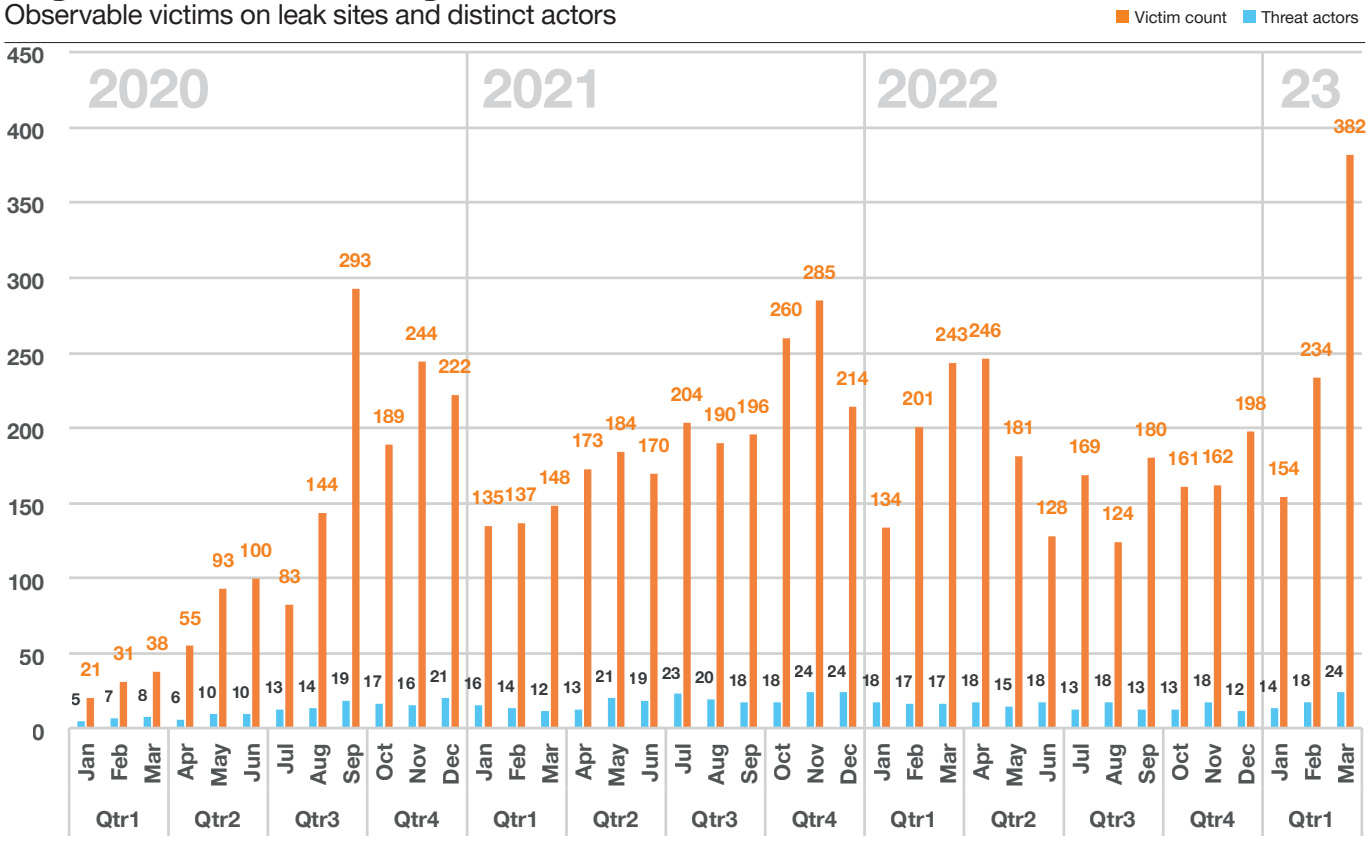
If we explore how the impact of threat actors changed between 2021 and 2022, we can see that threat groups are very volatile. Groups such as REvil, Avaddon, Conti, Grief and Prometheus closed operations or have been inactive between 2021 and 2022. On the other hand, we see threat actors' groups that have been very active in 2021 and 2022. Either they began operations in 2022 or they had an increased number of victims in 2022 in comparison to the year before.

Besides the groups that were already mentioned above due to their high victim count, we see long lasting groups such as RagnarLocker (+19 victims between 2021 and 2022), Quantum (+45) and Vice Society (+51). Vice Society bulk uploaded almost two dozen victims on the 19th of December 2022, half of which were from the Educational sector.

Looking at the victim count of 2022, we see a decrease, both in victim count and in unique threat actor count (see the chart on the next page). This is unusual since in the previous two years Q3 and Q4 have been the busiest periods.

Cy-X victims by month

Observable victims on leak sites and distinct actors



We suspect that what we're seeing in this decline might only be a temporary pause in activities. Indeed, from the Q1 2023 victim data we already have in, we can see an all-time high of victim counts in February and March of 2023.

One possible explanation for this apparent 'respite' could be the war in Ukraine, which disrupted the criminal ecosystem to some degree.

We dedicate the entire **chapter 3** of this report to the apparent impact of the Ukraine war on the Cy-X crime. Our assessment is that, rather than spawning a wave of cybercrime as many expected, threat actors were distracted by the ongoing war but are gradually returning to their criminal activities.

A second contributor to the 2022 slowdown might be the hole that was left when the Conti group disbanded, which led to the noticeable decrease in Q3 and Q4. By the end of 2022, however, some members of the Conti group resurfaced in new groups such as Royal, BlackBasta or Quantum[4].

Another factor to bear in mind is the time it takes from when the victim is compromised and exploited to when the victim becomes publicly known. We emphasize again that our view of this crime is generally only of the last stage of the attack chain.

From the time when Initial Access Brokers (IABs) have gained access to the victims' network and sold the access online, to the time when a buyer makes use of this access to further extort the victim and negotiate with them, many months could have passed.

This suggests that the trends we observe in leak site victim numbers portent to criminal activity that may have commenced much earlier.

Can we see a correlation between volume of access being sold and Cy-X victims being posted?

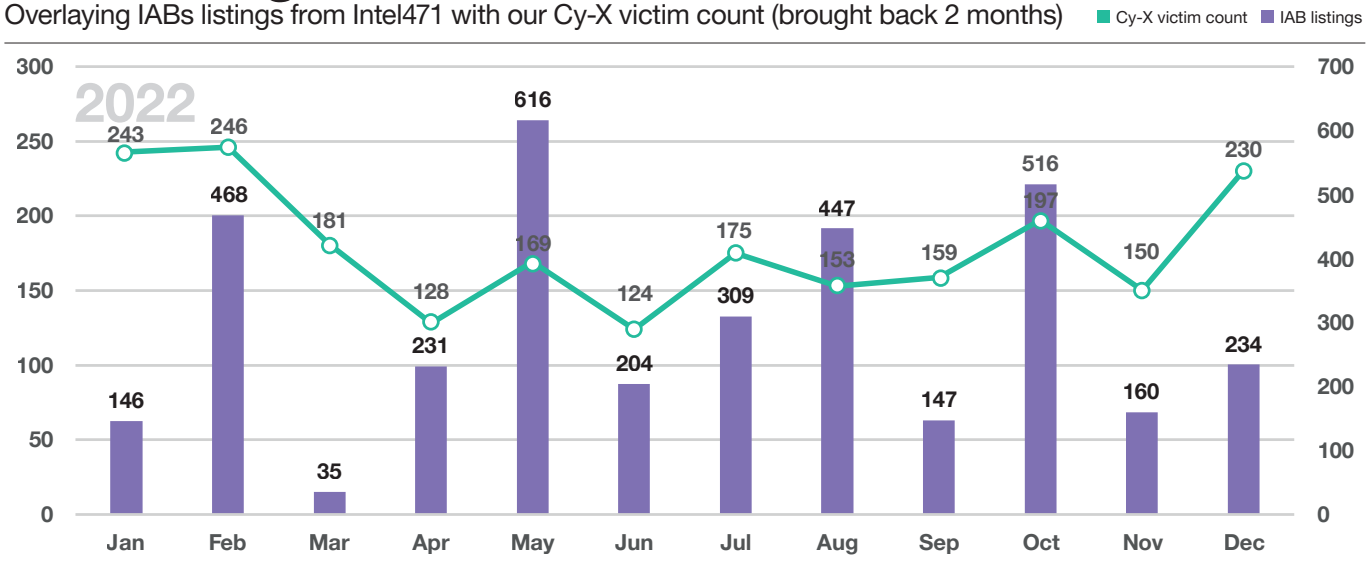
Intel471 examines exactly that question by collecting data from the dark web and tracking Initial Access Brokers' (IAB) activities. Orange Cyberdefense collaborates with Intel471 on a continuous basis, and we asked Intel471 to share some data on the number of accesses sold by IABs on the dark web.

The IABs listings are not only used for cyber extortion but many other forms of unauthorized access and further victimization. But we do know that cyber extortion groups and their affiliates in some cases work very closely with IABs and their so-called Initial Access Brokerage services[5] to gain remote access to compromised networks.

As we are currently exploring the apparent hiatus in observable Cy-X, we are curious about whether we might see such a delay by combining our victim data with Intel471's IABs data. In the chart on the following page, we consider two months delay between the access being sold, and an organization becoming a victim of a Cy-X attack and after failed negotiations, ending up on the leak site.

IAB listings vs. victim count

Overlaying IABs listings from Intel471 with our Cy-X victim count (brought back 2 months)



As can be seen, we do see similar trends in the volume of listings in both datasets. The x-axis represents the timeline of the IAB listings on the dark web, while the Cy-X victim count undergoes a two-month delay, meaning that in January we see 146 accesses being sold, resulting in 243 victims being posted in March 2022. The 468 access listings in February, result in 246 victims that were posted in April in the Cy-X timeline; and so forth.

Interestingly, when we combine both datasets, we notice a significant drop in selling accesses in March – just after the Ukraine war began – that almost determines a much lower number of Cy-X victims throughout 2022.

We do however know that correlation between those two datasets is difficult, the delay is very dependent on how the sale of the access goes and when the access is being used for criminal activities.

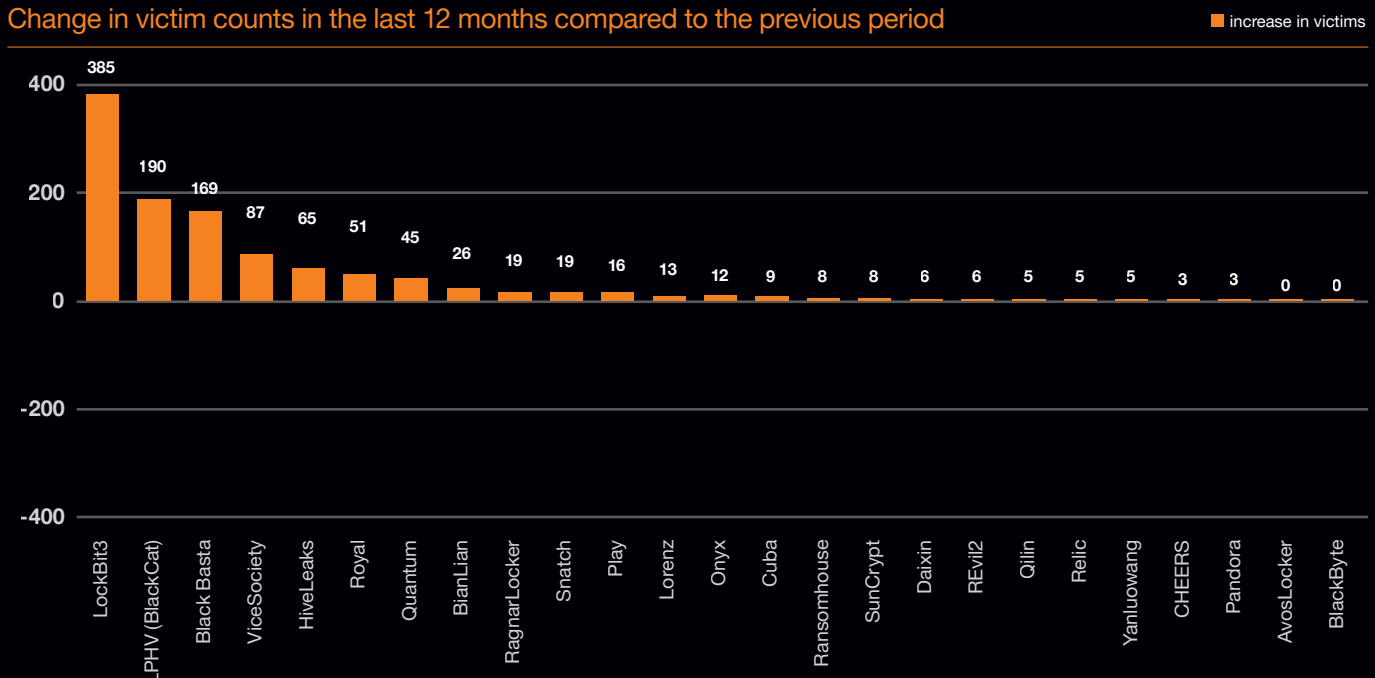
In the next chapter we will outline what movements of Cy-X victims we tracked during 2022.

Tracking re-brands and affiliation over time

Rebranding is common among ransomware groups. A new name is often taken, either because the group merged with another one, or because the group split into sub-groups. However, rebranding is also useful when a group wants to evade sanctions or law enforcement. It might also be useful when the threat actor wants a fresh start after a security failure (such as a leak of their code or a flaw in the encryption process).

Actors that claimed more victims

Change in victim counts in the last 12 months compared to the previous period



There have also been cases where affiliates formed a criminal group on their own after understanding the ransomware payload that another criminal group rented to them. Rebranding makes tracking these groups harder but isn't a fundamental obstacle.

One of our research objectives is to track threat actors and the malware they use. When we encounter a new ransomware name or a new threat actor name, we need to determine if we are dealing with rebranded malware or groups. The fastest way is to check marketplaces and known leak sites to search for similarities with known operations.

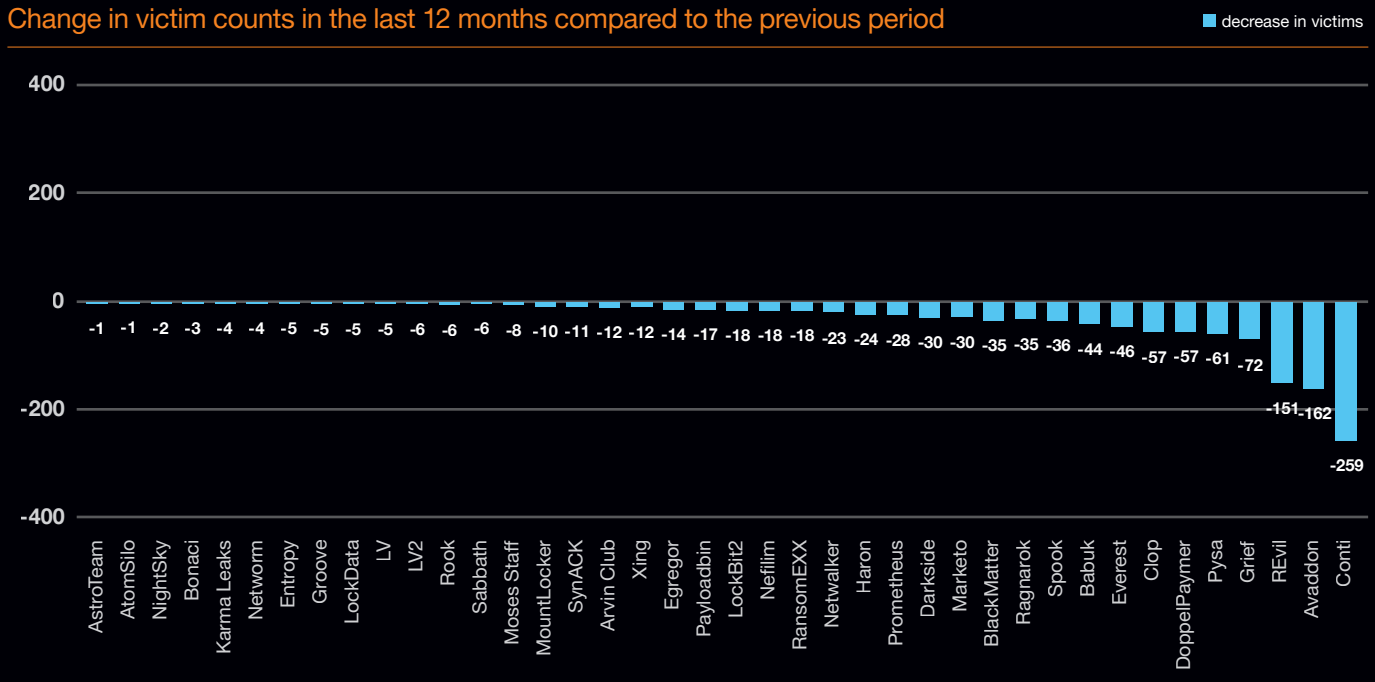
A more rigorous way is to search for matches between announced victims but also overlaps in the pseudonyms criminals use to announce their victims on forums or leak sites.

Our Cybercrime Monitoring Team focuses on tracking such evolutions every day. However, open-source intelligence is often not enough, and it is necessary to conduct in-depth source code analysis to identify overlaps with known groups' payloads and TTPs. Our reverse engineers help us confirm whether one strain is based on another.

On the one hand, leaked documents are very useful when it comes to understanding the internal organization of a threat actor. On the other hand, it pushes threat actors to improve their security, which might lead on to rebranding. Among threat actors, leaks and doxing are being used as a weapon to disrupt rivals, which is what likely happened to the threat actor Yanluowang on the 31st of October. However, they might also be the result of an internal fight, as was the case for Conti.

Actors that claimed fewer victims

Change in victim counts in the last 12 months compared to the previous period

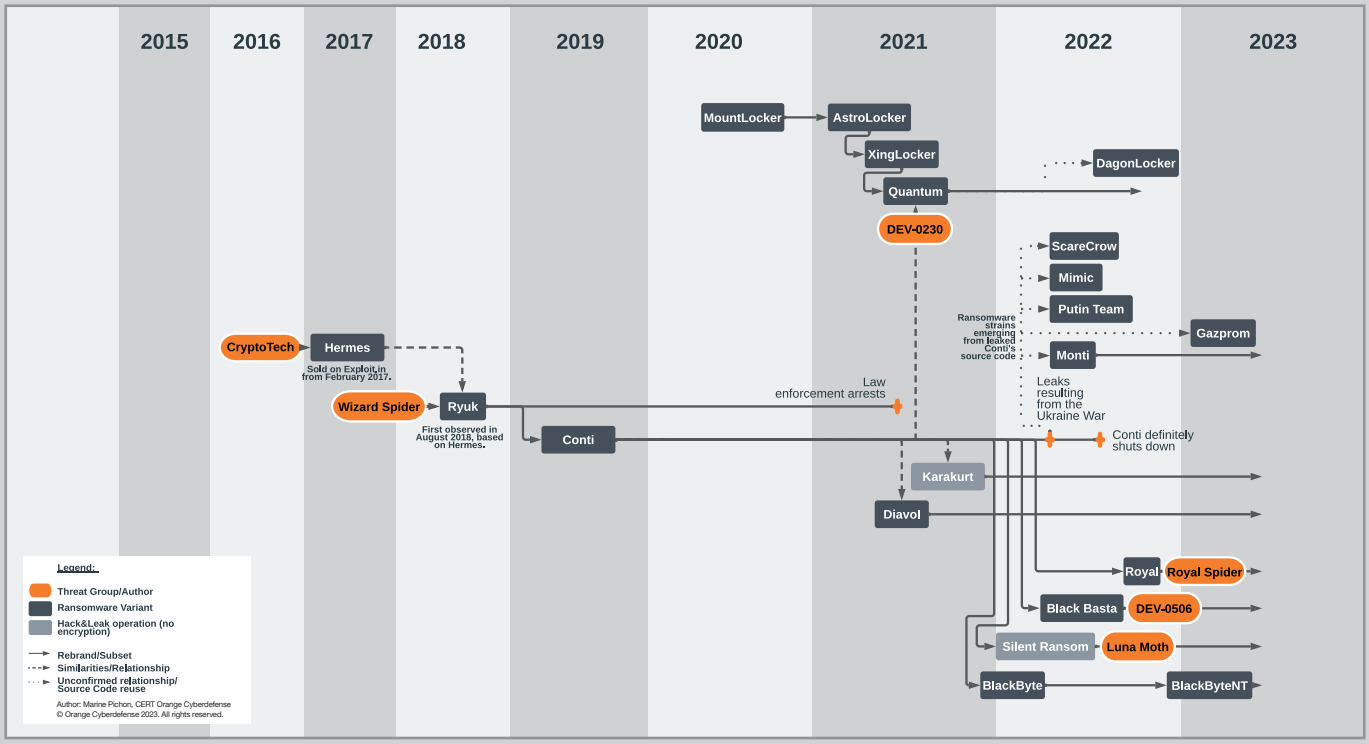


The case of Conti: division and rebranding

The most significant rebrand in 2022 came out of Conti shutdown. Active from 2019, Conti's latest operation was the ransomware attack impacting nearly thirty public institutions from Costa Rica, which led the president of the country to declare a state of national emergency.

Even if the group had already started to divide up in early 2022, the unexpected internal leaks following the start of the war in Ukraine forced Conti to speed up the dismantling of its RaaS operation.

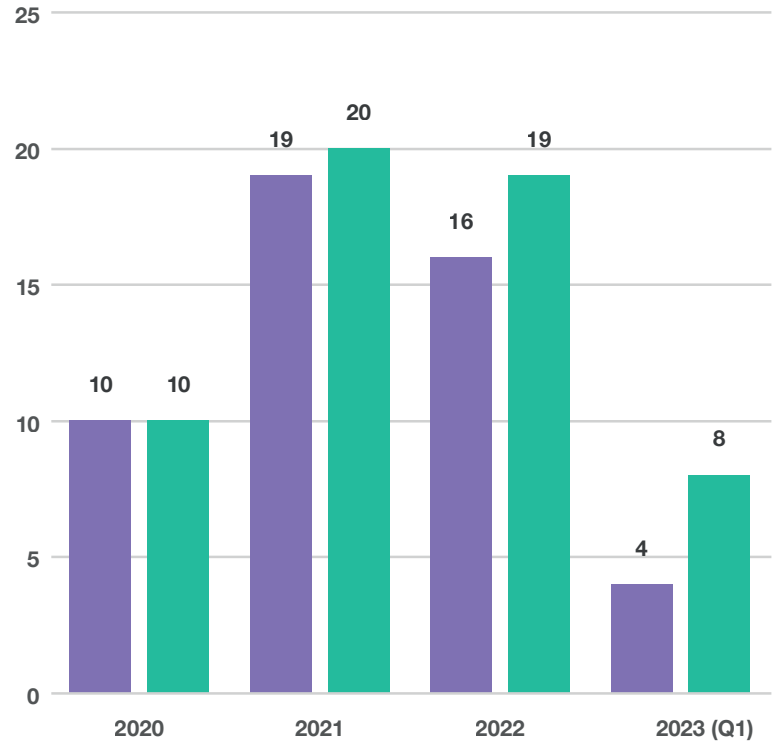
As a result, Conti divided itself into smaller operations such as Royal, Black Basta and BlackByte, which are all still active today. Allegedly published by a Ukrainian security researcher, the leaks contained internal chat conversation but also source code for the Conti ransomware encryptor, which gave birth to at least five new ransomware strains: Monti, Mimic, Putin Team, Meow and ScoreCrow.



Orange Cyberdefense World Watch's ransomware ecosystem map tracks ransomware rebranding dating back to 2015.

New actors vs. rebranded ones

Number of ransomware operations performing Cy-X identified from 2020 to 2023 (Q1)



The rise of new actors in 2022

As we have already pointed out, tracking cyber extortion groups is a full-time job, and the nature of their different functions and roles can make it difficult to accurately track and interpret changes in the ecosystem.

It is clear, however, that the systemic forces that enable cyber extortion persist, so one group's disappearance is simply another's opportunity.

Thus, we have observed several new groups during 2022. 19 new threat actors were identified in 2022, compared to 20 in 2021, suggesting the cyber extortion ecosystem remained relatively unchanged for two years.

This chart, once again based on the Orange Cyberdefense World Watch, highlights the number of threat actors that emerged between 2020 to 2023 (Q1).

Conclusion

Because of its 'fluid & flexible' nature and the difficulties attributing individuals to actors and threat actor groups, we don't know how big of a problem we are dealing with. As several others have termed it[6], we are experiencing a 'gig economy' approach to Cy-X, meaning that individual threat actors are renting and selling their services, ready-made tools and code is re-used and 'workers' are only temporarily joining the criminal group.

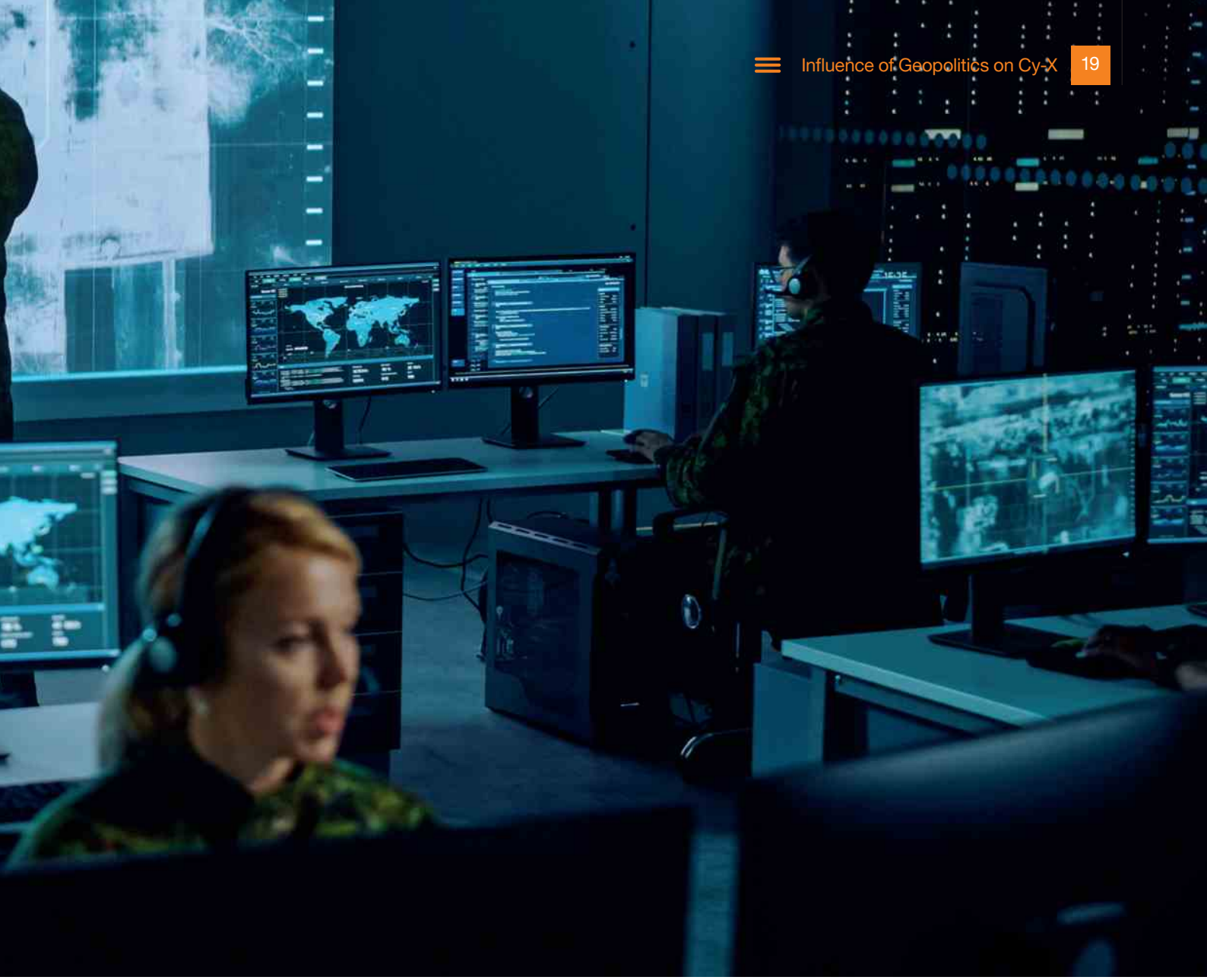
Hence, making the criminal ecosystem appear bigger than it is. As Chainalysis states in its latest Crypto Crime Report "A rideshare driver may have his Uber, Lyft, and Oja apps open at once, creating the illusion of three separate drivers on the road — but in reality, it's all the same car[7]."

The influence of geopolitics on Cy-X

Did Russia's invasion impact the Cy-X ecosystem and the choice of victims?

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.

In this chapter, we will more closely examin what impact the Ukraine War had on cyber extortion, especially in terms of victimology.



Before the war

Russian state-backed cyber operations against Ukraine have been a common occurrence since at least 2013, with the so-called 'Black Energy' incident, which denied power to hundreds of thousands of Ukrainians for several hours, being a notable example. The most (in)famous incident, however, became known as 'NotPetya'.

This 2017 variant of the Petya family of malware was spread via the software update mechanism of M.E.Doc - an ubiquitous Ukrainian tax preparation program - allegedly by the infamous Sandworm APT, which is part of the Russian GRU (the General Staff of the Armed Forces of the Russian Federation).

Given the long-held belief that several criminal gangs have very close relationships with the Russian state apparatus, there was a reasonable expectation that criminal cyber activities would accelerate in support of Russian state activities on the ground and in cyberspace.

War disrupts

In 2022 many factors impacted the Cy-X ecosystem, but the war in Ukraine is likely the most important one.

Since the invasion, with a few notable exceptions, Russian state-backed APT groups have primarily used wiper attacks to target critical Ukrainian entities, sometimes masquerading them as ransomware like (WhisperGate, HermeticWiper, IsaacWiper and CaddyWiper) and coordinated DDoS attacks.

As the war escalated, many expected cyber-attacks on Ukraine and the West, including financially motivated cybercrime, exploded. Apart from an obviously increased level of animosity toward the West, one of the predictable consequences of the war was the end of the cooperation between Russia and the West against cybercriminal activities conducted by Russian citizens. Before the beginning of the invasion, following the ransomware attacks against major organizations such as Colonial Pipeline and Kaseya, Russia had been facing massive pressure from the US to act against cybercriminals within its borders.

This eventually may have led to the unexpected arrests in Russia of 14 members of the notorious REvil cyber extortion group in January 2022. But with the war now in full swing, and possibly lasting years, any cooperation between Russia and Western countries is likely over for a long time, resulting in Russia remaining a safe harbor to launch cyber-attacks against enemies of the Russian state.

Once the Russian invasion started, many envisioned more attacks from pro-Russia criminal groups against Ukrainian and Western entities in support of Russian military goals. But this dire prediction failed to materialize.

While opportunistic by nature and financially motivated, we have always understood many cybercrime gangs to have a close relationship with the Russian state. Why then, with means, motive, and opportunity so apparently in place, were the Cy-X gangs apparently less active than in previous years?

One of the apparent contributors to the decline in Cy-X victim numbers was the collapse of the Conti group. On February 25, Conti was (one of) the only groups openly taking a pro-Russian position, and it paid a heavy price for it. Another Ransomware-as-a-Service group, CoomingProject has also taken a pro-Russian stance and was targeted afterwards. Indeed, the pro-Ukraine group AgainstTheWest doxed six members of CoomingProject, claiming that they were based in France. As a result of these claims, the group's Telegram channel was taken offline.

For RaaS gangs, taking a pro-Russian position against Ukraine appeared to be an unwise decision, as many top affiliates lived and worked in Ukraine. Following this backlash, other Cy-X gangs like LockBit and BlackCat took a neutral position in the conflict, claiming they were only interested in money.

NATO countries

Looking at the overall decrease in Cy-X victim numbers over the year, we were curious about whether Cy-X victim counts in NATO countries increased since the full invasion of Ukraine began in February 2022. Here we consider the country in which the victim is headquartered and whether the country is a member of NATO.

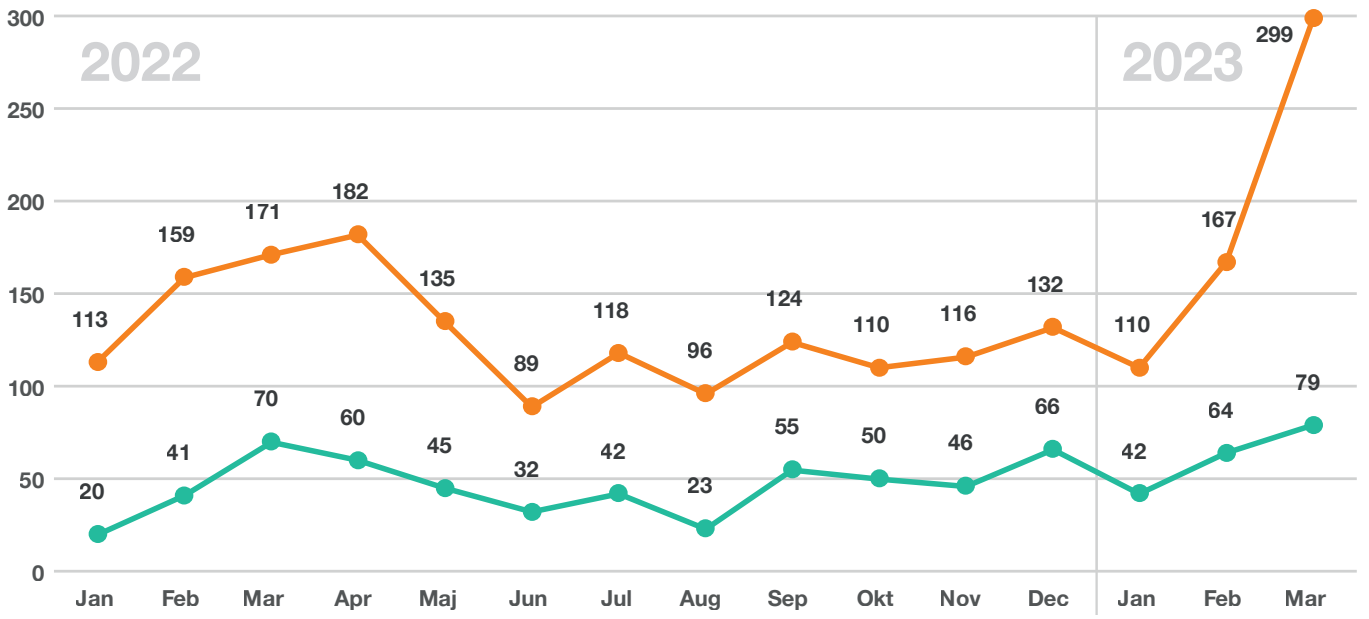
Of the 31 member countries, 28 countries are present in our victim data and only Iceland and Latvia – to our knowledge – have not seen victims of Cy-X between 2020 and March 2023. At the time of data analysis, Finland had not joined NATO yet, and was therefore not included in this grouping.

As you can see in Fig.4, NATO member countries are generally more affected by the Cy-X threat than others. In fact, of the victims in our data set, 74% are in NATO member countries and 26% operate in non-NATO countries. In March 2022, just after the war began, we observed a curious, temporary increase in non-NATO victims.

How this is influenced by the political situation of the Ukraine war is not entirely clear, but it can be said with some confidence that the war has not spawned an increase in Cy-X incidents for NATO member countries.

Cy-X victims by alliance alignment

Observable victims in NATO countries and non-NATO countries



To provide a baseline, we looked at the distribution over the last two years, one year without war, one year and a few months with war. What we see is that the gap between non-NATO countries and NATO countries has decreased over the past two years, and the trend looks like we are going to see potentially more non-NATO member countries proportionally victimized and fewer NATO members, as shown in the chart below.

The chart above suggests that, as a proportion, Cy-X impacting NATO countries decreased dramatically at the start of the war and continued to decrease as the war progressed. Whatever pro-Russian threat actors were doing over this time, it apparently did not result in a proportional increase in Cy-X victims among NATO member countries.

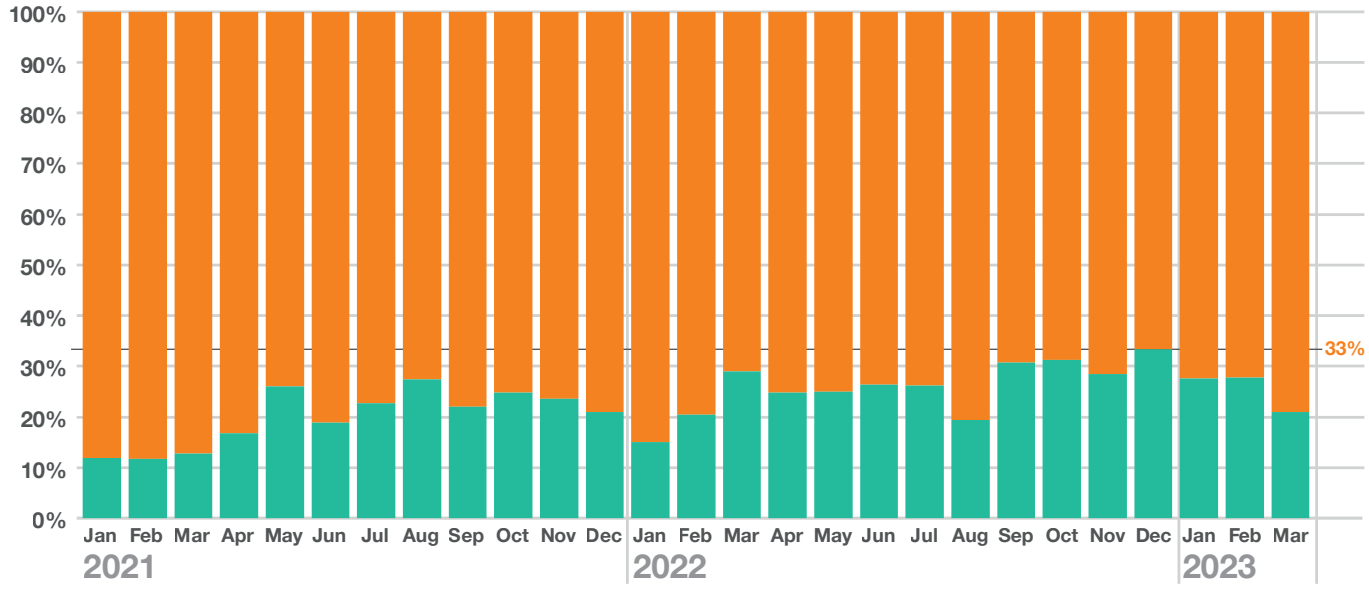
Q1 2023 and especially March 2023 show a different trend, but whether this is going to continue is difficult to predict.

On the contrary, Google's Threat Analysis Group (TAG), has reported an over 300% increase in Russian phishing campaigns directed against individuals in NATO countries in 2022[8]. Phishing is one of the major attack vectors used by threat actors to compromise their victims and gain initial access, so it is somewhat surprising that these high levels of phishing haven't translated into high levels of Cy-X.

One explanation could be that these phishing campaigns support deliberate attacks with a different end objective, like intelligence collection or destruction.

Proportion of Cy-X victims over time

Percentage of victims in NATO countries and non-NATO countries 2021-2023



History of high-Profile cyberattacks between Ukraine & Russia (since 2013)

2013 – Armageddon
Cyber-espionage campaign targeting Ukrainian government that led to the compromise of 1500+ systems

2014 – Snake
Cyber-espionage on military, energy and other critical computer networks

2015 – BlackEnergy
Malware disconnected an electrical substation causing a power outage for 200k+ consumers

2016 – Groundbait
Cybersurveillance program primarily targeting separatists in eastern Ukraine

2016 – State Treasury
Payment system outage causing disruption and 3TB of data were destroyed

2017 – NotPetya
Malware spread using MeDoc tax accounting, irreversibly encrypting data, for a total impact of ~10B USD worldwide

2022 – 2022 Assault
70+ government websites defaced (Jan-14) and DDoS attacks against the Ukraine's defense ministry and the 2 largest banks (Feb-15)

Nordic countries

Another interesting question in the context of the war is whether we have seen more victim organizations from Sweden or Finland, which in our definition belong to the region 'Nordics'. Sweden and Finland both started the process of joining the alliance of NATO after the full invasion of Ukraine by Russia. Finland formally joined NATO on April 4th, 2023[9], while at the time of writing this report Sweden is still in the process. This is indeed a historic shift and will enable northern Europe access to resources of the alliance in case of an attack.

The Kremlin reacted to Finland's membership by calling it a 'mistake', which makes you wonder whether Russia's claim of being forced to take 'counter measures' as a response could be observed in the Cy-X victim counts in our dataset. Any change in Cy-X victimology resulting from Finland's formal membership of NATO would only be observed after the timeframe we are considering in this report.

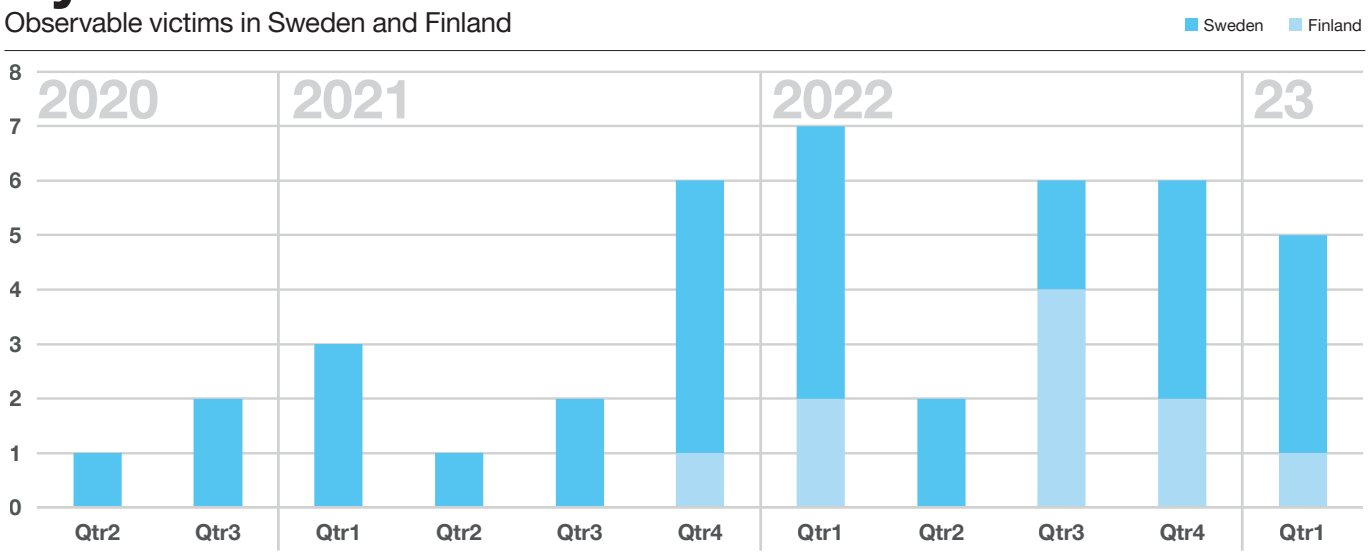
Nevertheless, the effort to join NATO has been ongoing throughout 2022 for both countries, and we could therefore expect both countries to be impacted.

As you can see in the chart below, while the total number of Cy-X attacks in Sweden and Finland is relatively small, we do observe a proportional increase in victims from both countries since late 2021. Finland saw its all-time high in Q3 2022, while Swedish victims increased notably in Q4 2022.

While our dataset of Nordic victims is too small to draw any meaningful conclusions from, we expect to continue to observe this apparent trend through mid-year 2023 as Sweden continues its efforts to join NATO.

Cy-X victims in the Nordics

Observable victims in Sweden and Finland



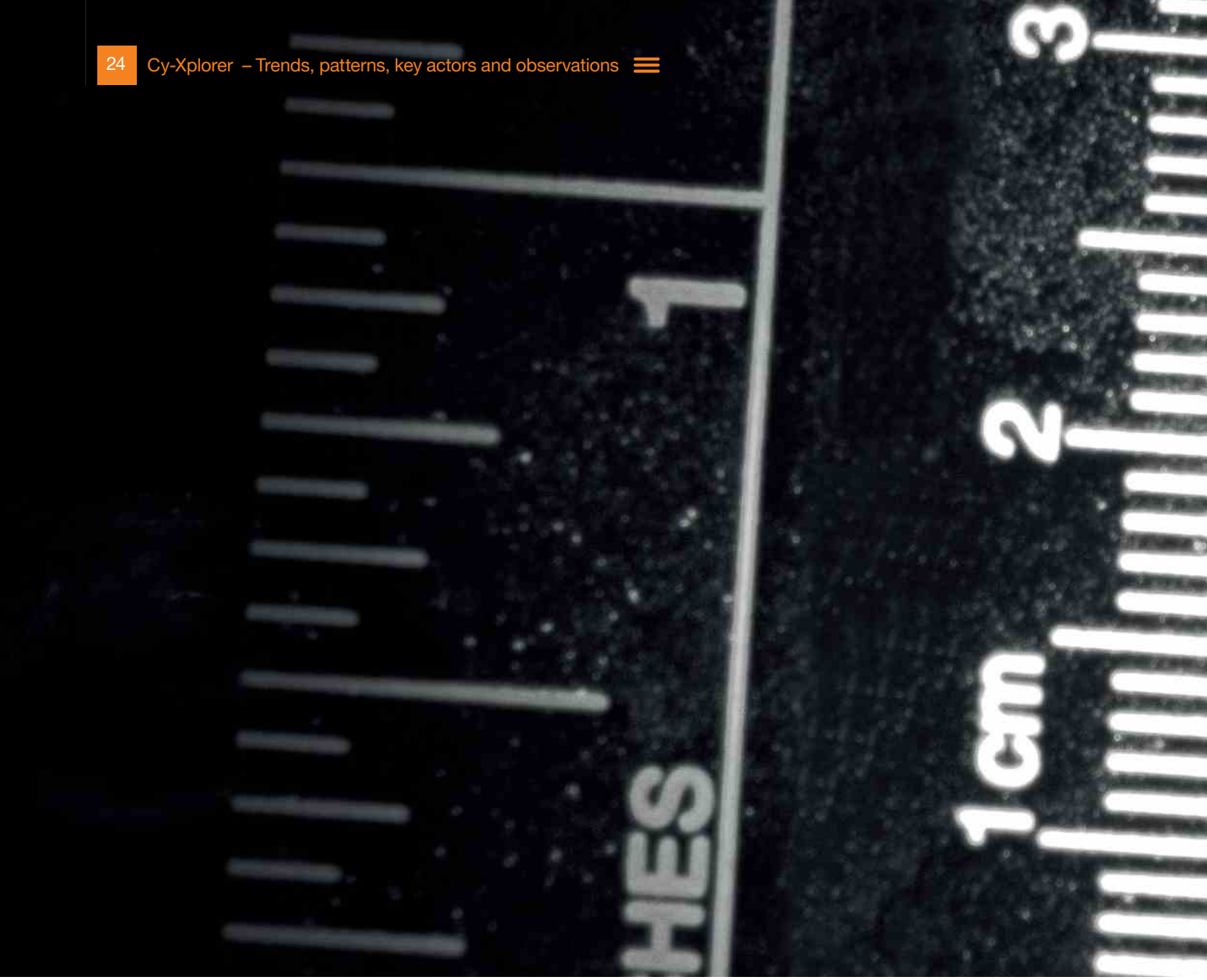
Conclusion

In the end, the victimology of Cy-X is driven by opportunity and financial motivation. As we have previously argued, we believe that the proportional number of victims in each country generally corresponds with the country's wealth. However, as outlined above, this financially motivated crime may be affected by political and geopolitical factors. Consequently, in 2022 we witnessed the ongoing war against Ukraine impact the cyber extortion landscape.

However, we have not seen clear evidence that cyber extortion increased, or that Russia's apparent enemies were impacted more, because of the war.

Certain threat actor groups have publicly announced themselves to be pro-Russian, while others did the opposite. Conti experienced a significant internal data leak by a Ukrainian researcher who taught us a lot about their criminal organization and the Kremlin very recently experienced the Vulkan files leak[10], again by an anti-war whistleblower. This shows how vulnerable data is, and that data loss can happen (literally) to anyone: a nation state at war, a threat actor group that usually makes a living off stealing data, or a Western military organization as demonstrated by the Pentagon leaks[11].

If anything, what the war in Ukraine has brought to the cyber threat landscape is a blurring of clear lines between government-backed actors and hacktivists. And what makes this war so unique is the fact that for the first time, cyber is a fully integrated component in the war.



Deep dive into the Tactics, Techniques, and Procedures (TTPs)

Convergence of delivery and diffusion on the extortion strategy

Many groups copycat the latest TTP “du jour” and fine-tune their attacks whenever a new malicious service or malware is available, or a new vulnerability is disclosed.

Some threat actors only go for low-hanging fruit, opportunistically targeting a broad range of organizations with minimal prior reconnaissance work. But some more advanced groups hunt for specific 0-day exploits to use (for example, Cl0p leveraged an unknown vulnerability in January 2023 against GoAnywhere) or ways to counter security solutions (Magniber first bypassed the Mark-of-the-Web security feature from Microsoft).


TTPs

Overall, we notice a trend toward the use of similar TTPs, because:

- Affiliates move from one group to another on a regular basis.
- Threat groups rebrand to evade sanctions and law enforcement actions.
- Many players in the field rely on common third-party cyber-crime-as-a-service providers.
- ransomware developers follow the latest security research findings (E.g., encryption flaws found by researchers).

Initial access

Initial access vectors for pre-ransomware activity range from malware sent through phishing to exploiting vulnerable Internet-facing assets (directly with vulnerabilities or through RDP bruteforcing). We observe a variety of those being used by attackers, in some cases threat actor groups gain initial access themselves, in other cases this part is outsourced to IABs who sell access to cyber extortion operations.

Phishing as top initial access vector

Looking at the initial vectors' trends in 2022, Phishing remains the top vector deployed for cyber extortion[12]. We observe multiple kind of lures sent to social engineer victims. Amongst others, we noticed for example:

- Seasonal opportunities (tax refund, pre-Christmas deliveries, or adhoc news headlines i.e., major catastrophe, diplomatic visit).
- Sectorial focus (specific logistics, HR, finance, defense lures).
- Job-related decoy documents (I.e., DocuSign, resumés, etc.).

Consequently, threat actors seem to jump on opportunities to lure their victims very dynamically, by adapting to current world events to increase the likelihood that victims will click on a link or open an attachment. The specificity of the lures can give the (false) impression of deliberate targeting.

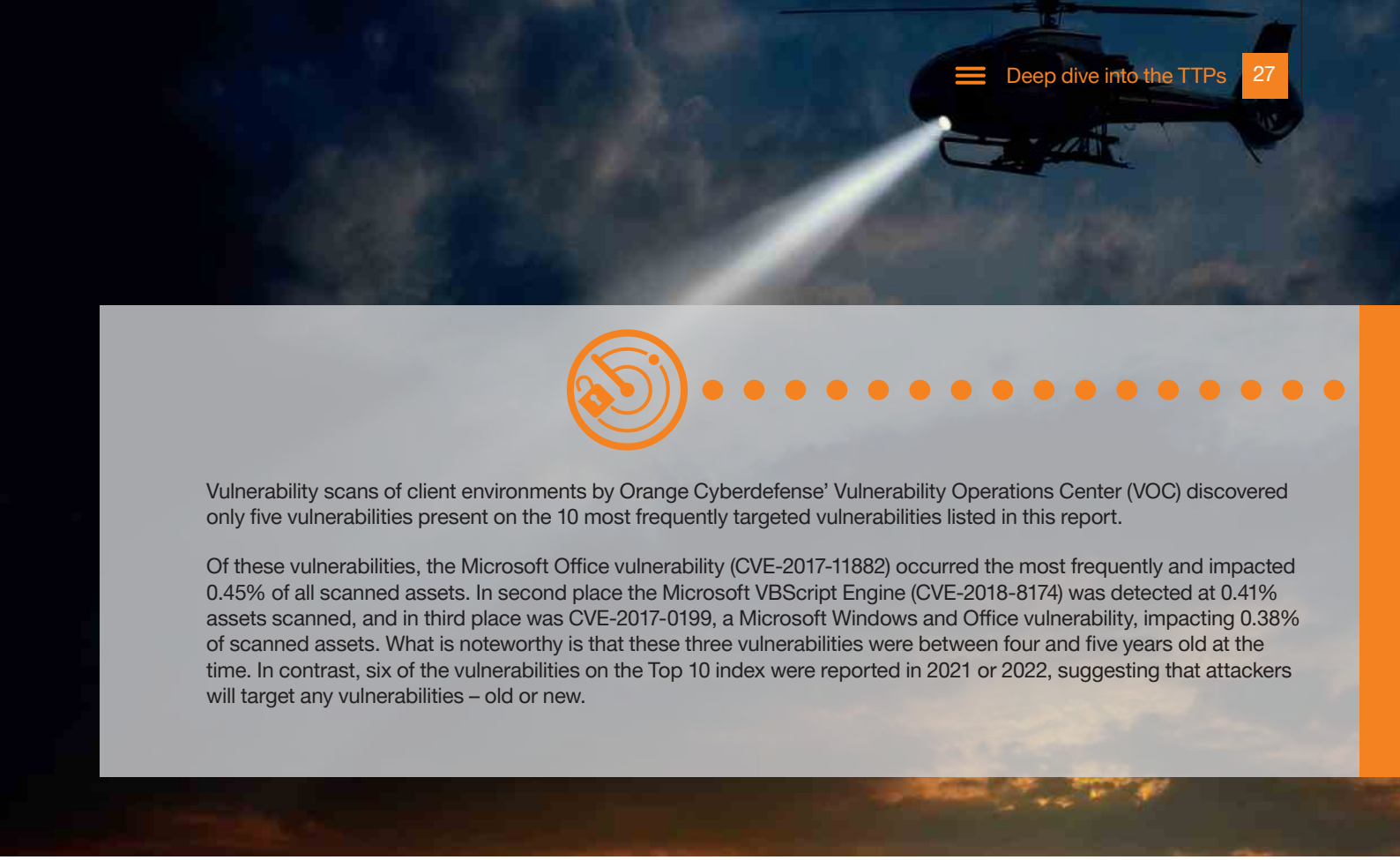
A lure that is tuned for one specific group, industry or country may be used simply because it has a high probability of success but may lead us to believe that the threat actor has a specific interest in that target group. Most IABs don't adapt to requests from ransomware affiliates, but target widely and later sell whatever accesses they managed to get to whoever is interested.

Exploiting vulnerabilities

Another significant attack vector is software vulnerabilities. Dozens of vulnerabilities were leveraged in Cy-X attacks in 2022, and numerous RDP servers were successfully brute forced.

According to Palo Alto Networks, 31% of around 600 incidents they investigated (not just Cy-X) began with a vulnerability, just less than phishing which initiated 37% of the cases. The most commonly seen vulnerabilities were not very recent, with 35% of the 56 new vulnerabilities associated with Cy-X dating from before 2019. This is in line with what our CSIRT teams observe, where the initial infection vector is listed as vulnerabilities or phishing in 28% of classified cases.

A recent report published by CSW, Securin, Cyware and Ivanti also provides an analysis of vulnerabilities used by attackers to deploy ransomware[13]. It reveals that the number of vulnerabilities exploited during ransomware attacks grew from 310 in Q1 2022 to 323 in Q3 2022.



Vulnerability scans of client environments by Orange Cyberdefense' Vulnerability Operations Center (VOC) discovered only five vulnerabilities present on the 10 most frequently targeted vulnerabilities listed in this report.

Of these vulnerabilities, the Microsoft Office vulnerability (CVE-2017-11882) occurred the most frequently and impacted 0.45% of all scanned assets. In second place the Microsoft VBScript Engine (CVE-2018-8174) was detected at 0.41% assets scanned, and in third place was CVE-2017-0199, a Microsoft Windows and Office vulnerability, impacting 0.38% of scanned assets. What is noteworthy is that these three vulnerabilities were between four and five years old at the time. In contrast, six of the vulnerabilities on the Top 10 index were reported in 2021 or 2022, suggesting that attackers will target any vulnerabilities – old or new.

The vulnerabilities affecting Microsoft Exchange (ProxyShell from 2021 and ProxyLogon from late 2020) were among the most frequently used vulnerabilities. In 2022, a vulnerability dubbed 'ProxyNotShell' – the direct descendant of Proxyshell - was used by cyber extortion groups including Play[14], within less than a few weeks of its disclosure.

While some threat actors can weaponize vulnerabilities publicly disclosed in hours or days, we were curious to know if it was possible to determine how long it could take before some flaws are targeted. To find out, we used two sources. We used the Known Exploited Vulnerabilities (KEV) catalog maintained by CISA and combined it with publicly available information produced by a Special Interest Group from FIRST.org. This data-driven effort is open and well documented and aims to assist defenders by providing a score that can be used to predict the likelihood that a software vulnerability could be exploited. We used the EPSS v2 score for this experiment as EPSS v3 was not available for the period 2021 – 2022.

To calculate the number of days to exploitation we used the number of days that lapsed from when a CVE is entered into the KEV catalog to when the EPSS value reaches or exceeds a selected threshold value. By selecting an EPSS threshold of 30% we could calculate that it would take roughly 13 days on average for all the applicable KEV CVEs available at the time to be considered exploited. If we take a more conservative EPSS threshold of 70%, then the number of days to possible exploit rises to 29 days on average.

Ultimately, certain types of vulnerabilities are more likely to be exploited than others. Attackers will gravitate to vulnerabilities that guarantee a desired outcome. We encourage vulnerability researchers to share details of newly discovered flaws with the respective vendor that maintains the software. Orange Cyberdefense is committed to sharing intelligence, as is shown on our GitHub repository[15] dedicated to the issues found by our Pentest teams.

We also know that some discovered vulnerabilities remain secret and could stay unpatched for several months or years. Some vulnerabilities that are fixed may be accompanied by proof-of-concept (POC) exploit examples, but even if the vulnerabilities do not have a public exploit, there are enough smart and capable hackers that can deduce a potential exploit. Over time, as exploits become freely available and the techniques to exploit these vulnerabilities become reliable, more people will be able to leverage the respective flaws.

LockBit, for example, simultaneously impacted hundreds of organizations by leveraging a vulnerability in an open-source component called ZK, which is embedded in a backup management product from ConnectWise called R1Soft.

In early 2023, Cl0p extorted around 130 organizations thanks to a 0-day in a File Transfer product called GoAnywhere sold by Fortra. In 2021, Cl0p did something similar by abusing a vulnerability in the Accellion's legacy File Transfer Appliance[16].

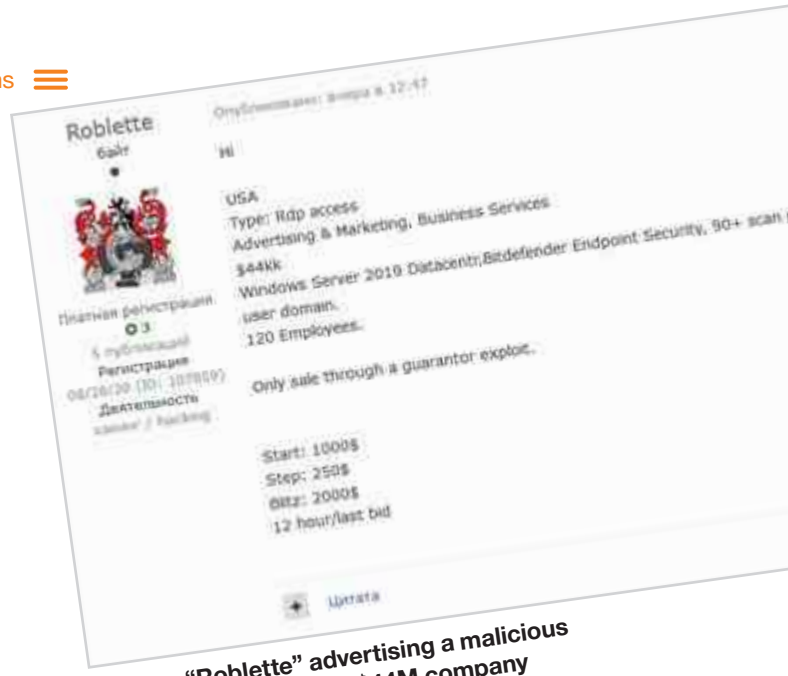
Weak credentials

Bruteforcing open RDP ports has been widely used by IABs to compromise poorly secured systems over the last 10 years. It is also a frequent lateral movement enabler inside the compromised network. MedusaLocker for example, heavily abused RDP servers, although this group stopped its operations in 2021. (It should not be confused with a new group also called Medusa that emerged in 2022).

SEO poisoning

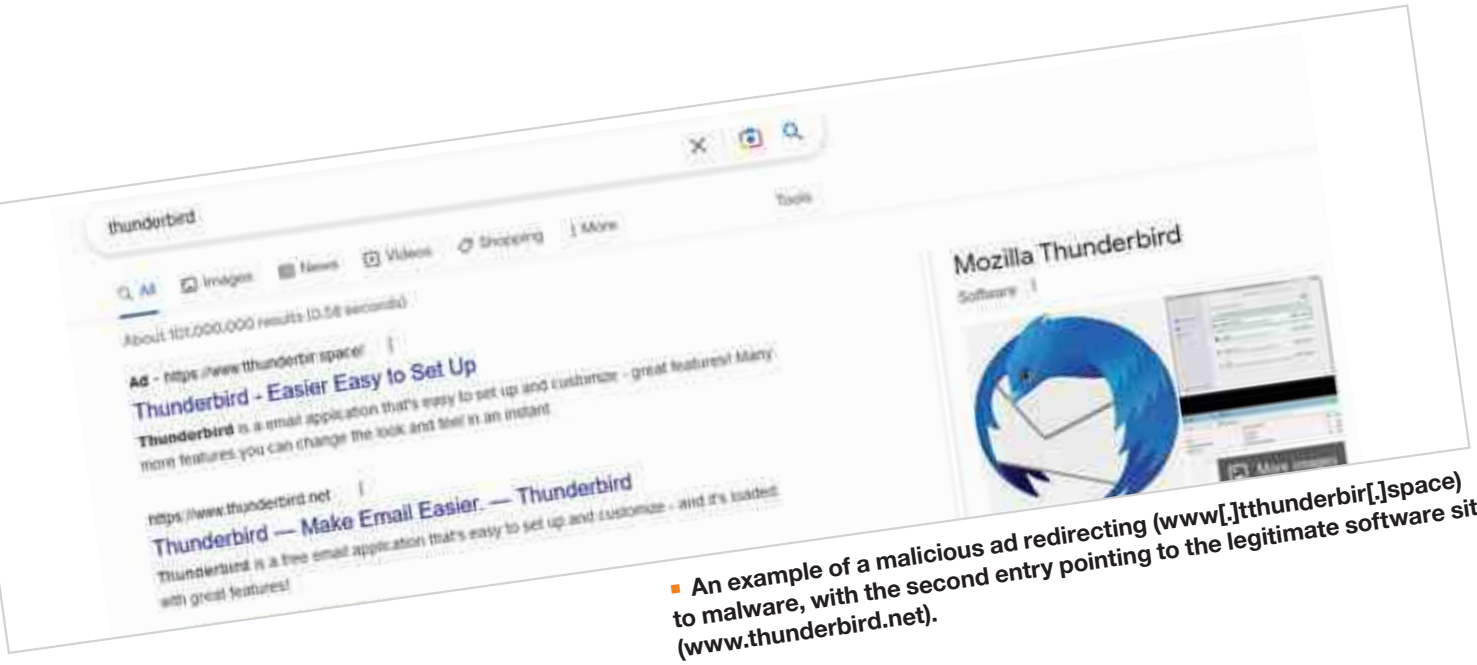
In 2022, an old technique has resurfaced again: SEO poisoning. It consists of manipulating sponsored results displayed in the top position of search engines results (and social networks paid contents).

Multiple groups started using this technique from Q3 2022, to drop first-stage malware (see next chapter) such as BatLoader. The 50 most infringed software products according to us were:



▪ **"Roblette" advertising a malicious RDP access to a $44M company**

1Password	CCleaner	Inkscape	Paint.net	Tor Browser
7-Zip	ChatGPT	Java	Photoshop	TunnelBear
Adobe Reader	Cisco AnyConnect	LibreOffice	Pixlr	TurboTax
AMD	Citrix	Lightshot	PowerISO	Virtualbox
AnyDesk	CPU-Z	Malwarebytes	PuTTY	Visual Studio Code
Audacity	Docker	Microsoft Teams	Python	VLC
Awesome Miner	Figma	NordVPN	Rufus	Webex
Bitwarden	FileZilla	NotePad++	Slack	WinRAR
Blender	foxit reader	NVidia	TeamViewer	WinSCP
Brave Browser	GIMP	OBS	Thunderbird	Zoom



▪ **An example of a malicious ad redirecting (www[.]tthunderbir[.]space) to malware, with the second entry pointing to the legitimate software site (www.thunderbird.net).**

Initial Access listings landscape

As IABs play an important role in the criminal ecosystem of Cy-X, we wanted to dive into some trends observed by our partners at Intel471, who track IABs and their listings on the dark web.

As you can see below, most Initial Access sales are for Virtual Private Network (VPN) access, with VPN, GlobalProtect, Fortinet, PulseSecure and Cisco AnyConnect all contributing to the category. This access will come in the form of compromised accounts, either through phishing or from data breaches, or the IAB could have compromised a device by exploiting a vulnerability and then created accounts to be used. VPN access is the most popular choice as it places the attacker directly on the victim's network, although access could still be hampered by compliance checks and network restrictions applied by the VPN solution or other internal controls.

The next most popular form of access for sale are logins for remote access including Remote Desktop Protocol (RDP), Remote Desktop Web Access (RDWeb) and Citrix.

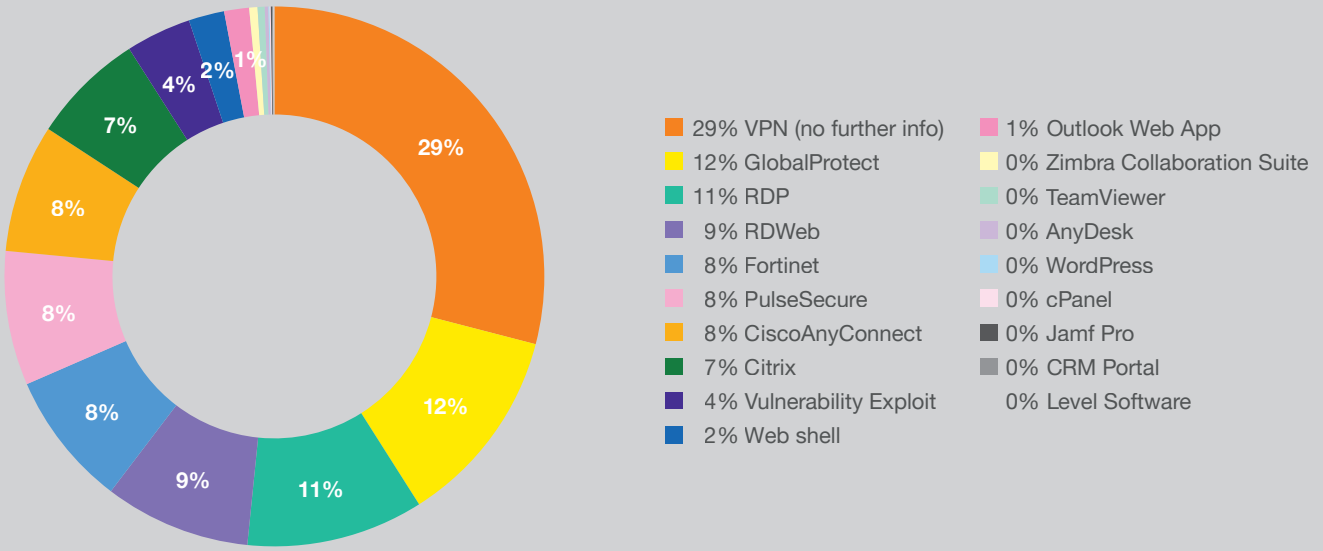
Rather than placing the attacker-controlled infrastructure directly on the network, these solutions present a virtual desktop, usually pre-populated with specific applications the user needs, which is then able to access specific resources on the network. These virtual desktops should be locked down and have restricted network access but are often left accidentally exposed due to mistakes or misconfigurations.

Despite the restricted access they are still of value to an attacker as they provide an initial entry point that may allow them to gain a foothold further inside the network.

The remaining four access methods on the list are nowhere near as popular. This is due to the complexity required to use them or the limited amount of access they provide for an attacker. That said, email solutions such as Outlook Web App and Zimbra Collaboration Suite can be abused to reset passwords or perhaps intercept some forms of Multi-Factor Authentication (MFA)[17].

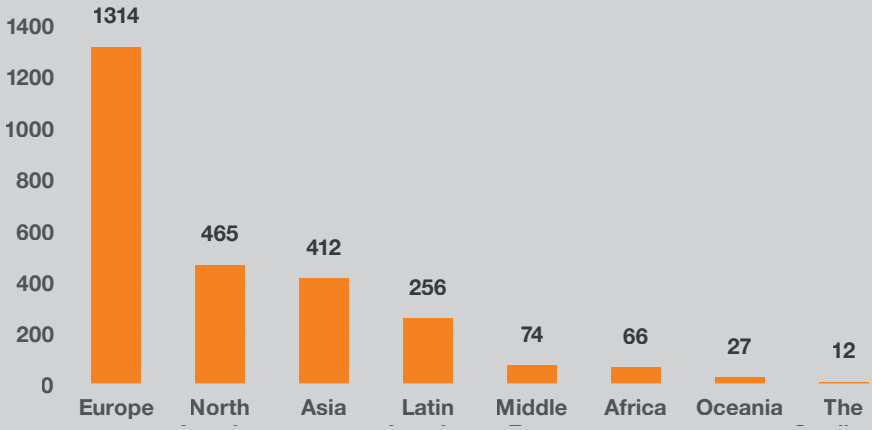
Top Access Types sold in 2022

Methods sold and used by criminals to gain access to their victim's networks (Intel471)



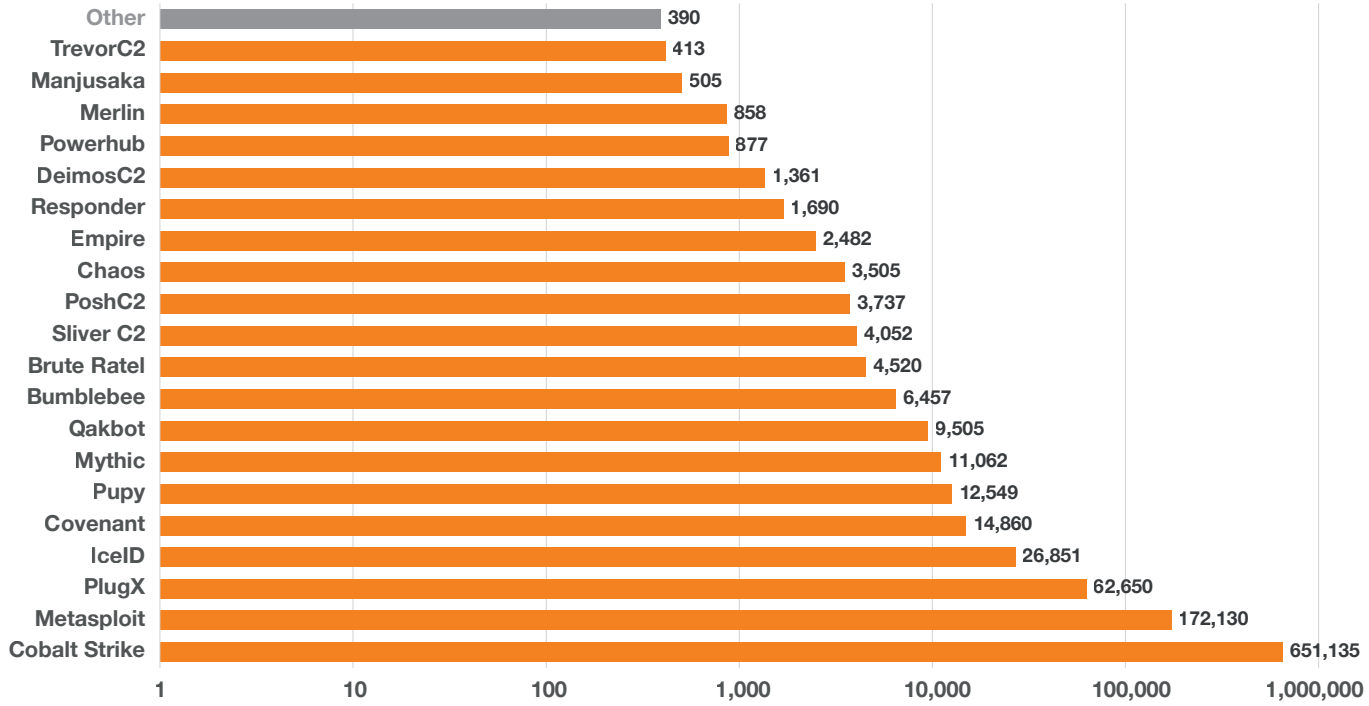
Access by region

When looking at the regions where IAB listings originate from, we see that half are from Europe, followed by North America (18%), Asia (16%), Latin America (10%) and the Middle East with 3%, in the top five. These are regions we also see many of the Cy-X victims in, an area we explore further in a later chapter.



Attack tools in 2022

Number of first- and second stage payload command & control (C2) servers identified in 2022



First stage payloads

The hands-on-keyboard actions happening during most human-operated ransomware cases start after one stable initial access is achieved. The brokers behind this first step usually launch first-stage payloads directly themselves or rely on yet other cybercrime-as-a-service providers to do so.

That is why some advanced malspam distributors (i.e., TA551 pushing mostly Gozi or TA542 distributing Emotet) are often not the ones developing the first-stage payload itself.

Major ransomware affiliates regularly test new loader strains, such as BumbleBee or BatLoader in 2022. On the other hand, some of these malware-as-a-service fully disappeared last year (for example BazarLoader or Hancitor).

In 2023, that criminal ecosystem kept renewing itself with new providers called AresLoader or SilkLoader.

Most new strains are built by already existing development teams, such as BumbleBee that is tied to BazarLoader's developer.

And some families just keep being improved over the years, such as Qakbot, GootLoader or IcedID, that remain active as of today.

Back to USB propagation?

Raspberry Robin is a specific first-stage payload type, already identified in thousands of networks. Presumably part of the toolset from a major cybercrime nexus (Evil Corp), it hasn't been seen used in many Cy-X attacks (yet).

It uses a rarely seen but efficient propagation vector: USB keys acting like a worm. By infecting a USB key inserted into a compromised machine, that key can then infect the next computer it is used on.

■ **Capture of our sandbox triggering on a Roshtyak[18] (RaspberryRobin backdoor)**

Encryption payloads

The encryption phase is key to applying pressure on victims. Throughout the years, threat actor groups have been attempting to maximize their chances to be paid by hindering any possible recovery. They for instance simultaneously encrypt both workstations and servers (with Windows, Linux and ESXi variants), delete Volume Shadow Copies (VSS)[19], target backups and external drives.

Also, groups are improving the encryption speed process. Once the encryption payload is activated, modern security solutions may trigger alerts and possibly prevent some systems from being encrypted. That's why advanced groups such as LockBit started using intermittent encryption, i.e., not overwriting the full file, but part of it to manipulate more files in the same amount of time.

But multiple groups have also been making mistakes in their code directly (or in their OpSec i.e., Operations Security) which allowed researchers to create free decryptors.

Orange Cyberdefense discovered for example a hard-coded private RSA key in one Lorenz sample reverse engineered in mid-2021. This enabled us to decrypt other victims compromised by the threat actor group.

More recently, SentinelOne identified a flawed encryption algorithm in the Linux variant used by Cl0p since December 2022. And the FBI hacked the Hive group during a six-months period and provided 300 victims of the group with their associated decryption keys.

- Law enforcement and Industry-wide initiative NoMoreRansom.org, with +135 decryptors available

4 minutes to encrypt 220000 files

Recently, Checkpoint[20] analyzed a new strain of ransomware, tested its performance and deemed it the fastest at encrypting systems in the world, above the presumed former leader, LockBit 3.0.

Lab environment

- 6 CPUs, 8192MB RAM, SSD
- Test: try 5 times to encrypt 220000 files
- local drive only

ransomware	Average approximate time of encryption
LockBit v. 3	7 minutes
Rorschach	4 minutes, 30 seconds

A view from the CSIRT

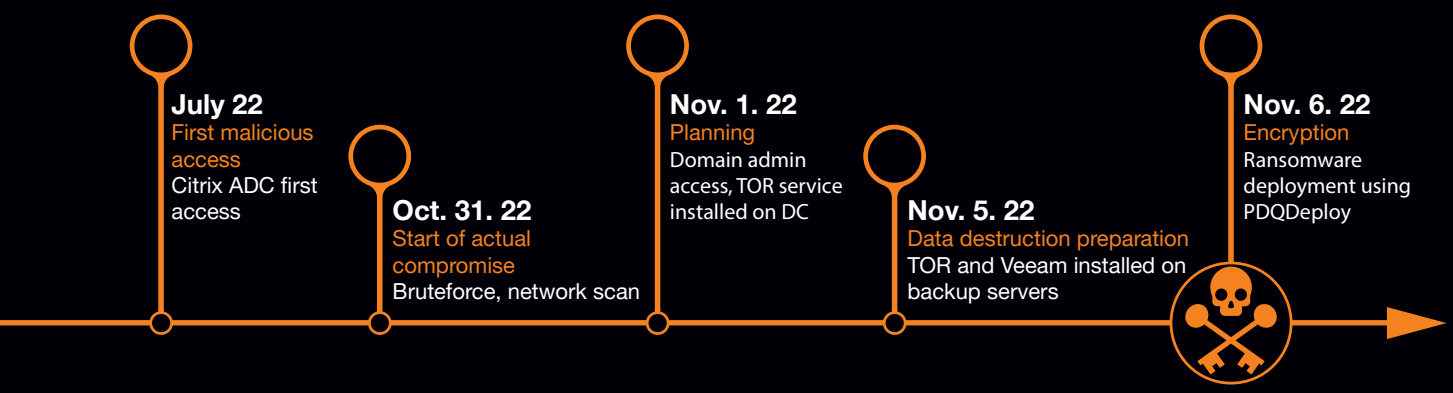
```
Veeam
├── Agents
├── Backup
│   ├── Tape_Eject
│   │   ├── Job.Tape_Eject.XXX.log
│   │   └── Job.Tape_Eject.YYY.log
│   ├── Tape_Erase
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.1.log
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.2.log
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.3.log
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.4.log
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.5.log
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.6.log
│   │   ├── Agent.Tape_Erase.TapeErase.TapeHost.log
│   │   └── Job.Tape_Erase.TapeErase.log
│   ├── Tape_Library_Discovery
│   │   ├── Job.Tape_Library_Discovery.WWW.log
│   │   ├── Job.Tape_Library_Discovery.XXX.log
│   │   ├── Job.Tape_Library_Discovery.YYY.log
│   │   └── Job.Tape_Library_Discovery.ZZZ.log
│   ├── Tape_Library_Inventorying
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.1.log
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.2.log
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.3.log
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.4.log
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.5.log
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.6.log
│   │   ├── Agent.Tape_Library_Inventorying.TapeInventory.TapeHost.log
│   │   ├── Job.Tape_Library_Inventorying.XXX.log
│   │   └── Job.Tape_Library_Inventorying.YYY.log
```

We recently presented during the BotConf.eu conference an incident response engagement our CSIRT conducted, in which RansomCartel group, a spin-off from the infamous REvil gang, went as far as erasing magnetic backup tapes (i.e., LTO tapes) by installing on purpose the Veeam backup management product on the compromised network.

The log shows the threat actor looking for and permanently erasing the drive of a magnetic tape.

Attack timeline

This example shows the somewhat typical steps from initial access to encryption



Extortion techniques in 2022

Cyber extortion as the name suggests uses extortion techniques to increase the pressure towards a victim organization to make them comply to specific demands from threat actors. In some cases, data exfiltration and extorting victims with the value and sensitivity of that data is enough leverage. In other cases, threat actors encrypt the victim's files and systems and not only threaten confidentiality and integrity but availability. Disruption can therefore be a very impactful means to make them comply with the ongoing extortion demands. We noticed a trend towards pressuring victims through a few new techniques.

In 2022, the use of heavily redacted victims' names on data leak sites, revealing only a few characters each new day, emerged. This strategy used first by the Play threat actor in November then soon after by BianLian, is supposed to put pressure on victims that don't want their names publicly listed on cyber extortion data leak sites, which are constantly monitored by journalists (and security companies, regulators, other threat actor groups, etc.).

On top of the leak site hosted on Tor, some groups such as ALPHV or Lorenz have been registering typosquatted domains to host look-a-like websites showing evidence of stolen data. ALPHV even proposes a search feature to conveniently browse this data.

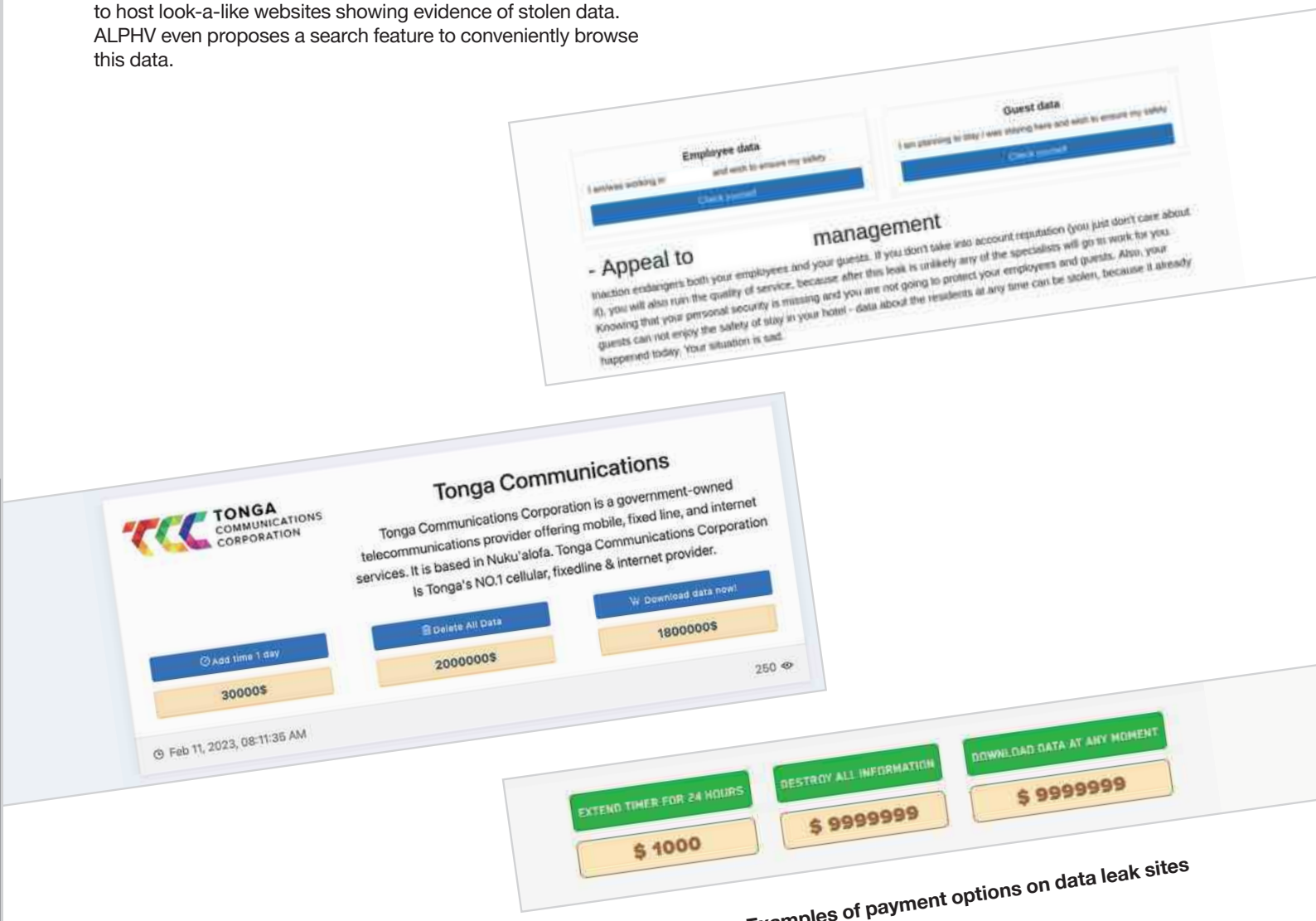
In one other case, a lengthy video recorded by the ransomware group explained what kind of data was stolen (and how bad this was for the impacted people), and Vice Society even called students of an Educational institution impacted[21] by one leak.

Another extortion tactic attempted by Medusa group was to provide additional payment options to their victims:

- Pay a small amount to extend the deadline for 24 hours.
- Pay a big sum to have the cybercriminals delete the data they stole.
- Pay a close amount to recover all exfiltrated data.

But the biggest evolution might be that more groups rely exclusively on data extortion (i.e., RansomHouse, Silent Ransom, Karakurt or more recently BianLian).

This might be because organizations are increasingly able to recover using their backups. They are also heavily discouraged from paying ransoms by their insurer and law enforcement, particularly if the group is sanctioned by the US authorities.



Examples of payment options on data leak sites

Victimology: region, industry and size

Who are the victims?

In 2022, the victimology of cyber extortion attacks has seen major changes, which were mostly unexpected. Despite that, we recorded fewer attacks in 2022 (2087) when compared with 2021 (2296).

A total of 96 different countries were impacted by cyber extortion meaning we saw organizations from those countries fall victim.

Geographic distribution

For several years, the business model of these ransomware groups has been to attack organizations located in wealthier countries that are more likely to pay. However, in 2022 ransomware groups have launched more attacks against organizations located in developing countries. According to our data, the North American area remains by far the most targeted area, receiving nearly 45% of all ransomware attacks. In 2021, this number was 53.5%, which highlights a notable drop, particularly in the Canada (-28%) and US (-21%).

We have previously argued that English-speaking countries were mostly impacted due to their presumed wealth, on top of the language often mastered by the Russian speaking authors and information readily available on the victims (revenue, clients, etc.). Nevertheless, by the end of 2021, we noticed a shift towards non-English speaking countries, such as European or Latin American countries. Surprisingly, the number of victims headquartered in Europe has been experiencing a drop in cyber extortion attacks since the beginning of the Russian invasion of Ukraine.

As we're seeing a decrease in victims in regions such as North America and Europe, we would expect that countries from other regions must be experiencing an increase. In 2022, threat actors did indeed launch more attacks against developing countries. In Latin America for instance, the number of attacks has increased since Q3 2022. For example, we have detected a worrying trend of attacks against government entities in Costa Rica, Peru, Mexico, Ecuador, Brazil, and Argentina by ransomware groups such as Conti, ALPHV, LockBit 2.0, and BlackByte.

Yet, since the end of 2022, cyber extortion groups have also increasingly targeted regions that were previously marginally affected, including Africa, Oceania (AU and NZ), and Southeast Asia (SEA).

By numbers, Africa remains the least impacted region in the world, even if RansomHouse succeeded in breaching the continent's largest supermarket chain, Shoprite, back in April 2022. We saw the highest proportional increase in the Southeast Asia region, where countries such as Indonesia, Singapore, Thailand, Philippines, and Malaysia were the most impacted.

It could be the case that threat actor groups do not expect as big a reaction from these countries in comparison to the US or European countries.

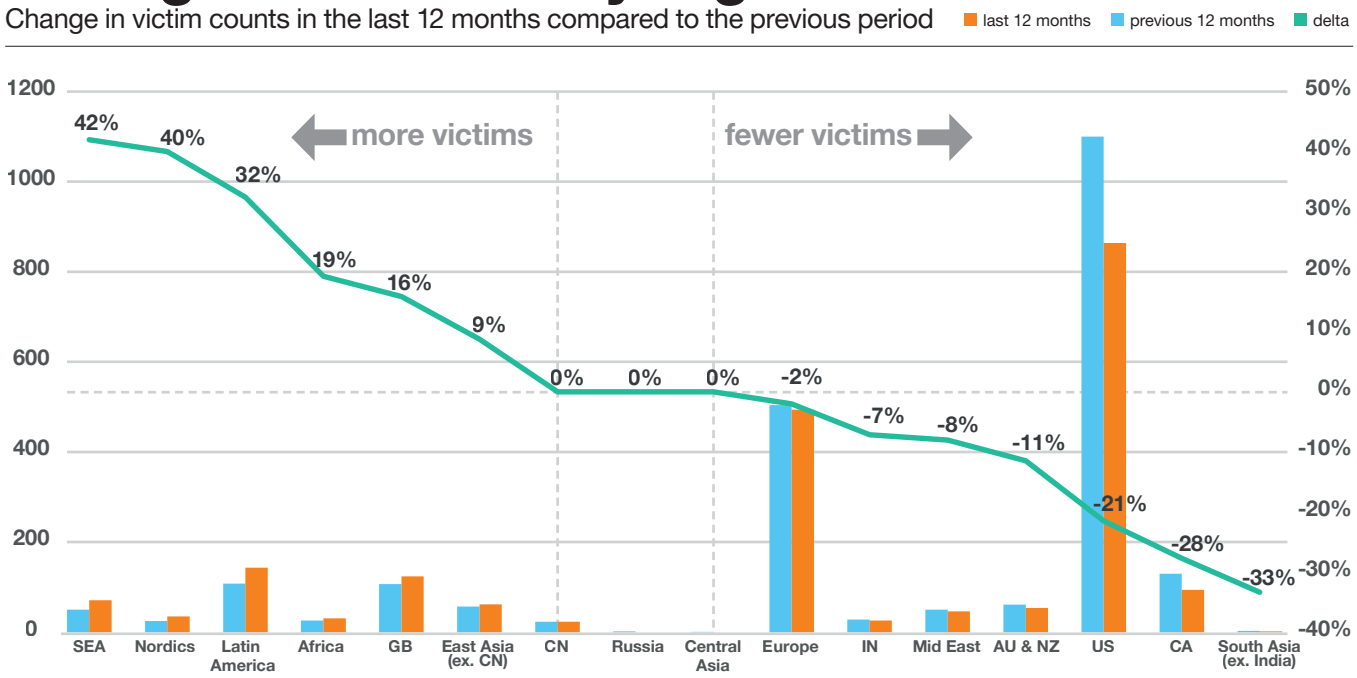
This could also potentially be one explanation as to why we are seeing those specific regions impacted by the Cy-X threat. However, let's explore the question of why certain countries occur more frequently in our dataset than others in more detail.

Another way of looking at this could be if we pose the question of whether we see those regions being impacted because they simply have a lot of businesses to begin with. To explore this hypothesis, we can make use of the data provided by the NAICS Association[22], showing the global business count per country (last updated: 2022-11-30). We can then look at the top 30 countries with the highest business count, which results in a total of 171,744,618 businesses.

When we overlay the top 30 countries with the most businesses with our Cy-X victim data, looking at our full dataset dating back to January 2020, we see that our top countries with the highest victim count is represented in the top 30 group. This means that we can partially agree that countries with a high number of businesses are impacted by Cy-X because there are just more organizations that can be victimized. However, there are some deviations when looking at the most impacted victim countries.

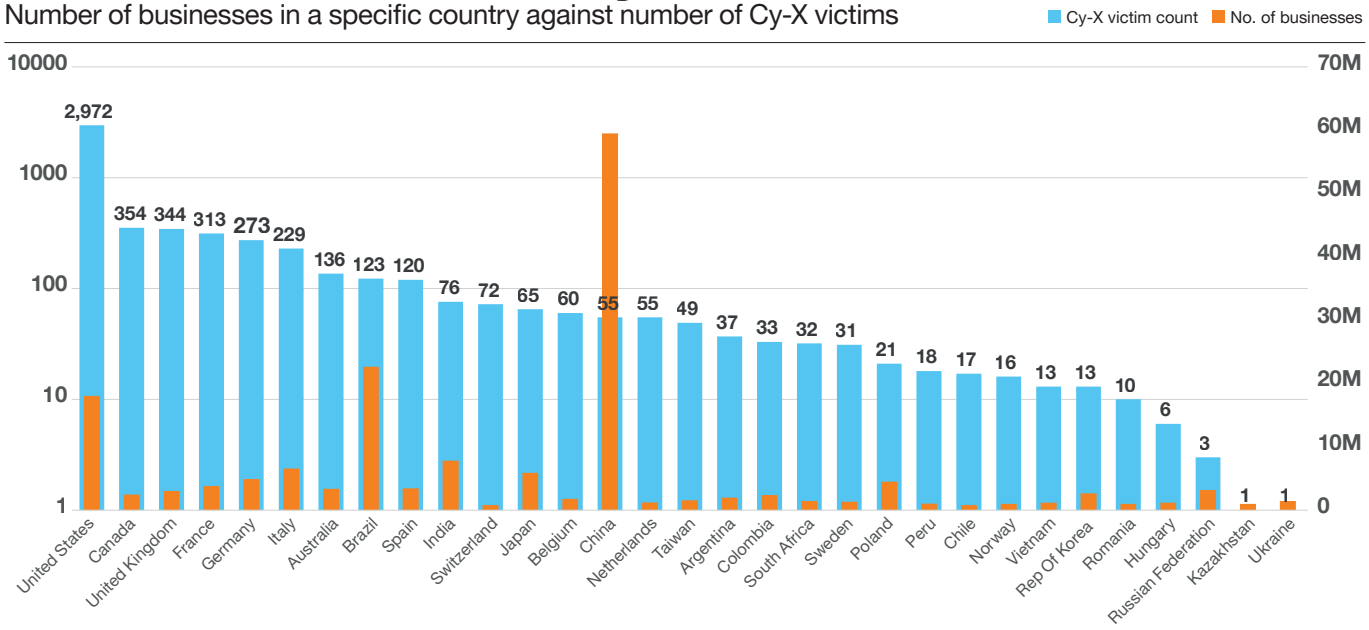
Changes in victims by region

Change in victim counts in the last 12 months compared to the previous period



Business count vs. Cy-X victim count

Number of businesses in a specific country against number of Cy-X victims



We see that the US is the country most impacted by Cy-X when looking at absolute numbers, but it is only the 3rd biggest country by count of registered businesses.

Generally, the first top seven victim countries are also countries that have a lot of businesses. Therefore, we can argue that this threat could be driven by the opportunity to victimize 'someone'. Moreover, we see that Brazil is the second biggest country in business count but had only 123 victims in the past three years, representing the 8th most impacted country. We have always found it challenging to explain the low ranking of Brazil in our data set, but the challenges presented to threat actors by difference in culture and language could be the explanation for this observation.

And then there is China, which is the biggest country worldwide when it comes to business count but is not very present in our victim data. In fact, from Jan 2020 until Q1 2023, we documented 58 victim organizations headquartered in China, ranking low at 14th place in the victim database.

Other countries that have a relatively high number of businesses but aren't very present in our dataset are Poland (top eight in business count), Russia (top 12 in business count) and the Republic of Korea (ranking 14). It is worth noting that if we look at the five countries with the lowest victim count, we are not surprised to see countries such as Kazakhstan (region: CIS), Ukraine (region: CIS), Russia (region: CIS), Hungary (region: Eastern Europe), Romania (region: southeastern Europe).

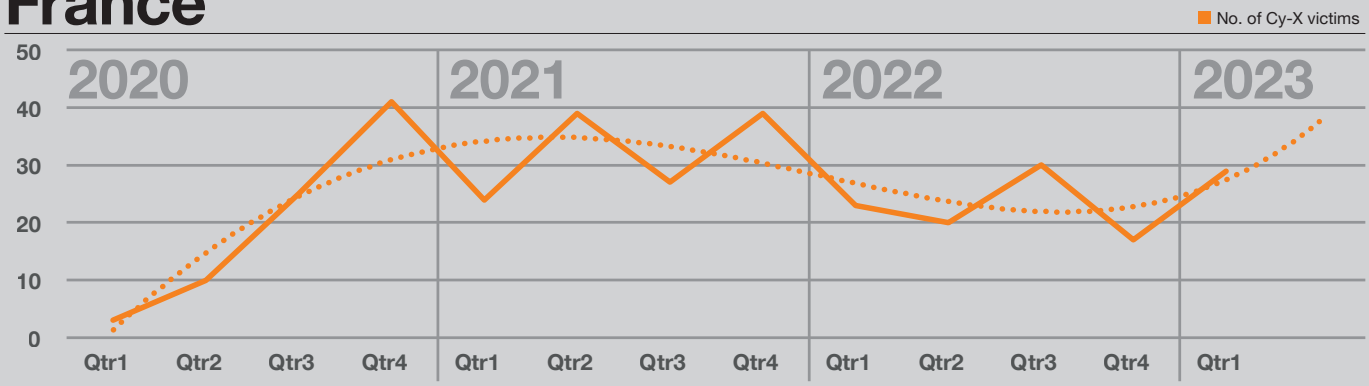
Those regions may not have been impacted by Cy-X given that threat actor groups might originate from these regions or have some form of promise to not victimize businesses from regions such as the Commonwealth of Independent States (CIS). In fact, if we check our whole dataset of over 6000+ victims, we find 3[23] of the 12 countries of the CIS region present. The total amount of victims from those three CIS countries is five, and therefore very small.

However, the so-called 'brotherhood' might have been shaken up due to the Ukraine war[24], where we witnessed many data breaches of Ukranian citizens being dumped in online forums. Consequently, we cannot be sure what the future will bring, especially for regions that were considered to be 'protected'.

In our NATO exploration, we looked at whether NATO member countries were more impacted, which we could not confirm. But what we did observe is that we see more non-NATO countries impacted by Cy-X over time. The question that remains is, what were the major non-NATO victim countries during 2022? According to our victim data, the top 10 countries impacted by Cy-X within the non-NATO group were: Brazil (18%), Australia (15%), Switzerland (11%), Thailand (9%), Taiwan (9%), Japan (8%), Mexico (7%) and Argentina with 7%. We will describe more geographical distribution of victim organizations in a later chapter.

Interestingly, Intel471, who has shared some of their data with us on victim organizations whose access was sold on the Dark web or online forums in 2022, see similar victim countries being offered for sale. Of the top 20 victim countries offered by IABs; Intel471 saw 7% of the access sold was from victims in Brazil, 4% from Thailand, 3% from Argentina, 2% from Taiwan and 2% from Mexico.

France



France is being heavily hit by ransomware attacks and as expected, private organizations rank first by victim count. France is the fifth most impacted nation in terms of Cy-X attacks, with the highest number of French organizations victimized in September during 2022.

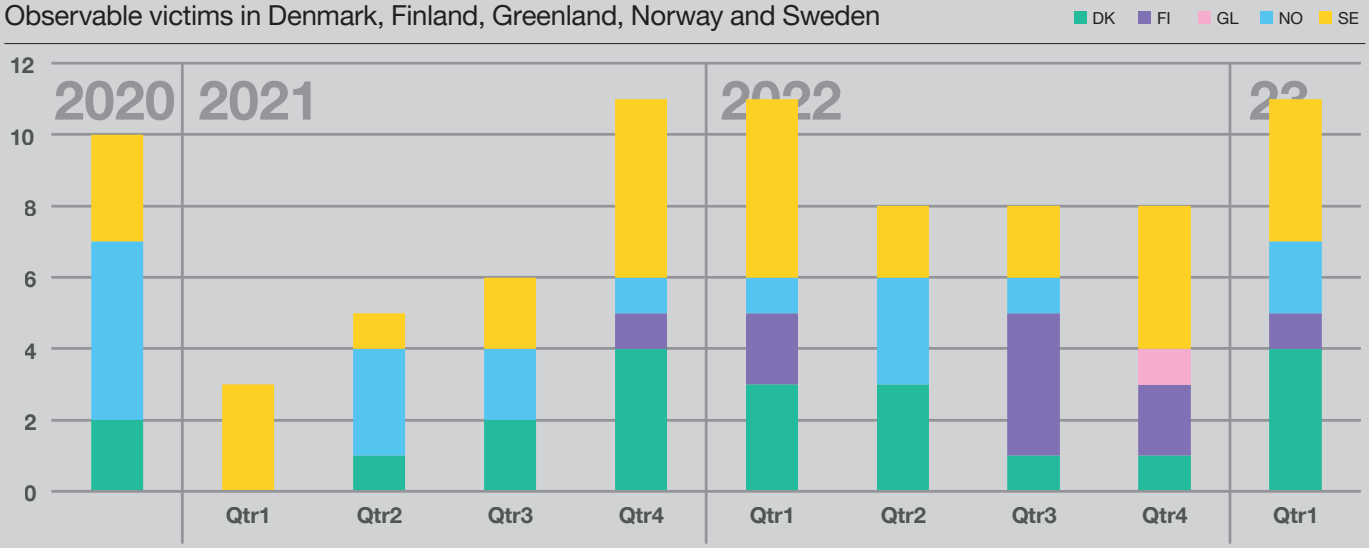
However, France's public sector is far from being spared as it represents the industry vertical most affected.

Indeed, adding up public Education and administration with healthcare and medical industry victims, those represents nearly one fourth of all victims recorded. The most hit by ransomware amongst French industries includes municipalities, hospitals, and higher Education institutions.

We note that the polynomial projections reflected as orange dashed lines in the charts in this section are based on small datasets and therefor not very reliable. Readers are thus urged to interpret those projections accordingly.

Nordics

Observable victims in Denmark, Finland, Greenland, Norway and Sweden



The Nordics (SE, DK, NO, FI, GL) is the second biggest region that has seen an increase in Cy-X attacks in 2022 by 40%. If we breakdown the countries, we see that Sweden has been impacted the most (41%), followed by Denmark (24%) and Norway (21%).

As we explored in the Ukraine war chapter, while proportionally we observe more victims coming from other regions, we see an increasing trend of Nordic victims since 2021. In 2020, we saw 10 victims caused by six unique actors, by 2022 we registered more than three times as many victims caused by 13 different groups.

Because of the geopolitical situation of two countries of this region - becoming members of NATO, we think this region might see more cyber-related disruptions, whether this is by Cy-X attacks or others is difficult to say at this point.

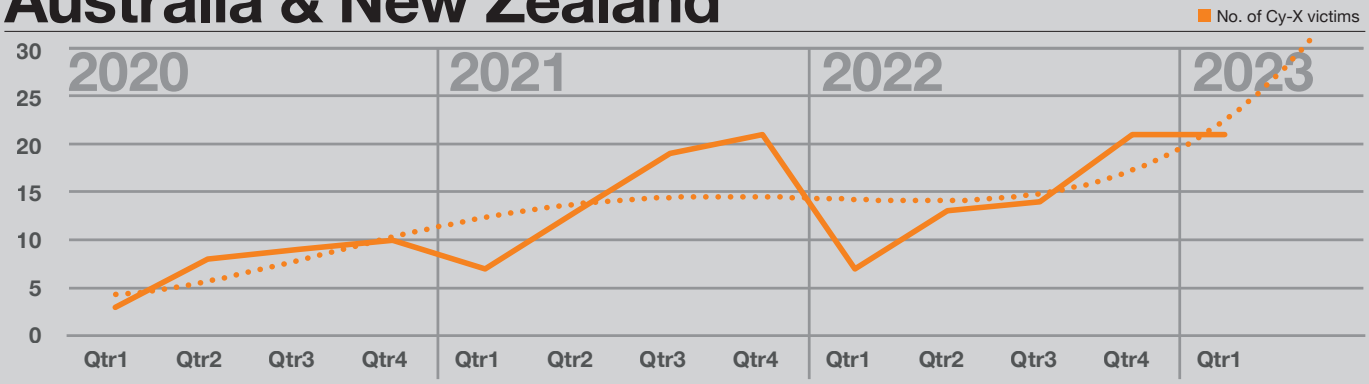
An outlook into what 2023 might bring us shows that the Nordics can most likely expect to become victims of Cy-X more frequently, as shown in the chart above.

Other countries & regions

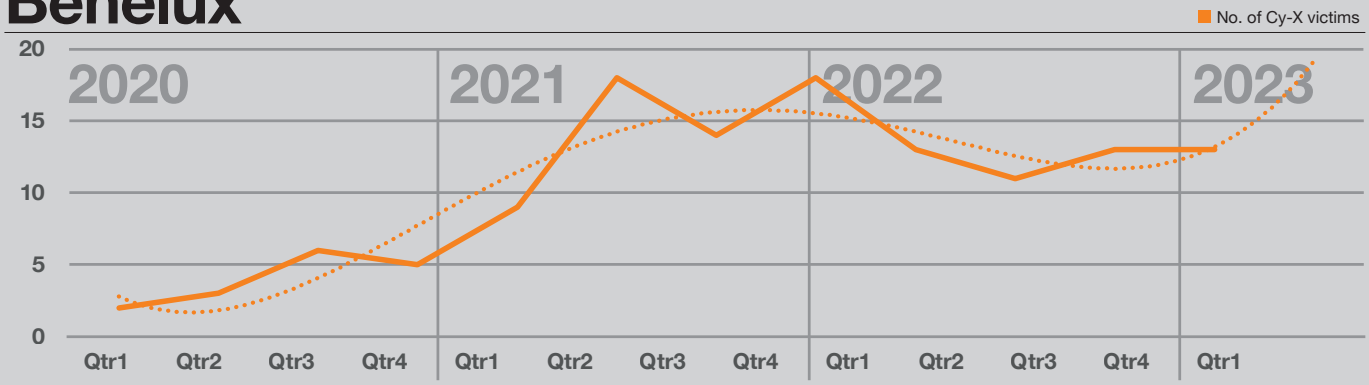
We will now present an overview of victim trends in different regions. Based on the forecast at the time of writing this report, we anticipate an overall increase in Cy-X incidents in most regions.

Once more, we note that the polynomial projections reflected as orange dashed lines in the charts in this section are based on small datasets and therefor not very reliable. Readers are thus urged to interpret those projections accordingly.

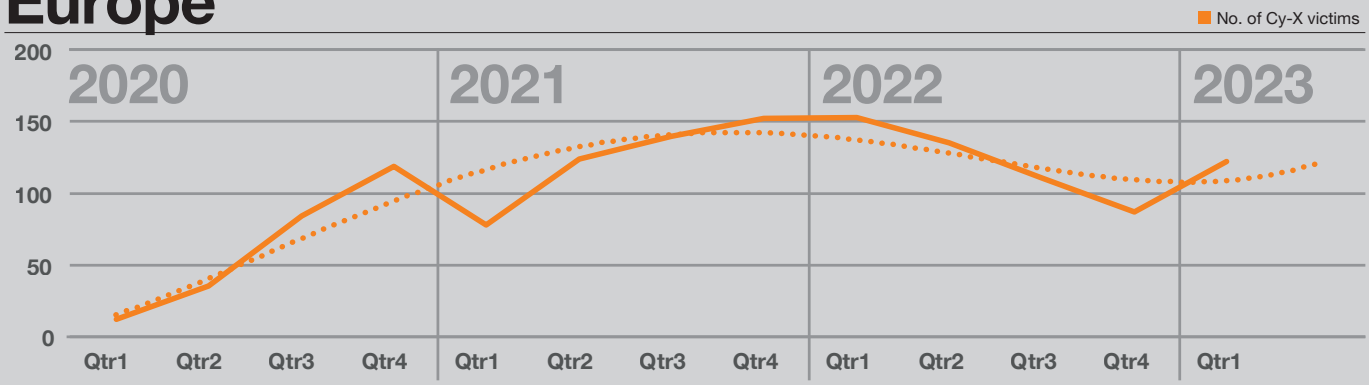
Australia & New Zealand



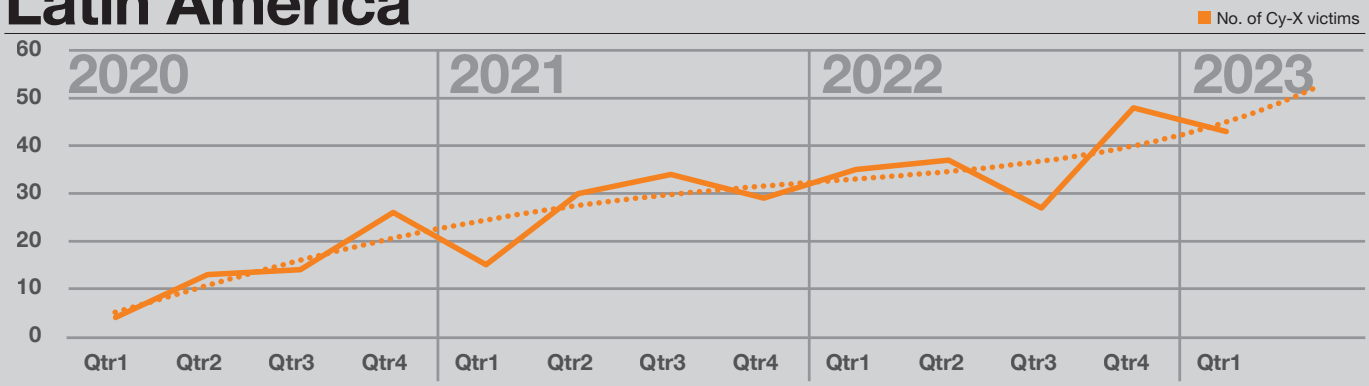
Benelux



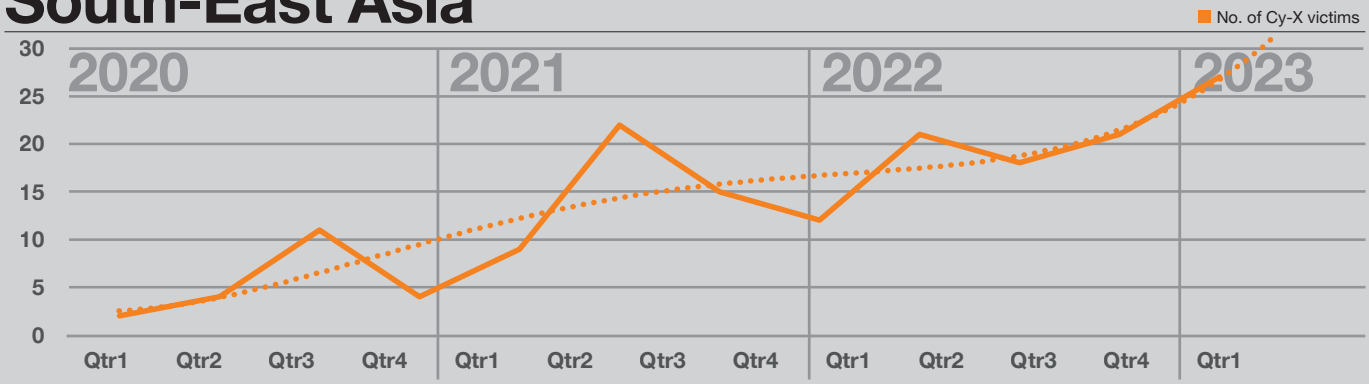
Europe



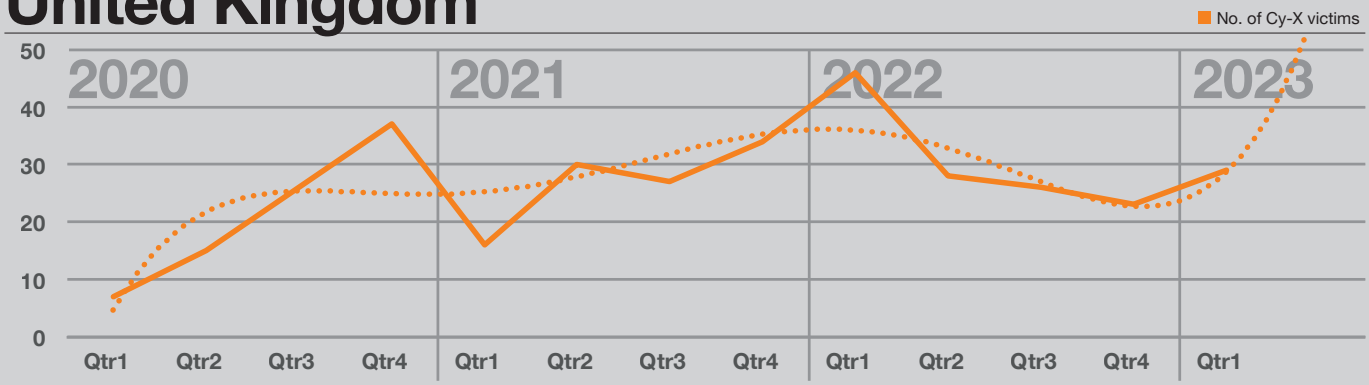
Latin America



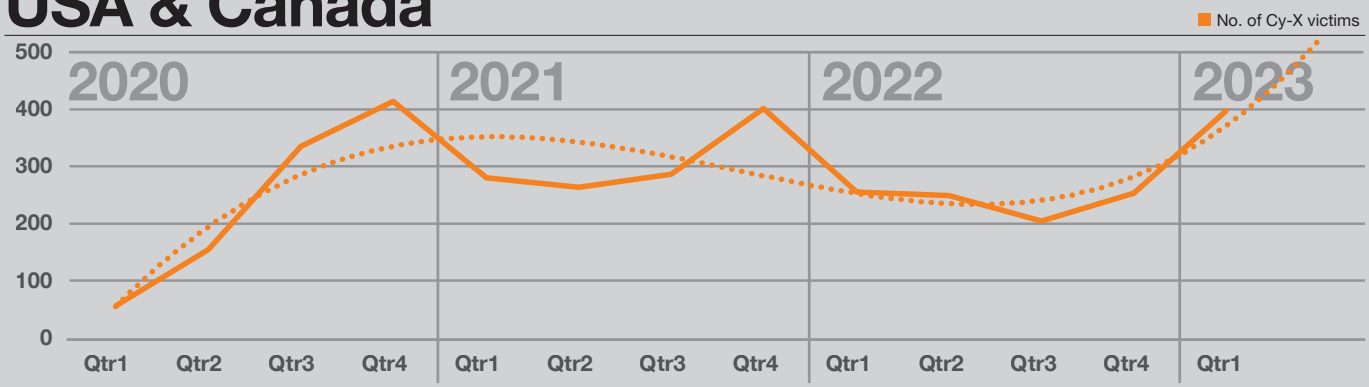
South-East Asia

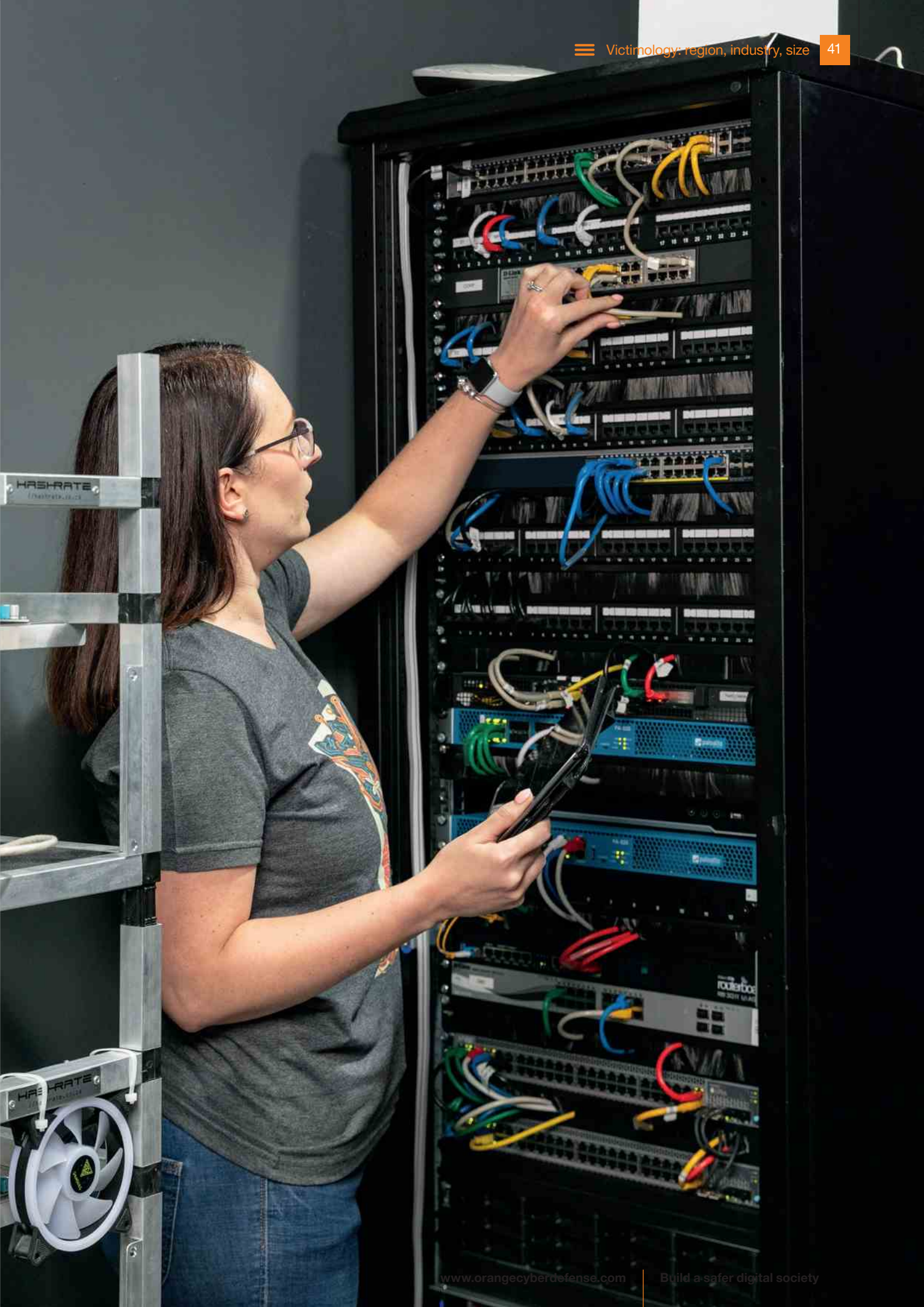


United Kingdom



USA & Canada




HASHRATE
routerboard

Industry distribution

In 2022, of all the victim organizations that suffered from a Cy-X attack, Manufacturing was the biggest industry impacted. Roughly one-fifth of all victims originated from this industry classification.

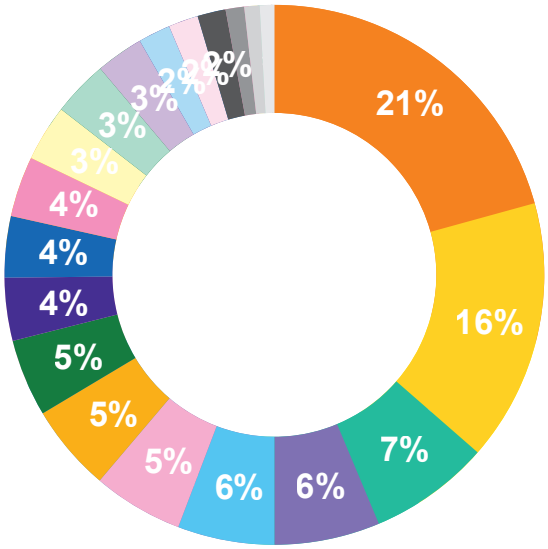
This does not come as a surprise to us since Manufacturing has been on top since we started collecting the victim data. However, if we compare this to the previous year, we register a decrease of 39% for the Manufacturing sector. In the second half of 2022, we notice a much lower number of victims from Manufacturing. One possible explanation for this is the shutdown of Conti's criminal operations, which we will examine further in the Sub-Industries section. Among all industries, only the Manufacturing sector still shows signs of Conti's impact on the number of victims in 2022, despite their activities being active only during the first half of the year.

The second biggest industry impacted is Professional, Scientific, and Technical Services with 327 victim organizations publicly shamed on Cy-X leak sites, accounting for 16% of the total share. Together with Manufacturing, these two sectors have always been the most impacted. It is our belief that the reason for this is likely because these two sectors are inherently large, resulting in a high number of potential victim organizations. Therefore, it is somewhat surprising that we have observed a 25% decrease in the number of victims from the Professional Services sector.

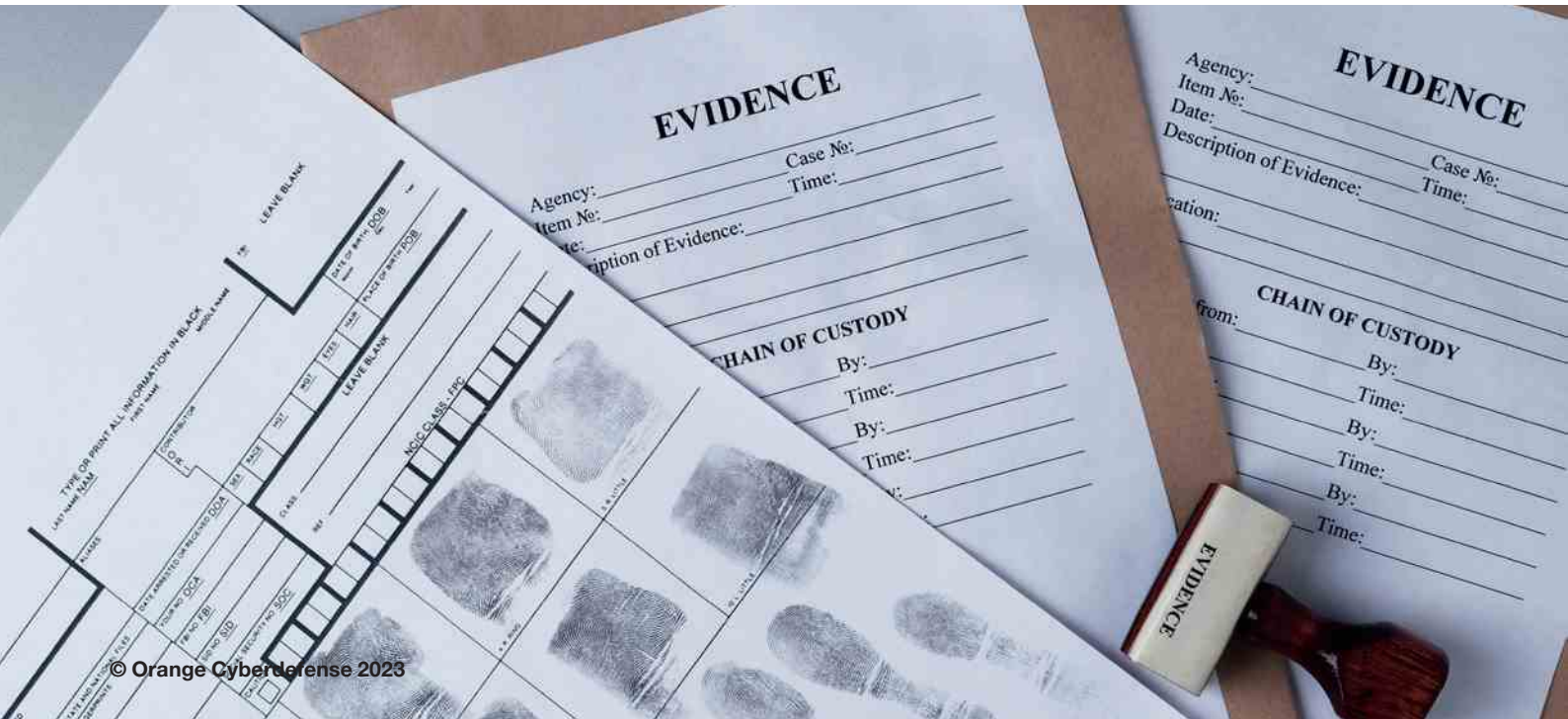
This trend of our 'usual' most impacted industries continues with a decrease in Wholesale Trade (-67%), Public Administration (-21%), Construction (-13%) and Retail Trade (-11%). Over the last two years we have seen the above listed industries heavily impacted, but this might have changed over the period of 2022. Nevertheless, some decrease can most likely be explained by the 8% decrease we are witnessing from 2021 to 2022 in total victim count.

Top 20 Industries impacted 2022

Extortion victims observed on monitored leak sites by vertical

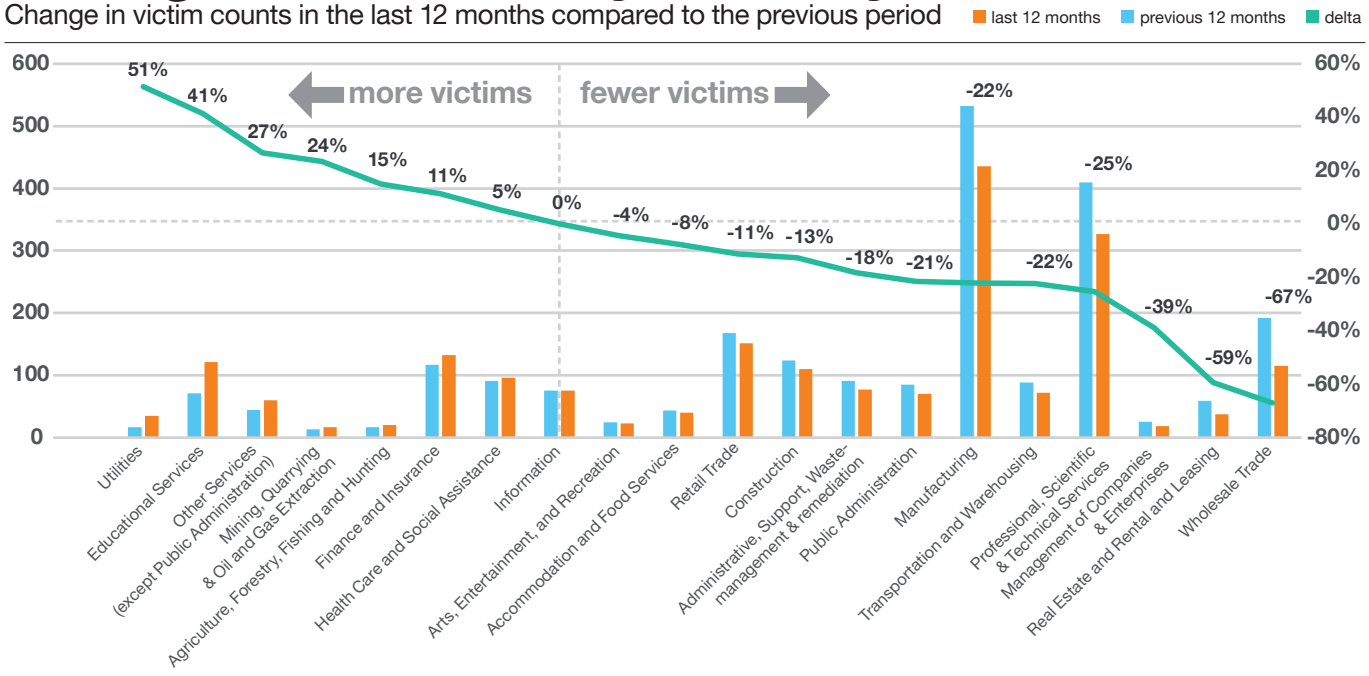


- 21% Manufacturing
- 16% Professional, Scientific & Tech. Services
- 7% Retail Trade
- 6% Finance and Insurance
- 6% Educational Services
- 5% Wholesale Trade
- 5% Construction
- 5% Health Care & Social Assistance
- 4% Unknown
- 4% Administrative, Support, Waste Mgnt & Remediation Services
- 4% Information
- 3% Transportation & Warehousing
- 3% Public Administration
- 3% Other Services (except Public Administration)
- 2% Accommodation & Food Services
- 2% Real Estate, Rental & Leasing
- 2% Utilities
- 1% Arts, Entertainment & Recreation
- 1% Agriculture, Forestry, Fishing and Hunting
- 1% Management of Companies and Enterprises



Changes in victims by industry

Change in victim counts in the last 12 months compared to the previous period



Interestingly, the Education sector experienced a higher number of attacks in 2022 compared to the previous year, with a recorded increase of 41%. The Vice Society group has had a particularly significant impact on the Education sector, with universities and colleges globally suffering more at their hands than any other group. In fact, if we look at Vice Society's victim profile, we see that Educational Services (36%) is the top industry impacted by them.

This trend was also noted by the Cybersecurity & Infrastructure Security Agency (CISA), the FBI and the MS-ISAC and resulted in a joint alert being published in September 2022[25]. Interestingly, almost one year before the bulk upload of victims in December 2022, Vice Society uploaded another 19 victims, of which 40% were from the Education sector. But we will need to wait until the end of the year to determine if this is a recurring behavior of theirs, assuming they remain active until then.

The Financial sector has seen an 11% increase in Cy-X attacks. We will dive into details of who has caused this in the next sub-chapter. Additionally, we notice an increase in the Mining, quarrying, and oil and gas extraction sector (+24%). But the biggest increase we see is in Utilities. However, both Mining and Utilities' victims are relatively small in numbers. Although, it stands to reason that this trend will continue.

Utilities saw an increase of 51%. While this seems significant, and despite the diversity of countries (20) represented among the victims, the actual number remains relatively low at 35. However, it is concerning that they are all from the Electric Power Generation, Transmission, and Distribution Industries.

Sub-Industries Q4 2022 – Q1 2023

We have been gathering victim data for over three years, which has made us curious as to why certain industries are more present than others. One part of answering this question is to understand who exactly becomes a victim within a certain sector. We would like to dive into some more specifics we have observed between 2021 and 2022.

We have chosen to focus on two sectors that have seen a significant increase in 2022 and are of particular interest to us - the Educational Services sector and the Financial sector.

Secondly, we intend to examine the top two sectors in terms of victim count in 2022, namely Manufacturing and Professional Services.

As this is a relatively new addition to our data enrichment process, our view on this is only partial. Our sub-industry data from Q4 2022 to Q1 2023, gives us six months of victim data (1,289 victims), providing us with deeper insights into sub-industries. On the next pages, you will find the selected sub-industry breakdown, we limited the charts to the top 10 sub-industries, which in some cases can result in relatively small numbers. Nevertheless, we do believe these provide some insight into who the victim organizations are that suffered the most from Cy-X attacks.

Finance and Insurance

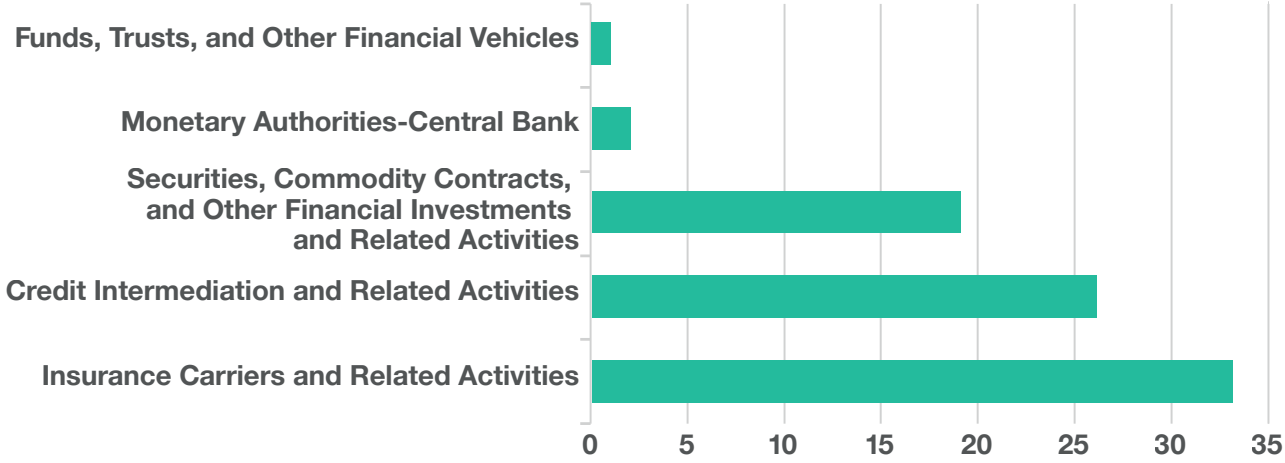
In 2022:

- Over 130 financial institutions became victims of Cy-X.
- An average of 11 organizations per month are being publicly exposed on the dark web.
- Top five countries impacted: US, Brazil, Germany, France and UK.
- Top three threat actor groups: LockBit2&3, ALPHV (BlackCat) and Black Basta.
- 75% of all victims have under 1,000 employees.
- At least 11% of all attacks are 'Data Extortion only' attacks, meaning that no encryption took place.

During the last six months (Oct 2022 – Mar 2023):

- Here we only saw 5 sub-industries
- Approx. 40% of all victims were Insurance Carriers and Related Activities, followed by Credit Intermediation and Related Activities (32%) and Securities, Commodity Contracts, and other Financial Investments (23%) or banks with 3%.
- 82 victims in the past six months.
- Top three threat actors executing the attacks are: LockBit3, Cl0p & ALPHV (BlackCat).
- Top three countries impacted: US, Australia and Canada.

Sub industries: Finance



Professional, Scientific, and Technical Services

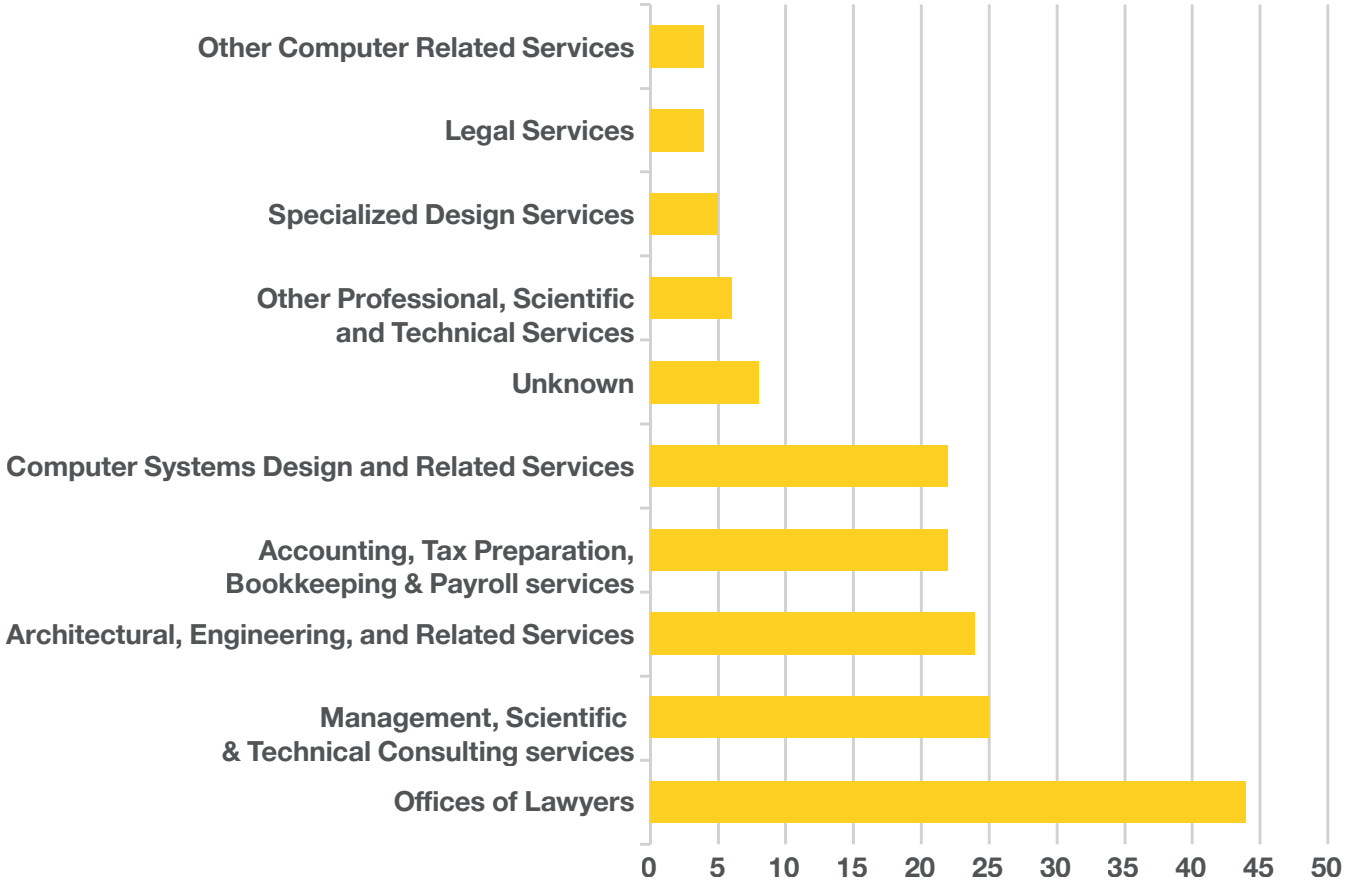
In 2022:

- Over 320 organizations within Professional Services became victims of Cy-X.
- An average of 27 organizations per month are being publicly exposed on the dark web.
- Top five countries impacted: US, UK, Germany, Spain and Australia.
- Top three threat actor groups victimizing: LockBit2&3, ALPHV (BlackCat) and Black Basta.
- 11% of all victims have over 1,000 employees.
- At least 9% of all attacks are 'Data Extortion only' attacks, meaning that no encryption took place.

During the last six months (Oct 2022 – Mar 2023):

- Approx. 203 victims.
- Almost one third of all victims are either from law firms (27%) or Legal Services (3%), followed by Management, Scientific and Consulting Services, Architecture and Engineering Firms and Accounting Services.
- Top three threat actors executing the attacks are: LockBit3, ALPHV (BlackCat) and Cl0p.
- Top three countries impacted: US, UK and Germany.

Sub industries: Professional Services



Manufacturing

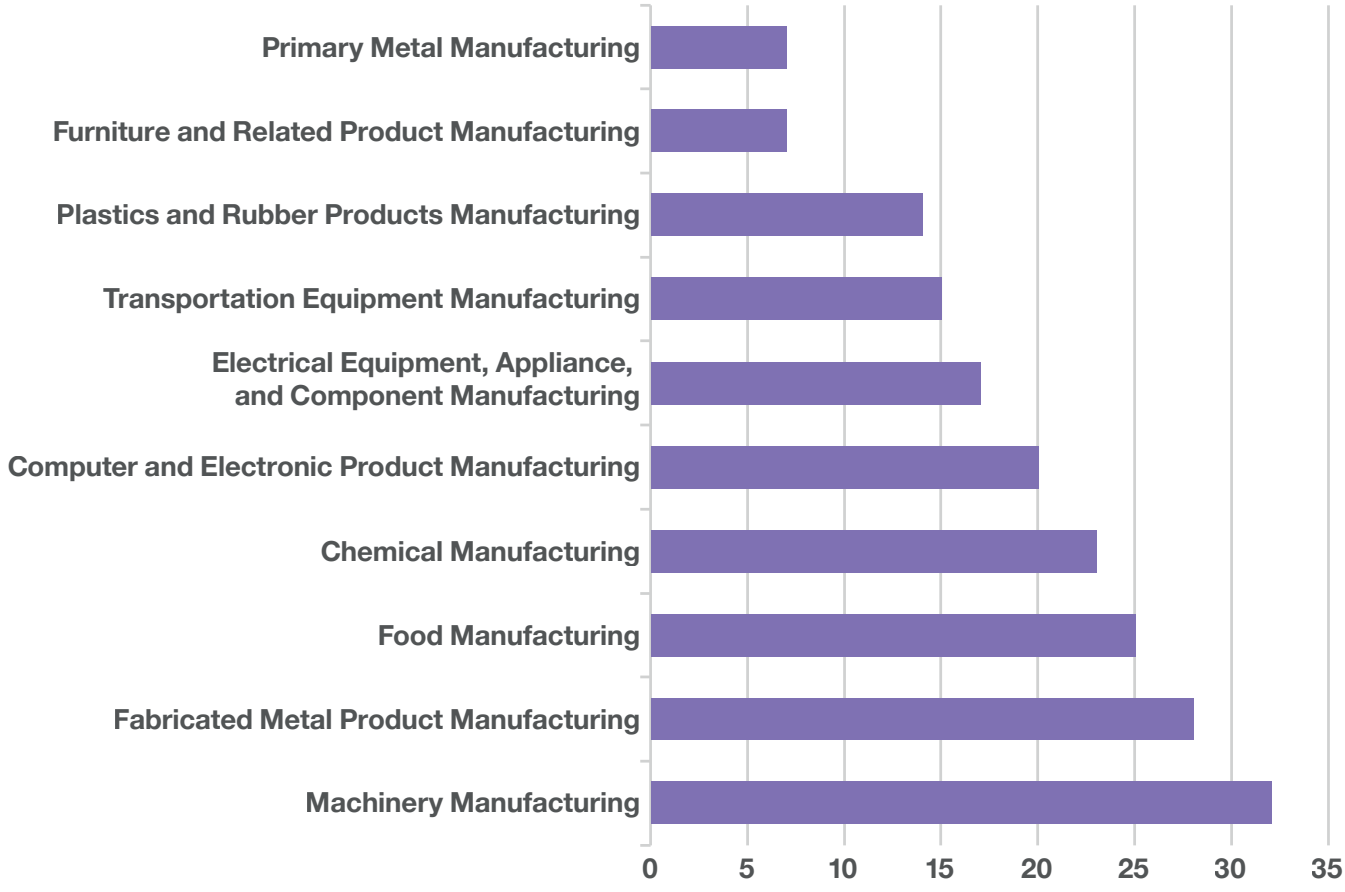
In 2022:

- Over 435 organizations within Manufacturing became victims of Cy-X.
- An average of 36 organizations per month are being publicly exposed on the dark web.
- Top five countries impacted: US, Germany, Italy, Canada and UK.
- Top three threat actor groups victimizing: LockBit2&3, Conti and Black Basta.
- As Manufacturing facilities tend to be large, it comes as no surprise that we saw 26% of all victims with over 1,000 employees.
- At least 14% of all attacks are 'Data Extortion only' attacks, meaning that no encryption took place

During the last six months (Oct 2022 – Mar 2023):

- Approx. 267 victims.
- Manufacturing has many sub-industries, the most impacted are Machinery Manufacturing, Fabricated Metal product Manufacturing and Food Manufacturing.
- Top three threat actors executing the attacks are LockBit3, ALPHV (BlackCat), and Black Basta.
- Top three countries impacted: US, Canada and UK.

Sub industries: Manufacturing



Educational Services

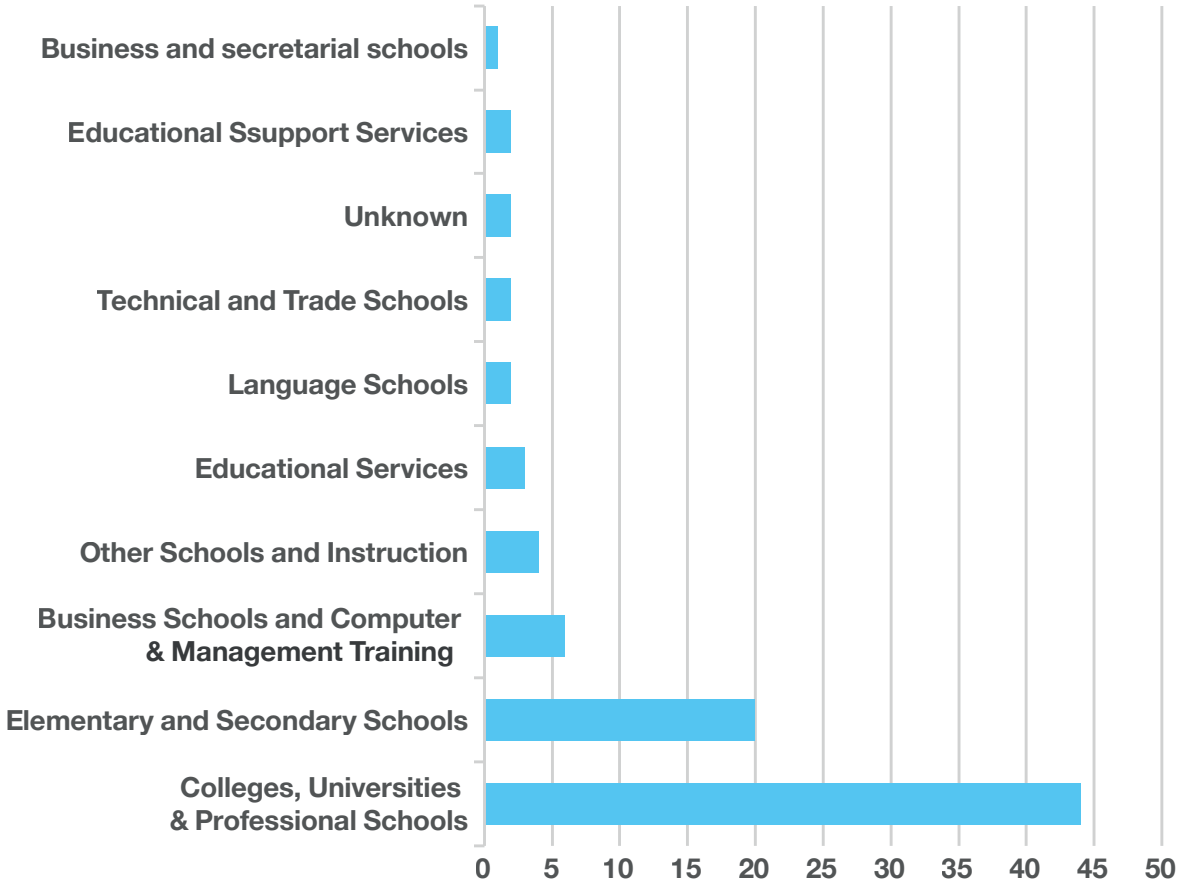
In 2022:

- Over 120 Educational institutions became victims of Cy-X.
- We saw an average of 10 organizations per month from the Educational sector being publicly exposed on the dark web.
- Top five countries impacted: US, UK, Spain, France and Australia.
- Top three threat actor groups victimizing: Vice Society, LockBit2&3, ALPHV (BlackCat).
- 23% of all victims have over 1,000 employees.
- At least 10% of all attacks are 'Data Extortion only' attacks, meaning that no encryption took place.

During the last six months (Oct 2022 – Mar 2023):

- 90 victims in the past six months.
- Almost half of the victims were Universities, Colleges, and Professional Schools, followed by Elementary and Secondary Schools, we even have Nursery Schools in our victim data as well.
- Top three threat actors executing the attacks are: Vice Society, LockBit3 & Royal.
- Top three countries impacted: US, UK and Australia.

Sub industries: Educational Services



A difficult choice to make – too big, too small, too political, too poor

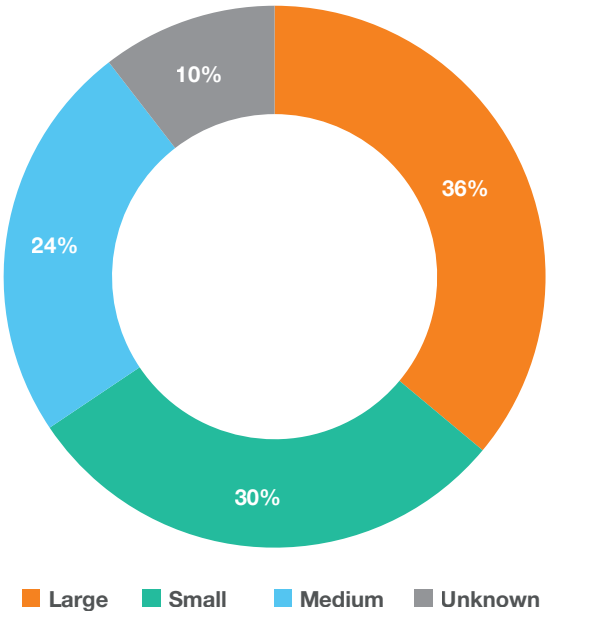
If we look at which businesses are impacted the most by the ongoing Cy-X threats when considering business size and employee count, we first need to address how we define business size. As with many things in the cyber security industry, there is no one single standard to classify business sizes. Last year, we attempted to adjust our data classification to align with the OECD classification as closely as possible. Our business size classification is as follows:

Employee count	Size class
1-49	Small
50-249	Medium
250+	Large

In 2022, we observed that most victims were large organizations, accounting for 36% of all victims. Small organizations were the second most impacted group, making up 30% of all victims. Medium-sized organizations represented 24% of all victims. This is an interesting finding, as each business group takes approximately one-third. However, we were unable to find the employee count for 10% of victims, and hence, they are classified as 'Unknown'.

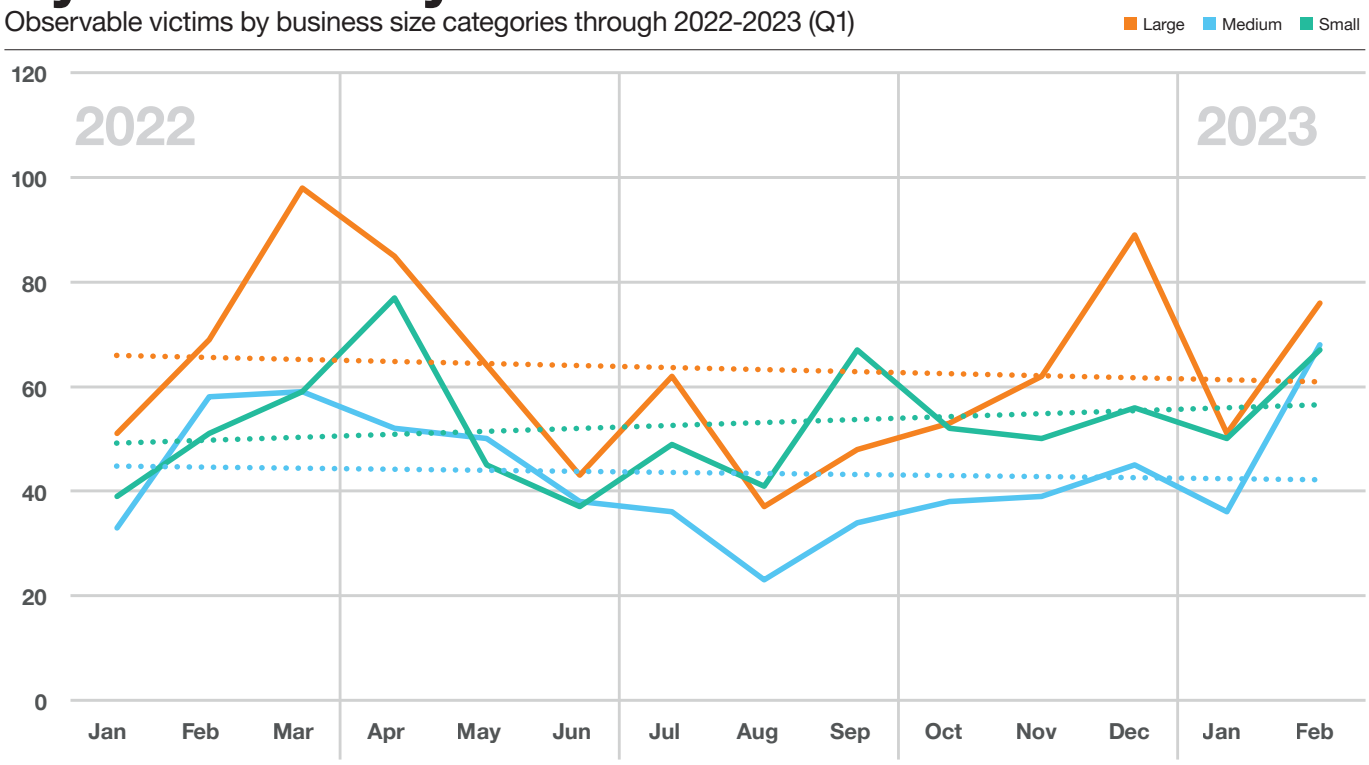
However, in the chart below we see that during 2022, small organizations have had a slight increase in victim count, while both medium-sized and large organizations saw a slight decrease. Nevertheless, since we are experiencing a busy Q1 2023, we expect all three business groups to be impacted by Cy-X moving forward in 2023.

Number of victims in each business size in 2022



Cy-X victims by size over time

Observable victims by business size categories through 2022-2023 (Q1)



Large organizations

Large organizations that became victims of Cy-X in 2022 were either from the Manufacturing sector (27%), Professional, Scientific, and Technical Services (11%), Educational Services sector (8%), Retail Trade (8%) and transportation and warehousing with 6%. These are the top five industries among large organizations targeted by Cy-X.

Small organizations

While small organizations were from the Professional, Scientific, and Technical Services sector (22%), Manufacturing (16%), finance and insurance (9%), Construction (7%) and Retail Trade (7%), for the top five industries.

Medium organizations

Medium-sized organizations were from the Manufacturing sector (21%), Professional, Scientific, and Technical Services (18%), Wholesale Trade (8%), Construction (7%) and health care and social assistance (5%), for the top five industries.

Size doesn't matter (too much)

In most cases, cyber extortionists opportunistically breach their victims. Once it is done, the malicious actors will conduct reconnaissance to determine the size of the organization. Through our observation, we noticed that threat actors do not do an extensive analysis but use publicly available information on revenue to calculate their ransom demands and use this specific number to determine whether a victim organization is able to pay it. Therefore, business size by employee count does not seem to matter too much regarding threat actors' choice of victim. In some cases, the process of choice, which we argue is opportunistic, is not targeted and seems to be an afterthought without any effort exerted to research the victim. As we have learned from the Conti leaks, in some cases, threat actors discuss AFTER victimization whether they should continue with their criminal activities or stop their attack due to principles of exclusion that threat actors sometimes pretend to have.

Additionally, what we are observing is that threat actors have been 'burning' themselves a little by targeting too big of an organization and consequently attracting too much attention to themselves by authorities.

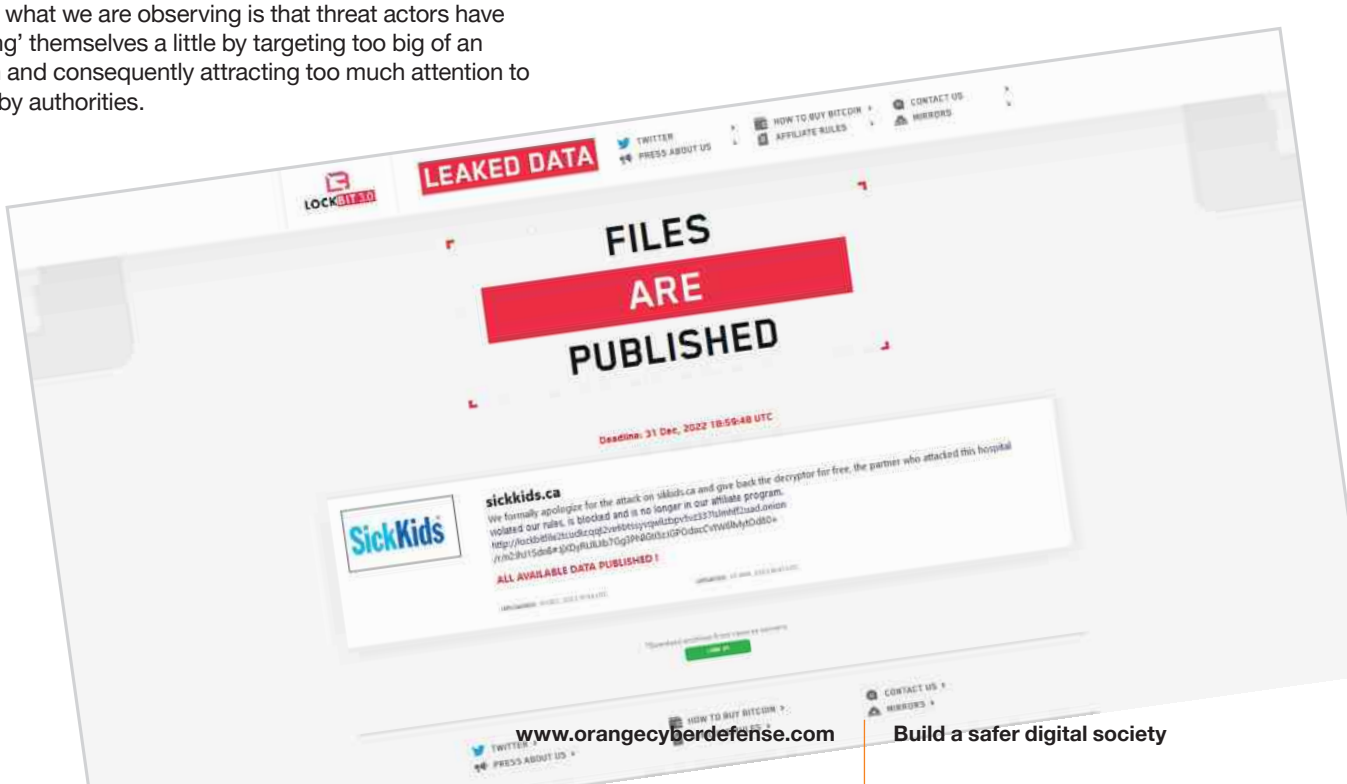
For example, when BlogXX, which is likely linked to REvil, breached Medibank back in October 2022, the group was not expecting such extensive media coverage and response. Australian authorities have made several official statements condemning foreign threat actors attacking Australian citizens, claiming they pose a threat to their national security. The country has since taken the lead in an international coalition against ransomware, which we will explore in chapter 7 "**Disrupting Cy-X**". This kind of political attention is bad for the Cy-X business as governments might ask (and even forbid) organizations to pay any ransom to these cybercriminals.

Yet, some of these groups know this and take it into account, as the world observed with Conti attacking Costa Rica in April 2022, compromising 27 different ministries over several weeks[26], resulting in Costa Rica declaring a state of emergency.

Other groups try to apologize and remedy their criminal actions. Indeed, back in December 2022, a LockBit affiliate breached Toronto's Hospital for Sick Children (SickKids) which resulted in a major backlash against them. More than 10 days after the attack, LockBit apologized, released a free decryptor and presumably fired the affiliate who victimized the hospital, adding that their rules do forbid attacks against institutions where damage to the files could lead to death. However, on April 27, 2023, another hospital was uploaded to LockBit's leak site. The hospital in question reported that for an entire weekend the access to ambulances for the emergency department were blocked[27]. Therefore, it is not advisable to rely on any statements made by threat actors.

Consequently, for Cy-X groups, targeting smaller entities will not draw too much attention to themselves. However, smaller victim organizations might have less means to pay the demanded ransom.

Another option for Cy-X groups is to target critical infrastructure in small or developing countries like Vanuatu, Costa Rica, Chile, Montenegro or African countries.



Countering the menace:

Disrupting Cy-X

In 2022 we have witnessed several activities by governments, local authorities and international collaborations to attempt to disrupt the criminal activities of cyber extortionists. In this chapter we will explore what has been done in 2022, and how this might have affected the criminal ecosystem.


POLICE

Law enforcement activities

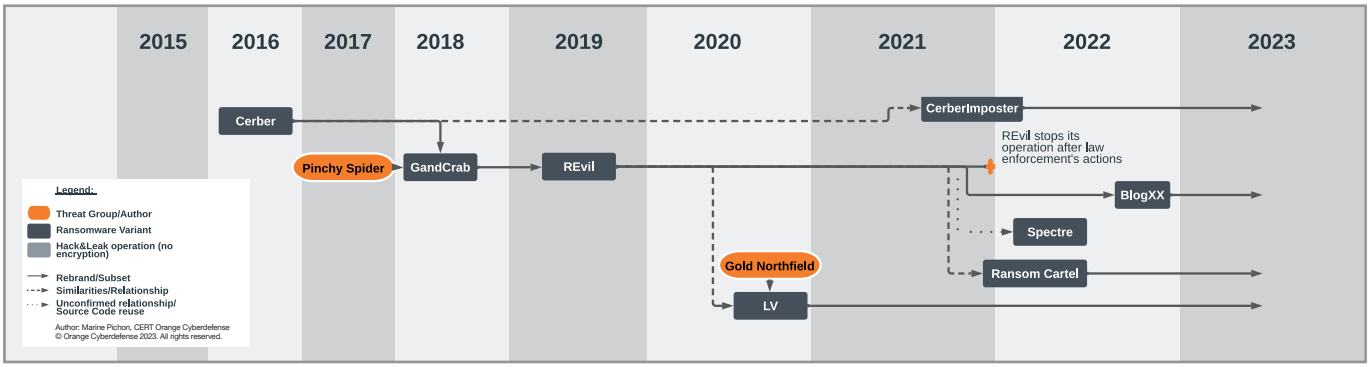
In 2021, we observed a rise in efforts to combat Cy-X, which we considered significant but not sufficient in reducing the prevalence of this crime. We assessed the number of victims and found that despite the increased efforts by law enforcement and governments, Cy-X continued to increase among organizations worldwide in 2021. However, we are interested in exploring if this trend has changed in 2022 and whether these activities had any potential disruptive impact on the criminal ecosystem.

In January 2022, 14 members of the prominent Cy-X group REvil were arrested by Russian law enforcement[28].

To date, this was one of the rare instances where Russia responded to a request from the US to arrest Russian nationals suspected to be involved in the REvil criminal operation.

In hindsight, it is possible that Russia's actions were not solely aimed at disrupting cybercrime but rather an attempt to distance itself from the cybercriminal network, which is believed to have many Russian nationals. Although the timing of Russia's arrests of suspected REvil members is suspicious, as they occurred just a few weeks before Russia's invasion of Ukraine.

Others speculate that this might have been an attempt to steer the media narrative and distract from ongoing cyberattacks, such as the deployment of a wiper called WhisperGate against Ukraine[29].



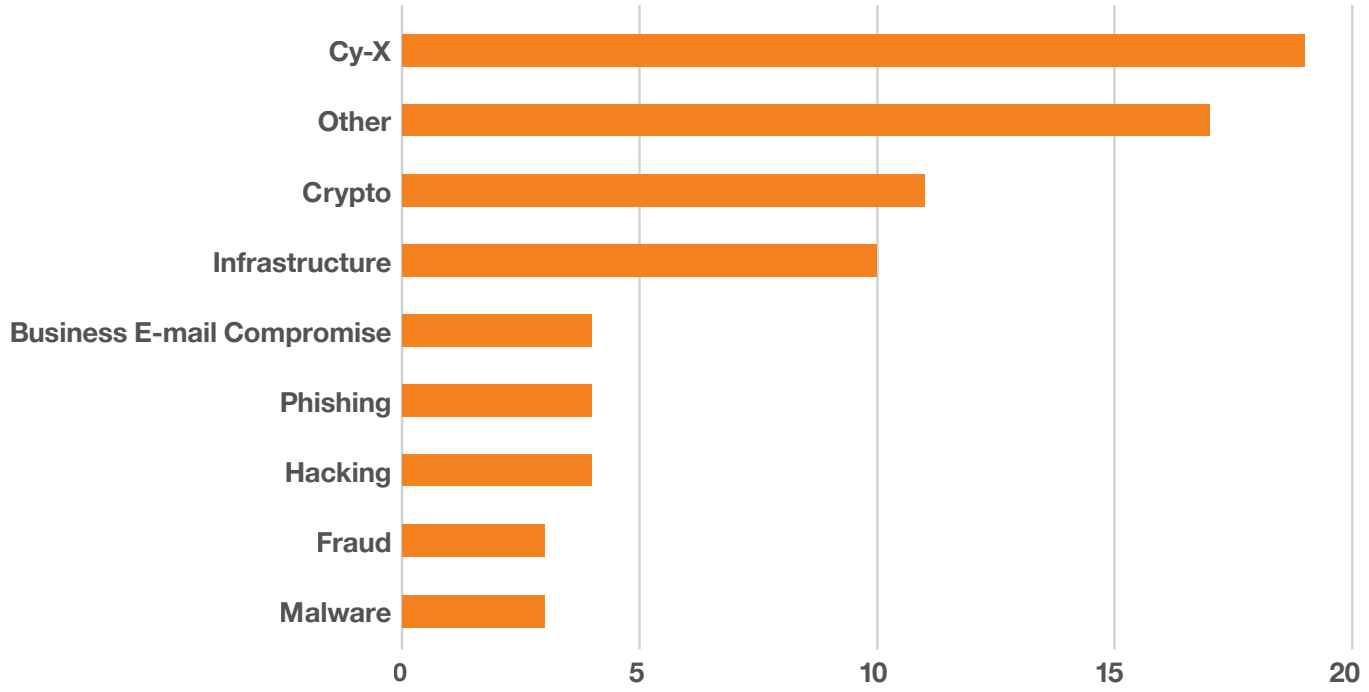
Disruption of the REvil group by law enforcement

For the Cy-X threat landscape, the REvil arrest has not shown too much effect as their criminal operation had been presumably offline since July 2021 (after the Kaseya attack) but was in the process of rebranding into new sub-groups such as BlogXX or RansomCartel[30].

Therefore, we did not see any impact on the victim count directly resulting from those arrests. In general, Orange Cyberdefense has tracked 75 law enforcement activities in 2022 and Cy-X-related activities were the most frequently addressed, as shown below.

Countering Cybercrime: Law Enforcement

Types of cybercrime activities targeted by law enforcement in 2022



The predominant type of Cy-X-related law enforcement activity in 2022 we saw was arrests, followed by extraditions. There were also announcements of sentences of individuals involved in Cy-X, albeit to a lesser extent. Finally, some governments announced and established collaborative initiatives to fight Cy-X, which we will briefly explain in this chapter.

An example of disrupting Cy-X in 2022 is the operation against Hive. In July 2022, the FBI infiltrated the Hive systems. The FBI remained in the Hive's network without their knowledge for six months and assisted hundreds of victims by providing decryption keys.

In January 2023, they seized Hive's servers and leak site, resulting in the takedown of Hive infrastructure and the end of their ongoing extortion operation[31]. This was one of the first cases in a long time where we observed 'hacking back' capabilities used within the criminal field of Cy-X, resulting in a somewhat successful technical disruption of this group's operation:

"The Department of Justice's disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators," said Deputy Attorney General Lisa O. Monaco. "In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than $130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat.[32]"

It remains to be seen whether this action will prove to be truly effective and for how long. While no arrests were made,[33] this gives the threat actors the option to lay low, start over under a new name, or join an existing RaaS operation.

In the Fall of 2022, there was an instance where the response of law enforcement agencies had a discouraging effect on criminal activities.

On September 22nd, a group known as "optusdata" claimed to have stolen data from more than 10 million customers of the Australian telecommunications company Optus. The criminals demanded a ransom of $1 million in cryptocurrency. The Australian Federal Police in cooperation with other law enforcement agencies responded with its own counter-operation and the following statement:

"We are aware of reports of stolen data being sold on the dark web and that is why the AFP is monitoring the dark web using a range of specialist capabilities. Criminals, who use pseudonyms and anonymizing technology, can't see us but I can tell you that we can see them.[34]"

This immediately prompted the threat actors to stop their extortion demands and claims about deleting a stolen copy of the data, and apologize to both the Australian citizens whose data was already leaked and to Optus for the attack:

"Optus if your reading we would have reported exploit if you had method to contact. No security mail, no bug bountys, no way too message. Ransom not payed but we dont care any more. Was mistake to scrape publish data in first place.[35]" [sic]

Just a few weeks after the Optus breach, Australian health insurer Medibank experienced a large-scale Cy-X attack. On October 12, Medibank detected suspicious activity on their network, which over the course of several weeks turned into a nasty attack, in which threat actors used REvil's old leak site called "BlogXX" to start leaking Medibank's customer data.

Screenshot from the leak posted by the threat actor

As a result of these events, on November 12, the Australian government announced the launch of an offensive taskforce against cybercriminals and more specifically to "hack the hackers" behind the recent Medibank data breach[36]. The initiative "will day in, day out, hunt down the scumbags who are responsible for these malicious crimes against innocent people", said Cyber Security Minister Clare O'Neil[37].

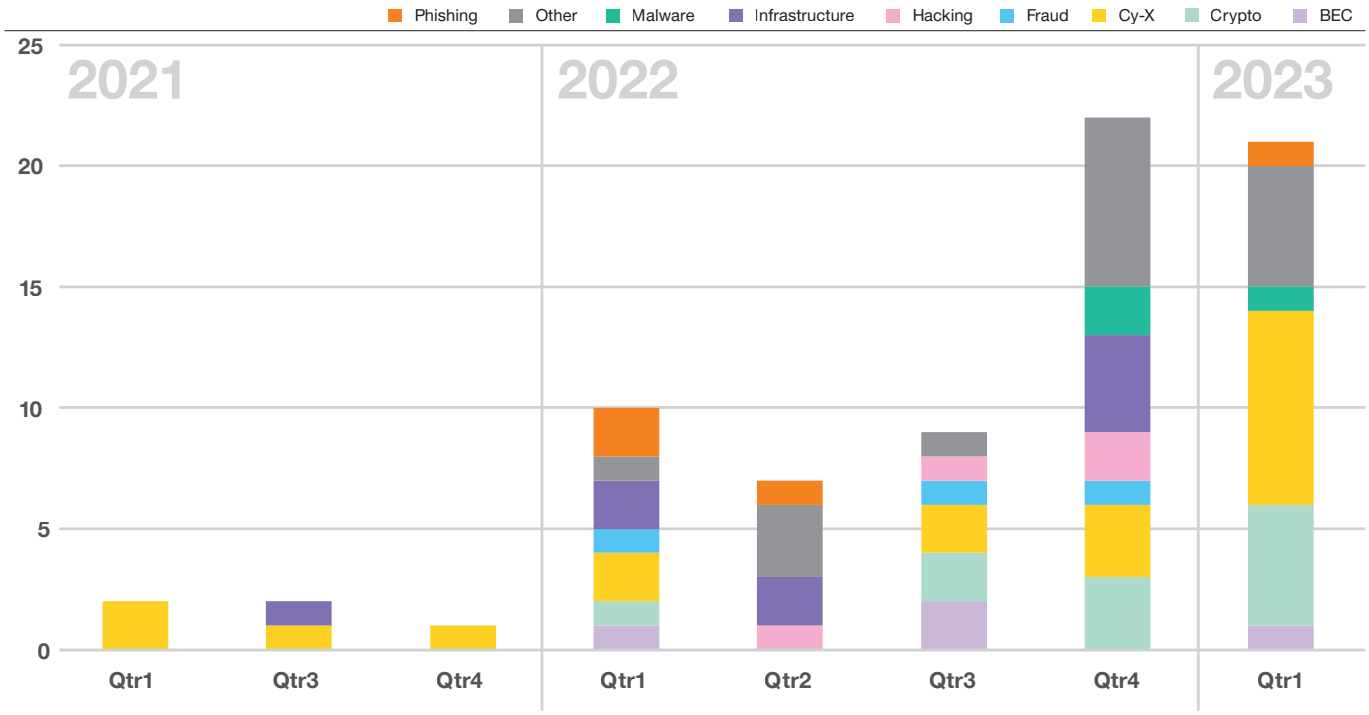
This was followed by the launch of an international task force to fight ransomware in January 2023. The task force sits under the US-led International Counter ransomware Initiative, that involves 37-like-minded governments[38].

We believe that this incident further supports our previous observation that when Cy-X victims generate too much attention, governments may respond with a deterrent action that could potentially impact cybercriminals in a positive way.

Collaborative initiatives such as the one mentioned previously are relatively new and have a reactive approach. But given the significant impact of Cy-X on individuals, organizations, and society, there is a pressing need for international cooperation and public-private partnerships across various sectors.

Law Enforcement over time

Cybercrime activities targeted by law enforcement over time



Another important step towards disrupting financially motivated crime is to address the means of payments. As shown above, we saw law enforcement activities related to illicit cryptocurrency payments increase in 2022. As Chainalysis describes in its 2023 Crypto Crime Report, victim payments have decreased lately as paying has become riskier due to sanctions[39] and a changing cyber insurance landscape imposing new restrictions on insurance payouts[40]. Additionally, we see law enforcement arrests on top of sanctions against cryptocurrency exchanges[41] and tumbler/mixer services[42], helping to disrupt the ransomware ecosystem.

In 2022 we noticed an increase in the usage of technical infrastructure takedown by threat actors, as shown in the chart above. This can be potentially effective in temporarily disrupting Cy-X. The US announced on April 24, 2023, that its focus will not be on arrests but disruption, as it did with Hive[43].

This goes in line with the recently announced US National Cybersecurity Strategy list of five objectives to Disrupt and Dismantle Threat Actors[44]:

1. **Integrate federal disruption activities**
2. **Enhance public-private operational collaboration to disrupt adversaries**
3. **Increase the speed and scale of intelligence sharing and victim notification**
4. **Prevent abuse of U.S.-Based infrastructure**
5. **Counter cybercrime and defeat ransomware**

Conclusion

In 2022, we have seen an increased number of law enforcement activities. Most actions were of a reactive nature, with Cy-X operators being disrupted when they start impacting too many victims, caused high losses to those impacted, or undermined critical infrastructure in certain countries.

However, these increased law enforcement activities shows threat actors and those providing services to them that their activities do not go unnoticed nor unpunished. Over the past two years, we have witnessed that when threat actors attack a large-scale victim organization, it triggers a response from governments. Activities observed the most in 2022 were: arrests, infrastructure takedowns, hacking back, and even sanctions against cryptocurrency services.

Consequently, all these actions combined might have a positive impact in combating cybercrime, and specifically Cy-X. We are curious and hopeful to see what effect the international taskforce led by Australia will have and what capabilities we are yet to see in disrupting this crime.

In the end, collaboration is key, a collective effort between the public and private sector will hopefully show an impact in the long-term.

Predictions

Outlook to 2023

While the changes in victim distribution across countries and industries are significant trends in the threat landscape of 2022, they provide limited insight into what may happen in 2023.

The 'calm before the storm' is over

Unfortunately, the first quarter of 2023 saw the largest number of victims ever recorded. This came as a surprise and makes us wonder whether 2022 was the year of 'distraction' and rebranding for some of the major Cy-X operations that Orange Cyberdefense is monitoring.

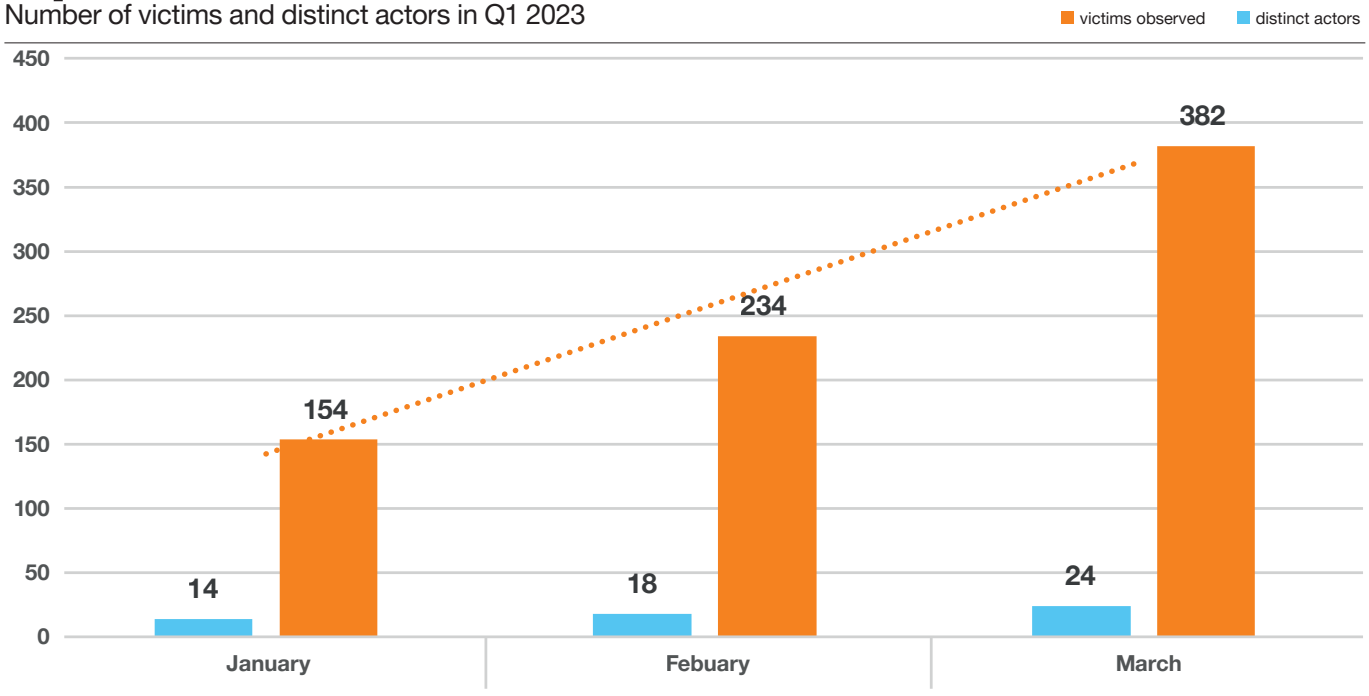
We believe collaboration between the public and private sectors can be improved to demonstrate a united front in combating this type of crime. Here are some potential developments that could emerge in 2023 and beyond:

- The government actions that disrupted Cy-X operations in 2022 and early in 2023 may lead some groups to consider other cybercriminal activities with higher returns on investment and lower risk.
- Private organizations have become more difficult to compromise (as evidenced by the shift towards less developed countries and smaller victims).
- GAFAM's anti-cybercrime improvements will cause ransomware groups to find it harder to gain a foothold (one example of this is the default blocking of macros in Office). This explains why infrequently used initial access vectors emerge again (SEO poisoning, USB worms, etc.). No doubt the more advanced groups have already launched R&D programs to overcome the limitations that information and security solutions now embed. Groups might also move to a more data-centric extortion focus (vs. a system- i.e., encryption one).
- Any available misconfiguration and vulnerability (including in third-party solutions, cloud instances, etc.) will be researched and exploited.
- Cyber extortionists will rely on much more aggressive techniques to apply pressure on victims, using the very data they exfiltrated. We are already seeing groups contacting their victims and partners by phone for example, including members of the board. One potential trend for 2023 is that threat actors may take greater risks and invest in new technical capabilities to improve their extortion strategies and continue profiting from malicious activities.

Overall, despite the increase in victim numbers during the first quarter of 2023, there is hope that the continuous efforts to combat the Cy-X threat may yield some positive outcomes and victories in 2023. But to achieve this, we must pull together as an industry and keep sharing information about threats and attacks. By partnering with your industry peers, you can stay one step ahead of Cy-X groups and be in a much stronger position to safeguard your organization and help build a safer society for tomorrow.

Update 2023

Number of victims and distinct actors in Q1 2023



Report summary

We have to keep the pressure up!

The Cy-X threat landscape continued to evolve and become more complex in 2022. Threat actors demonstrated increasing levels of sophistication and determination, while also leveraging cybercrime-as-a-service offerings to expand the market to entry-level operators.

But, despite cybercriminals striving to continually improve their capabilities, such as boosting their encryption speed, they still face several obstacles from their suboptimal operational security practices, such as the complete leak of internal communications by Conti, the leak of the LockBit builder, and discovering that the internal network of Hive had been hacked by law enforcement for six months. Despite these mistakes, Cy-X threats continue to accelerate (as Q1 2023 victim data shows).

While the impact of geopolitical world events, such as the war in Ukraine, created a potential risk for organizations in NATO-member countries, the organizations in Latin America, Southeast Asia, and Oceania experienced the biggest increase in victim numbers. There are several explanations for this trend:

1. Firstly, the countries that are most affected by Cy-X are those with the highest number of registered businesses, meaning that the level of impact is determined by the availability of potential victim organizations (and their wealth).
2. Secondly, Cy-X is primarily a financially motivated crime, and while it may have had some political implications in the aftermath of the Ukraine invasion, cybercriminals are still predominantly driven by the prospect of financial gain. The recent Conti incident highlights the perils of cyber criminals drawing too much attention to themselves.
3. Lastly, we have observed an increase in offensive responses from governments and law enforcement agencies towards cyber extortionists. We hypothesize that victim organizations from developing regions might be more appealing to cybercriminals as they are less likely to trigger a harsh response, such as those seen in the US. Although this also aligns with the incidents in Australia, where the country experienced two large-scale attacks within a few weeks in Q3 2022 (Optus & Medibank). The response resulted in a newly formed government task force to combat Cy-X attacks.

But the question of whether law enforcement activities in 2022 have been effective is a challenging one. Despite the increased efforts to combat ransomware, the number of victims has not seen much of a decrease. Nevertheless, we remain optimistic that the more proactive measures taken to disrupt the Cy-X criminal ecosystem will eventually lead to a positive impact in the long run.

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.

Appendix A

Ransomware group	Still active in 2022?	Only extortion	RaaS	Leak site
Abrahams Ax	Yes	No	No	Yes
Atomsilo	Yes	No	Yes	Yes
Avaddon	Yes	No	Yes	Yes
AvosLocker	Yes	No	Yes	Yes
Axxes (Haron/Middas)	Yes	No	Yes	Yes
BianLian	Yes	No but now yes	N/A	Yes
Bl00dy	Yes	No	No	Yes (Telegram)
Black Basta	Yes	No	Yes	Yes
BlackByte	Yes	No	Yes	Yes
BlackCat	Yes	No	Yes	Yes
BlackMagic	Yes	No	No	Yes
BlogXX	Yes	No	N/A	Yes
Board Of Shame/RedAlert	Yes	No	N/A	Yes
CerberImposter	Yes	No	Yes	No
Cl0p	Yes	No	Yes	Yes
Conti	Yes (now defunct)	No	Yes	Yes
Cuba/VisVendetta	Yes	No	No	Yes
DagonLocker/QuantumLocker	Yes	No	Yes	No
Daixin	Yes	No	No	Yes
Dark Angels	Yes	No	No	Yes
DataLeak	Yes	Yes	No	Yes
Diavol	Yes	No	Yes	No
DJVU	Yes	No	N/A	No
DoppelPaymer/Grief	Yes	No	Yes	Yes
Entropy	Yes	No	N/A	Yes
Everest Ransom Team	Yes	Yes	No	Yes
Gwisin	Yes	No	No	No
Hive	Yes (now defunct)	No	Yes	Yes
Icefire	Yes	No	N/A	Yes
Karakurt	Yes	Yes	No	Yes
Lapsus$	Yes	Yes	No	Yes (Telegram)
Lilith	Yes	No	N/A	Yes

Ransomware	Still active in 2022?	Only extortion	RaaS	Leak site
Lockbit	Yes	No	Yes	Yes
Lorenz	Yes	No	N/A	Yes
LV ransomware	Yes	No	Yes	Yes
Mallox	Yes	No	N/A	Yes
Medusa Blog	Yes	No	No	Yes
MedusaLocker/ransomwareBlog	Yes	No	Yes	Yes
Mimic	Yes	No	N/A	No
Monti	Yes	No	N/A	Yes
Mortal Kombat	Yes	No	No	No
Moses Staff	Yes	No	No	Yes
n3tw0rm/Pay2Key	Yes	No	No	Yes
Nevada	Yes	No	Yes	Yes
Nokoyawa	Yes	No	N/A	Yes
Onyx	Yes	No	No	Yes
Rook/Night Sky/Pandora	Yes	No	Yes	Yes
Payload.bin	Yes	No	No	Yes
Play	Yes	No	No	Yes
Pysa	Yes	No	Yes	Yes
Qilin	Yes	No	Yes	Yes
Quantum	Yes	No	Yes	Yes
Ragnar	Yes	No	Yes	Yes
Ransom Cartel	Yes	No	Yes	Yes
RansomEXX	Yes	No	Yes	Yes
RansomHouse	Yes	Yes	No	Yes
Relic	Yes	No	No	Yes
Royal	Yes	No	No	Yes
SchoolBoys/TommyLeaks	Yes	Yes	No	N/A
Silent Ransom	Yes	Yes	No	N/A
Snatch	Yes	No	Yes	Yes
SolidBit	Yes	No	Yes	No
Stormous	Yes	No	No	Yes
Suncrypt	Yes	No	Yes	Yes
Trigona	Yes	No	N/A	Yes
Vice Society	Yes	No	Yes	Yes
Xing Team	Yes	No	N/A	Yes
Yanluowang	Yes (now defunct)	No	Yes	Yes
Zeppelin	Yes	No	Yes	No

Appendix B

Country/region definitions we use in this report

Country	Region
AO	Africa
BH	Mid East
BR	Latin America
BR	Latin America
CA	CA
CN	CN
DE	Europe
DK	Nordic
DZ	Africa
EG	Africa
ES	Europe
ET	Africa
FI	Nordic
FR	Europe
GB	GB
IN	IN
IT	Europe
JO	Mid East
JP	East Asia ex CN
KE	Africa
KW	Mid East
MA	Africa
NG	Africa
NO	Nordic
QA	Mid East
SA	Mid East
SE	Nordic
SY	Mid East
TR	Mid East
US	US
ZA	Africa
IL	Other
IR	Other
AU	AU & NZ
MX	Latin America
PT	Other
AE	Mid East
BE	Europe
CY	Europe
CZ	Europe
GR	Europe
ID	SEA
KR	East Asia ex CN
TW	East Asia ex CN

Country	Region
AR	Latin America
AT	Europe
CH	Europe
CO	Latin America
CR	Latin America
DO	Latin America
IE	Europe
JM	Other
LU	Europe
MY	SEA
NL	Europe
PE	Latin America
PL	Europe
VN	SEA
MK	Europe
NZ	AU & NZ
PR	Latin America
SG	SEA
TH	SEA
LK	South Asia ex India
HK	East Asia ex CN
SK	Europe
ZZ	Other
CL	Latin America
BS	Other
DR	Other
HR	Europe
PK	South Asia ex India
UA	Europe
PH	SEA
RO	Europe
ZW	Africa
BO	Latin America
LT	Europe
FJ	Other
MT	Europe
RU	Russia
Unknown	Other
EC	Latin America
EE	Europe
HU	Europe
TH	SEA
MY	SEA
TH	SEA

Country	Region
VE	Latin America
ZM	Africa
HN	Latin America
x	Other
HT	Other
PA	Latin America
PY	Latin America
MN	East Asia ex CN
SC	Africa
BF	Africa
CI	Africa
NI	Latin America
SV	Europe
BW	Africa
BA	Europe
BD	South Asia ex India
KRW	Other
KZ	Central Asia
VI	Other
BB	Other
LB	Mid East
GH	Africa
SI	Europe
CG	Africa
GF	Other
GT	Latin America
KY	Other
RS	Europe
SN	Africa
TN	Africa
TZ	Africa
OM	Mid East
BG	Europe
AL	Europe
EA	Other
-	Other
ME	Other
UY	Latin America
GA	Other
TT	Latin America
GL	Nordic
GM	Africa
MC	Europe

Literature & sources

[1] https://www.census.gov/naics/

[2] ttps://data.oecd.org/entrepreneur/enterprises-by-business-size.htm

[3] The Vocabulary for Event Recording and Incident Sharing - http://veriscommunity.net/

[4] https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

[5] https://intel471.com/blog/a-ransomware-forecast-for-2023

[6] https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

[7] https://go.chainalysis.com/2023-crypto-crime-report.html

[8] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

[9] https://www.reuters.com/world/europe/finland-set-join-nato-historic-shift-while-sweden-waits-2023-04-04/

[10] https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics?CMP=share_btn_link

[11] https://edition.cnn.com/2023/04/10/politics/classified-documents-leak-explainer/index.html

[12] https://unit42.paloaltonetworks.com/incident-response-report/

[13] https://cybersecurityworks.com/

[14] https://www.orangecyberdefense.com/global/blog/playing-the-game

[15] https://github.com/Orange-Cyberdefense/CVE-repository

[16] https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

[17] https://www.rapid7.com/blog/post/2022/10/06/exploitation-of-unpatched-zero-day-remote-code-execution-vulnerability-in-zimbra-collaboration-suite-cve-2022-41352/

[18] https://p2a.cert.orangecyberdefense.com/analysis/174844/publicshared/5CMH8DIYPKH56H3W

[19] https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service

[20] https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/

[21] https://www.nbcnews.com/tech/security/ransomware-hackers-new-tactic-calling-directly-rcna6466

[22] ttps://www.naics.com/business-lists/counts-by-country/

[23] Present: Kazakhstan, Russia, Ukraine. Absent: Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, Uzbekistan

[24] https://www.recordedfuture.com/russias-war-against-ukraine-disrupts-cybercriminal-ecosystem

[25] https://www.cisa.gov/resources-tools/resources/stopransomware-vice-society

[26] https://www.ft.com/content/9895f997-5941-445c-9572-9cef66d130f5

[27] https://www.wired.it/article/cyberattaccomultimedica-pronto-soccorso-lombardia/

[28] https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/

[29] https://www.recordedfuture.com/russias-war-against-ukraine-disrupts-cybercriminal-ecosystem

[30] ttps://therecord.media/revil-gang-shuts-down-for-the-second-time-after-its-tor-servers-were-hacked

[31] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

[32] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

[33] https://therecord.media/ransomware-experts-laud-hive-takedown-but-question-impact-without-arrests

[34] https://www.malwarebytes.com/blog/news/2022/09/optus-data-breach-attacker-says-sorry-it-was-a-mistake

[35] https://www.bleepingcomputer.com/news/security/optus-hacker-apologizes-and-allegedly-deletes-all-stolen-data/

[36] https://theconversation.com/a-new-cyber-taskforce-will-supposedly-hack-the-hackers-behind-the-medibank-breach-it-could-put-a-target-on-australias-back-194532

[37] https://www.abc.net.au/news/2022-11-12/medibank-cyber-hack-optus-data-breach-task-force-afp/101647168

[38] https://minister.homeaffairs.gov.au/ClareONeil/Pages/australia-leads-global-task-force-to-fight-ransomware.aspx

[39] https://home.treasury.gov/news/press-releases/jy0916

[40] https://go.chainalysis.com/2023-crypto-crime-report.html

[41] https://therecord.media/law-enforcement-takes-down-crypto-exchange-allegedly-used-to-launder-15-million-in-ransomware-payments

[42] https://www.theblock.co/post/220108/europol-shuts-crypo-tumbler-chipmixer-seize-46m-in-bitcoin?utm_source=rss&utm_medium=rss

[43] https://cyberscoop.com/doj-cybercrime-disruption-ransomware/

[44] https://spock.int.orangecyberdefense.com/pages/viewpage.action?pageId=167863623

Teams involved

This report is the outcome of a collaborative effort among various teams at Orange Cyberdefense and an external partner, employing a specific methodology to gather and analyze the information we collected. Our aim is to gain a comprehensive understanding of Cy-X crime and the constantly evolving threat landscape of this criminal ecosystem. Please find below details of our teams and partners.

Global CERT Orange Cyberdefense constantly monitors threat actors, to anticipate new threats impacting our clients. For instance, we help them to discover vulnerabilities affecting their assets.

The **World Watch team** conducts daily searches for new malware and IOCs, techniques or infrastructure set up by attackers.

We conduct hundreds of response engagements with our **CSIRT teams** each year to investigate attacks that most of the time have an extortion motive.

The **Cybercrime Fighting team** focuses on detecting and mitigating cybercriminal threats, 24/7. The team deals with different operational, tactical, and strategic threats targeting Orange Cyberdefense customers every day.

Security Research Center is a specialist security research unit within Orange Cyberdefense that helps us fulfil our mission of being a trusted partner to our customers by ensuring that we identify, track, analyze, communicate, and act upon significant developments in the security landscape that may impact them. Our team of dedicated researchers is globally recognized and frequently showcased at international security events and in leading publications.

Intel471 (external) – Intel 471 is a global CTI business that empowers organizations to win the cybersecurity war with comprehensive coverage of the criminal underground. Leveraging its SaaS intelligence platform TITAN, it arms businesses with cyber threat intelligence enabling security teams to identify, prioritize, and prevent attacks before they occur.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 18 SOCs, 14 CyberSOCs and 8 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

www.orangecyberdefense.com
Twitter: @OrangeCyberDef