Orange
Cyberdefense

Security Intelligence | Research Report

Quarterly Report
June 23

Contents

Introduction

Apple Zero Day
Apple has issued a new round of Rapid Security Response (RSR) updates to address a zero-day bug reported to have been exploited in attacks on iPhones, Macs, and iPads. The company warns that these patches provide important security fixes and are recommended for all users. The flaw is found in Apple's WebKit browser engine, allowing attackers to gain arbitrary code execution on targeted devices.

At the time of writing Apple pulled the software update. This came after reports that some websites, including Instagram, Facebook and Zoom, began showing "Unsupported Browser" errors in Safari on patched devices.

Another MOVEit SQLi
Progress Software has discovered and patched another critical SQL injection vulnerability in its MOVEit Transfer secure file transfer software. The vulnerability, tagged as CVE-2023-36934, could allow unauthenticated attackers to gain unauthorized access to the database. This vulnerability is critical as it can be exploited without logging in, therefore allowing attackers without valid credentials to exploit it. The latest security update also addresses two other high-severity vulnerabilities: CVE-2023-36932 and CVE-2023-36933.

BlackCat Cy-X Group Claim Barts Health Attack
Barts Health NHS Trust has allegedly been targeted by Russian ransomware gang BlackCat (aka ALPHV), who claim to have stolen over 7TB of sensitive data in a cyber-attack. The trust, which oversees over 2.5 million patients, has been listed on the gang's dark web leak site where they claim to have stolen data including CVs, financial reports, and internal hospital information. The trust was set a deadline for cooperation, but this has passed with no sign of any data being published.

At a glance

Apple has now patched ten zero-day flaws, since the beginning of 2023, used to attack iPhones, Macs, and iPads.

Three zero-days being used to deploy Triangulation spyware on iPhones via iMessage zero-click exploits were patched earlier this month.

In May, Apple fixed three more zero-days, one of which it was reported was likely used for the installation of mercenary spyware.

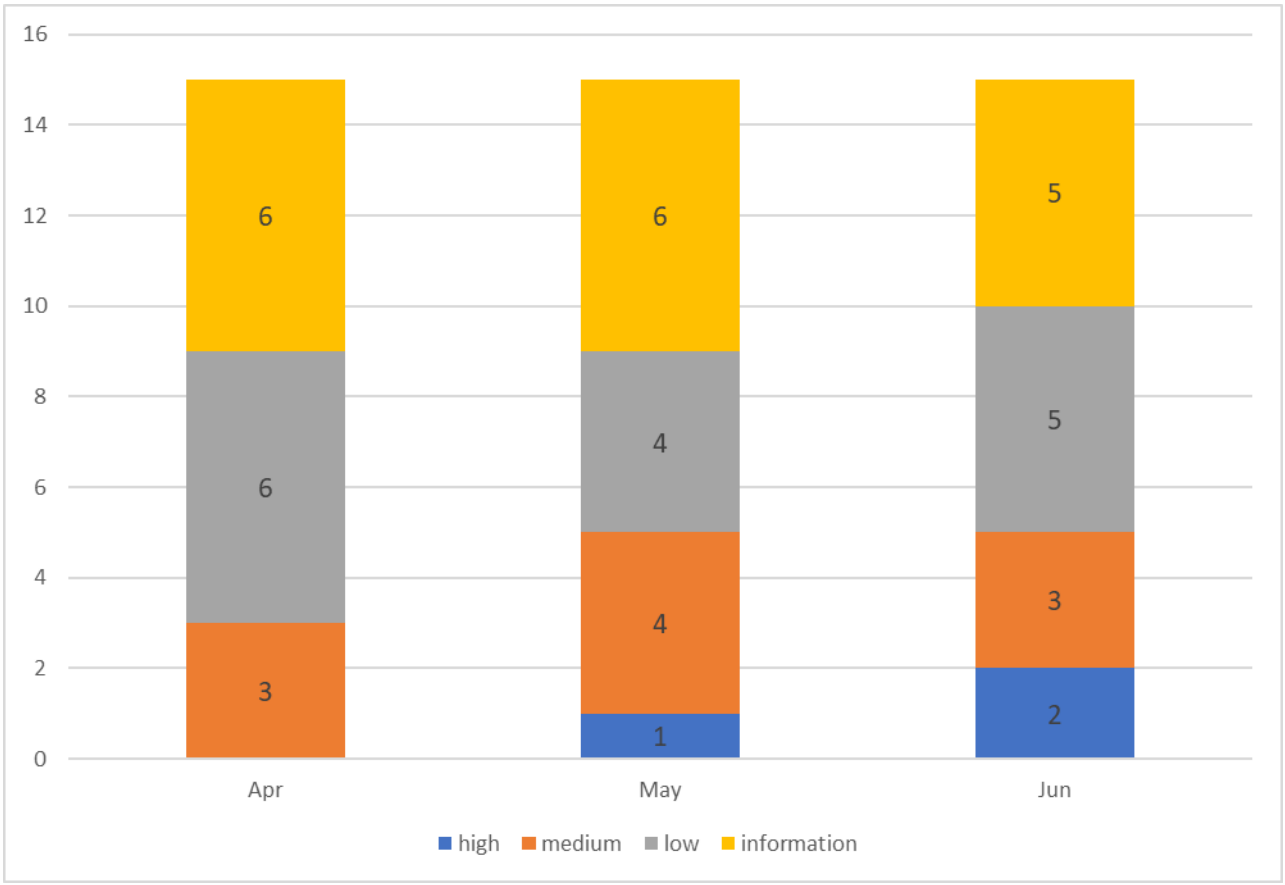
In April, Apple fixed two other zero-days, used in Android, iOS, and Chrome exploit chains, to deploy spyware on high-risk targets devices.

In February, Apple patched another WebKit zero-day, allowing code execution on vulnerable iPhones, iPads, and Macs.

Despite Apple halting the rollout of the latest Rapid Security Response update, you should try and deploy it as soon as possible once Apple releases a fixed version.

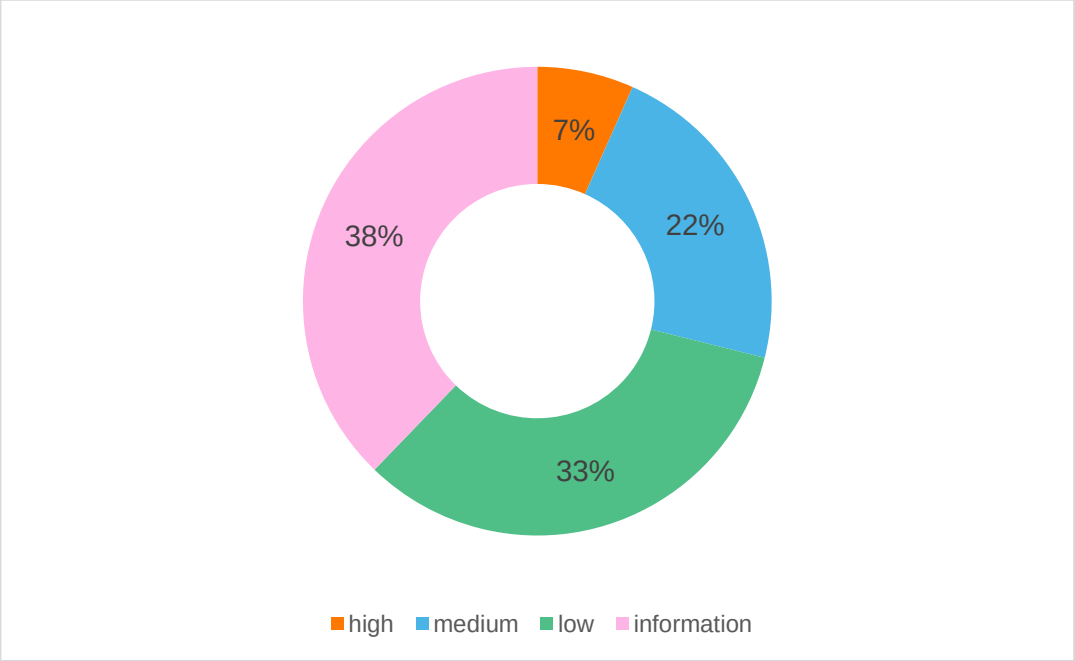
World Watch Review

The Orange Cyberdefense CERT published a total of 45 new World Watch advisories from April 2023 up to and including June 2023, along with updates to a further 67 previously published advisories. The volume of new advisories has dropped slightly from Q1 with there being eight less than the previous quarter.



Breakdown of new advisories by severity for Q2 2023

As in Q1 2023 we again did not publish a critical rated advisory in Q2 either, with the last critical advisories being published in Q4 2021. The severity rating of advisories for Q2 is predominantly made up of advisories rated as Information or Low urgency, with eleven Medium and just three rated as High.



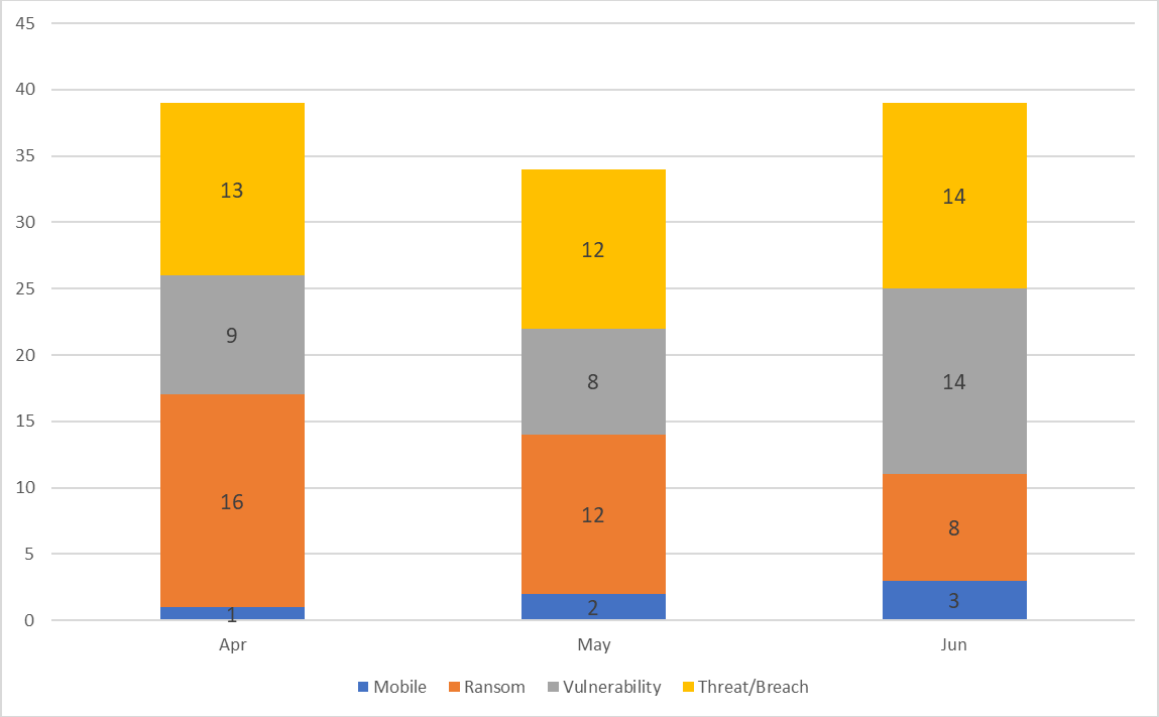
Breakdown of new advisory severity for Q2 2023

Different Approach

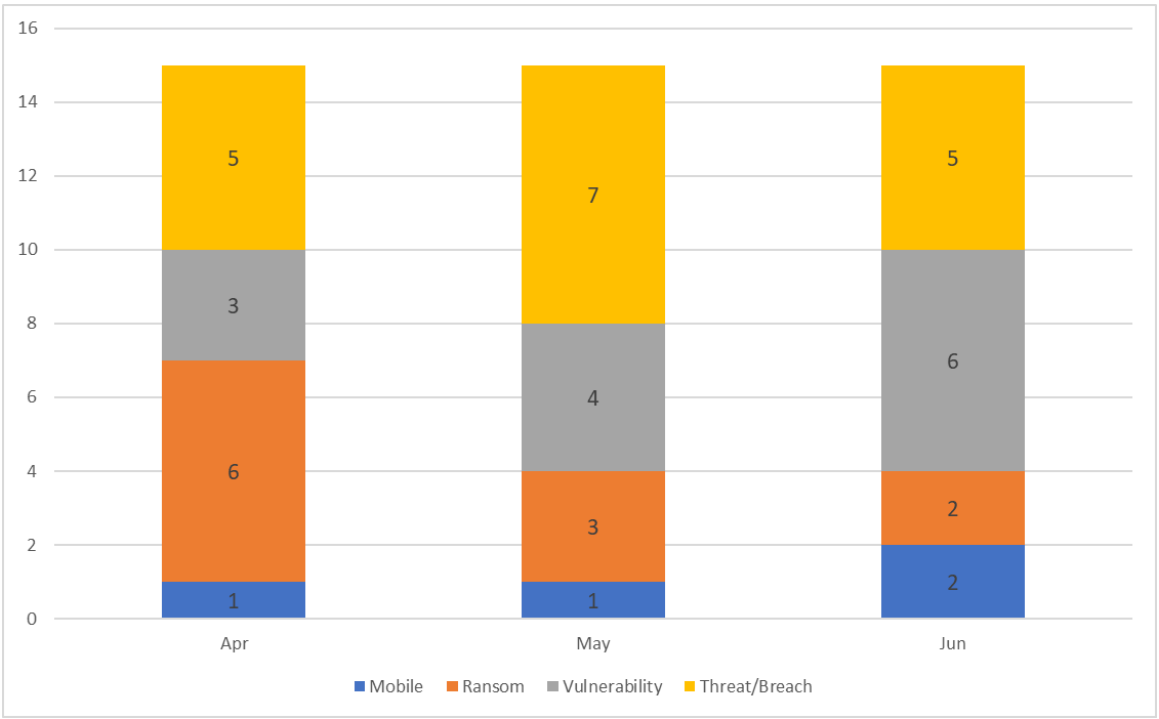
As we did for Q1 of 2023 we are again looking at Q2 using an approach we used in compiling parts of the OCD **Security Navigator 2023** report, namely using Machine Learning (ML) to help analyze published advisories. ML algorithms were used to highlight potentially interesting occurrences of keywords such as CVEs and related vendors. We also used ML to ascribe themes to the advisories. These themes are limited to Vulnerabilities, Threat/Breach, Ransom, and Mobile.

Advisory Summary

This quarter the number of advisories classified as Threat/Breach dropped slightly compared to Q1 2023, in fact this quarter saw a fairly even spread across all advisory classifications, excluding Mobile which we still see very little of. When examining just the new advisories we see this same pattern remains.



All World Watch advisories published by theme in Q2 2023



New World Watch advisories published by theme in Q2 2023

As alluded to above our machine learning classifier again identified very little discussion involving attacks against mobile phones during Q2. Of the four new advisories labelled as Mobile one was published in each of April 2023 and May 2023, with the remaining two being published in June 2023. Those advisories are respectively:

712329 - Israeli spyware vendor QuaDream spotlighted by the Citizen Lab and Microsoft

- Microsoft Threat Intelligence and the Citizen Lab just released two joint deep-dive reports on a commercial spyware vendor named QuaDream. Based in Israel, the company specializes in the development and sale of advanced digital offensive technology to government clients. The company is known for its spyware marketed under the name “Reign”, which, like NSO Group’s Pegasus spyware, reportedly utilizes zero-click exploits to hack into target devices.
- The spyware was notably used to target at least five civil society victims in North America, Central Asia, Southeast Asia, Europe, and the Middle East, including journalists, political opposition figures, and an NGO worker. According to the Citizen Lab, an important part of QuaDream’s clients are countries which are already known to abuse spyware to infringe human rights.

732381 – 9 million Android smartphones sold pre-infected with malware

- At the 2023 BlackHat Asia conference in May, Trend Micro presented their research on “Lemon Group”, a new threat actor who compromised multiple Android smartphones’ ROM images with a malware named Guerilla. On May 17, Trend Micro published a report looking deeper into the planted malware. Almost nine million Android devices sold across the world over the past five years seem concerned.
- Precisely, the malware has been found in original equipment manufacturer (OEM) firmware images of over 50 brands of low-cost Android smartphones. The implant is a tempered dependency library loading the main plugin into the zygote process. The implant can then fetch new plugins for additional malicious capabilities

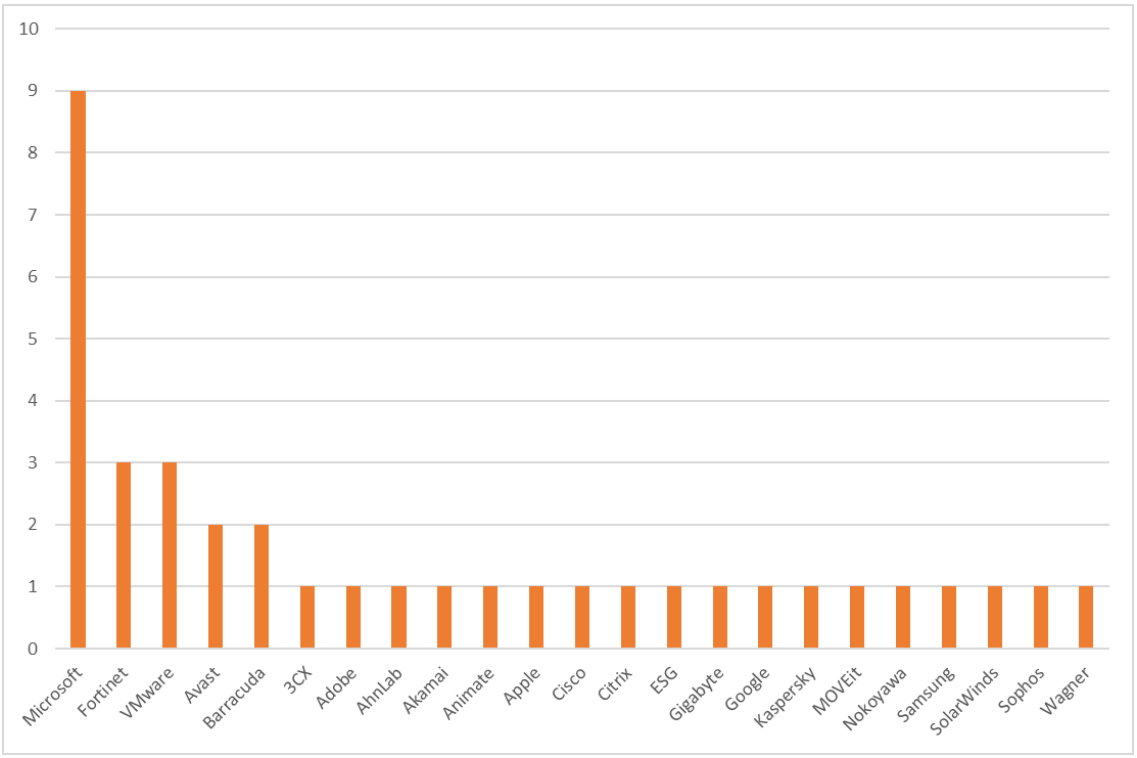
736303 – Russian antivirus DrWeb discovers SpinOk spyware in 100 mobile apps

- Russian antivirus vendor Doctor Web has discovered that a new Android malware distributed as a marketing-driven SDK has been collectively downloaded over 400 million times. Dubbed "SpinOk", this spyware steals private data stored on users' devices and sends it to a remote server.
- Nevertheless, it's important to note that this malevolent SDK has been embedded mostly in around 100 entertainment applications. It lures developers to use it by promising to increase the app user retention, through various "daily rewards". For this reason, it is unlikely that smartphone devices managed by IT departments will be affected by this threat.

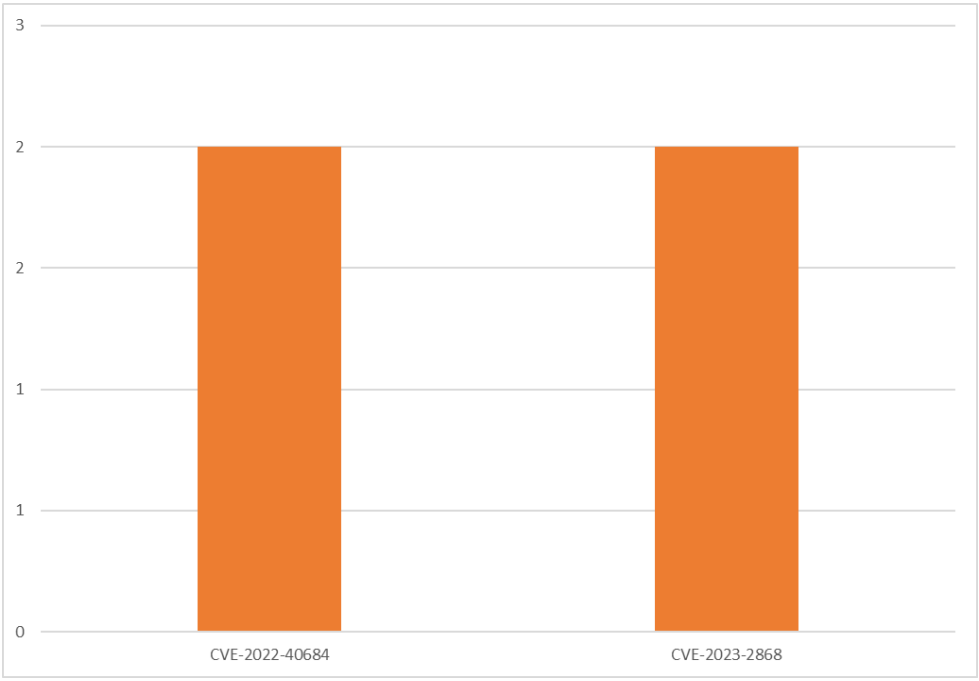
736923 – Unknown threat actor targeting Russian iPhones with zero-click exploit since 2019

- Kaspersky uncovered a still-ongoing espionage operation targeting iPhones, and added that the company itself is one the targets of this campaign led by an unknown threat actor. Russia's Federal Security Service (FSB) announced Russian diplomats were also targeted. The FSB accuses Apple of collaborating with U.S National Security Agency (NSA) to infect Russian devices.
- The campaign leverages a zero-click iMessage exploit on iOS 15.7 and previous versions of the operating system. According to Kaspersky, the operation is still ongoing and seems to have started in 2019.

When we consider the advisories classified as vulnerabilities during Q2 2023 we note several prominent vendor names, which is to be expected. Microsoft, for example, will likely always be present due to their monthly Patch Tuesday release cycle, other vendors who only release patches on an ad-hoc basis when vulnerabilities are discovered and reported will come and go.



Vendors mentioned in Vulnerability World Watch advisories for Q2 2023



CVEs encountered more than once in Vulnerability World Watch Advisories for Q2 2023

CVE ID	Vendor / Product
CVE-2022-40684	Fortinet Multiple Products
CVE-2023-2868	Barracuda Email Security Gateway (several versions)

Subset of CVEs encountered more than once in Vulnerability World Watch Advisories for Q2 2023

741103 - Fortinet fixes critical pre-authentication remote code execution vulnerability in SSL-VPN devices

- Fortinet released new Fortigate firmware updates, without mentioning that they patch the CVE-2023-27997 vulnerability, an undisclosed pre-authentication remote code execution (RCE) flaw in SSL VPN appliances. By doing so, the security company wishes to give administrators time to patch this vulnerability. Indeed, it was shared with Fortinet's partners, including Orange Cyberdefense as early as May 24th. Unfortunately, although the vulnerability has been embargoed, an advisory from French cybersecurity firm Olympe Cyberdefense has leaked this still confidential information.
- It was discovered by Charles Fol and Dany Bach of Lexfo. According to them, the flaw allows a threat actor to gain access through the VPN, even if MFA is enabled. Fortunately, the vulnerability is patched in the following latest versions:
  - 7.4.0
  - 7.2.5
  - 7.0.12
  - 6.4.13
  - 6.2.14
- Fortinet was planning to publish the information publicly and the CVE number of the vulnerability tomorrow, on June 13, 2023. Nevertheless, following this leak, the researchers who discovered the vulnerability shared more information such as the CVE number and the nature of the vulnerability, but did not publish any PoC or technical details. Moreover, there is no evidence of known exploitation in the wild at present, as they responsibly contacted the vendor.
- In the past, this kind of vulnerability in Fortinet products was exploited by threat actors after only a few days following the release of the patch. For example, at the end of October 2022, CISA and several cybersecurity actors announced that the **CVE-2022-40684** vulnerability was being exploited by threat actors.

733445 - CrowdStrike digs into Volt Typhoon's modus operandi

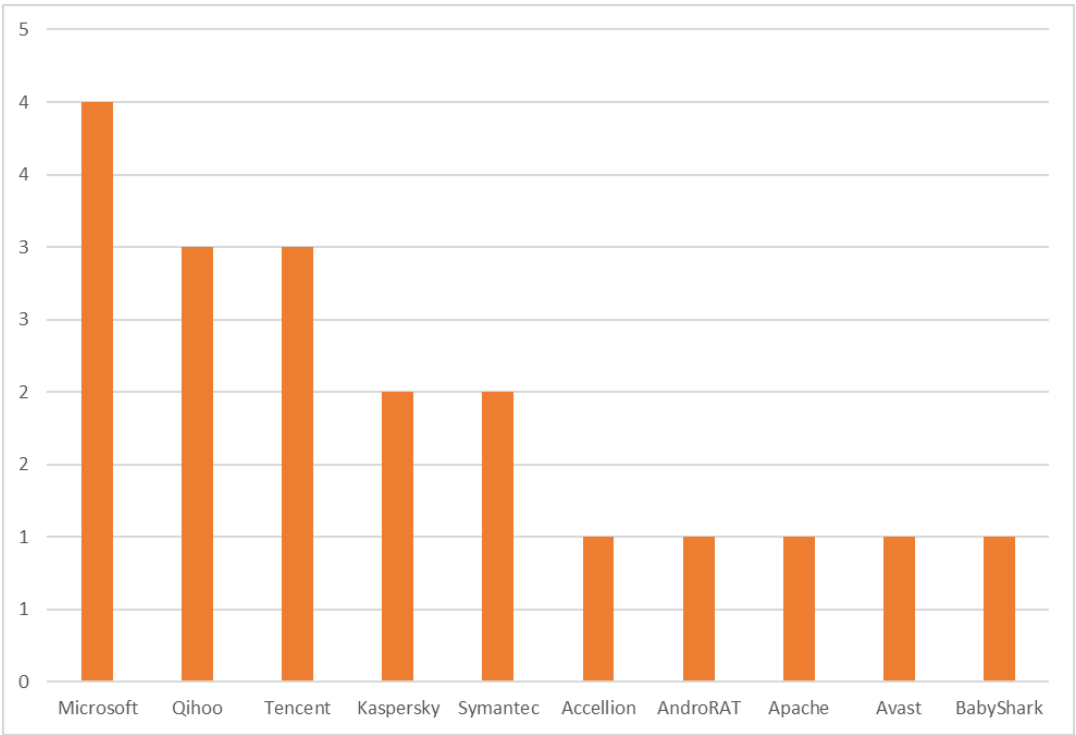
- On June 22, CrowdStrike published a blogpost detailing some Volt Typhoon's (aka Vanguard Panda) attacks they observed since at least mid-2020. Based on their observations, the China-based threat actor "consistently employed exploits against ManageEngine ADSelfService Plus to gain initial access, custom webshells (and backdoored Apache Tomcat) for persistence, and living-off-the-land (LOTL) techniques for lateral movement".
- Interestingly enough, CrowdStrike stated that "Vanguard Panda's actions indicated a familiarity with the target environment, due to the rapid succession of their commands, as well as having specific internal hostnames and IPs to ping, remote shares to mount, and plaintext credentials to use for WMI [Windows Management Instrumentation]", suggesting the threat actor's operations rely on extensive prior reconnaissance.
- Not only Volt Typhoon seems able to customize its actions based on the target, but the threat actor seems also keen to be discreet. The custom webshell deployed at early stages masquerades itself as a legitimate file of ManageEngine ADSelfService Plus, a popular identity

security solution. As pointed out by CrowdStrike, this webshell matches CISA's Yara rule included in their report on Volt Typhoon activity.

- Although the threat actor tried to cover its tracks by erasing access logs including the Apache Tomcat ones, CrowdStrike was able to identify forgotten source code of Java files loaded by the Jasper 2 JSP Engine (an Apache Tomcat's component). The threat actor deployed backdoored version of the Tomcat's WebSocket Java archive. The specially crafted backdoor likely provided Volt Typhoon "with several commands triggered via HTTP URLs".
- Fortinet also confirmed the suspicions that Volt Typhoon was among the groups that exploited the critical FortiOS authentication bypass (**CVE-2022-40684**) we discussed here. But that the more recent critical vulnerability (CVE-2023-27997) was not presumed to have been used by the group before the patch was released in June.

733535 - Barracuda fixes a critical 0-day vulnerability exploited in Email Security Gateway

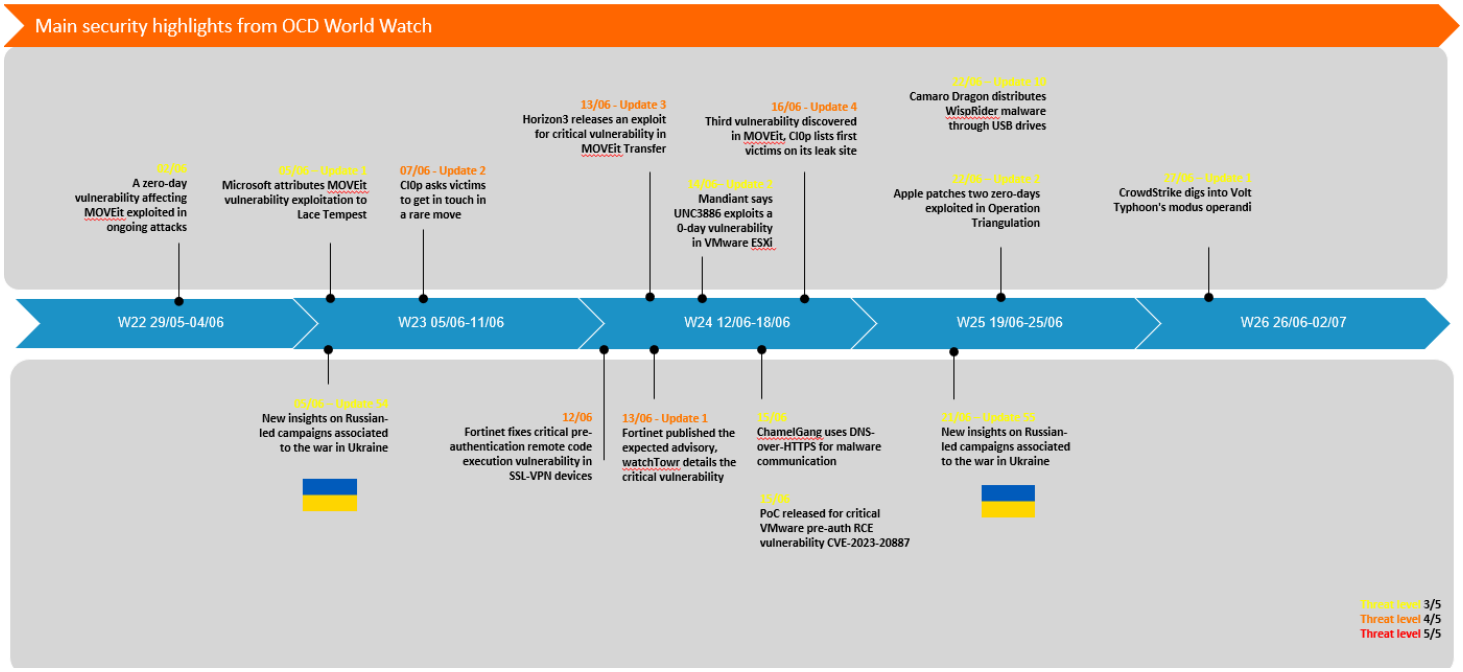
- Barracuda, a company known for its email and network security solutions, has issued an alert about a 0-day vulnerability in the ESG (Email Security Gateway) appliances. Tracked under the identifier **CVE-2023-2868**, this command injection vulnerability allows an attacker to remotely execute system commands with the privileges of the Email Security Gateway product. This security issue received a CVSS v3 score of 9.8 out of 10 and is thus considered critical. Nevertheless, the issue was resolved as part of the latest patch that was automatically applied to all customer appliances on May 20 and May 21. However, it remains yet unclear against how many organizations the vulnerability was exploited in the wild at this time.



Subset of vendors or threat actors in World Watch Advisories discussing Threats or Breaches for Q2 2023

Advisory Summary – June 2023

Security Incidents - Highlights



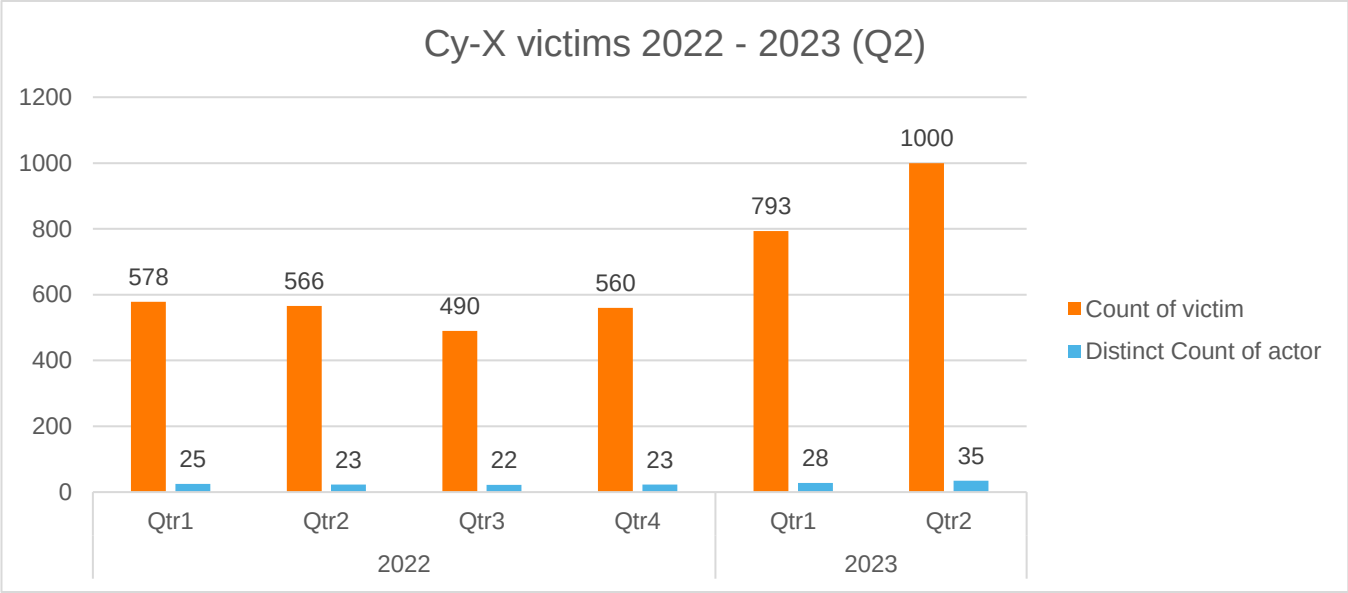
Cyber Extortion (Cy-X) Trends in Q2

Summary

- We recorded **1,000** businesses being victimized on cyber extortion leak sites
- Q2 has seen an increase of **26% in victims.**
- Over 150 victims became victim because of the MOVEit vulnerability exploited by Cl0p
- The top **5 cyber extortion groups** contributing to the Q2 2023 victims were: LockBit3 (24%), ALPHV (aka BlackCat) (12%), Cl0p (9%), BianLian (8%), Play (7%), and Others (40%)
- English speaking countries in top 3 (US, GB, CA) followed by Germany, France & Italy

General Trends

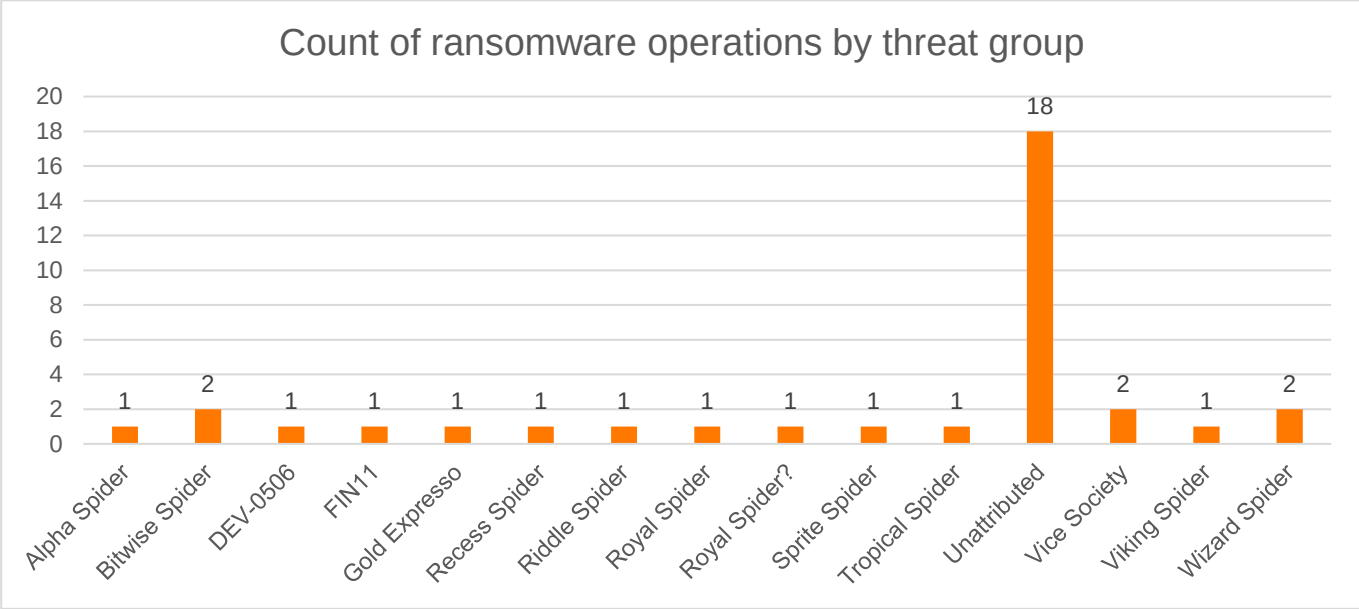
While we reported Q1 2023 to be the quarter with the highest recorded victims, Q2 has seen even more. We have registered 1,000 organizations that have fallen victim to cyber extortion (Cy-X) between April and June 2023. One explanation for this is that Q2 has seen the most active amount of threat actor groups / leaksites. One year ago, Q2 2022 saw 23 different leaksites actively naming and shaming victims on their darkweb blogs. In Q2 2023, we saw a 52% increase of leaksites posting victim organizations. Hence, it makes sense that when we see an increase of actors, we also register an increase in victim count.



Extortion incidents & unique threat actor count recorded from Jan 2022 to June 2023 (n=3,987)

We then would like to explore the question whether the ecosystem has been growing substantially or if certain groups operate several variants or extortion operations in parallel and thus make the ecosystem seem bigger than it actually is (as we have argued previously). For this we turn to our ransomware map maintained by Orange Cyberdefense's CERT team, which can be found here. By mapping the leaksites that we call 'Distinct Count of actor' in the figure above to the 'Ransomware operations' of the Ransomware map, we find that the majority of actors in this field seem not to operate several leaksites/ operations in parallel. In fact, we are only able to identify 3 operations that are most likely connected to the same threat group. However, there are two things that are important to bear in mind. First of all, attribution is always difficult. And secondly, for the majority of leaksites/ Ransomware operations/distinct

actors that actively named victim organizations in Q2, we were unable to find a connection to any threat group (see below).



Count of ransomware operations by threat group

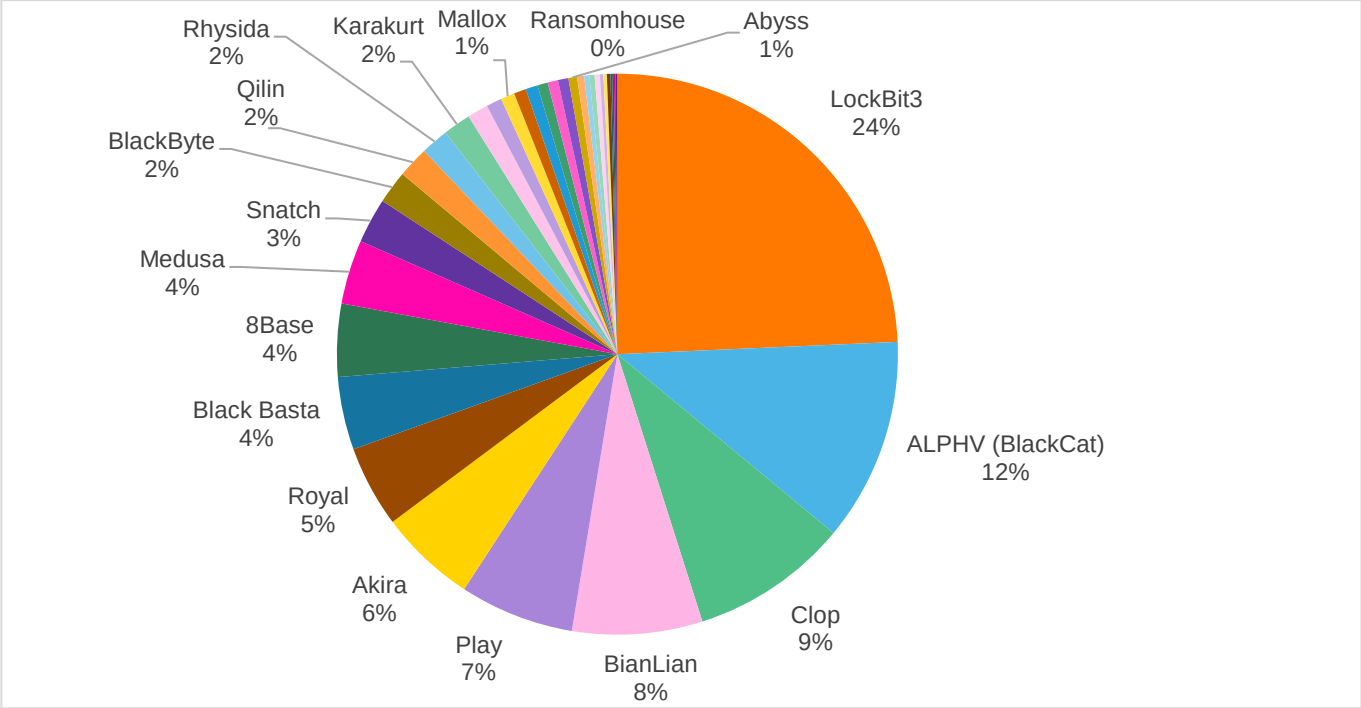
Another trend that has shown its face in 2023 and made an appearance in Q2 again is the exploitation of a 0-day vulnerability. While in Q1 2023, Cl0p exploited the GoAnywhere vulnerability and claiming over 130 victims through that; in Q2 they repeated their modus operandi exploiting the MOVEit vulnerability. This time, Cl0p made a general post on their leaksite, informing the public about the MOVEit vulnerability and asking the victim organizations to reach out them to handle the data extortion incident. This is unusual, since threat actors normally leave ransom notes with instructions to get in contact with them. This time, most likely to the sheer volume of victims, they ask the organizations impacted by the MOVEit vulnerability to reach out to them, adding the deadline of the 14th of June.

At the time of writing, we observed 150 victims. Other reports state as many as 231[1] victims, but we cannot confirm the latter.

Threat actor activity

In Q2, we saw 35 different operations victimizing organizations around the world. Similar to Q1, the top 3 threat actor groups remain unchanged. LockBit3 caused ¼ of all victims in Q2, followed by ALPHV(BlackCat) with 12% and Cl0p causing 9% of all victims. As we mentioned above, Cl0p exploited a vulnerability (again), and thus started exposing victim organizations on their leaksite mid-June. However, of the 150 victims that we are connecting to the MOVEit vulnerability, 89 victims were posted in June, an additional 61 in July, up until the 13th of July/ the time of writing this report.

[1] https://twitter.com/vxunderground/status/1677442776105975808/photo/2

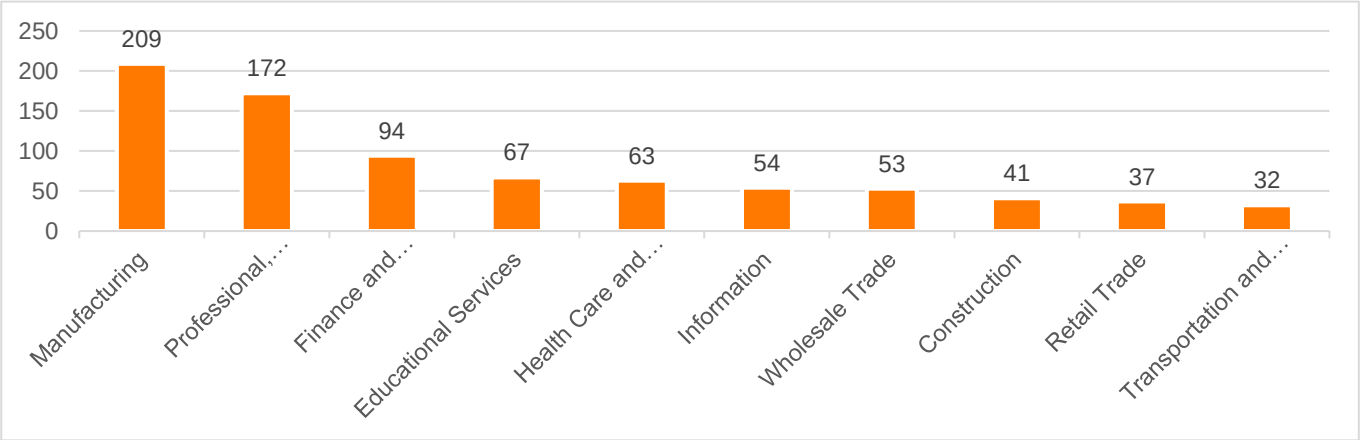


Top 20 contributors to cyber extortion leaks in Q2 2023

Of the 35 threat actors that we observed to have victimized organizations during Q2, 17 were operations that we discovered in 2023 and added to our tracking. This means that half of the cyber extortion operations are new, or began new under a new brand. The other 18 were operations that we have been tracking already, some from 2021, others from 2022.

Victimology of Q2 2023

We observed a small shift in industry distribution, however the top 2 industries impacted by Cy-X remain the same. 1/5 of all victims were from the Manufacturing sector, and Professional Services.

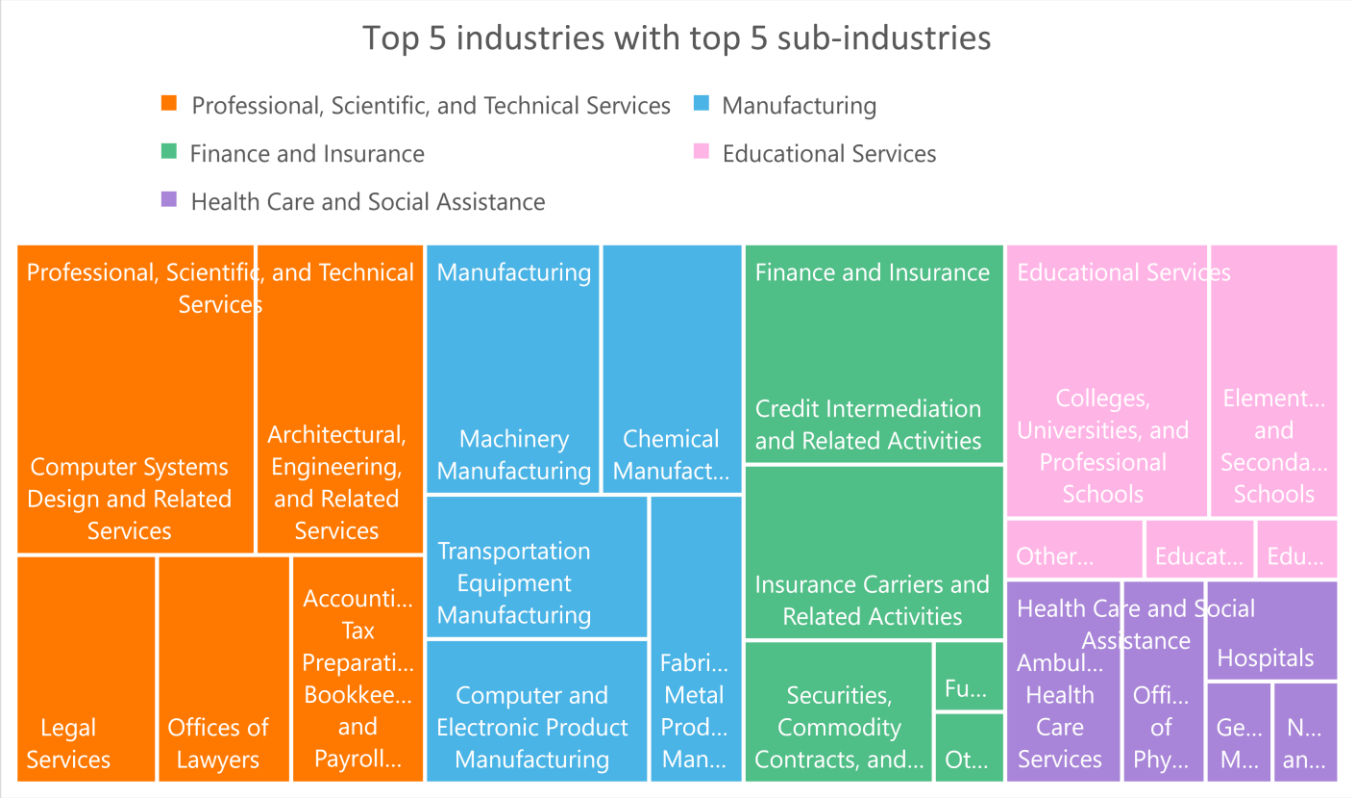


Top 10 industries impacted by Cy-X in Q2

An interesting observation is that the Financial Sector has seen an increase in victims. This can partly be explained by the Cl0p event that has caused around 1/3 of the victims from this sector. When diving into

the question who from the Finance sector has been impacted the most, we find that Banks were impacted the most, followed by Insurance Carriers and other financial-related services. Education and Healthcare have also been much more impacted in Q2 than before. Here we observe colleges, universities and schools in general being hit. Within the healthcare sector, we register most victims from the ambulatory and healthcare service or offices of physicians or hospitals. Despite the fact that several threat actors claim to not extort the healthcare sector, and especially hospitals; we see a contradictory trend. In Q2, we observed 8 hospitals in our victim dataset.

Top 5 industry breakdown with top 5 sub-industry breakdown in Q2 (n=420)



For Professional Services, we noticed that many victims were somehow related to offering digital services. Here we saw the majority of organizations working, creating or offering some sort of software solutions or other technical services. Another theme within Professional Services is the legal services part, those can be law firms or other businesses offering legal services.

And lastly, we found that English-speaking countries saw an increase again in our victim dataset. Almost half of all businesses that suffered from cyber extortion were headquartered in the U.S. (48%), followed by the U.K. (6%) and Canada (5%). Within the top 10, we also registered Europe to be notable, in particular Germany (top 4), France (top 5), Italy (top 6) and Spain (top 10). Besides English-speaking countries and the European countries, we saw Australia (top 7), India (top 8) and Brazil (top 9) represented in our top 10 list.

Conclusion

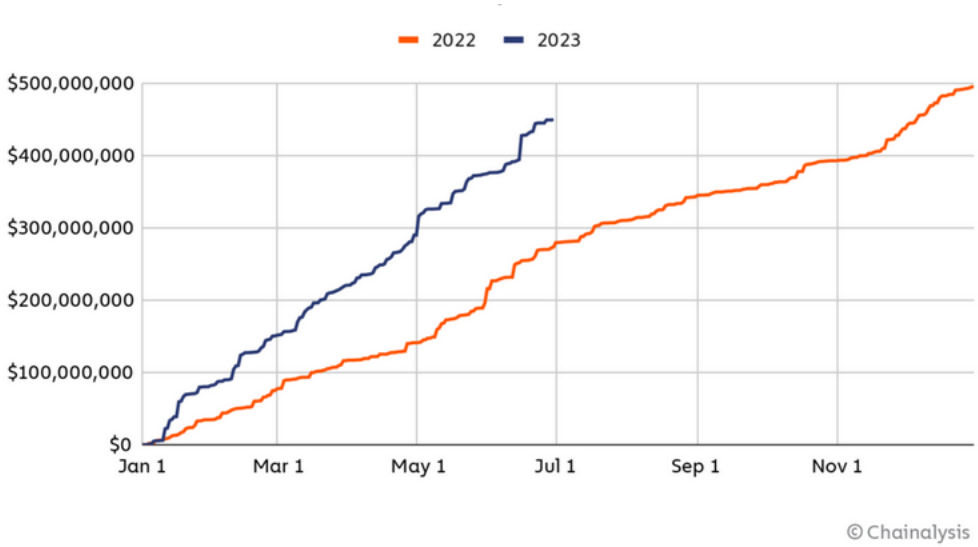
We have shown that cyber extortion has significantly grown (again) since the beginning of 2023, but specifically in Q2. The 8% decrease that was observed in 2022 will unfortunately not be a continuous trend. While we observed around 2,100 businesses being victimized in 2022; we have reached already 1,793 victims in the first half of 2023!

Consequently, we do not believe the victim numbers will decrease nor that the threat of cyber extortion is going away anytime soon.

However, there are two things we believe are happening at this moment, or will happen in the near future. Those two observations are made by someone else but we would absolutely agree with them based on the experience we have gained by observing this form of crime for a few years now.
First of all, Chainalysis who just published their mid-year report[2] highlights that ransom payments have unfortunately grown significantly (see below). In H1 2023, the cumulative ransomware revenue has almost reached already the level of all 2022. This sounds very familiar to what we also just realized. Victim numbers are close to the point of the whole last year, ransom revenue follows this trend. This means, we are seeing high volumes this year. High volumes of activity, more threat actors contributing to cyber extortion, many new 'players' causing higher volumes of victims. The question remains whether or not the likelihood to pay has increased in the first half of 2023 or if the quantity of victimization makes up for the higher ransom revenue Chainalysis found.

The report explains further that they see that both very small payments and very large payments increased in 2023. For example, in 2023 the ransomware variant Cl0p has had an average payment size of $1,730,486; while other variants such as Dharma only made an average of $265. So again, they see this increasing trend for low and high payments.

Cumulative yearly ransomware revenue, 2022 – 2023 (Q1-Q2)



The second observation that we also believe is going to happen in the next two month is that we expect threat actors to take vacations. Especially in 2020 and 2021, we saw usually a calmer summer period while Q3 and Q4 registered high volumes of activity. This trend wasn't continued in 2022, and we believe the war might have 'interrupted' the ecosystem in 2022, causing this anomaly.

Like our expectations, we saw a recent tweet from vx-underground[3] asking the LockBit3 group exactly that. According to the tweet, LockBit3 confirms to have taken a summer break (see screenshot).

[2] https://blog.chainalysis.com/reports/crypto-crime-midyear-2023-update-ransomware-scams/
[3] https://twitter.com/vxunderground/status/1677448226050383872

Screenshot: Vx-underground inquiring LockBit about low activity

Editor's Notes

Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

Charl

EPSSecially Problematic

We've spoken before about the 'Exploit Prediction Scoring System' (EPPS) – a project by the First Organization that seeks to produce predictions of how likely a given software vulnerability (designated by CVE ID) is to be exploited within the next 30 days.

"The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. Our goal is to assist network defenders to better prioritize vulnerability remediation efforts. While other industry standards have been useful for capturing innate characteristics of a vulnerability and provide measures of severity, they are limited in their ability to assess threat. EPSS fills that gap because it uses current threat information from CVE and real-world exploit data. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited."
https://www.first.org/epss/

EPSS is causing a stir within the security community, primarily it promises a solution to the apparently intractable problem of prioritizing efforts under Vulnerability Management programs. Research we've produced, as well as studies by others, have clearly shown that most organizations simply can't keep abreast of the tidal wave of new vulnerabilities being disclosed each month, let alone the deep well of legacy patches that cannot be addressed for some reason. It may be that as little as 10% of new vulnerabilities are being patched on average.

At the same time, we assess that exploitable vulnerabilities are being weaponized and exploited in just a few weeks, sometime only days, which means that a failure to patch the right bug at the right time can have brutal consequences. Data and several anecdotes illustrate how real this issue is, most recently through the Cl0p MOVEit rampage that has led to the compromise of data from over 150 businesses at last count.

Traditional approaches of applying vulnerability severity scores and asset value to determine patching priority have failed to get us ahead of the curve, and are also being shown to be extremely inefficient. Since only around 5% of vulnerabilities ever actually get exploited in the wild, efforts to patch based on severity rating result in multitude of patches being deployed that ultimately never address a real threat, and the consequent waste of time and human resources.

EPSS promises to improve matters by providing timely intelligence to guide patching efforts, demonstrably improving both effectiveness (we patch what we need to) and efficiency (we don't patch what we don't need to).

But the intelligence EPSS provides is very exciting for security researchers also – providing for the first time a way to model the true (or apparently true) impact of

vulnerabilities, and of Vulnerability Strategies. The data produced by the model is being used in all kinds of interesting ways by researchers across the world to examine the challenge of Vulnerability Management and has reignited essential debates about why Vulnerability Management appears to be failing so badly, and how we could do it better.

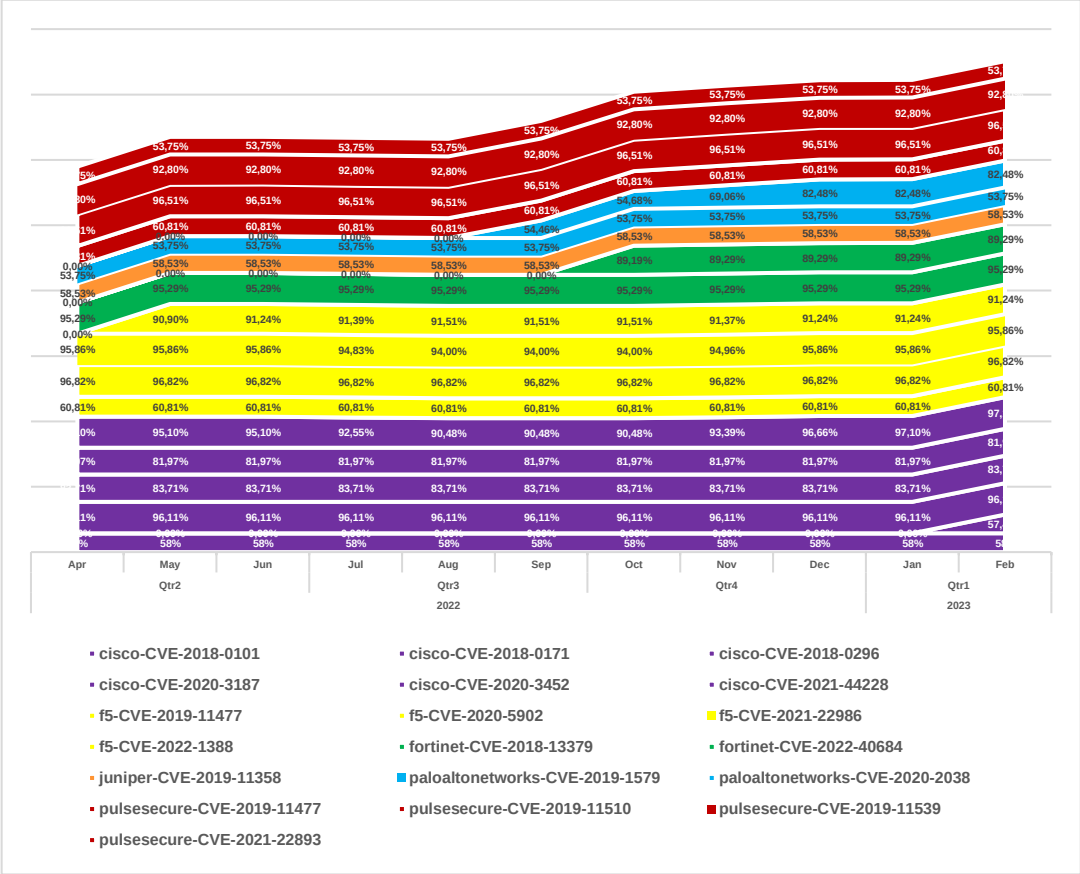
Our team has enthusiastically joined in on the project and our unique access to real operational data from vulnerability scanning, penetration testing and incidents is allowing us to make some meaningful contributions, including:

- A presentation on the effectiveness of penetration testing delivered at the Insomnihack conference in Switzerland: https://youtu.be/1yIj0h8R9eE
- A blog post on the applicability of vulnerability intelligence sources like EPSS to our customers: https://www.orangecyberdefense.com/global/blog/research/in-pursuit-of-more-secure-systems
- A webinar discussion with researchers from Nucleus, our partner in providing our Vulnerability Management service: https://youtu.be/Ik-eTFn0n5M

Another conversation that's simultaneously making waves in the security research space is the apparent problem of vulnerabilities and exploits impacting cyber security vendors. I won't regurgitate this whole discussion here, but by way of illustration, take a look at the list of 'Top Routinely Exploited Vulnerabilities' published by the US Cyber & Infrastructure Security Agency (CISA) in August 2022: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a. I count 9 vendors in the list of the 15 most exploited vulnerabilities. Five of them are security product vendors. How did we get there???

This week yet another vulnerability in the Fortinet firewall platform was disclosed: https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-rce-flaw-in-fortios-fortiproxy-devices/ . More disturbing than the new vulnerability even, is the news that over 330 thousand firewalls are still missing the previous security patch, more than a month after it was disclosed.

With these two themes in mind, I experimented with illustrating the EPSS scores of vulnerabilities for significant security product vendors Cisco, F5, Fortinet, Juniper, Palo Alto, and Pulse Secure. Here's what I came up with:



Each line represents a CVE, and I grouped them together by vendor using colors. Bear in mind that the percentage score reflected is the average EPSS for the month and is a prediction that the vulnerability will be exploited in the wild over the next 30 days. For various reasons I've opted not to include the names of the vendors – ultimately it doesn't add to the conversation.

We consider an EPSS score of anything over 60% to be serious, though some would go as low as 30%. Essentially, if you've managed any of these products on the internet then you would've had to deal with a serious, probably weaponized vulnerability over the last 12 months. For some vendors, there have been several such vulnerabilities. For a small number of these vulnerabilities the probability of exploitation has increased over time, but it's interesting to note that for the most part, at least in this dataset, the prediction scores have remained quite consistent.

I don't intend to offer any headline takeaway here, except perhaps to highlight (again) how important it is to ensure robust vulnerability management processes for security technologies, or to ensure that your service providers demonstrably have such processes in place.


Ric

Ric's Paper in RICSS Workshop

This month I was at the IEEE European Symposium on Security and Privacy workshop Re-design Industrial Control Systems with Security (RICSS), which was held at the Delft University of Technology (TU Deflt) in Delft, Netherlands. I was there to present our latest paper - To me, to you: Towards Secure PLC Programming through a Community-Driven Open-Source Initiative. Although it was a very brief stopover at the conference before returning home, it was rather successful as we won the award for best presentation! But that isn't what is interesting, the paper content is!

Recently my research has centered around two main themes: process comprehension and PLC programming practices; this work is firmly located within the latter. It stems from current PLC programming practices and initiatives for secure PLC programming practices. More specifically, it stems from how both of those concepts are unfortunately incongruent at present.

PLCs are not programmed how you'd program an IT device, there are no terminals or IDEs, no interpreters or compilers as such. Instead, bespoke software is used to write a configuration of control logic that is *downloaded* (yes, I know) to the PLC, which runs through the configuration each CPU cycle. PLC control logic is almost exclusively built with vendor-provided *library functions* found in the configuration software, which are essentially pre-written blocks of code. These library functions are useful because they speed up and reduce the complexity of writing control logic, as well as standardizing it. One major issue with these library functions is that they are proprietary, meaning they cannot be viewed or edited.

Control logic can be, and frequently is, vulnerable; this can range from basic logic flaws to serious vulnerabilities that would allow an adversary to manipulate vast swathes of the operational process. As alluded to, secure PLC programming practices exist to reduce such vulnerabilities. However, with current practices relying heavily on proprietary, vendor-provided library functions that can't be viewed or edited, those secure PLC programming practices are challenging or impossible to implement.

As part of the work, we explored the idea of open-source library functions as an alternative. Indeed, they can be viewed and edited, meaning that secure PLC programming practices can be implemented with their integration. However, we didn't know if open-source library functions even contained the same vulnerabilities – perhaps they were already secure. To understand this, we set up a small experiment to find vulnerabilities in some library functions from the Siemens Open Library. We configured the library functions exactly as described in the accompanying documentation, then downloaded them to a PLC in an operational technology (OT) testbed to be scanned while running.

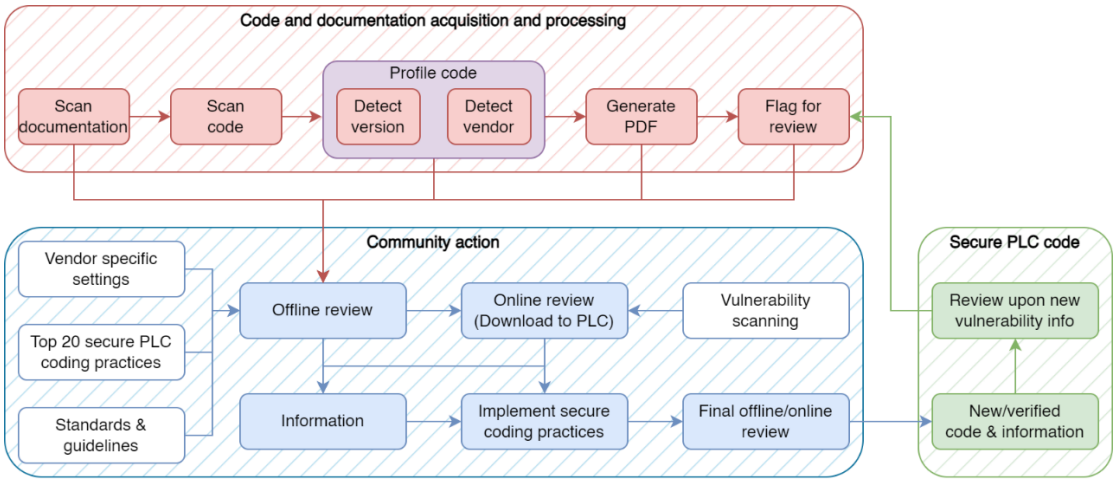
The vulnerability we were looking for was the ability to permanently write to memory over the network, without authentication, and therefore the ability to control variables within the library function. This is particularly bad because it would afford the adversary the ability to entirely control the operational process should these vulnerabilities be prevalent in an OT environment. We looked for this with our PLC variable block scanner (PLC-VBS) from prior research (see my editorial released in March). The scanner will try and overwrite bytes in memory, over the network, and

then read it twice: once immediately to verify it was overwritten, then again after 5 seconds to verify persistence of the overwrite.

We found that, of the bytes scanned (n=117), 41% were vulnerable, meaning almost half of all variables within the chosen library functions were vulnerable. Therefore, while open-source library functions are an alternative to those proprietary ones provided by the vendor, they aren't the solution yet.

One bonus vulnerability we found was within the guidance documentation, which recommended insecure configuration. One in particular was for 'deadband', variables which represent periods of time that values must remain over a threshold before raising an alert. This is used in occasions where, for example, water may be sloshing around in a tank – you don't want a sensor to keep alerting that the tank is full every time the water sloshes close to it. In the documentation, it is recommended to leave this 'deadband' as '0' to have it disabled. However, this is already left as '0' by default, as a *default variable* – one which leads it to being permanently overwritten i.e., vulnerable. This means that an adversary could permanently overwrite this variable over the network, setting it to a non-zero value to enable it, ensuring it is abnormally high such that it will never raise an alert, and therefore creating unsafe conditions.

From this brief experiment we now know that open-source library functions to program PLCs can be the solution to better and more easily implement secure PLC programming practices because they are not proprietary and can be viewed and edited. However, those secure programming practices would have to be implemented in the first place because they are unfortunately not secure at present. Because of this, we put together a proposal in the form of a framework for a community-driven, open-source initiative to secure PLC code, that you can see below.



Here, the framework (most likely in the form of a website) would ingest the PLC code and its accompanying documentation, profile it, and begin an audit trail by generating a PDF. It would then be put to the community to be reviewed. The first review would be offline, keeping in mind vendor settings, secure PLC coding initiatives' guidance, and standards and guidelines. The second review would see the code downloaded to a PLC and scanned for vulnerabilities with a specific control

logic vulnerability scanner such as our PLC-VBS. These reviews would then both feed into implementing secure coding practices for code under review as well as creating a further audit trail of what vulnerabilities were found, which were fixed, and perhaps which had to remain to keep the code operationally functional. After the code has been reviewed, it will go for one final round of reviews to ensure the vulnerabilities have been fixed before being disseminated to end users. Finally, the framework suggests that upon new vulnerability information pertinent code will get flagged for review.

Clearly this work is very positional, spending more of its time exploring a very nascent problem space and describing how and why these issues occur. This means that the framework proposal is just that, a proposal. However, we do believe that this would be an excellent cause that would improve vast swathes of vulnerabilities encountered deep within OT environments and be available for anyone to use. If this initiative resonates with you or you'd like a preprint of the paper, we'd love to hear back!

Diana

A one year research project comes to an end!

In mid-July 2022, we published our first blogpost on our research project that we termed '*Neutralization Techniques – Do ransomware and cyber extortion threat actors know deep down that their activities are criminal or deviant?*' On the 12th of July, we published our last part of this blog series.

In this project, we collected contextual data, also known as qualitative data, to analyze negotiation chat contents, interviews, and leaksite content to answer the question whether or not we find evidence that threat actors engaging in the crime of ransomware and cyber extortion apply neutralization techniques in order to justify their criminal actions and make it more acceptable to them.

In 1957, Sykes and Matza established the five techniques of neutralization, a theoretical approach to understand delinquency. In their observations, they opposed the idea that delinquents would learn their deviant behavior through sub-cultures, learning (anti-)social behavior and values in the process of social interaction as their new alternative set of norms. Instead, they noticed that delinquents would still show guilt or remorse and thus argued that delinquents would come up with 'extensions of defenses to crimes in the form of justifications for deviance'. These justifications would then enable the offender to 'drift' away from the socially accepted norms and values and partake in delinquent behavior. This does not mean that offenders reject social norms of society entirely but that through techniques of neutralization they would then rationalize themselves away from the moral restraints, and thus social control.

We looked at 5 sub-techniques:

1. **Denial of injury** (no one actually got hurt)

2. **Denial of victimhood** (can't see the victim, or injury is a rightful retaliation, punishment)
3. **Appealing to higher loyalties** (prioritize law-abiding values of a smaller social group over society)
4. **Condemning the condemners** (pointing fingers to those who disapprove)
5. **Denial of responsibility** (negating personal accountability)

In our research, we found that *denial of victimhood* was the most frequently applied technique, followed by *denial of injury* and *denial of responsibility*.

Additionally, to recognizing that neutralization techniques are actively applied by threat actors we also found other patterns closely connected to the techniques.

First, when looking at **denial of injury**, we found that threat actors would position their malicious and harmful behavior as a legitimate service. Here, they would imitate business language to *reframe* their engagement in crime. In other cases, threat actors simply believed that no injury occurred because (according to them) the victim could afford to pay the ransom.

Analyzing the active adoption of **denial of victimhood**, showed us how some threat actors stepped into the *vigilante* role. Attempting to shift the focus of their criminal actions towards the victim and how, through the threat actor's actions, they were able to show the world unethical business practices and corruption. Secondly, under the denial of victimhood, we would see threat actors blaming the victims. First of all, due to bad cyber security practices, threat actors could access the victim's network; and secondly because the victim chose not to pay the ransom and thus 'for their services'; the victim suffered the data leak.

Another technique that was used by threat actors to rationalize their criminal activities was the **appeal to higher loyalties**. Here, threat actors sacrifice social norms and expectations in favor of another social group. We saw this in different forms. One form was *altruism*. Some would claim to donate part of the ransom payments to charities, others ransomware brand would façade as helping the poor and starving people, as we saw with the threat actor group calling itself 'HolyGhost'. Another justification that was very present was that their actions would consequently lead businesses around the world to take information security practices more seriously in the near future; and thus portraying themselves as *catalysts for change*.

When we started looking at the technique called **condemning the condemners** we found that threat actors would often focus on members of the cybersecurity industry, journalists, governments and institutions as the condemners. Through this, they would enable themselves to *frame* actions of these entities as being negative and, even more, harmful. Threat actors would continue to condemn and thus point fingers not only to individuals but *corrupt systems* that they reveal to the world.

And lastly, while looking at **denial of responsibility**, we found that trust is imperative. If threat actors loose trust in them being capable and willing to decrypt systems, unlock data and delete data as well as access that they previously gained; they will not receive payments. Nevertheless, we found that threat actors put quite some effort in keeping up their public images that seem to be socially responsible and trustworthy. The responsibility of the experienced cyber attack *shifts* towards

the victims themselves, in a way blaming them to be responsible for becoming a victim in the first place.

If you are interested, you can read the entire blog series here.

Good News Cyber

LockBit Affiliate Was in Arizona…Now Arrested
Twenty-year-old Ruslan Magomedovich Astamirov from the Chechen Republic was recently arrested and charged for his involvement in deploying the LockBit ransomware strain against computer systems in the US and abroad. It is alleged that he directly executed at least five attacks.

Astamirov is now the third defendant to have been charged for being involved with the LockBit ransomware campaign, and the second to be arrested. This follows the arrest of Mikhail Vasiliev by Canadian authorities who is now awaiting extradition to the US, as well as the indictment of Mikhail Pavlovich Matveev

Another BreachForums Domain Seized
The FBI in parallel with a number of other organizations from the US, UK, Netherlands & Australia have finally managed to seize the surface web domain Breached[.]vc which was associated with the BreachForums cybercrime marketplace. As a cheeky touch the FBI's domain seizure page included a modified version of the avatar used by the admin, who was arrested months ago, wearing handcuffs.

EncroChat Takedown Outcomes
Europol recently announced that the taking down the EncroChat encrypted chat network has led to the arrest of more than 6,558 people globally along with the seizure of $979 million of illegal funds. The Europol press release states “Since the dismantling, investigators managed to intercept, share and analyse over 115 million criminal conversations, by an estimated number of over 60 000 users.”

The full results from all authorities involved in the investigations is below:

- 6 558 suspects arrested, including 197 High Value Targets
- 7 134 years of imprisonment of convicted criminals up to now
- EUR 739.7 million in cash seized
- EUR 154.1 million frozen in assets or bank accounts
- 30.5 million pills of chemical drugs seized
- 103.5 tonnes of cocaine seized
- 163.4 tonnes of cannabis seized
- 3.3 tonnes of heroin seized
- 971 vehicles seized
- 271 estates or homes seized
- 923 weapons seized, as well as 21 750 rounds of ammunition and 68 explosives
- 83 boats and 40 planes seized

Akira Ransomware Decryptor
Security researchers from Avast have released a free decryption tool for organisations to use on files that have been encrypted by the Akira ransomware since it first emerged in March 2023.

The ransomware is alleged to have been responsible for several high-profile attacks. Victims of an Akira ransomware attack will see that many of their data files are renamed to add the extension .akira, with their contents encrypted, and a ransom note will have been dropped in each folder.