Orange
Cyberdefense

Security Intelligence | Research Report

Monthly Report
March 23

Contents

Introduction

Microsoft Muddies the Waters?

Microsoft have announced that they are adopting a new threat actor naming taxonomy utilising a weather-themed system. According to Microsoft, with this new taxonomy they "intend to bring better context to customers and security researchers that are already confronted with an overwhelming amount of threat intelligence data. It will offer a more organized, memorable, and easy way to reference adversary groups so that organizations can better prioritize threats and protect themselves."

It is fair to say though that this move has elicited mixed reactions from people in the industry. Whilst some are welcoming of the clarity and transparency, they believe it will provide, others are questioning the need for yet another naming taxonomy to keep track of claiming it will just add complexity and more confusion.

The top-level family name mappings Microsoft is now using are:

Affiliation	Family Name
China	Typhoon
Iran	Sandstorm
Lebanon	Rain
North Korea	Sleet
Russia	Blizzard
South Korea	Hail
Turkey	Dust
Vietnam	Cyclone
Financial motivated	Tempest
Private sector offensive actors	Tsunami
Influence operations	Flood
Groups in development	Storm

Macs Held to Ransom

It has been reported that the notorious Cy-X group Lockbit have developed a ransomware variant that is believed to be the first to target macOS. MalwareHunterTeam first discovered the ransomware which is believed to target Apple Silicon Macs, however a build has been seen that is for PowerPC Macs.

QuaDream Over

Following a report published by CitizenLab that stated their tools were being abused in illegal surveillance operations, the Israeli spyware vendor Quadream has allegedly shut down its operations. Although it will surely only be a matter of time before another similar company with a “clean” brand makes an appearance…..

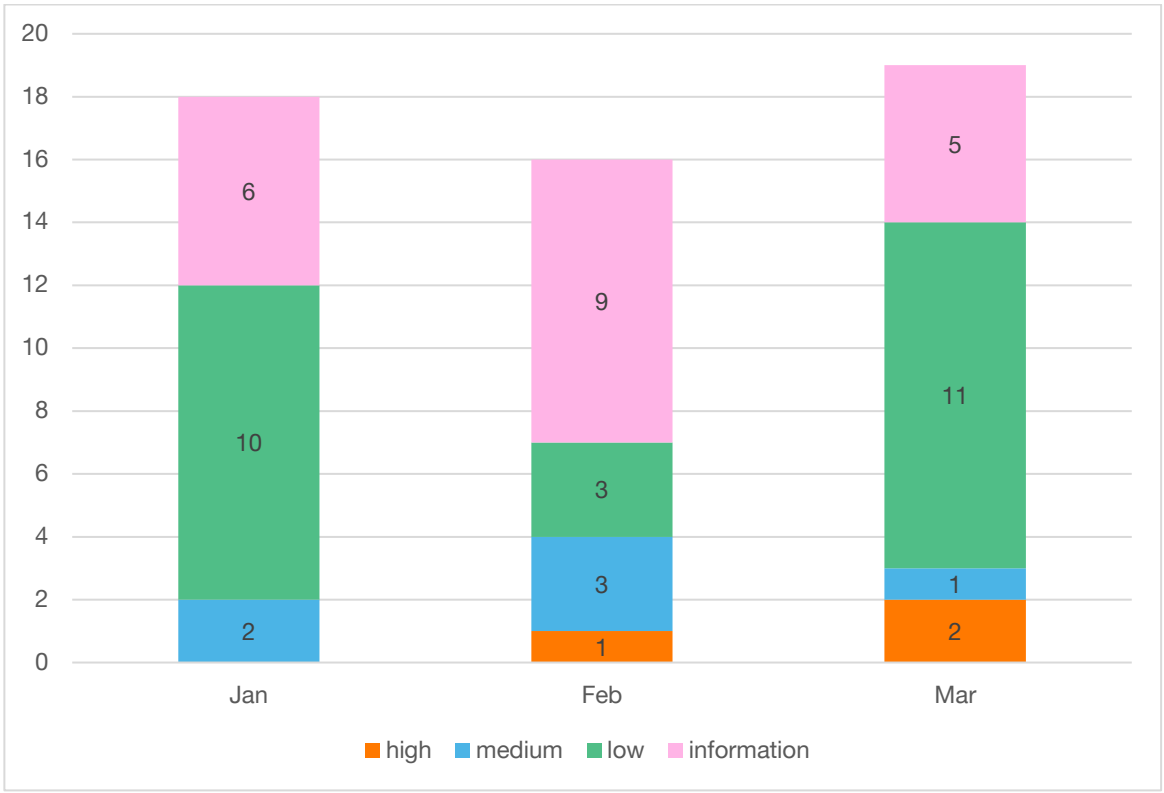
At a glance

Q1 Cy-X Trends

- We recorded 770 businesses being victimized on cyber extortion leak sites
- Q1 has seen an increase of 56% in victims.
- Over 100 victims became victim because of the GoAnywhere vulnerability exploited by Cl0p
- The top 5 cyber extortion groups contributing to the Q1 2023 victims were: LockBit3 (36%), Cl0p (14%), ALPHV (aka BlackCat) (11%), Royal (9%), Play (5%) and Others (25%)
- English speaking countries in top 3 (US, CA, GB) followed by France, Germany & India

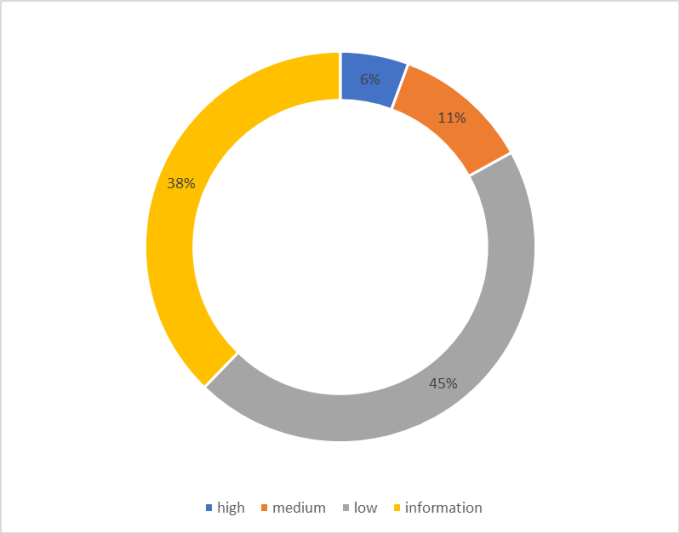
World Watch Review Q1 2023

The Orange Cyberdefense CERT published a total of 53 new World Watch advisories from January 2023 up to and including March 2023, along with updates to a further 63 previously published advisories. This volume of new advisories is keeping steady and is just one less than the previous quarter.



Breakdown of new advisories by severity for Q1 2023

We did not publish a critical rated advisory in Q1 2023, with the last critical advisories being published in Q4 2021. The severity rating of advisories for Q1 is predominantly made up of advisories rated as Information or Low urgency.



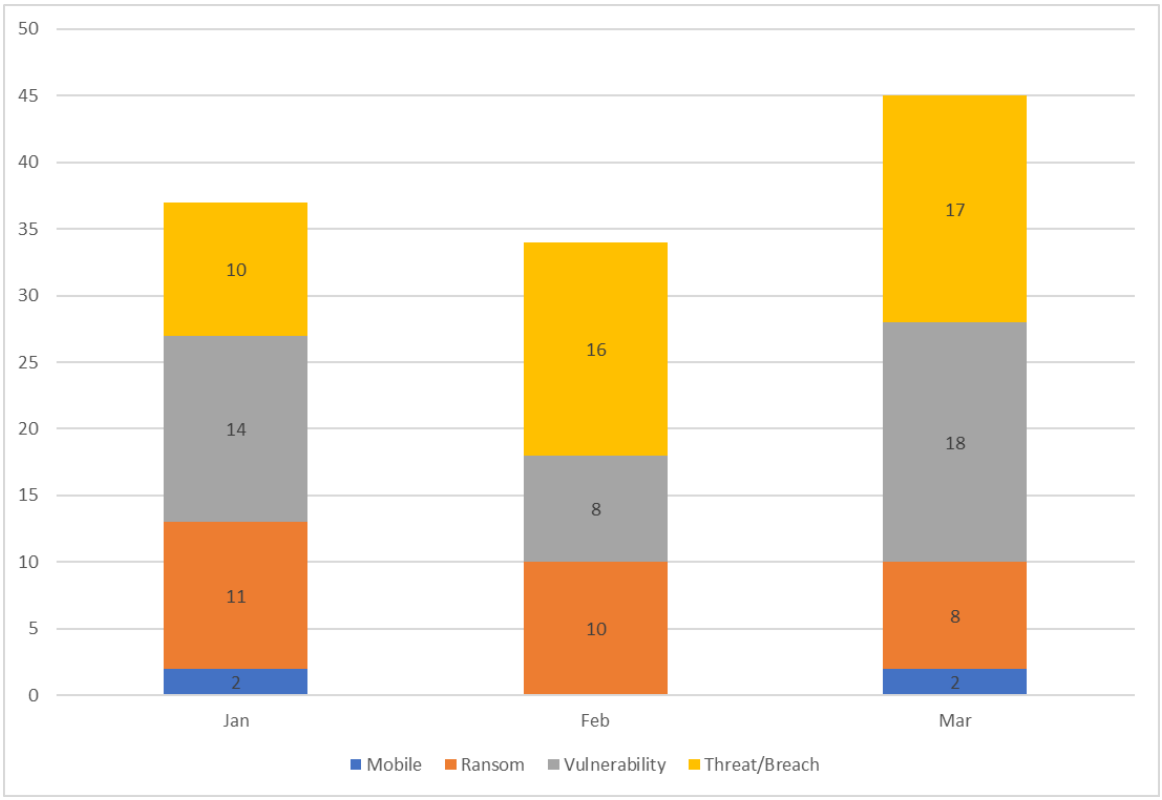
Breakdown of new advisory severity for Q1 2023

Different Approach

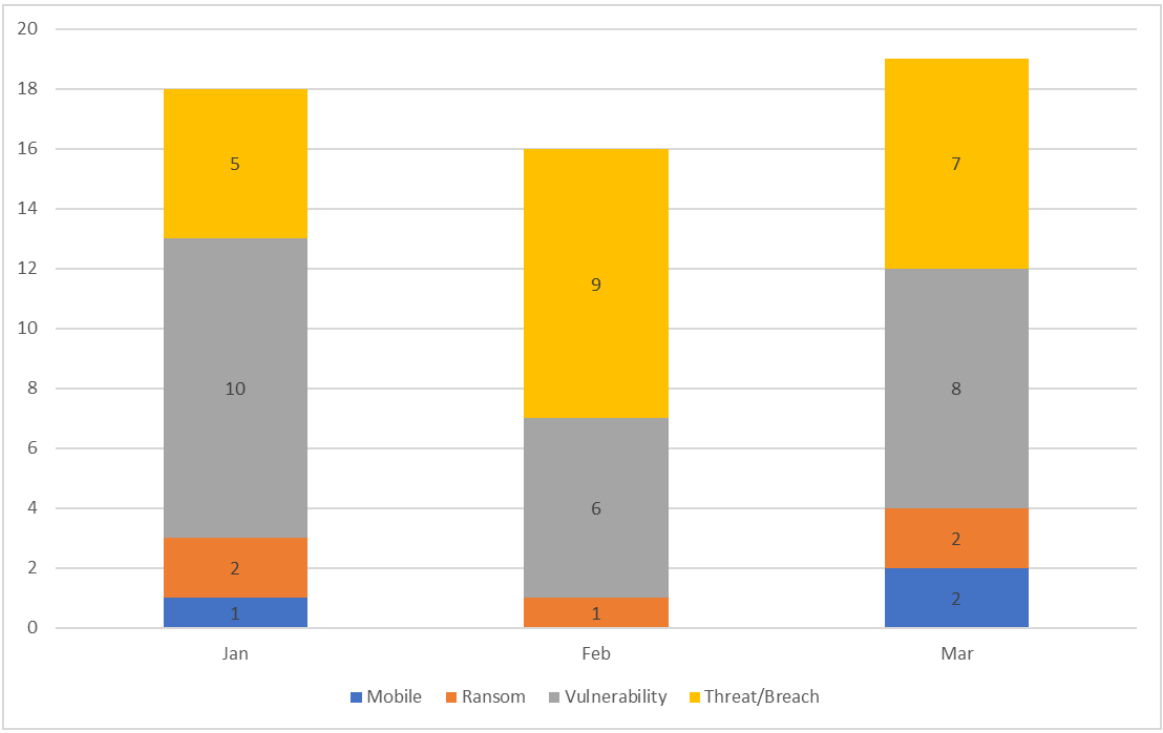
This month we are again looking at Q1 of 2023 using an approach we used in compiling parts of the OCD **Security Navigator 2023** report, namely using Machine Learning (ML) to help analyze published advisories. ML algorithms were used to highlight potentially interesting occurrences of keywords such 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 Threat/Breach advisories weren't as prevalent by volume as in Q4 2022, in fact this quarter saw a more even spread between them and advisories classified as Vulnerability. When examining just the new advisories we see this same pattern remains.



All World Watch advisories published by theme in Q1 2023



New World Watch advisories published by theme in Q1 2023

Our machine learning classifier identified very little discussion involving attacks against mobile phones. The three new advisories labelled as Mobile were published in mid-January 2023 and late March 2023 and are respectively:

671065 – Data from digital forensics companies Cellebrite and SMAB leaked online

- On January 15, the "Enlace Hacktivista" and "DDOSecrets" hacktivists groups published 1.7 TB of internal data from the Israeli company Cellebrite and its Swedish competitor, MSAB. Enlace said that they received the files from an "anonymous whistleblower" and leaked them because tools from both companies were used in the past for human rights abuses. Cellebrite and MSAB are known for selling forensics software to law enforcement agencies.
- The scale of the leak for Cellebrite is presumably massive as it contains practically the entire product and is available now for free online.

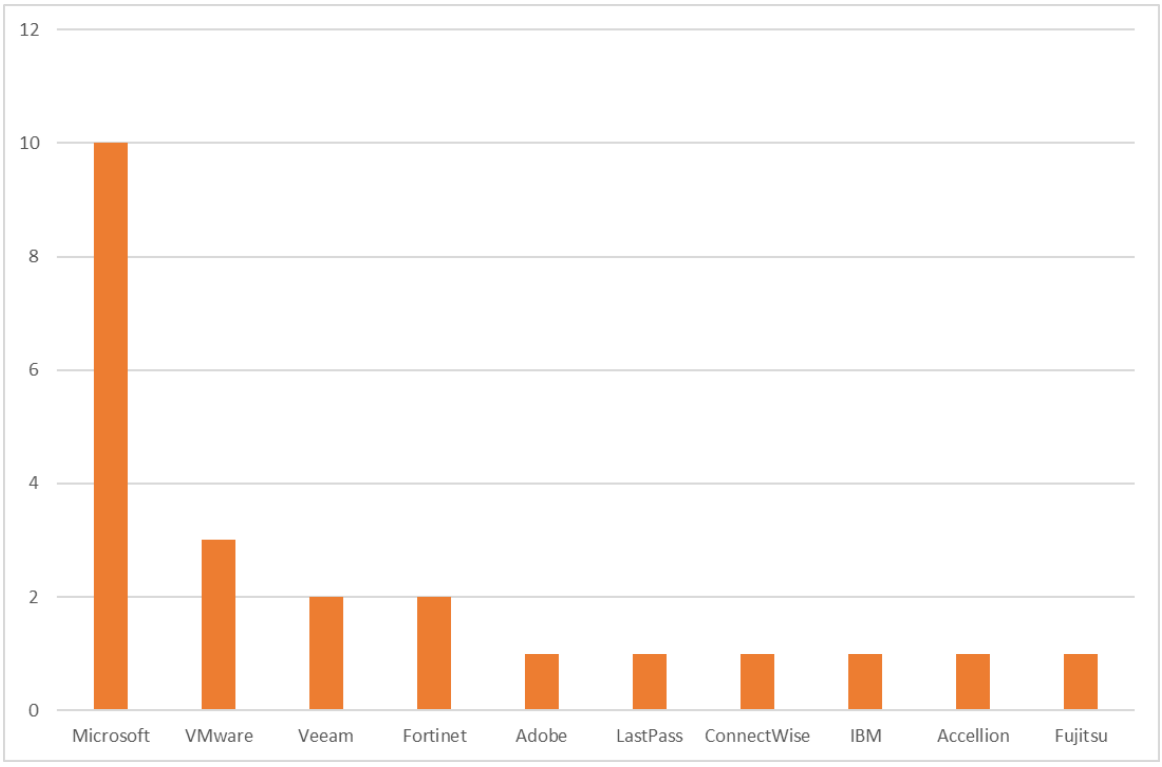
705325 – Pinduoduo (Chinese legitimate e-commerce mobile application) leverages exploits tied to recent Android vulnerability

- Pinduoduo, a legitimate e-commerce mobile app installed on 750 million devices, mostly by Chinese users, presumably contained exploits leveraging 3 Samsung and 1 Android vulnerabilities. These exploits enabled the application to perform malicious activities, such as stealing and monitoring user data, deleting other apps, inflating the number of active users, etc.
- However, since the vendor denied the claims, this raises suspicions over a possible supply chain and/or insider attack. Although the effective malicious use of these capabilities has not been confirmed by us so far, the presence of malicious code has been proven. Fortunately, the application contained the exploits only when installed from third party stores (including mobile manufacturers' ones), not when directly downloaded from Google's Play store. Nevertheless, Google removed the app from their store as a precaution until the vendor clarifies the situation. Google Play Protect - Google's on-device program to surveil installed app and to detect malicious activity - will display an alert if Android users try installing it from outside of the Play Store for now.
- Even though the risk remains limited for now, media attention could heavily grow as TikTok, another prominent Chinese application, is increasingly banned by Western public administrations.

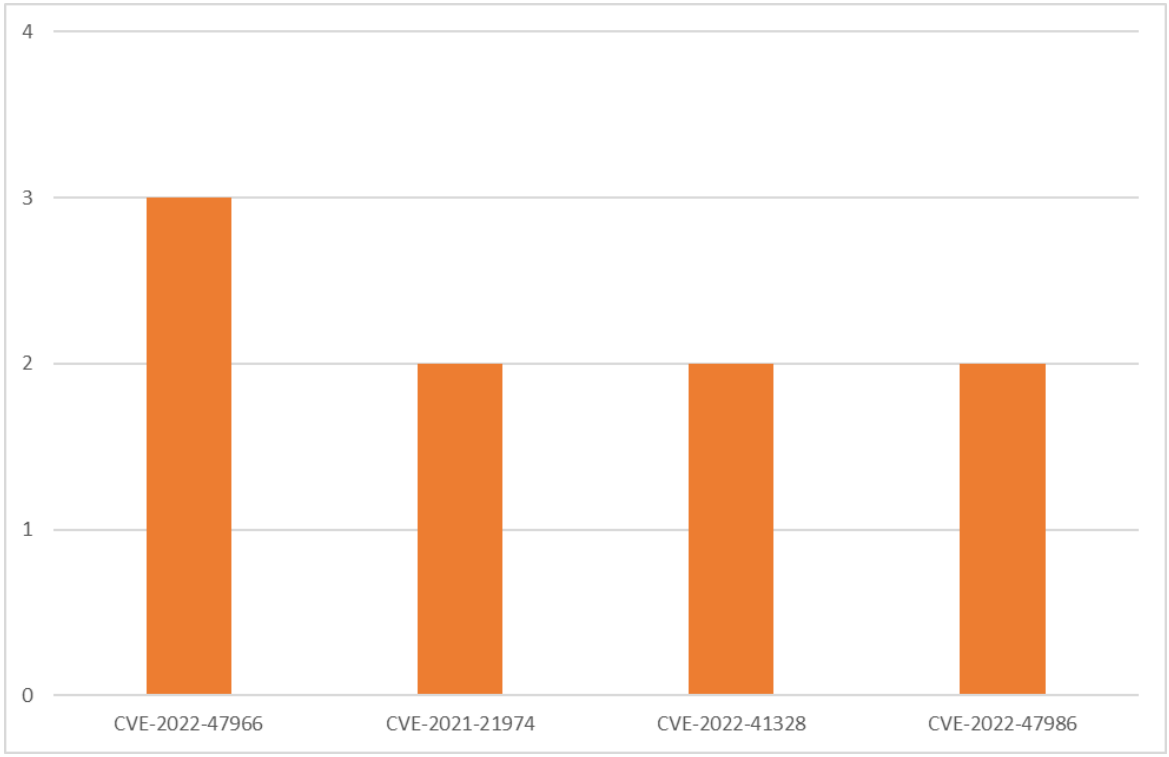
705833 – Android, iOS and Chrome zero-day exploits used to deploy commercial spyware

- Google Threat Analysis Group (TAG), in collaboration with Amnesty International, recently disclosed several exploit chains used in two distinct campaigns to deploy advanced commercial spyware to users in Malaysia, Kazakhstan, the United Arab Emirates, Indonesia, Belarus and Italy.
- Various zero-day vulnerabilities were exploited alongside n-day vulnerabilities during the campaigns, which took advantage of the large time gap between the release of a security update and its deployment on end user devices.
- The first campaign was not attributed to any spyware vendor, although Google pointed out some of the exploit code bears strong similarities with exploit code used by Cytrox. As for the second campaign, it used landing pages identical to the ones deployed by Variston, so Google attributes it to Variston or one of their partners/customers.

Looking at vulnerabilities during the first three months of 2023 we note several prominent vendor names. Some are regulars, while others such as Fujitsu, LastPass, and IBM occur much less frequently.



Subset of Vendors mentioned in Vulnerability World Watch advisories for Q1 2023



Subset of CVEs encountered more than once in Vulnerability World Watch Advisories for Q1 2023

CVE ID	Vendor / Product
CVE-2021-21974	VMWare Cloud Foundation & ESXi (several versions)
CVE-2022-41328	Fortinet FortiOS (several versions)
CVE-2022-47966	Zoho ManageEngine (several versions)
CVE-2022-47986	IBM Aspera Faspex (several versions)

Subset of CVEs encountered more than once in Vulnerability World Watch Advisories for Q1 2023

678367 - New ESXiArgs ransomware campaign targets ESXi servers

- A massive campaign by a possibly new ransomware threat actor impacts many outdated ESXi servers throughout the world. Indeed, several of our clients as well as at least 3 cloud providers hosting such servers for their clients warned us privately that some servers running old versions of ESXi had been encrypted. Servers running versions 6.x and maybe 5.x, that are currently End-of-Life thus not fully maintained by VMware, are in the scope of this attack.
- One 2-years old vulnerability in ESXi's OpenSLP, tracked as CVE-2021-21974, has been most presumably leveraged at least in some of these incidents. Patched in February 2021 by VMware, this vulnerability was not known to be massively exploited in the wild. A PoC was nevertheless publicly disclosed soon after the fix was released, as well as a stable exploit. Another less likely vulnerability could be the one VMware disclosed last December, as Scaleway (a French hoster) mentioned publicly in a tweet. The patch includes in particular a vulnerability numbered CVE-2022-31696, that enables an attacker to escape a sandbox and thus impacts the full ESXi servers' VMs (i.e. multiple clients). Nonetheless, this issue requires local access.

696477 - FortiOS vulnerability exploited in the wild targeting governmental entities

- On March 7, Fortinet disclosed and patched the vulnerability tracked as CVE-2022-41328. Located in the "execute wireless-controller" command, exploitation of this vulnerability requires a local attacker with high privileges, and allow them to read and write files on the underlying Linux system. The list of affected products includes:
    - FortiOS version 7.2.0 through 7.2.3
    - FortiOS version 7.0.0 through 7.0.9
    - FortiOS version 6.4.0 through 6.4.11
    - FortiOS 6.2 all versions
    - FortiOS 6.0 all versions
- On the incident observed by Fortinet, the attacker exploited this vulnerability to modify the FortiGate devices' firmware image, adding a new file executed before proceeding with the regular boot-up actions. This malicious payload examines received ICMP packets, and when it detects a hardcoded string, it then extracts a C2 IP address from the packet and establishes a connection

with the C2 using an ICMP tunnel. The malware can then perform various actions, such as data exfiltration, downloading/uploading files and executing a remote shell.

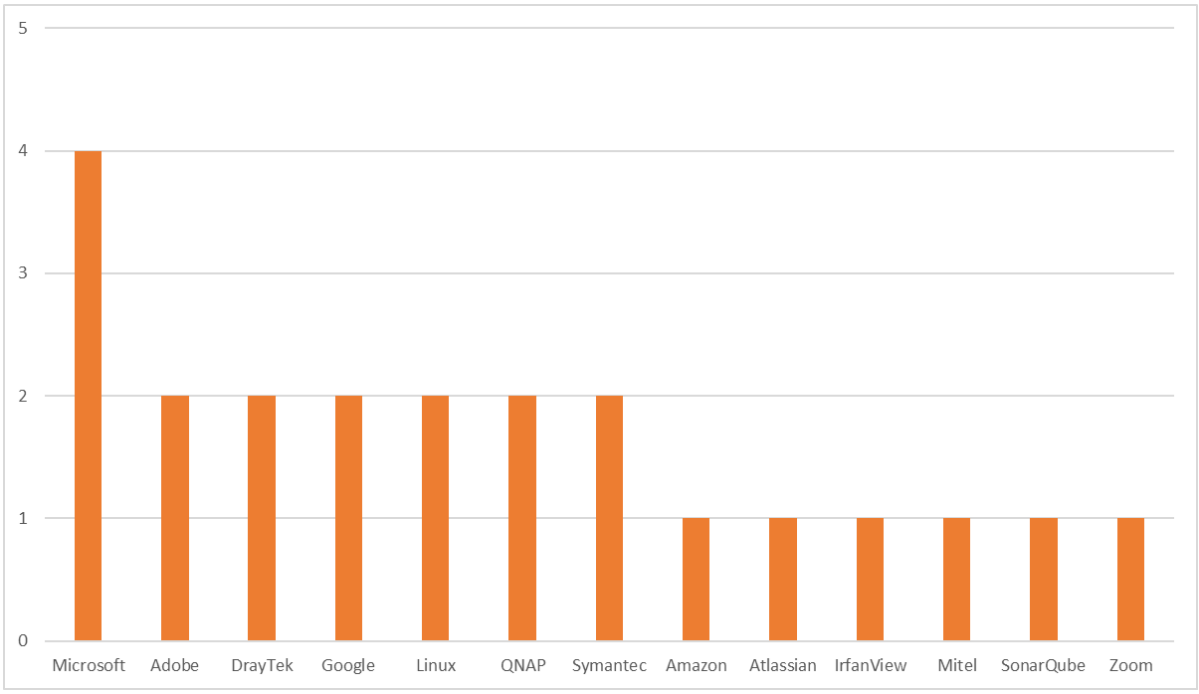
671301 - Critical ManageEngine vulnerability now exploited in the wild

- On January 13, 2023, Horizon3 published a blogpost for the vulnerability tracked as CVE-2022-47966. This security flaw, which impacts a large number of ManageEngine products, allows an unauthenticated attacker to create a SAML request with an invalid signature that trigger a RCE. It is important to note that to be exploited, this vulnerability requires that SAML single sign-on is enabled or has already been enabled in the past. Moreover, according to the researchers' publication, the vulnerability is easy to exploit and enable attackers to "spray and pray" on the Internet in order to compromise victims.
- Indeed, given the nature of these impacted products, this vulnerability allows attackers to gain initial access on target appliances and then move laterally with highly privileged credentials. Nevertheless, it is necessary that these services are available on the Internet. According to the article, there could be several thousands vulnerable instances online, with the below examples:
    - 500+ exposed instances of ServiceDesk Plus with SAML enabled,
    - 300+ exposed instances of Endpoint Central with SAML enabled.

694335 - IceFire ransomware targets Linux servers in ongoing worldwide campaign

- The IceFire ransomware-as-a-service operation was first detected on March 2022 while targeting Windows systems, with the first victim posted on their leaksite only in August. The group then was mostly inactive between November 2022 and January 2023. Since a few weeks, IceFire is back and is actively targeting Linux systems worldwide. Most targeted organizations are located in Turkey, Iran, Pakistan, and the U.A.E, countries which are not known for being widely targeted by other ransomware gangs.
- According to SentinelOne researchers, once deployed in a targeted system, IceFire doesn't encrypt all files on Linux and avoids encrypting specific paths, allowing critical system parts to remain operational. The group likely wants to prevent a complete shutdown which could cause full disruption to the company, unabling them to even pay the ransom, or wants to be in an advantageous position during the negotiation process. When executed, IceFire ransomware encrypts files, appends the ".ifire" extension to the filename, and then covers its tracks by deleting itself and removing the binary.
- To breach their targets, IceFire affiliates deliver phishing messages and pivot using post-exploitation frameworks. For Linux systems, the attackers exploit a high-severity pre-authentication RCE vulnerability affecting the IBM Aspera Faspex file-sharing software (CVE-2022-47986). The vendor patched the flaw back in January but following the release of an exploit code by AssetNote on February 2, the vulnerability has been exploited by malicious actors. On February 21, US cybersecurity agency CISA ordered all federal agencies to patch their systems by March 14. According to the Shodan search engine, more than 150 Aspera Faspex servers are still exposed online, most of them located in the United States and China.

Looking at vulnerabilities exploited by attackers we see some familiar vendors as well as some uncommon names. Note the vendor names present in the following chart is a curated subset.



Subset of vendors in World Watch Advisories discussing Threats or Breaches for Q1 2023

CVE ID	Vendor / Product
CVE-2012-4869	Sangoma FreePBX 2.10 and earlier
CVE-2014-9727	AVM FRITZ!Box
CVE-2017-5173	Geutebruck Ip Camera G-cam Efd-2250 version 1.11.0.12
CVE-2019-15107	Webmin 1.920 and older
CVE-2020-15415	Draytek Vigor (several versions)
CVE-2020-8515	Draytek Vigor (several versions)
CVE-2022-24816	GeoSolutions JAI-EXT before 1.1.22
CVE-2022-26134	Confluence Server and Data Center (several versions)
CVE-2022-32548	Draytek Vigor (several versions)
CVE-2022-36267	Airspan AirSpot 5410 0.3.4.1-4 and earlier
CVE-2022-4257	C-DATA Web Management System
CVE-2022-46169	Cacti 1.2.22 and earlier

CVE-2022-47523	Zoho ManageEngine Access Manager Plus before 4309, Password Manager Pro before 12210, and PAM360 before 5801

Subset of CVEs encountered in Threats/Breaches in World Watch Advisories for Q1 2023

504636 - ShellBot and MooBot botnets target old vulnerabilities in Realtek and Cacti products

- A new variant of the Mirai (DDoS) botnet is using known flaws in D-Link, Netgear and SonicWall devices, as well as newly-discovered flaws in unknown IoT devices to add infected systems to a botnet. According to an analysis provided by Palo Alto Networks, these attacks are still ongoing.

690183 - Servers running GeoServer massively targeted by threat actors

- On February 28, Shadowserver announced that threat actors are targeting servers running a vulnerable instance of the GeoServer solution to deploy the Kinsing miner. GeoServer is an open source software for sharing geospatial data. According to Shadowserver, attackers leverage one of two critical unauthenticated RCE vulnerabilities received a CVSS score of 9.8 out of 10.
- One of those vulnerability currently exploited by the attackers is tracked as CVE-2022-24816, with the other more recent one being: CVE-2023-25157. The first bug is located in a GeoServer's dependency, allowing an attacker to inject and then execute code remotely using a network request. This vulnerability has been fixed with version 1.1.22 of jt-jiffle (Maven) last April. Unfortunately, an article from last August describes it in details, and since October 12, 2022, a PoC is publicly available. It is therefore strongly recommended to deploy the latest version that fixes this issue.
- According to passive scanners fingerprinting exposed assets, up to 2,500 potentially vulnerable instances including around 200 in France were identified.

692709 - Lumen discovers new malware dubbed Hiatus affecting SOHO routers

- On March 6, Lumen (i.e. named CenturyLink previously) published a report about a malicious campaign that targets end-of-life Vigor routers from DrayTek to secretly spy on victims in Latin America, Europe and North America since at least July 2022. The DrayTek Vigor products exploited belong to the DrayTek 2960 and 3900 models. These are SOHO (Small Office/Home Office) routers typically used by small and medium-sized businesses (SOHO) as VPN i.e. for remote connectivity to corporate networks.
- Dubbed Hiatus by researchers, this campaign involves a remote access trojan called HiatusRAT and a tampered variant of "tcpdump", a legitimate network packet capture tool. Tcpdump is a command line utility that allows the user to retrieve and analyze network traffic passing through the system. The use of this tool may point towards a campaign dedicated to steal information from victims.
- According to the researchers' analysis, as of mid-February 2023, 4,100 DrayTek 2960 and 3900 models were exposed to the Internet and at least 100 devices were compromised, which represents about 2% of the total number of DrayTek exposed online routers.

672045 - Critical vulnerability affecting Cacti exploited in the wild

- According to a research conducted by Censys, most of Internet-exposed Cacti installations have not been patched against a critical command injection vulnerability tracked as CVE-2022-46169. This is all the more worrisome as this flaw is already being exploited in ongoing attacks to deploy malware such as Mirai and IRC botnets.
- Cacti is a famous open-source Web-based network monitoring and graphing tool that offers an operational monitoring and fault management framework. It is also a front-end application for the data logging utility RRDtool.

669565 - Zoho urges clients to fix a security issue in ManageEngine access management products

- Enterprise software provider Zoho has urged its customers to patch specific ManageEngine products against a high-severity vulnerability. Impacting 3 ManageEngine management solution products (Password Manager Pro, Privileged Access Management 360 and Access Manager Plus), the vulnerability is tracked as CVE-2022-47523 and is of SQL injection type.
- This vulnerability affects the following product versions:
  - Password Manager Pro: version 12200 and lower
  - Access Manager Plus: version 4038 and lower
  - PAM360: 5800 and lower
- Using this vulnerability, an authenticated remote attacker can access or alter database information using specially crafted queries. This vulnerability exists due to a lack of validation of user input in an internal framework.
- In order to fix this vulnerability, Zoho has added appropriate validation to prevent the exploitation of this security issue.
- It is important to note that as we reported already, Zoho vulnerabilities are regularly exploited by nation-state (then other) threat actors. For this reason, CISA added such vulnerabilities in their "Catalog of Known Exploited Vulnerabilities," and requires U.S. government agencies to patch their Zoho devices by a specific date.
- It is therefore highly recommended to patch this vulnerability in order to reduce the risk of attack.

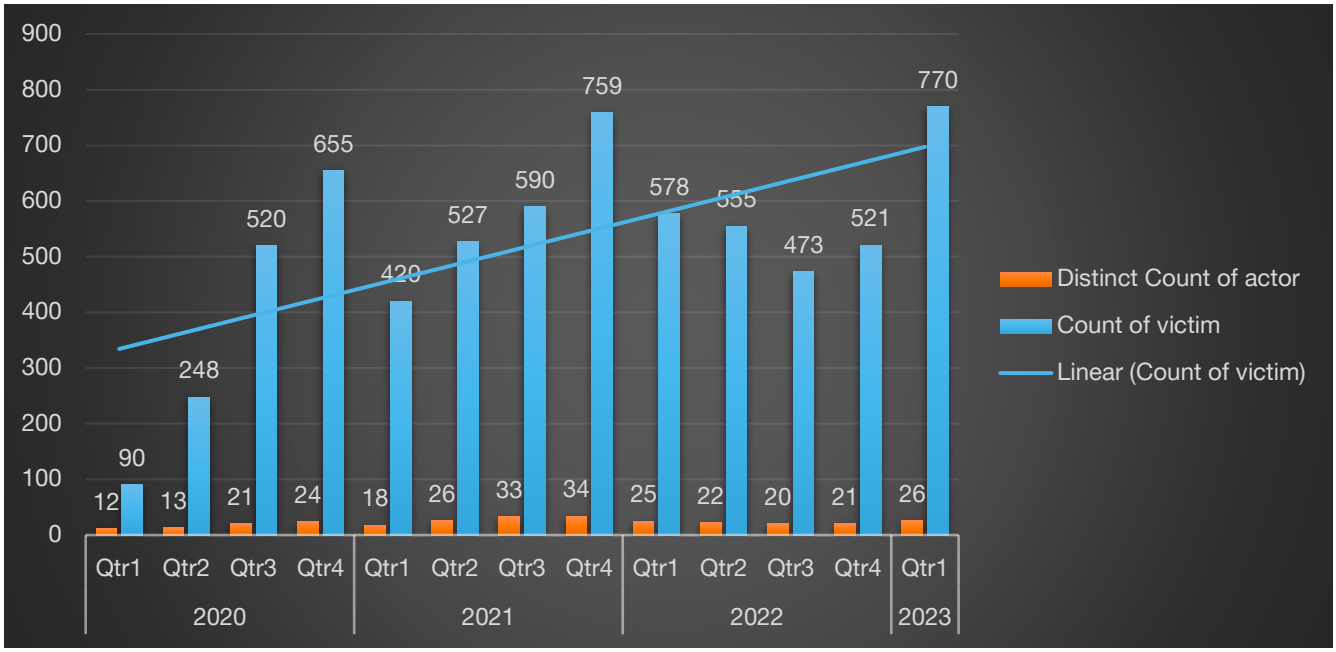
Cyber Extortion (Cy-X) Trends in Q1 2023

Summary

- We recorded **770** businesses being victimized on cyber extortion leak sites
- Q1 has seen an increase of **56% in victims.**
- Over 100 victims became victim because of the GoAnywhere vulnerability exploited by Cl0p
- The top **5 cyber extortion groups** contributing to the Q1 2023 victims were: LockBit3 (36%), Cl0p (14%), ALPHV (aka BlackCat) (11%), Royal (9%), Play (5%) and Others (25%)
- English speaking countries in top 3 (US, CA, GB) followed by France, Germany & India

General Trends

Q1 has been one of the busiest quarters we have seen since we started documenting cyber extortion victims three years ago. While January was still relatively low in terms of victim numbers, February began to show victim counts that we hadn't seen since April 2022, the month Conti closed their criminal operations. In March, the threat actor group Cl0p exploited the GoAnywhere vulnerability and victimized over 100 organizations around the world. Cl0p's victims were from the U.S., UK, Canada, Australia and India.

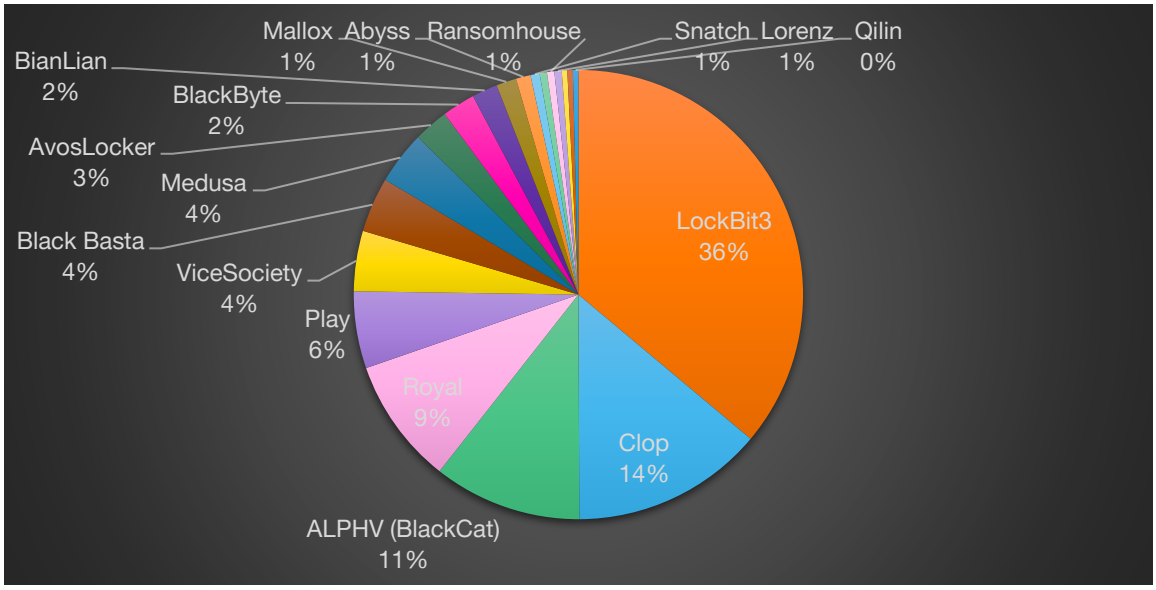


Extortion incidents & unique threat actor count recorded from 2020 to March 2023 (n=6,707)

Threat actor activity – Interesting observations

As mentioned above, we have seen a slight shift in contributing threat actors. LockBit3 remains the threat actor group that is causing the most victims around the world during Q1 2023. The Cybersecurity & Infrastructure Security Agency (CISA) has finally published a joint alert in March 2023 on LockBit3[1]. According to the alert, LockBit3 shows similarities with ransomware strains such as BlackMatter and ALPHV (BlackCat). LockBit3 only infects machines that do not have language settings matching with languages such as Romanian (Moldova), Arabic (Syria), and Tatar (Russia), just to mention a few; if those are present, execution will stop.
LockBit is definitely a group to watch out for, in 2022, 41% of all victims suffered a cyber extortion attack by LockBit2 or LockBit3, causing damage to over 800 organizations around the world.

Cl0p is one of the threat actor groups whose life cycle is surprisingly long lasting in comparison to other threat actor groups. Cl0p surfaced as a Ransomware-as-a-Service (RaaS) operation way back in 2019. Similar to the recent GoAnywhere exploit they victimized over 100 businesses in February 2021, using Accellion's File Transfer Appliance.[2] Therefore, Cl0p seems to be one of the groups that looks for specific 0-day exploits.



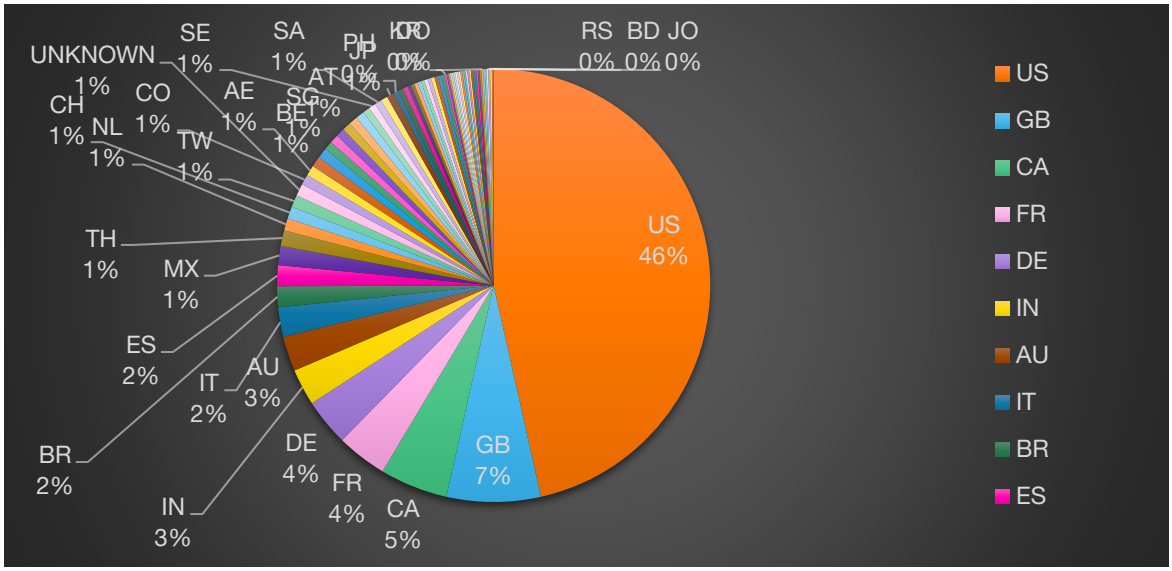
Top 20 contributors to cyber extortion leaks in Q1 2023

During Q1, we have added the following new cyber extortion operations to our tracking: Money Message (first victims documented in March 2023), Abyss (first victims documented in March 2023), MONTI (first victims documented in March 2023) & Medusa (first victims documented in January 2023) .

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
[22] https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

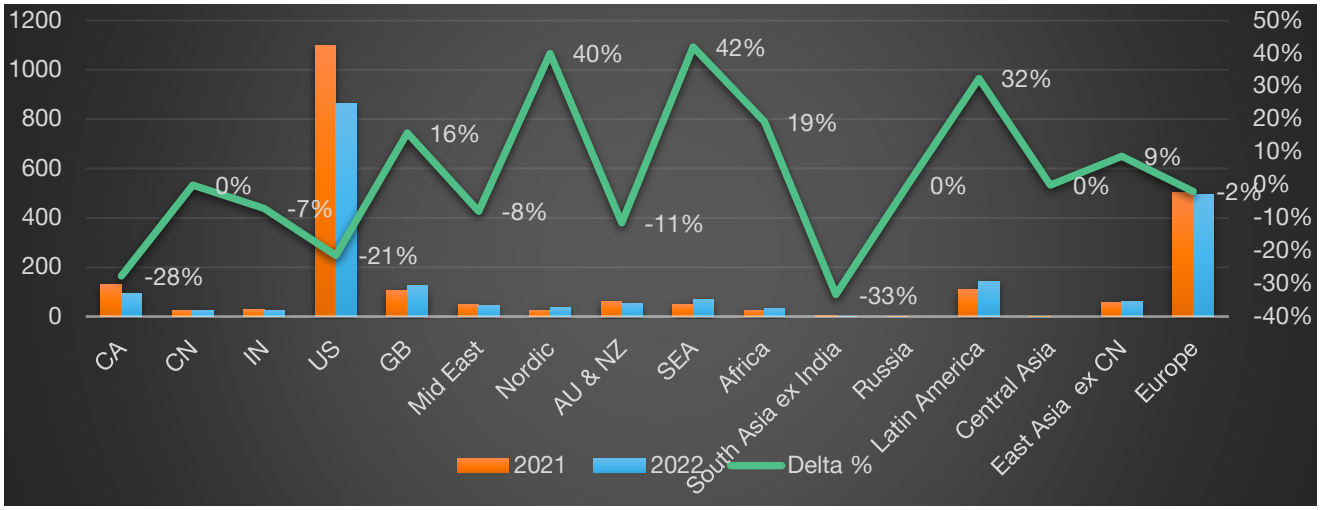
Victimology of Q1 2023

Of the 770 victims observed in Q1, 46% of all victims were headquartered in the U.S., followed by the United Kingdom (7%) and Canada (5%). One interesting observation for this time period is that we have seen more Indian victims than usual. LockBit3 has uploaded most of them to their shame site on the darkweb. Most of the victims from India were uploaded in March.



Top 20 Victim organization's country in Q1 2023

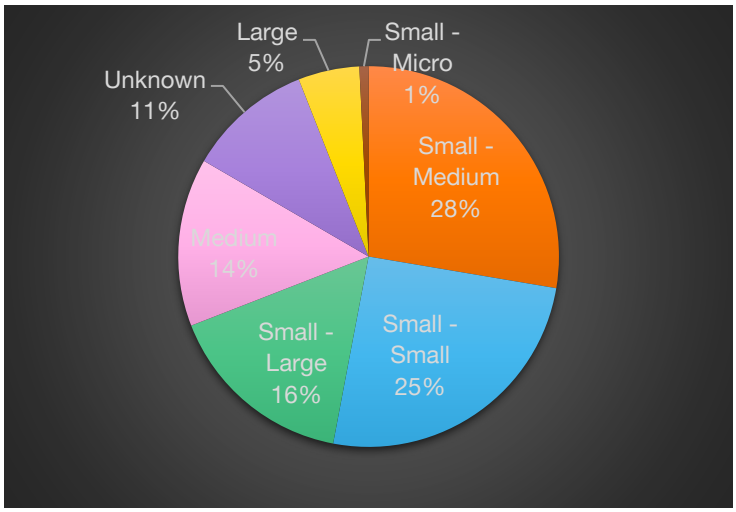
As we have analyzed the 2022 Cy-X threat in depth, we can also see a shift in regions. Below you see the regional shift from 2021 to 2022.



Regional shift of Cy-X victims between 2021 and 2022

We notice a downward trend in North America, more specifically the U.S. (-21%) and Canada (-28%). While the UK experienced an increase of victims in 2022. The biggest increase we documented was in the Southeast Asia region, with countries such as Malaysia, Thailand, Vietnam, Philippines to just mention a few. The second biggest region we saw an increase of Cy-X attacks are the Nordics, which includes Sweden, Denmark, Norway, Finland and Greenland. Latin America, including South and Middle America have also seen an increase, here we see victims from Mexico, Brazil, Columbia & Argentina, to mention just a few. An unexpected finding is that we saw a small decrease in European countries being impacted by Cy-X, however this decrease is very small and we do not expect this to continue.

And finally, if we look at what businesses have been impacted the most in regards of business size; we see businesses with 50-249 employees victimized the most in Q1 (28%). Closely followed by businesses with employee count 10-49 (25%). If we combine the victim organizations that have an employee count 250+, we see that 35% of all victims are from this group. Generally, it is almost an even split between those 3 groups, showing that anyone from any business size can become a victim of Cy-X.



Business size classification

Small – Micro: 1-9 employees
Small – Small: 10-49 employees
Small – Medium: 50-249 employees
Small – Large: 250-999 employees
Medium: 1000-9,999
Large: 10,000+

11% of all victims were impossible for us to classify. This happens when we are unable to find the employee count of a victim organization.

Conclusion

Q1 2023 has certainly changed the threat landscape of Cy-X. While we saw a decrease of 8% during 2022, we registered the highest number of victims documented in the past 3 years. While we do not know for sure, we do think there is a connection between the ongoing Ukraine war and the threat actors activity of Cy-X in 2022. As we have seen in the very beginning of the war, some threat actor groups are indeed pro-Russian and have openly announced support for Russia. While Cy-X is a financially motivated crime, it has become quite geopolitical due to the Ukraine war. This led for example to the closure of the criminal operation of Conti in 2022, which made room for splinter groups of Conti and others to fill up the space.

In Q1, we have seen several groups popping up, and other fairly new ones claiming the space of opportunity for their criminal activities. With one exception, Cl0p has claimed over 100 victims in March, exploiting once again a 0-day vulnerability. If we can be sure of something, it is the unpredictability of the threat landscape of Cy-X.

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.

Wicus

The responsible party

The more we become dependent on technology the heavier the burden of managing privacy, security, and safety gets. Some Internet users, in their private capacity, struggle to protect their email account credentials adequately and it's only a matter of time before their account is breached. Those accounts that have not been compromised are the lucky ones. What then about the other accounts we have on social media platforms, streaming platforms, on-line shopping, etc.? There is clearly a line of responsibility when it comes to protecting the credentials of accounts – it is with the owner of the account.

When it comes to vulnerabilities in the platforms, software, or hardware the lines are less clear. For anything that a user has direct control over such as hardware or software the responsibility for maintaining and securing these is the responsibility of the owner. This is like owning a car. The owner is responsible for ensuring that the car is roadworthy according to current traffic regulations and that the vehicle is in good running condition. In most cases the manufacturer of the vehicle has no further obligation, but there are cases where the manufacturer issues a recall on a specific model of vehicle. A recall is a very calculated process based on potential future legal claims, punitive fines, brand risk, etc. Each manufacturer has their own formulas and will issue a formal recall if they deem the negative impact to be greater than the loss suffered with no recall. This still leaves those defects that could impact people but are classified by the manufacturer as "acceptable risk".

Mature software and hardware technology vendors may issue fixes for defects if they deem it impacts the quality of their product. Defects are a combination of design choices and or implementation errors that cause unintended behavior. Some defects can have an impact that weakens the product so that attackers can exploit these for various purposes. Like automobile manufacturers, software and hardware vendors perform an assessment of a defect and then decide when and if they are going to allocate resources and people to fix the defect.

In both the automobile manufacturing industry and the software and hardware industry, defects can impact people's lives. Arguably the automobile industry has travelled a longer road and understands this much more acutely since safety is part of the design aspect of vehicles. Safety ratings have been assigned to vehicles as part of a system to allow potential buyers to make an informed decision about how likely an injury could be sustained when the vehicle is in an accident. These safety rating systems are also an incentive for manufacturers to

show commitment to designing safe vehicles. These safety systems were required by governments due to political pressure to force vehicle manufacturers to be more responsible and accountable for their products [3] [4].

Where the car analogy becomes weak is when we consider the nature of the defects and what triggers them. With automobiles there could be flaws that make it easier for thieves to steal the vehicle or gain unauthorized access to the vehicle. The high impact defects are typically something that could result in loss of life or extended loss of property. The former is straightforward to understand, if the seatbelts or airbags fail under some conditions, then the passengers could be injured or killed. In the case of extended loss of property, for example if a vehicle is parked in a motor garage and catches fire then that fire could result in damage to the garage and the rest of the attached property. Except for criminal intent, automobile manufacturers must work hard to minimize the loss of human life and property.

Recently we have had cases of so called “self-driving” cars that were involved in accidents that resulted in severe injury or even loss of life. These are edge cases for the most part, but it will become scrutinized more as more manufacturers adopt these technologies. It is expected that government scrutiny on these types of features will become stricter [5].

It might be a far stretch to say that defects in software and hardware, in general, could result in fatalities. This may be true for some cases, but for most cases we assume that no human is physically injured due to software or hardware defects. There are exceptions where the application is specifically designed to prevent human harm while performing its task.

One would error to confuse security with safety and vice versa. The blend of both safe and secure systems introduces complexities that can become costly to build and manage, but that all depends on the priorities of each. Having a super secure vehicle may be a safety risk for passengers if it is difficult to open the doors or windows to escape the vehicle. Ultimately there must be a conscious design choice to balance the tradeoffs.

Let’s park the car analogy.

Software or hardware vulnerabilities impact is broadly defined in terms of the impact it has on confidentiality, integrity, availability, or a combination of the three. The experienced impact is based on the damage that is inflicted by attackers and can sometimes be limited to a few victims, but it could also be widespread.

[3] https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed
[4] https://en.wikipedia.org/wiki/New_Car_Assessment_Program
[5] https://www.politico.eu/article/eu-plans-to-approve-sales-of-fully-self-driving-cars/

The 3CX supply chain incident that made headlines at the end of March 2023 probably rang déjà vu for many with flashbacks to the December 2020 SolarWinds incident. Then with a sigh of relief we learned it's only North Korea – possibly [6]. Everyone knows that DPRK is only after Bitcoin, right? So, no big deal! Looks like the compromise of a trading platform allowed DPRK to jump into 3CX's environment through a supply-chain compromise predating the 3CX incident [7].

What does this type of incident mean for businesses? The 3CX incident once again highlighted the inherent risk that we accept. It is the cost of doing business. When software or hardware is installed inside the business, we must acknowledge that there are going to be security issues that surround this product. The more products present in a business, the greater the potential risk becomes that must be managed.

What is becoming more evident is that the opportunity for widespread attacks is increasing. Fortunately, the world seems to be more ready for cyberattacks in 2023 than it was in 2017 when the WannaCry "ransomware" wreaked havoc, (also) courtesy of our North Korean friends. Several security vendors detected the maliciously laced software embedded in the 3CX software update. Unfortunately, some treated the alarms as false positives and recommended that the software be added to the permitted software list to avoid further notifications. What was encouraging was that many questioned this and started digging further and 3CX also recognized the real threat. From subsequent reports it seems that of the potential 600 000 victims only a handful were impacted [8] [9]. So less sinister than the SolarWinds incident, but we expect to learn more about what transpired over the course of the year.

Looking forward to the political and regulatory landscape. In the US the Biden-Harris administration published a fact sheet titled "Biden-Harris Administration Announces National Cybersecurity Strategy" on March 2, 2023 [10]. This statement contains two key points namely to "rebalance the responsibility to defend cyberspace" and "realign incentives to favor long-term investments". These are the bold parts of the two points and there is supportive text that gives greater context, but what I read is the acknowledgement that technology vendors need to be held more responsible for the choices they make about their products. The message is very diplomatic as well as pragmatic since it is addressed to vendors serving the US government, the critical infrastructure of the US, and the people of the US. For now, this is an important distinction, but it should get the attention of those serving other markets as it is a harbinger for things to come and signals political will to increase pressure.

[6] https://www.3cx.com/blog/news/mandiant-initial-results/
[7] https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
[8] https://therecord.media/3cx-attack-north-korea-lazarus-group
[9] https://unit42.paloaltonetworks.com/3cxdesktopapp-supply-chain-attack/
[10] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

This statement by the US executive office is an important milestone for cybersecurity practitioners as well as IT teams. I see it as an acknowledgement that there ought to be repercussions and shared responsibility. For many applying software patches is like practicing some old esoteric and cultist ritual to ward off evil spirits. If your patch ritual was good, then you are safe until the next full moon. And until then you need to have special talismans in place just in case the boogeyman is perhaps hiding under your bed. Unfortunately, that is what is required because systems are devilishly complex and as time passes these systems become even more complex with the inherent legacy that is bestowed on them because of that.

Another reality is that mandatory cyber incident reporting will become a requirement. Examples include the recent Network and Information Security (NIS) Directive v2.0 issued by the European Union. Countries such as the United States and even India have imposed mandatory cyber incident reporting requirements. The challenge here is that these reporting requirements are not necessarily aligned and may create increased overheads for businesses operating in these countries as it may require multiple reporting streams to run in parallel, as a recent Harvard Business Review article pointed out [11].

This means that even if a business has applied all their security patches, use phishing resistant MFA to protect against credential theft, and deployed the latest security controls, they can still have an incident that they need to deal with if a vendor's product they use is compromised through a supply-chain attack. Cyber insurance might cover this and pay for the incident response and forensics, but someone must still report the incident in every jurisdiction you operate that mandate this. This will also raise the question whether guilty vendors could be sued to recover potential losses suffered by the incident.

Holding vendors directly accountable for their design and implementation choices as well as their security practices will be an important milestone. For businesses this means that the selection of vendors and the due diligence that needs to be done before engaging with vendors will become much more important in the future. We are entering new territory as it's going to become a lot more complex to find partners to trust and work with. Trust is granted not earned[12].

[11] https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready
[12] https://mike-robbins.com/trust-is-granted-not-earned/


Ric

Hacker Voice "I'm in (your head)": The Doctrine of Cognitive Effect

The 'cyber war', or lack thereof, may not have been what many pundits expected to happen since the start of the conflict in Ukraine in February 2022 – fortunately we have not seen anything like the frequently touted 'cyber Pearl Harbor' or 'cyber 9/11'! However, that does not mean that 'cyber' is something that states have or will leave uncontested, by any means.

In 2022, the UK government released their National Cyber Strategy (NCS), which stated that the UK will continue to be a responsible and democratic cyber power. Supporting that aim is the National Cyber Force (NCF), established in 2020 by drawing on personnel from Government Communications Headquarters (GCHQ), Ministry of Defence (MoD), Defence Science and Technology Laboratory (Dstl), and the Secret Intelligence Service (SIS). The NCF, in line with the NCS, aims to operate continually, supporting the UK armed forces and foreign policy to disrupt a wide range of threats.

On the 4th April 2023, the NCF released a document that sheds light on their plans and practices, called Responsible Cyber Power in Practice[13]. The document aims to provide some transparency into the type of operations performed by the NCF as well as the diligence and oversight taken throughout. As the document alludes to later on, this is a crucial step for the NCF in navigating the fine balance between secrecy and transparency.

The NCF's document lists adversaries not limited to state actors such as Russia and Iran, but terrorist and organized crime groups, as well as ideological driven actors such as hacktivists who have been seen aligning themselves with certain conflicts such as the recent Russia-Ukraine conflict.

As a response, offensive cyber operations are said to be a complementary addition to the existing measures at the UK's disposal. This is because such cyber-attacks can be measured, precise, and without geographic constraints, all while reducing any physical destruction or the need to be physically present during the attack. However, whether offensive cyber capability can be used as a valid deterrence is still unknown due to a lack of evidence.

Naming it the 'doctrine of cognitive effect', the NCF state that their aim is to change adversary behavior by using accountable, precise, and calibrated cyber operations to exploit their reliance on digital technology. As you may guess from

[13] https://www.gov.uk/government/publications/responsible-cyber-power-in-practice

the criteria put forward, this means that the NCF does not intend to launch wide-sweeping disinformation campaigns as we have seen from adversaries; rather they want to, as they state, affect an adversary's ability to acquire, analyze, and exploit the information they need or limit their ability to communicate and coordinate – effectively reducing the confidence the adversary has in their digital technology. Furthermore, operations with abrupt, destructive impacts, such as denying an adversary's access to digital technology, are generally eschewed for more clandestine operations, which affect an adversary's systems over a period of time. However, such operations are not ruled out entirely and are said to remain an option where they are the most appropriate solution.

The NCF recognizes that cyber operations are rarely decisive on their own and are most effective when coordinated with other activities. Therefore, cyber operations are used in conjunction with other capabilities such as physical engagements so that one may enable or enhance the other, depending on the type of engagement.

Interestingly, the NCF maintains operational flexibility and agility by developing 'blocks of capability' for their cyber capability development. This ensures that they may respond in a precise, calibrated, and timely manner to threats with minimal tailoring required.

In further keeping with the criteria of accountable, precise, and calibrated, the NCF takes great care in responsible planning of their operations. This includes strict adherence to the Intelligence Services Act 1994, the Investigatory Powers Act (IPA), and the Regulation of Investigatory Powers Act 2000 (RIPA), and where armed conflict is involved, the Law of Armed Conflict. On top of this, ethical concerns are considered in operational planning in order to ensure that operations are consistent with their democratic values. Moreover, the NCF states their activities are subject to approval by ministers, judicial oversight, and Parliamentary scrutiny.

Understandably, there are challenges to address for an organization such as the NCF. Firstly, recruiting and retaining the right people with the right skills is difficult, particularly when the public sector struggles to compete with private sector when it comes to remuneration. As well as recruiting and retaining those people with the right skills, maintaining their pace of development alongside the pace of technology's evolution compounds that challenge. Furthermore, with the nature of operations following the 'doctrine of cognitive effect', the NCF have stated it will be particularly challenging to measure the effectiveness of operations with such nebulous desired outcomes as changing the adversary's behavior. Finally, the careful balance between secrecy of operations and capability vs the required transparency to set the UK public at ease is a particularly delicate challenge.

It is difficult to pass any comment on such a document when, despite this being a monumental milestone in transparency, it is still clearly in line with the NCF's effort to maintain ambiguity and secrecy. Perhaps the most interesting element to take away from this is the 'doctrine of cognitive effect' whereby the NCF have clearly stated they won't be utilizing any 'cyber weapons' to be causing significant damage to critical infrastructure. However, as Rory Cormac stated in a recent RUSI article[14], this isn't an entirely new approach for UK covert operations – just a new landscape in which such an approach is conducted. Regardless, it is recommended that you read the document for yourself to make up your own mind.


Diana

Cyberspace – recent developments of formal guardianship

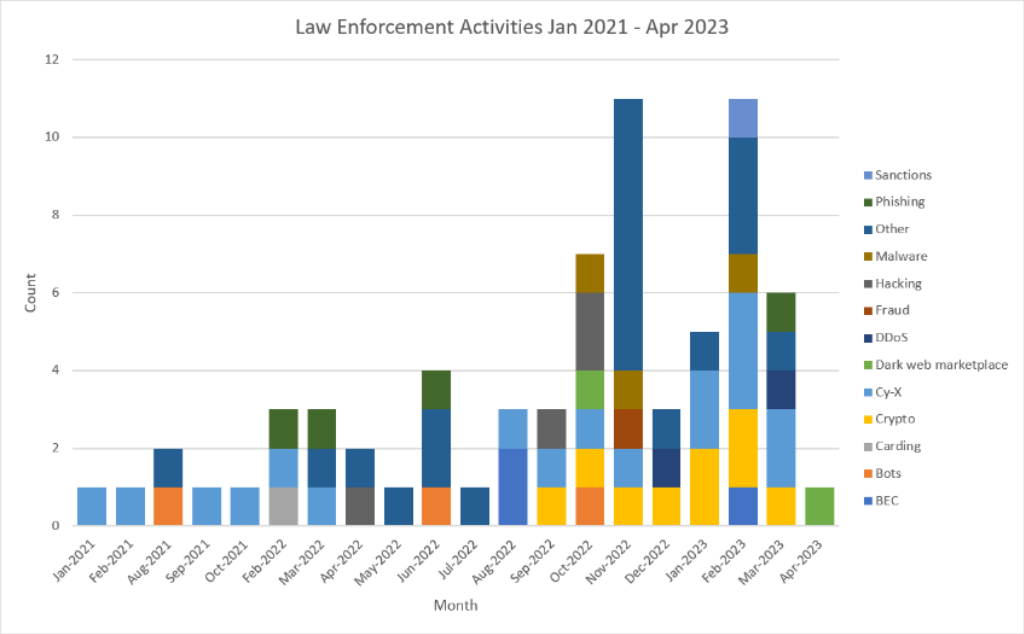
Cyberspace is a tough one when it comes to the controversial questions on how it is protected and who should govern that space in the first place? But in one aspect, we might all agree, it's a challenging space to protect, given the nature of anonymity, the degree of *un*certainty and the issue of jurisdiction.

If we have wrongdoing in the real world, we certainly will have similar anti-social behavior in cyberspace. As we have argued previously, if we then look at crime theory in order to understand and come up with strategies to combat cybercrime; we might want to look at '*The lack of a capable guardian*'. A guardian can be a person or an object. In cyber security context this could mean technical security controls with all their capabilities as well as limitations. It could mean a human or a collective of humans (community) considered informal, social guardianship that would help deter crime. And finally, it could also mean formal guardianship such as law enforcement.

We are currently looking at developing a new data set where we want to track formal guardianship in cyber space to attempt to answer the *question if law enforcement activities are effective*. This will be a joint project with our CERT team where we want to not only look at activities over time but also the type of activity, the resulting consequences, e.g. arrests and who has been involved in those, e.g. Interpol, National police agency etc. It will be interesting to observe the development of such activities, whether or not we can see effect on the threat landscape and different forms of crime that we are monitoring and as a 'side product', to get insights on how long it takes between arrests and sentencing.

[14] https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice

We are yet to define the details, but here comes a sneak preview of our dataset that we consider *beta*.



As we can see above, we have seen much more law enforcement activities in 2022 and the beginning of 2023. With actions to combat cyber extortion (Cy-X) being the second highest type of law enforcement activities we observed; followed by Cryptocurrency related activities. This is an interesting trend to monitor, given the nature of how cybercrime is entangled with cryptocurrency. We also observed several site take downs, such as criminal market places and forums. As well as law enforcement being able to seize money to return to their victims. And last, 2022 might have been the year where law enforcement has shown their 'hacking back' capabilities as we have seen with the take down of the Cy-X group Hive; as well as governments starting public-private collaborations and mobilizing a collective strength to combat cybercrime such as the Australian government that has is leading the international task force to combat ransomware since January 2023.

Good News Cyber

Europol announced that a joint operation between law enforcement agencies of the United States of America and Germany shuttered a money laundering operation that specialises in obfuscating blockchain transactions. The operation resulted in the seizure of assets of cryptocurrency mixer ChipMix as well as the dismantlement of the platform. The authorities stated that ChipMix was used by cybercriminals and others.

Spanish law enforcement arrested a 19-year-old in connection with multiple cybercrimes. The 19-year-old was responsible for creating a platform that enabled them to sell large volumes of sensitive information to willing buyers. According to reports large amounts of cash was found at various properties. Authorities also confiscated several computing devices and documentation. The investigation into the alleged cybercriminal was sparked due to a cyberattack on Spain's national council of the judiciary (CGJP).

The FBI, along with assistance from law enforcement agencies in multiple countries, seized the domain names associated with a criminal marketplace called Genesis Market that specialise in selling malware that can steal account information form victims. According to Brian Krebs, who reported the story, confidential sources stated that arrest warrants are being served to suspects linked to the Genesis Market.

Ukrainian Cyber Police, with assistance of law enforcement from the Czech Republic, has arrested several individuals in connection with scams that relied on phishing and other social engineering practices. The lures pointed victims to scam web sites that allegedly sold items at unreasonably low prices, but the con was to steal credit card information. Authorities conducted more than 30 searches at various locations.