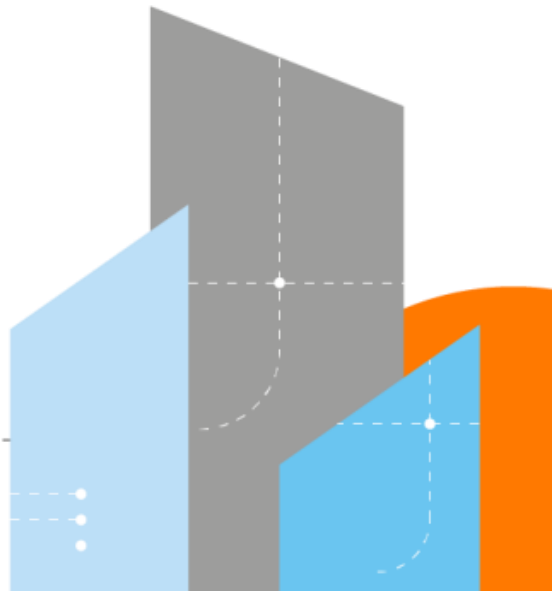
Orange
Cyberdefense

Security Intelligence

Quarterly Report

December 2022



CONTENTS

INTRODUCTION

Microsoft Exchange Server received several security patches. The infamous trio ProxyLogon, ProxyOracle, and ProxyShell were joined by ProxyRelay. Attackers have also been targeting other vulnerabilities in on-premises Microsoft Exchange Servers.

Old Microsoft Office vulnerabilities are still being used by attackers. New malware has been discovered that carries exploits for Microsoft Office 2016 and older. Similarly certain attackers are also targeting older vulnerable Windows features such as the Microsoft Equation Editor.

Citrix released a security fix to address flaws in their Application Delivery Center. The flaws are said to have been targeted by attackers.

Popular security products will remain in the firing line. Fortinet's FortiOS and FortiProxy received fixes to address serious vulnerabilities. Threat Intelligence reports also show that attackers are still gaining access as a consequence of vulnerabilities disclosed in 2018 impacting Fortinet products.

We recorded 494 businesses being victimized on cyber extortion leak sites. In Q4 2022, we saw an increase of 7% in comparison to Q3 2022 that totaled 460 victims. The top 5 cyber extortion groups contributing to the Q4 2022 victims were: LockBit3 (29%), ALPHV (aka BlackCat) (14%), Black Basta (11%), Royal (10%), HiveLeaks (5%) and Others (31%). The top 3 most reported cyber extortion victims originate from the United States of America, Canada, and Great Britain, followed by Germany, Brazil, and France

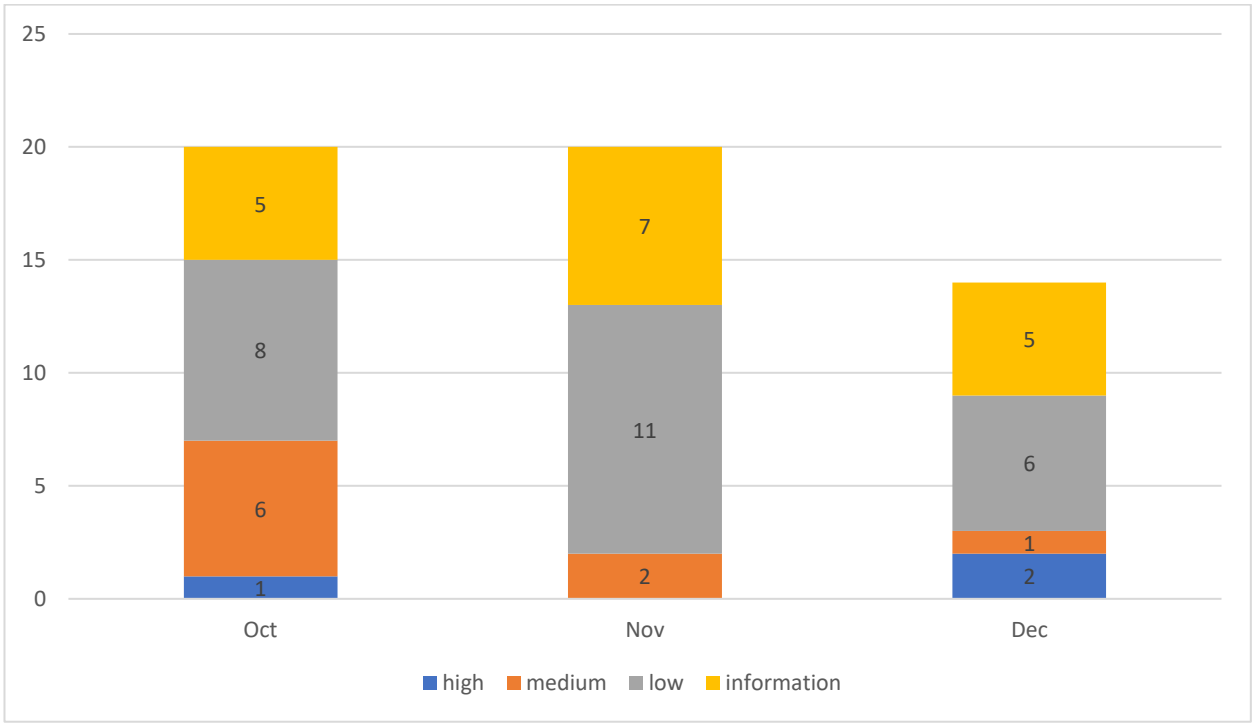
The EU Directive on Security of Network and Information Systems (NIS) version 2 came into effect on January 16, 2023. NIS2 addresses issues with the original NIS regulation and new clarifications have been introduced. NIS2 must be transposed into national law by EU Member States by 17th of October 2024 and its scope has broadened both in what types of organizations it captures, as well as what those organizations must do to be compliant.

At a glance

In Q4 2022, we saw an increase of 7% in the number of cyber extortion victims over the previous quarter.

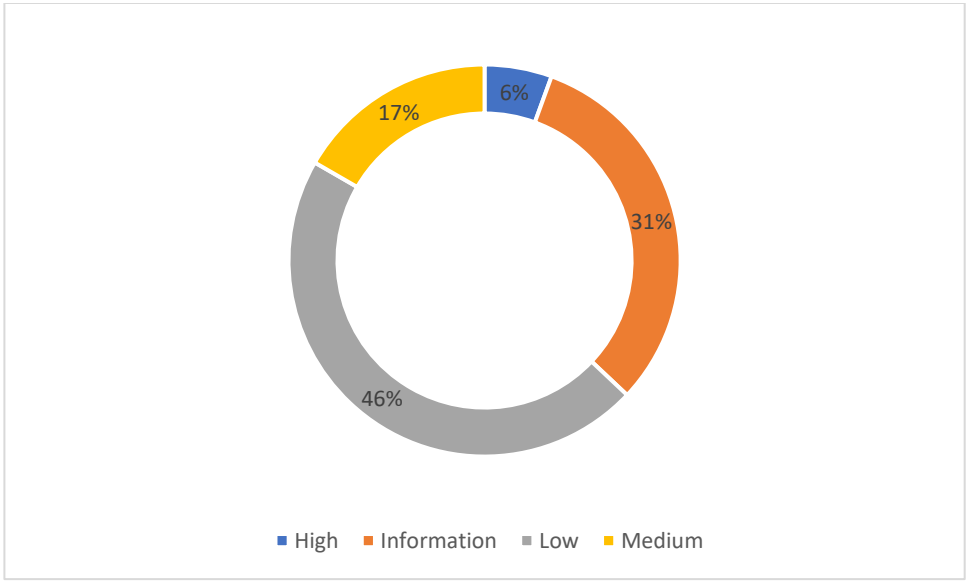
World Watch Review Quarter 4 of 2022

The Orange Cyberdefense CERT published a total of 54 new World Watch advisories from October 2022 up to and including December 2022, along with updates to a further 72 previously published advisories. This volume of new advisories is keeping steady and is slightly more than the previous quarter.



Breakdown of new advisories by severity for Q4 2022

We did not publish a critical rated advisory in Q4 2022, with the last critical advisories being published in Q4 2021. The severity rating of advisories for Q4 is predominantly made up of advisories rated as Information or Low urgency.



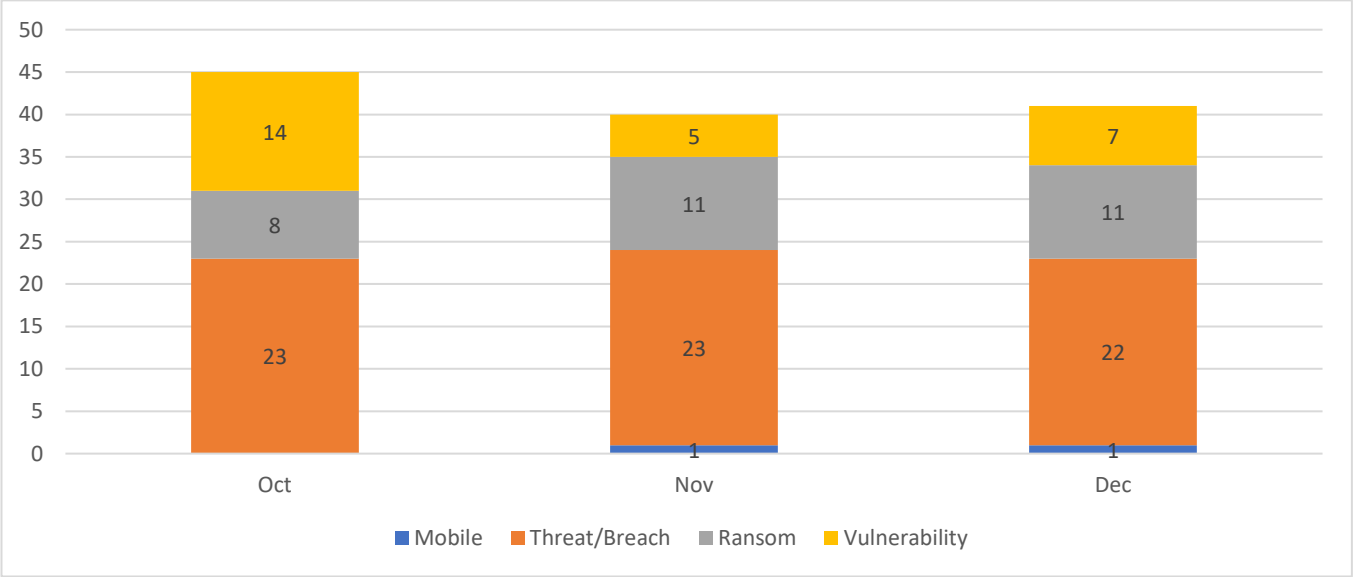
Breakdown of new advisory severity for Q4 2022

Different Approach

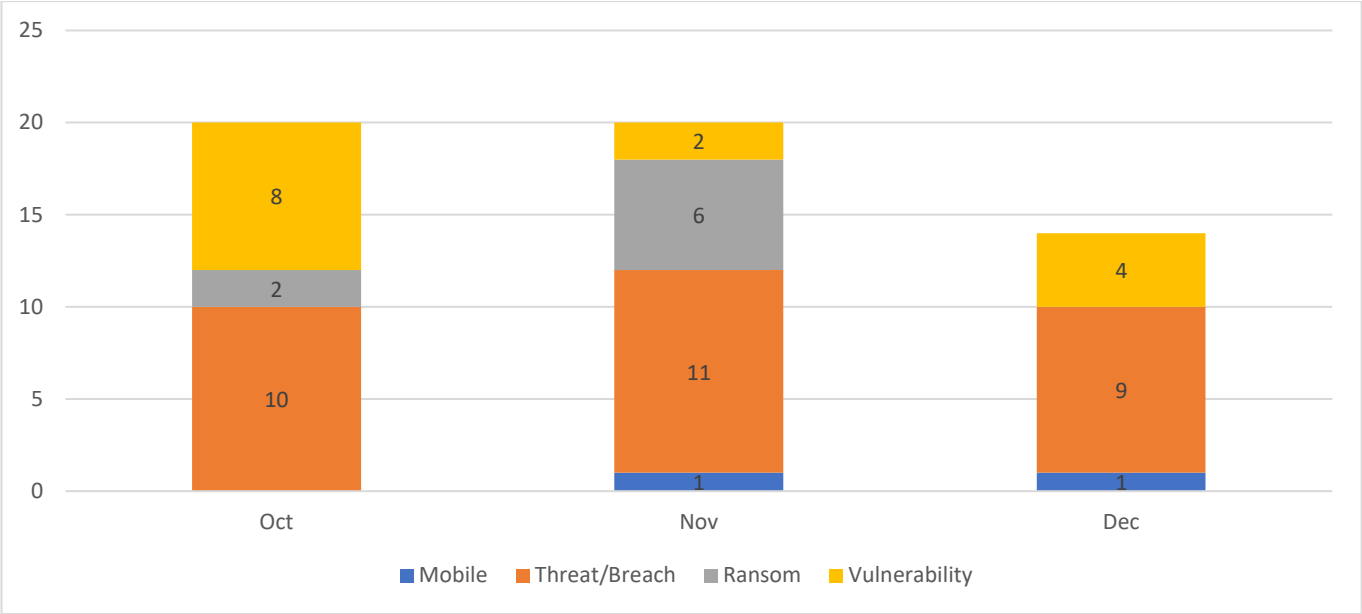
This month we are looking at Q4 of 2022 using an approach we used in compiling parts of the OCD **Security Navigator 2023** report, namely using Machine Learning (ML) to help analyze published advisories. ML algorithms were used to highlight potentially interesting occurrences of keywords such as CVEs 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

Advisories categorized as Threat/Breach are, by volume, the bulk of all advisories issued for either new advisories or updated advisories. Compared with the other themes combined, Threat/Breach outnumbered the balance 68 to 58, giving it a significant bulk of all advisories issued. When examining just the new advisories we see a similar pattern with advisories categorized as Threat/Breach outnumbering the balance 30 to 24.



All World Watch advisories published by theme in Q4 2022



New World Watch advisories published by theme in Q4 2022

Our machine learning classifier identified very little discussion involving attacks against mobile phones. The two advisories labelled as Mobile were published in late November 2022 and early December 2022 are respectively:

SIG-661823 – Cybermercenary group Bahamut infects Android users in highly targeted campaign

- Attackers are using trojanized VPN apps that is distributed through phishing links. If a user clicks these links then their Android phone will give the user the option to sideloaded the App. Sideloading is where the user install applications that do not originate from the official Google Play store, but rather from an arbitrary location and it is very difficult to validate the legitimacy of the application as this approach can be associated with malicious activity.
- Bahamut's malware is distributed through a fake website branded as "SecureVPN", pushing trojanized versions of two well-known legitimate applications: SoftVPN and OpenVPN. The spyware distributed in this campaign can exfiltrate data such as:
    - contacts,
    - SMS,
    - call logs,
    - device location,
    - recorded phone calls,
    - etc.

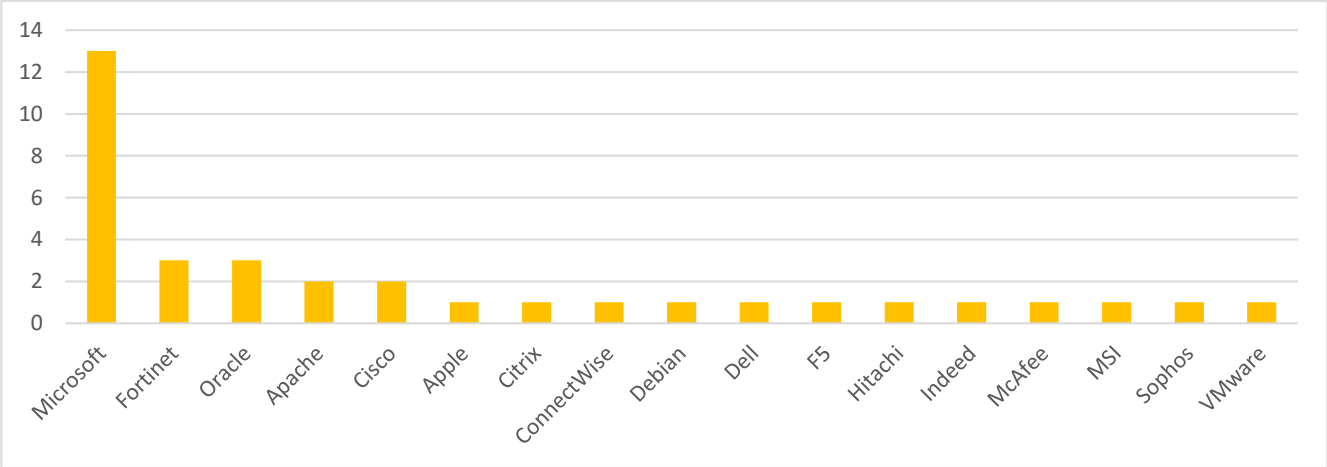
SIG-663413 – Legitimate certificates from Samsung, LG, Mediatek and others used to sign Android malware

- Google's Android Partner Vulnerability Initiative recently disclosed that multiple platform certificates used by Android OEM device vendors to sign core system applications have also been

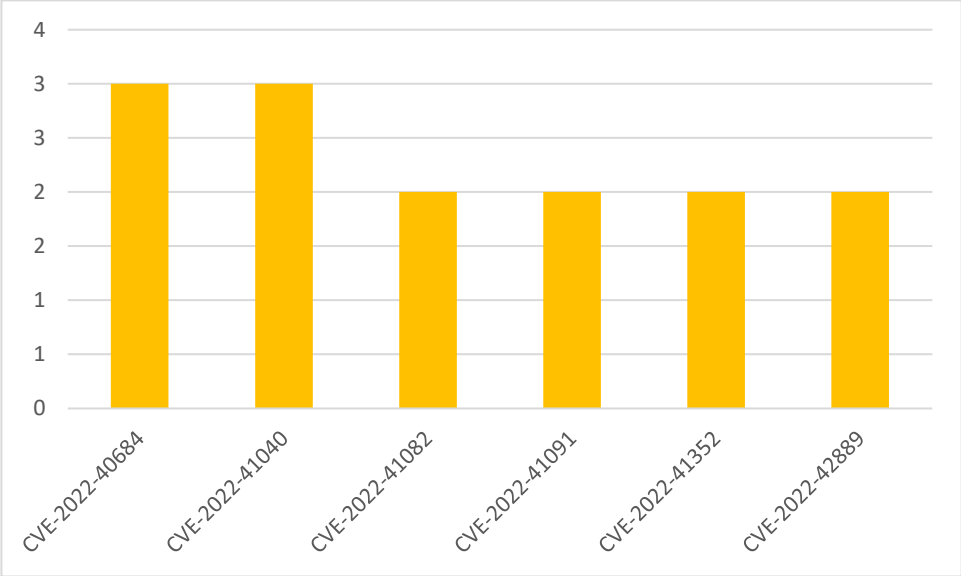
used to sign Android malware. Allegedly the compromised certificates belong to vendors such as Samsung, LG, Xiaomi, Mediatek and others.

- Android trusts any application signed with the same key used to sign the OS itself. By simply setting the user id of the application as “android.uid.system”, a malicious actor with access to the platform certificates can give malware full system-level permissions on an affected device. This includes permissions not normally granted to apps, such as managing ongoing calls, installing, or deleting packages and other highly sensitive actions.
- According to APKMirror, one of the compromised keys was used to sign Samsung apps in the last few days since the public announcement if the incident. This means the impacted keys have not yet been revoked and replaced.
- No malicious activity related to these stolen certificates has yet been reported.

Looking at vulnerabilities during the last three months of 2022 we note several prominent vendor names. Some are regulars, while others such as Hitachi, Indeed, MSI, and ConnectWise occur much less frequently.



Subset of Vendors mentioned in Vulnerability World Watch advisories for Q4 2022



Subset of CVEs encountered more than once in Vulnerability World Watch Advisories for Q4 2022

CVE ID	Vendor / Product
CVE-2022-40684	Fortinet FortiOS and FortiProxy (several versions)
CVE-2022-41040	Microsoft Exchange Server (several versions)
CVE-2022-41082	Microsoft Exchange Server (several versions)
CVE-2022-41049	Microsoft Windows Mark of the Web (several versions)
CVE-2022-41091	Microsoft Windows Mark of the Web (several versions)
CVE-2022-41352	Zimbra Collaboration (ZCS) 8.8.15 and 9.0
CVE-2022-42889	Apache Commons Text (several versions)

CVE-2022-44698	Microsoft Windows Mark of the Web (several versions)

Subset of CVEs encountered more than once in Vulnerability World Watch Advisories for Q4 2022

SIG-652349 - Highly critical vulnerability in FortiOS and FortiProxy

- This vulnerability, tracked under CVE-2022-40684, allows an attacker to carry out specially crafted HTTP/HTTPS requests on the administration interface. Using these requests, the attacker can bypass authentication and inject arbitrary commands that can be executed as an administrator.
- FortiOS till versions 7.0.6 and 7.2.1, with FortiOS version 7.0.7 and 7.2.2 are impacted.
- FortiProxy versions 7.0.6 and 7.2.0. with FortiProxy version 7.0.7 and 7.2.1 are impacted.

SIG-650623 - Microsoft has released new recommendations to mitigate CVE-2022-41040

- New set of vulnerabilities affects Microsoft Exchange Server
- On October 1, Microsoft released a mitigation tool (EOMTv2) for the CVE-2022-41040 vulnerability. This tool helps administrators to easily apply mitigation measures for the SSRF vector used in CVE-2022-41040 impacts on-premises Exchange servers.
- CVE-2022-41082 was also disclosed as part of the fix for the exploitation of Exchange Servers.
- Similar to the infamous ProxyShell vulnerabilities, this attack chain targets the Microsoft Exchange Autodiscover service, so it might be possible that the new vulnerabilities are related or even results from an incomplete ProxyShell patch that left working attack vectors.
- Microsoft now recommends:
    - disabling remote PowerShell access for non-administrator users to mitigate the risks from these vulnerabilities.
    - adding a blocking rule in "IIS Manager -> Default Web Site -> URL Rewriting -> Actions" to block known attack patterns.
    - new measures to detect malicious files listed in the appendices.
- The vulnerability is considered a zero-day attack as attackers have been detected targeting this vulnerability.

SIG-654761 - Details about authentication bypass issues in Exchange Server named ProxyRelay have been disclosed

- The vulnerability named ProxyRelay relates to attempts to work around Microsoft's patches for the ProxyLogon, ProxyOracle, and ProxyShell vulnerabilities that reduced the available attack surface. The security research, Orange Tsai, identified ways to relay NTLM authentication from an attacker-controlled Exchange Server towards other external Exchange Servers, which enabled the researcher to bypass authentication (and even get code execution in some cases).
- The ProxyRelay vulnerability consists of 4 vulnerabilities:
    - CVE-2021-33768 - Relay to Exchange FrontEnd
    - CVE-2022-21979 - Relay to Exchange BackEnd
    - CVE-2021-26414 - Relay to Windows DCOM
    - And a yet to be named CVE that is responsible for relaying to other services of Exchange.

- These vulnerabilities were responsibly disclosed to Microsoft and patches were released between July 2021 and August 2022. Also, no PoC has been made public, thus the risk for unpatched Exchange servers remains limited, even if the technical details shared could enable further work in this field.

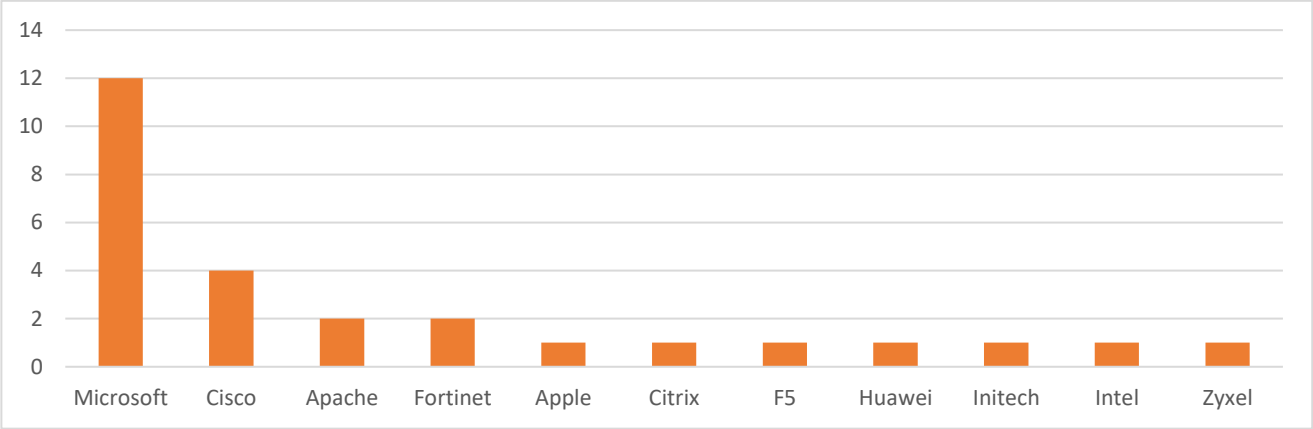
SIG-654567 - Updated - Microsoft's December Patch Tuesday fixes zero-day MotW bypass

- Usually, Windows automatically adds Mark of the Web (MotW) flags to all files downloaded from untrusted sources, including ones extracted from downloaded ZIP archives, using a special 'Zone.Id' alternate data stream. Therefore, these MotW labels enable Windows, Microsoft Office, web browsers, and other applications to generate warnings displayed to the user explaining that opening the files could lead to dangerous behavior, such as malware being installed on the device.
- However, vulnerability analyst Will Dormann has discovered that ZIP archives were not properly adding MoTW flags to decompressed files. This is a major security issue as for example Smart App Control will only work on files with MotW flags and Microsoft Office only block macros by default in documents tagged with MoTW. A malicious actor could then deliver malicious Word or Excel documents in a downloaded ZIP that would not have their macros blocked or would escape the inspection by Smart App Control.
- On December 13, Microsoft released security updates in their latest Patch Tuesday that included include a patch for CVE-2022-44698, a Mark-of-the-Web bypass exploit.
- Tworelated MotW flaws, CVE-2022-41049 and CVE-2022-41091, were patched as part of Microsoft's November 2022 patch cycle.
- There is a chance that the MotW flaw was exploited recently by malware such as IcedId and Bumblebee to avoid detection. Additional advisories were issued of attackers exploiting the flaw as part of Qakbot malware and Magniber ransomware activity as detailed in SIG-522818 Update 4 published on November 21, 2022.

SIG-654645 - Text4Shell, a patched arbitrary code execution vulnerability in Apache Commons Text

- On October 13, the Apache Software Foundation released an advisory about the CVE-2022-42889 vulnerability, a critical code execution bug in Apache Commons Text.
- Dubbed "Text4Shell", this code execution vulnerability was quickly exploit compared to the infamous Log4Shell because it impacts an open-source library and was presumed to have an impact on a wide variety of software that depend on it. However, this comparison is farfetched because less applications depend on this vulnerable library than first thought. Indeed, it is much less widespread than log4j. Furthermore, only specific versions of the JDK may be exploited so far using the publicly available PoC, which does not work on most JDKs.
- On October 20, the Wordfence Threat Intelligence team announced in a report that the CVE-2022-42889 vulnerability, also known as "Text4Shell" is exploited in the wild. They uncovered various activities targeting this vulnerability since October 18, such as IPs, listening hosts, parameters or query string headers. IOCs related to this campaign should be proactively integrated into your security detection solutions. It is important to note that most of the listening hosts cited in this report are running Interactsh servers, which are typically used by legitimate security teams. However, some of these attempts may have been carried out by bug bounty hunters or malicious actors.
- No reports of massive exploitation in the wild of the vulnerability have emerged yet.

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 Q4 2022

CVE ID	Vendor / Product
CVE-2017-0199	Microsoft Office 2016 and older
CVE-2017-11882	Microsoft Office 2016 and older
CVE-2018-0802	Microsoft Office 2016 and older
CVE-2018-13379	Fortinet FortiOS and FortiProxy (several versions)
CVE-2018-12613	phpMyAdmin 4.8.x before 4.8.2
CVE-2020-3153	Cisco AnyConnect Secure Mobility Client for Windows
CVE-2020-3433	Cisco AnyConnect Secure Mobility Client for Windows
CVE-2021-42013	Apache HTTP Server 2.4.49 / 2.4.50
CVE-2022-27510	Citrix Gateway (several versions)
CVE-2022-27518	Citrix Application Delivery Controller (ADC) (several versions)
CVE-2022-33891	Apache Spark (several versions)
CVE-2022-34301	CryptoPro Secure Disk bootloaders before 2022-06-01
CVE-2022-34302	New Horizon Datasys bootloaders before 2022-06-01
CVE-2022-34303	Eurosoft bootloaders before 2022-06-01

Subset of CVEs encountered in Threats/Breaches in World Watch Advisories for Q4 2022

SIG-660695 - LodaRAT malware adopted by various threat actors

- On November 17, Cisco Talos researchers released a report on new variants of the LodaRAT malware also known as Loda.
- This malware is motivated by information gathering and espionage purposes rather than direct financial gain.
- The malware has a version for Windows and Android. It is characterized by spying features such as recording the microphones and webcams of infected devices. Moreover, according to the report, LodaRAT seems to have attracted the attention of various threat actors. Indeed, this malware has been deployed alongside other malware including RedLine, Neshta and a previously undocumented VenomRAT variant named S500.
- It is important to note that LodaRAT has regularly been distributed via email campaigns containing Microsoft Word attachments with macros, exploits or packager shell objects (including through old vulnerabilities such as CVE-2017-0199).

SIG-665465 - Cloud Atlas APT targets Russia, Belarus and Ukraine in recent espionage campaigns

- Cloud Atlas is a sophisticated APT which conducts cyberespionage activities through custom malware.
- Cloud Atlas' payloads include the PowerShower backdoor and a new RtcpProxy tool.
- Cloud Atlas mostly relies on spear phishing containing malicious attachments. As CheckPoint noticed, the APT generally uses public email services like Yandex, Mail.ru and Outlook.com, but in some cases also attempted to spoof the existing domains of legitimate entities that are likely to be trusted by the target. The weaponized Office documents are carefully crafted based on the target, and generally retrieve a malicious remote template from the attackers' servers. Both Positive Technologies and CheckPoint pointed that these templates are RTF documents that exploit 5-year-old vulnerabilities in Microsoft Equation Editor, such as CVE-2017-11882 and CVE-2018-0802. This technique is far from being new in Cloud Atlas's TTPs but remains apparently somewhat effective.
- Cloud Atlas's target scope has slightly shifted with the Ukraine war. In March-April 2022, the APT was observed targeting entities in the pro-Russian Transnistria breakaway region of Moldova, where tensions were escalating amid fears that Russia would try to extend its sovereignty to this region. Since June 2022, multiple persistent campaigns were detected as well, against very specific targets in Belarus and in Russia. According to CheckPoint, Cloud Atlas is also maintaining its focus on the Russian-annexed Crimean Peninsula, and Lugansk / Donetsk regions.

SIG-653463 - Lebanon-based but Iran-backed POLONIUM APT targets Israeli organizations

- Active since September 2021, but first identified in June 2022 by Microsoft, the threat actor is based in Lebanon and coordinates its activities with other actors affiliated with Iran's Ministry of Intelligence and Security.
- According to ESET the POLONIUM APT group leverages cyberespionage activities in the Middle East region notably targeted against Israeli organizations.
- It could be possible the group used leaked VPN account credentials which were made available online last year, at least for some of the victims. Furthermore, Microsoft researchers uncovered that a large portion of the victims were running Fortinet appliances, suggesting POLONIUM might have managed to compromise these devices, for instance by exploiting the CVE-2018-13379 vulnerability.

- According to Microsoft, POLONIUM's activity clearly overlaps with multiple tracked actor groups affiliated with Iran's Ministry of Intelligence and Security including MERCURY (a.k.a. MuddyWater or Seedworm), DEV-0133 (a.k.a. Lyceum) and DEV-0588 (a.k.a. CopyKittens).

SIG-656089 - Threat actors are using vulnerabilities localized in the Cisco AnyConnect Secure Mobility Client

- Two high severity vulnerabilities located in Cisco AnyConnect Secure Mobility Client (for Windows) are currently exploited in the wild. Tracked as CVE-2020-3433 and CVE-2020-3153, these vulnerabilities were discovered and patched in 2020. Both require local access to the host with the impacted Cisco AnyConnect Secure Mobility Client present.
- On October 24, 2022 CISA added both CVEs to its "Catalog of Known Exploited Vulnerabilities", requiring U.S. government agencies of the Executive Branch to patch their Cisco devices by November 14.

SIG-667395 - Novel Golang botnet Zerobot spreads using various exploits

- Zerobot is a novel botnet written in the Go programming language that has increased activity since mid-October through IoT and web application vulnerabilities. It has mainly DDoS capabilities and is currently being offered as part of a DDoS-as-a-Service solution under the name ZeroStresser.
- The Zerobot botnet contains several modules described by Fortinet, including self-replication and exploits for at least 21 vulnerabilities against a variety of products, including:
    - F5 BIG-IP (CVE-2022-1388),
    - Zyxel firewalls,
    - Hikivision cameras,
    - D-Link and Huawei routers, and others
- In addition to the IoT vulnerabilities, the malware also features exploits for Spring4Shell and phpMyAdmin (CVE-2018-12613).
- Microsoft also claims that the latest variant of Zerobot has exploits to target CVE-2021-42013 and CVE-2022-33891, two flaws impacting Apache HTTP server and Apache Spark, respectively.

SIG-665813 - Critical flaw in Citrix ADC exploited by Chinese state-sponsored APT5

- A critical 0-day vulnerability in Citrix ADC and Gateway has been exploited by at least one understated Chinese state-sponsored dubbed APT5 (a.k.a. "Keyhole Panda" at CrowdStrike or "Manganese" according to Microsoft).
- Tracked as CVE-2022-27518, this bug allows an unauthenticated remote attacker to execute commands on vulnerable devices thus possibly take control of them. However, only devices configured with SAML SP (SAML Service Provider) or SAML IdP (SAML Identity Provider) configured are vulnerable, but those with OAuth, LDP, RADIUS, etc. authentication methods are not impacted.
- Another flaw tracked as CVE-2022-27510 and fixed in early November 2022, allows an attacker to bypass authentication by sending a request to a specially crafted path.

- Customers using Citrix Managed Cloud Services or Adaptive Authentication are not affected by this vulnerability.

SIG-654783 - New unconfirmed UEFI bootkit called BlackLotus sold as a service on undergound forums

- New malware sold under the name BlackLotus recently emerged in underground marketplaces such as Exploit.in. The malicious code presumably appears to be extremely sophisticated, offering capabilities usually linked to state-backed threat groups.
- BlackLotus is advertised as a Windows UEFI bootkit, i.e. an implant that targets the system's firmware and remains invisible to security software running within the OS because it loads in the initial stage of the booting sequence.
- Eclypsium had notably discovered three vulnerabilities (CVE-2022-34301, CVE-2022-34302 and CVE-2022-34303), enabling them to bypass Secure Boot. Bypassing the Secure Boot checks allow threat actors to modify the OS, disable security controls or install backdoors.
- It remains unknown if BlackLotus leveraged one of these vulnerabilities mentioned above.

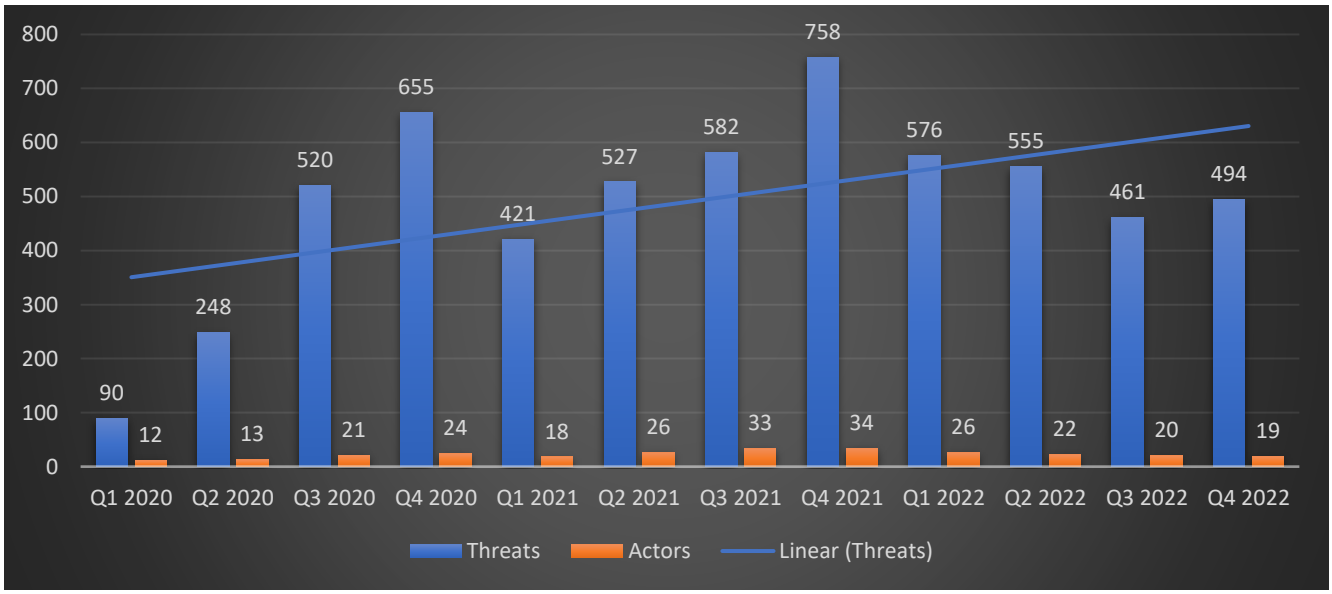
Cyber Extortion Trends in Q4 2022

Summary

- We recorded **494** businesses being victimized on cyber extortion leak sites
- In Q4, we saw an **increase of 7%** in comparison to the previous quarter (Q3 2022, n=460)
- The top **5 cyber extortion groups** contributing to the Q4 2022 victims were: LockBit3 (29%), ALPHV (aka BlackCat) (14%), Black Basta (11%), Royal (10%), HiveLeaks (5%) and Others (31%)
- English speaking countries in top 3 (US, CA, GB) followed by Germany, Brazil & France

General Trends

In Q4, we saw a relatively low number of threat actor groups extorting victim organizations around the world. In fact, we registered a total of 19 threat actor groups victimizing 494 organizations. The last time we saw under 20 active unique threat actor groups was in the beginning of 2021 – almost 2 years ago. Nevertheless, the number of victims increased during Q4, specifically during December 2022. When zooming into the month of December, we identify that the two threat actor groups 'Play' and 'Royal' were added to our monitoring.



Extortion incidents & unique threat actor count recorded from 2020 to December 2022 (n=5,897)

Additionally, the group ViceSociety changed its onion address, which led to 19 victims being collected on the same day, and thus might not represent the actual date and time of the postings of these victims.

In comparison to the previous quarter, we see that LockBit3 has significantly less number of victims. While we counted 237 victims in Q3 2022; Q4 shows that LockBit3 contributed to 1/3 of all victims, with a victim count of 145.

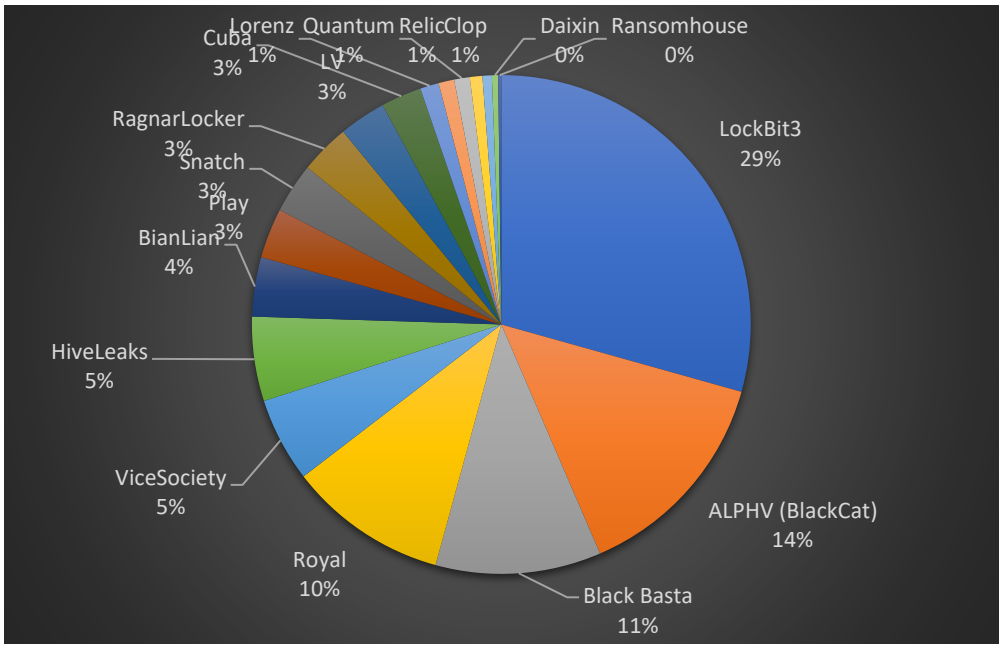
Threat actor activity – Interesting observations

In mid-December, multiple sources reported on the new ransomware variant 'Royal', which surfaced in November in our dataset but is said to be active already in early 2022. It is believed that some of the Conti members are running this ransomware operation. In November and December, we registered 51

businesses that have fallen victim to this group. Victims originated from countries such as U.S. (59%), Canada (8%), Brazil (6%), Germany (6%) and Austria (4%); showing 'the usual' mix of victim countries.

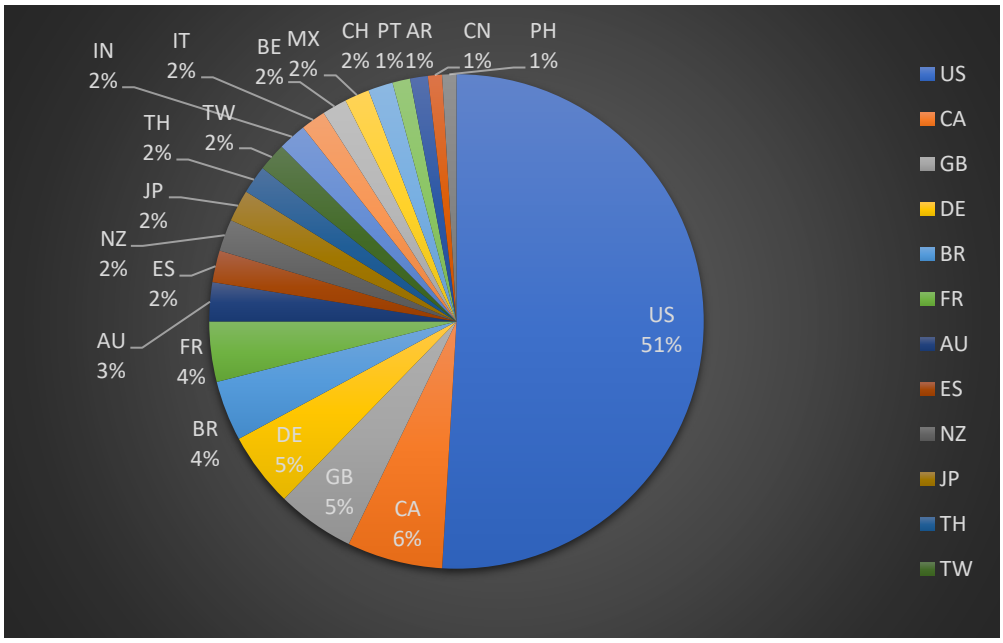
Victimology of Q4 2022

While the total of victims has slightly increased again during Q4, we observe a shift of threat actors contributing to this threat. This is not unusual given the opportunistic nature of this ecosystem, while some threat actor groups might cease operations, others are ready to 'take on their share' of victims. We are observing a reduction of businesses falling victim to the group LockBit3. At the time of writing there are no obvious reason to why this is (yet). Nevertheless, the number of victims has increased, groups such as ALPHV (BlackCat), Royal, ViceSociety, BianLian and Play have caused the higher number of victims in Q4.



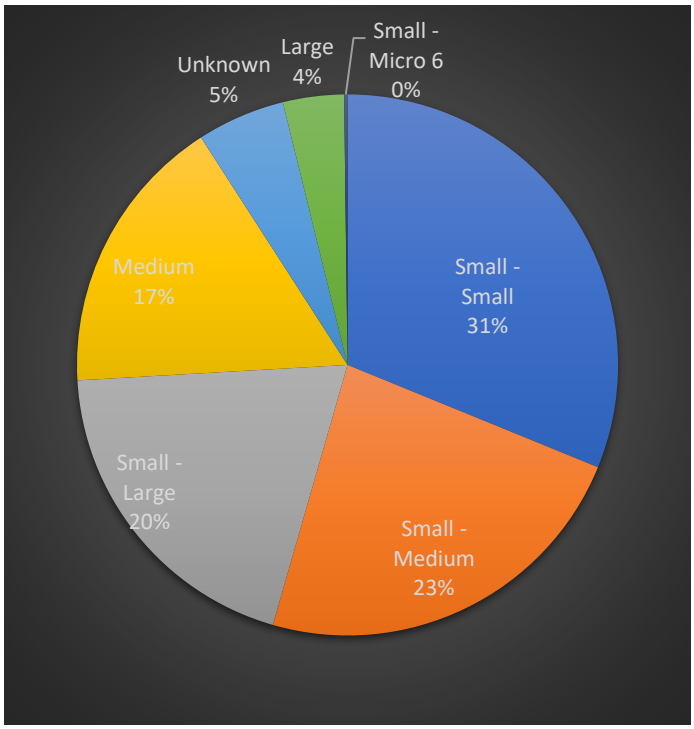
Top 20 contributors to cyber extortion leaks in Q4 2022

Looking at the top 20 countries impacted by this threat in Q4, more than half of all victims are headquartered in the U.S. Due to the fact that we zoom into the top 20 countries, the U.S. is taking a bigger share (51%) than if we would look at all victims from Q4 (U.S. = 45%). Nevertheless, U.S. based victims have increased. The second most present country during Q4 was Canada with victims from verticals such as Manufacturing (n=7), Information (n=4) and Wholesale Trade (n=3).



Top 20 Victim organization's country in Q4 2022

As can be seen in the chart above, English-speaking countries were the most impacted countries in Q4, closely followed by victims from Germany (n=21), Brazil (n=17) and France (n=17). French victims have decreased by almost half from Q3 to Q4. One reason can be that LockBit who caused over 80% of the French victims in Q3, has had less activity during Q4. While Brazil is proportionally the fifth position. In Q4, and especially during December 2022, we registered the highest amount of organizations from Brazil falling victim to cyber extortion.



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+

Size of businesses impacted by cyber extortion in Q4 2022

In Q4, we saw most victims originating from the business sizes small to medium, ranging from 1 to 999 employees. We see a slight increase in medium-sized businesses that range from 1,000 to 9,999

employee count. While we recorded 13% of all victims being medium sized in Q3, we see 17% in Q4. Businesses that we classify as ‘Large’ remained the same when comparing Q3 and Q4 (n=18).

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

The vulnerabilities that matter

In our annual Security Navigator report for 2023 (https://www.orangecyberdefense.com/global/security-navigator) we introduced a new section in which we examine data extracted from 10's of thousands of vulnerability scans and penetration tests to try and better understand the state of vulnerability management in the industry. The study yielded several (we think) fascinating insights, but as always there wasn't enough time or space to cover all the questions the data raised.

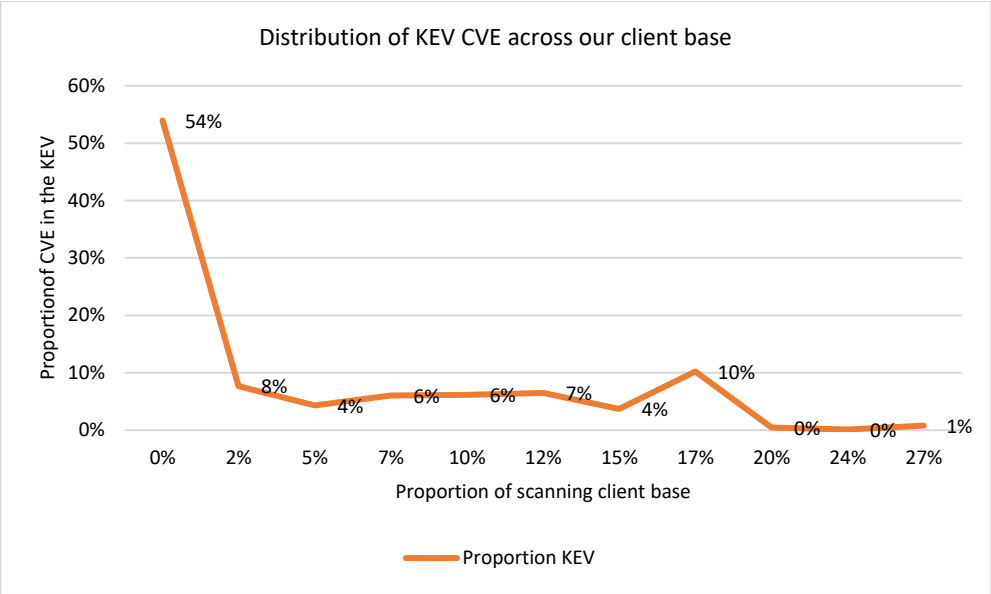
One area we never got to cover involves a set of vulnerability indexes that are designed to provide insight into which of the thousands of vulnerabilities disclosed each year are actually being exploited in the wild. This insight is obviously of huge value to security managers who can be easily overwhelmed by the sheer volumes and want to concentrate on the issues that matter.

One such index is published by the US government's 'CISA' agency and is called the Known Exploited Vulnerabilities (KEV) catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog). It is updated regularly from the agency's intelligence and currently contains over 860 unique vulnerabilities.

The notion of such 'Vulnerability Intelligence' promises to enrich vulnerability reports with this additional information to assist security teams in determining what vulnerabilities need to be patched, and how urgently.

We took our own vulnerability datasets extracted from Vulnerability Operations Center (VOC) scanning data reports to determine the extent the KEV Catalog features in what we observe and report on our client's estates.

The findings are really fascinating:



The chart above depicts what proportion of the KEV catalogue has been reported across our client base over the last two years. The Y-axis reflects a proportion of KEV, while the X-axis reflects the proportion of the clients we sampled.

We can search a sample of vulnerability scan reports for a significant subset of our clients to determine how frequently vulnerabilities in the KEV are reported on client assets. We note that this is a limited sample biased by the obvious fact that these clients have implemented robust, professional vulnerability management programs, and would thus not be fully representative of the entire cyberspace.

The resulting distribution is illustrated above. An examination of this data reveals the following:

- An astonishing 54% (464 CVEs) of the vulnerabilities listed in the KEV were not reported at any of the clients sampled. It's hard to understand why this would be, except that these vulnerabilities exist in technologies that are not very widely deployed and very specific to U.S. Government FCEB agencies.
- Not a single vulnerability in the KEV impacted more than 27% of the clients sampled.
- One percent (7 CVEs) of the KEV list was reported at 27% of clients – nearly a full third. 6 of these 7 CVEs are sequential (CVE-2017-0143 to CVE-2017-0148) and are related to SMBv1 within Windows operating systems, including 'EternalBlue' (CVE-2017-0144). The final CVE follows a similar pattern, in that it is another Windows vulnerability which received significant attention from the community – CVE-2019-0708 'BlueKeep'. These are vulnerabilities dating back to 2017 and 2019 respectively. Many of the affected hosts would eventually have been patched by our clients, of course, but **on average these 7 CVE persisted on hosts for 451 days**! In our 2023 'Security Navigator' report we note that the average age of a

vulnerability on our client estates is 'only' about 215 days. Considering the ubiquity and severity of these issues, this is a very concerning figure indeed.

- Interestingly, 10% (88 CVEs) were reported at 17% of clients, depicted by the bump in the graph featured above. These 88 vulnerabilities mostly impact common Windows components, which accounts for the large proportion of our clients that are impacted by them.
- A total of 303 vulnerabilities from the KEV each impacted less than 10% of our client base. This seems like an important observation, as it suggests that businesses can be severely impacted by an exploitable vulnerability in a technology that is not widely deployed, or an uncommon vulnerability that has not been patched.

All in all, these insights serve as a reminder that security managers need to take the severity and exploitability of a vulnerability into account, not just the frequency with which it occurs.

Ric

Out with the old, in with NIS2

In April 2016 the world was abuzz with talk about a new European Union (EU) regulation coming into force, the General Data Protection Regulation (GDPR), which focused on privacy, human rights, and protecting personal data. Naturally, GDPR emphasized information security, which piqued the interest of the information/cyber security industry. However, just 4 months after, in August 2016, the Directive on Security of Network and Information Systems (NIS) came into force to much less of a fanfare, despite seeking to achieve a high common level of cyber security for all EU Member States. NIS was to be transposed into national law by EU Member States by May 2018 and enforced by relevant competent authorities, ensuring that Operators of Essential Services (OES) and Digital Service Providers (DSPs) were appropriately guided and kept accountable for their NIS implementation and encompassing cyber security programs.

Almost 6 and a half years later, NIS2 has been adopted and came into force, on the 16th of January 2023 to be precise. NIS2 is the result of a consultation by the European Commission in 2020, which revealed there were several limitations in the original legislation. Most notable amongst the NIS limitations, organizations felt that there was a lack of clarity with regards to the expectations of NIS, particularly when transposed into national laws; organizations also felt that other regulations (such as GDPR) needed to be prioritized for implementation.

NIS2 must be transposed into national law by EU Member States by 17th of October 2024 and its scope has broadened both in what types of organizations it captures, as well as what those organizations must do to be compliant. So, let's have a look at some of the key changes to expect under NIS2.

The categories of OES and DSP were originally a point of ambiguity for both EU Member States and the organizations that may be relevant, due to passing the responsibility of such classification to the Member States themselves. The categories have now been changed such that there are two, more prescriptive lists of sectors falling under either 'Essential' or 'Important'; these include new sectors such as social media platforms, telecoms providers, medical or pharmaceutical manufacturing, postal services, and even space organizations. Fortunately for micro and small businesses, they may be exempt from the lists.

In NIS2, Essential organizations will have proactive supervision, meaning they can be audited both regularly and ad hoc, have evidence of compliance requested, and even be vulnerability scanned by the competent authority. Important organizations will only be subject to supervision if they appear to be non-compliant with NIS2. Competent authorities will also be given a minimum list of enforcement powers to wield for organizations who are found not to be appropriately compliant with NIS2. Those powers range from making the organization implement recommendations to publicly disclosing certain details of the infringement.

To complement the supervision and enforcement, NIS2 requires Member States to ensure the management bodies of Essential and Important organizations are sufficiently trained and knowledgeable to provide adequate oversight and approval of cyber security risk management processes. The management bodies must be held liable by the Member States' competent authorities for any infringements of such cyber security risk management processes.

Essential and Important organizations will be required to implement cyber security policies as part of NIS2, such as cyber security risk analysis policies, as well as policies and procedures to evaluate the effectiveness of cyber security risk management processes. Essential and Important organizations will also have to have in place adequate cyber security controls, where what is adequate is determined by an organizational risk assessment that takes into consideration the potential impact of a cyber security incident.

IT supply chain cyber security will be a point of focus of NIS2, requiring organizations to have appropriate cyber security policies and procedures for their IT procurement and supply chain. This means taking into consideration the cyber security posture of suppliers and including cyber security risk management controls into contracts, indirectly expanding the reach of NIS2.

Final of the headline NIS2 changes is reporting significant incidents to the competent authority or computer security incident response team (CSIRT), whereby 'significant' has now been defined as an incident which has the potential to cause severe disruption to services or financial losses to the organization or is capable of affecting people with its impact. Essential and Important organizations must submit an initial report of an incident within 24 hours of becoming aware of it. The initial report must be followed up with a more detailed report within 72

hours, and then a final, full report must also be submitted within 1 month of becoming aware of the incident. In return, the competent authority or CSIRT must respond within 24 hours of the initial report with feedback and be prepared to provide guidance if requested. For organizations who have not implemented the NIS2 guidance or do not notify the competent authority or CSIRT within the specified timeframes, the competent authority can oblige them to implement recommendations or impose financial penalties, up to the larger of €10 million or 2% of global turnover.

Overall, the changes and additions in NIS2 appear to be well thought out and the limitations discerned in the 2020 consultation have been addressed. It is possible that changing the sector category lists to Essential and Important will not clarify which organizations should be implementing a NIS2 program, and the IT supply chain controls and policies may blur the lines of what is required of managed service providers; however, it should be reasonably easy for organizations to consult with the relevant competent authority to find out their responsibilities.

It may be the case that some organizations captured by NIS2 will not relish additional cyber security legislation to comply with, particularly the newly added sectors who may have some catching up to do, but it does seem like those who implement it will have a good, holistic baseline cyber security program. Moreover, those organizations who purposefully implement a NIS2 program will probably reap additional operational benefits, particularly from areas such as policies and asset management.

Good News Cyber

Hive Ransomware Infrastructure was seized in a joint international law enforcement effort that consisted of authorities from Canada, France, Germany, Ireland, Lithuania, the Netherlands, Norway, Portugal, Romania, Spain, Sweden, the U.K., and the U.S. The seizure included the dedicated leak site and victim negotiation portal according to the article by The Hacker News.

A 21-year-old French citizen appeared in a Seattle (USA) court in late January 2023 on a nine-count indictment for conspiracy, computer intrusion, wire fraud and aggravated identity theft. The French citizen was arrested in 2022 in Morocco and was extradited to the U.S.

Europol released a statement in which they disclosed their success in taking down scam cryptocurrency call centers. Suspects from call centers in Bulgaria, Cyprus, Germany, and Serbia tricked victims into investing large amounts of money in fake cryptocurrency schemes, also known as 'Pig Butchering' cryptocurrency scams. Europol said that law enforcement arrested 15 suspects in Germany and Serbia after searching 22 locations in Bulgaria, Cyprus, and Serbia and questioning 261 individuals. Seizures also included 3 hardware wallets with about USD 1 million in cryptocurrencies on it and about EUR 50 000 in cash, 3 vehicles, electronic equipment and data back-ups, documents.