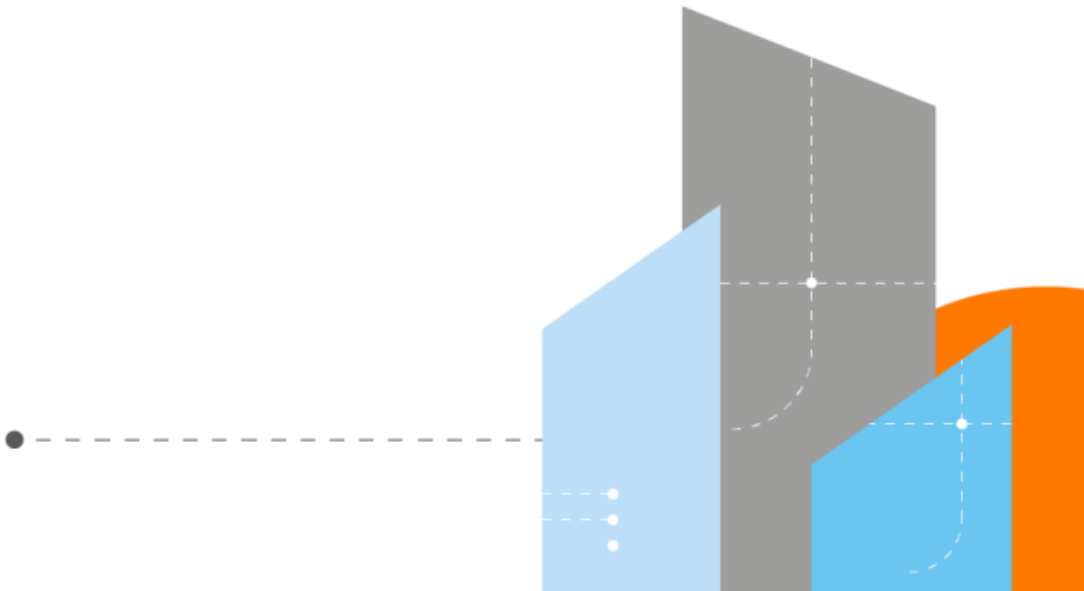
Orange
Cyberdefense

Security Intelligence

Monthly Report

January 2023



CONTENTS

CONTENTS 2

INTRODUCTION 3

World Watch Review January 2023 4

Editor's Notes 7

Mass exploitation of ESXi hosts 7

CSI: RTU 14

On the question of 'why' – an exploration of reasoning of cyber extortionists conducting ransomware attacks and data extortion. 15

Good News Cyber 17

INTRODUCTION

Reddit, the popular social news aggregation platform, has stated that they were the victim of a security breach that enabled unknown threat actors to gain unauthorized access to internal documents, code, and internal business systems. The cause of the breach was attributed to a "sophisticated and highly-targeted phishing attack"

Microsoft's Digital Threat Analysis Center (DTAC) has attributed a recent attack targeting the satirical French magazine Charlie Hebdo to an Iran-linked threat actor they call NEPTUNIUM (aka Emennet Pasargad, Holy Souls). The attack is alleged to be in retaliation for the launch of a cartoon contest to ridicule Iran's ruling cleric.

In early January, the threat actor claimed to have obtained the personal information of more than 200,000 Charlie Hebdo customers. A sample of the data was released as a proof of the hack which showed data including the full names, telephone numbers, and home and email addresses of accounts that had subscribed to, or purchased merchandise from, Charlie Hebdo.

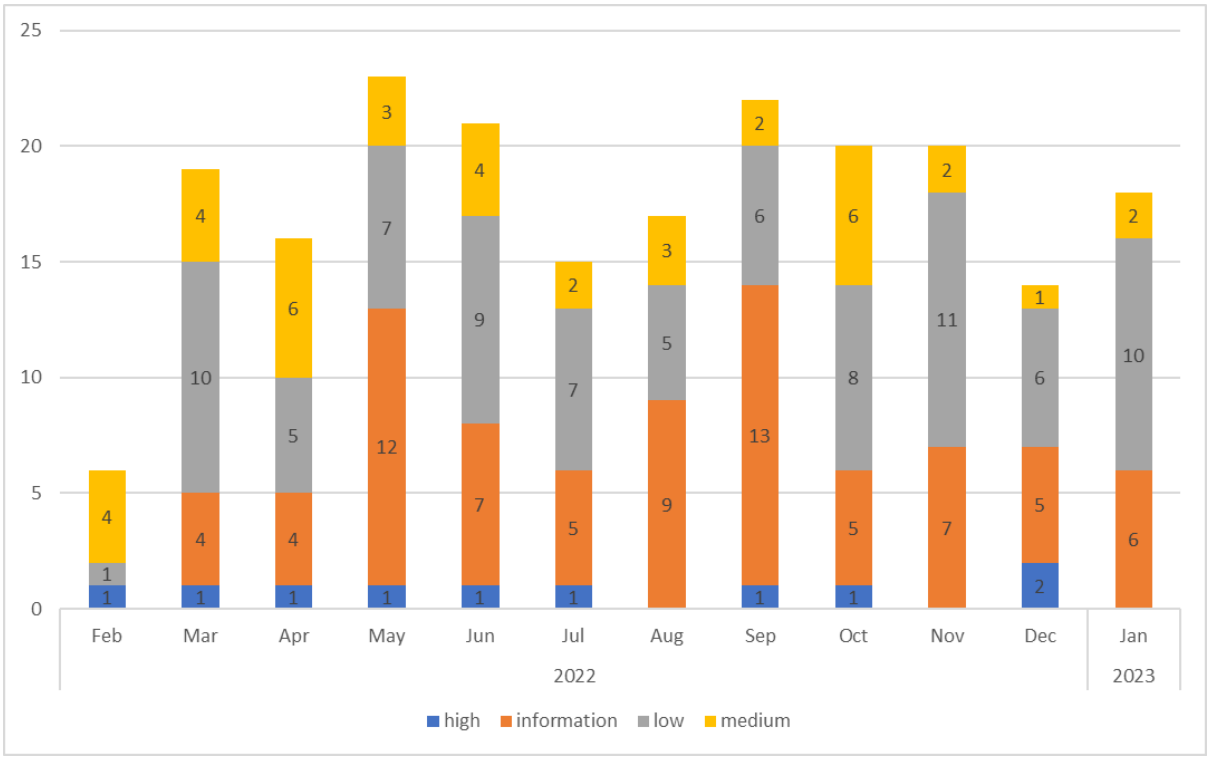
The LockBit Cy-X group has taken credit for the recent attack on the Royal Mail which led to disruption affecting both inbound and outbound international post. The group stated that it would release data stolen from the Royal Mail on February 9 if they didn't pay the ransom demand. However this deadline has come and gone without any data appearing to have materialised, other than a claim on the Lockbit leak site that the data has been published.

At a glance

VMware have warned customers to install the latest security updates and disable the OpenSLP service targeted in a large-scale campaign of ransomware attacks against vulnerable ESXi servers exposed to the Internet.

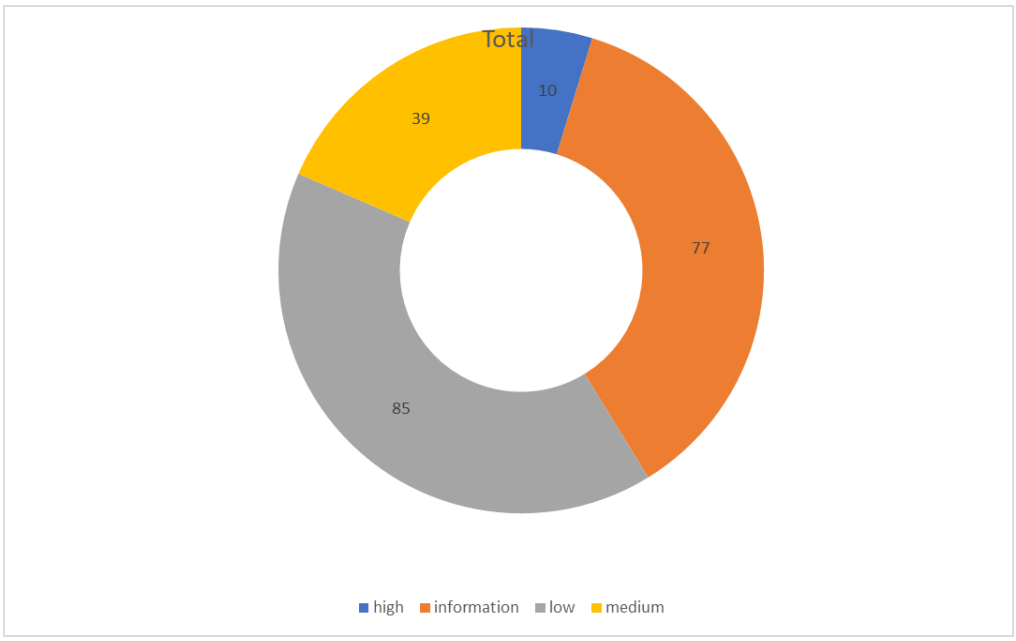
World Watch Review January 2023

The Orange Cyberdefense CERT published a total of 18 new World Watch advisories during January 2023, along with adding updates to a further 19 previously published advisories. This is an increase on the volume seen in December where the Christmas holiday period likely accounted for a slump in activity.



Breakdown of Published Advisories Previous 12 Months

The advisories, as tends to be the norm, primarily consisted of Information and Low severities, although there were 2 rated as Medium.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As can be seen above the advisories this month were all given criticality ratings of low, medium or information when initially published. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase our criticality level as required if circumstances should change. Some advisories of note this month are:

671301 - Critical ManageEngine vulnerability now exploited in the wild

- Horizon3 researchers have announced that they will soon release a PoC for one vulnerability tracked as CVE-2022-47966. This vulnerability located in most ManageEngine products, is a critical pre-authentication remote code execution bug. Using this flaw, an attacker can form specially crafted data to execute arbitrary code on the server.
- The vulnerability was fixed last year in ManageEngine products in various releases between July and October, but not clearly described in the release notes (and the CVE not initially mentioned). The issue was more clearly announced on November 7 in the vendor security advisory. According to the researchers, a few thousand instances of ManageEngine with the needed vulnerable SAML SSO component are currently exposed online.

669219 - SugarCRM fixed 0-day publicly disclosed on New Year's Eve

- A 0-day vulnerability has been recently discovered in the customer relationship management software SugarCRM. This critical vulnerability allows an unidentified remote attacker to execute code remotely. Unfortunately, the anonymous researcher behind it (dubbed "sw33t 0day") released an exploit for it publicly, so it is likely that threat actors will likely soon leverage this vulnerability to deploy backdoors on affected systems. Additionally, it is important to note that this security issue does not have a patch fixing it yet. Our experts from the Vulnerability Intelligence Watch team estimate that this irresponsibly-disclosed vulnerability has a high CVSS score of 9.8 out of 10.
- According to the search engine Censys.io, there are at least 1,300 exposed instances possibly vulnerable. But these specific servers might hopefully be segregated from the rest of the network in some cases.

670433 - Microsoft January Patch Tuesday fixes two serious vulnerabilities

- On January 10, Microsoft released as planned their Patch Tuesday updates, including security fixes for 98 vulnerabilities, with 11 classified as critical and 87 as important. Our Vulnerability Intelligence Watch team do list them in a monthly report you may find here. The main products affected are Microsoft Windows, Exchange and SharePoint. Among these vulnerabilities, 2 security issues need your particular attention.
- Identified as CVE-2023-21674 and located in Microsoft Advanced Local Procedure Call, the first bug allows a local attacker to elevate privileges. Despite being announced as currently being exploited in the wild (and reported to Microsoft by Avast), there is no public PoC for this vulnerability yet (which may means a use by sophisticated attackers for highly targeted purposes).

- The second one, tracked as CVE-2023-21549, is located in Microsoft SMB Witness Service. It also allows a local attacker to elevate privileges. However, although no malicious exploitation has yet taken place, Microsoft and Zero Day Initiative announce that a public PoC does exist, even though the researchers deny releasing publicly any information. The risk level for it is in any case lower as of now, as this flaw was reported through responsible channels.

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

Mass exploitation of ESXi hosts

On Friday February 3, 2023, news broke about an attack that targets VMware ESXi hosts.

VMware ESXi is a hypervisor that allows its users to run multiple virtual computers on a single piece of hardware. VMware offers the following definition of a hypervisor: "A hypervisor, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing."[1].

VMware ESXi has become popular among IT administrators as it offers similar functionality as the enterprise grade ESX vCenter with some features disabled. One contributing factor to why ESXi is so popular is that VMware offers it as a free download.

The apparent objective of the attackers is to encrypt the virtual machines hosted on the impacted ESXi hypervisor as part of a ransomware attack. Initial reports came from the French CERT[2] as well as commercial hosting and cloud service provider OVHcloud[3]. Later OVHcloud published an update to their initial blog post claiming that impacted ESXi hosts are bare metal hosts that are managed directly by clients and that managed ESXi hosts were unaffected. These reports indicated that attackers are targeting the exposed OpenSLP service, on port 427, remotely. The French CERT pointed to two potential vulnerabilities, CVE-2020-3992 and CVE-2021-21974, that are possibly exploited by attackers.

The attack was dubbed 'ESXiArgs'[4] based on the ESXi hosts being targeted and features of the malware that invoked several arguments on the impacted host, as well as appending the '.args' file extension to encrypted files. On Monday February 6, 2023, VMware added that they have not yet seen any evidence that this attack is related to an "unknown vulnerability" or a zero-day attack. Until proven otherwise, the more likely theory is that existing weaknesses are being targeted. By Monday February 6, more than 3200 potentially vulnerable hosts could be identified in search results returned from Censys and Shodan.

VMware have issued several security updates for the OpenSLP service in the past. VMware issued official updates in late 2020[5] and early 2021[6] for CVE-2020-3992 and CVE-2021-21974 respectively. VMware has also indicated that this service is disabled

[1] https://www.vmware.com/topics/glossary/content/hypervisor.html

[2] https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/

[3] https://blog.ovhcloud.com/ransomware-targeting-vmware-esxi/

[4] https://blogs.vmware.com/security/2023/02/83330.html

[5] https://www.vmware.com/security/advisories/VMSA-2020-0023.html

[6] https://www.vmware.com/security/advisories/VMSA-2021-0002.html

in the default ESXi configuration from ESXi version 7.0 U2c and ESXi version 8.0 GA[7] onwards. It is unclear if older versions had OpenSLP enabled by default and if this service then could be automatically exposed to the Internet based on normal network configuration found at hosting providers such as OVHcloud and others.

Proof-of-concept (PoC) exploits are also readily available for both vulnerabilities[8] [9] and have been available within months of the official vulnerability becoming public knowledge.

CISA's Known Exploited Vulnerabilities[10] (KEV) catalog lists CVE-2020-3992 with the entry dated November 3, 2021. Federal Civilian Executive Branch (FCEB) agencies were given until May 3, 2022, to patch vulnerable ESXi hosts. There is no entry for CVE-2021-21974 at the time of writing. There is, however, another critical OpenSLP vulnerability listed for ESXi, CVE-2019-5544[11], that was entered into the KEV catalog on the same day. No publicly available PoC code could be found that was tied directly to CVE-2019-5544, but since OpenSLP is open source, one could examine the code changes associated with the vulnerability and understand how it might be exploited.

A Rapid7 blog post[12] from November 11, 2020, referenced a Kevin Beaumont tweet that alerted the security community about active exploitation of ESXi vulnerabilities CVE-2019-5544 and CVE-2020-3992. The blog post also quoted Kevin Beaumont's almost prophetic words "[r]ansomware groups …bypass[ing] all Windows OS security, …shutting down VMs and encrypting the VMDK's directly on hypervisor."[13]. It also seems that the original fix for CVE-2020-3992 released in October 2020 was incomplete. But the November 2020 patch seems to have fully addressed the original vulnerability[14].

If CVE-2020-3992, CVE-2021-21974, and possibly CVE-2019-5544 were being exploited, then it seems that it is the first time anyone has exploited these at such a public scale. These attacks affected the availability of virtual machines on the impacted hosts, thus the attackers announced themselves very loudly. These attacks may have gone under the radar if the attackers were stealthier, for example if the attackers only exfiltrated data and did not halt and encrypt virtual machines.

In a World Watch Advisory[15], the Orange Cyberdefense CERT also highlighted another potential VMware ESXi vulnerability, CVE-2022-31696[16], that was fixed along with CVE-2022-31697, CVE-2022-31698, CVE-2022-31699 in December 2022. The former, CVE-2022-31696, could possibly allow an attacker with local access to escape the sandbox feature designed to partition virtual hosts off from the underlying hypervisor. Escaping the sandbox could potentially allow the local attacker to perform privileged actions. It is unclear if the security fix released by VMware in December

[7] https://blogs.vmware.com/security/2023/02/83330.html

[8] https://github.com/dgh05t/VMware_ESXI_OpenSLP_PoCs

[9] https://straightblast.medium.com/my-poc-walkthrough-for-cve-2021-21974-a266bcad14b9

[10] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[11] https://www.vmware.com/security/advisories/VMSA-2019-0022.html

[12] https://www.rapid7.com/blog/post/2020/11/11/vmware-esxi-openslp-remote-code-execution-vulnerability-cve-2020-3992-and-cve-2019-5544-what-you-need-to-know/

[13] Kevin Beaumont's tweets shared in the Rapid7 blog post are no longer valid.

[14] https://www.vmware.com/security/advisories/VMSA-2020-0023.html

[15] https://portal.cert.orangecyberdefense.com/worldwatch/678367

[16] https://www.vmware.com/security/advisories/VMSA-2022-0030.html

2022 was being targeted. None of these vulnerabilities are listed in CISA's KEV catalog at the time of writing. The OCD CERT noted that to exploit this vulnerability an attacker must already have local access to ESXi. This would require a multi-step exploit chain if the attack would have been launched remotely over the Internet. This makes mass exploitation in this noisy manner rather unlikely, as these types of chained exploits are not the hallmark of typical brutish ransomware crews.

The Orange Cyberdefense Vulnerability Operations Center discovered 42 ESXi hosts that were vulnerable to CVE-2021-21974. These hosts were discovered between February 2021 and October 2022. This first 6 vulnerable hosts were discovered on February 28, 2021, this is four days after the NVD published date of February 24, 2021. The remaining 36 vulnerable hosts were discovered between November 2021 and October 2022. This means that some hosts were unpatched anywhere between 270 days and 590 days. This is assuming the hosts were patched immediately after discovery. This specific vulnerability impacted 7% of our VOC client base.

The Orange Cyberdefense Ethical Hacking Team performed 122 assessments classified as either Internal, External, or Red Team from February 24, 2021, up to and including September 2022. This is the period that vulnerability CVE-2021-21974 was public knowledge and could have been encountered. A detailed blog post about the vulnerability appeared on May 25, 2021, meaning that if a vulnerable ESXi host was encountered and was in scope there existed the possibility that it might have been exploited using the exploit code published on GitHub[17] [18]. At this point, with a full explanation and exploit code, 105 assessments could possibly have yielded a potential finding. Fortunately, none of the clients we assessed had findings with reference to this vulnerability.

As stated earlier, the reported attacks have a noticeable impact on the target system. The attacks resulted in files on the ESXi hypervisor being encrypted after the attacker halted any running virtual hosts. Also, instructions to pay 2 Bitcoins into the designated wallet to obtain the decryption keys were found in files on several exploited ESXi hosts during the first wave of attacks. What was odd was that no ransomware group was named in the instruction file.

One victim shared such a ransom note[19] on Bleeping Computer's forum. The odd thing is that this note ends with what looks like a possible hint: "SSH is turned on" and "Firewall is disabled". VMware ESXi has an SSH service that can be enabled. Perhaps the attacker brute forced these hosts with known or weak credentials or exploited a weakness in OpenSSH? The reference to the disabled firewall could suggest that the attacker felt that, had a firewall been in place with appropriate configuration, then their attack might have been thwarted. Disabling or limiting remote access to any host exposed to the Internet is crucial as this greatly limits what attackers can do.

Another user of the Bleeping Computer forum posted on the same thread on February 8, 2023, stating that an ESXi host was compromised even though the "SLP service was turned off"[20]. If this is the case, then the OpenSLP vulnerability theory seems unlikely to be the only attack vector.

[17] https://straightblast.medium.com/my-poc-walkthrough-for-cve-2021-21974-a266bcad14b9

[18] https://github.com/dgh05t/VMware_ESXI_OpenSLP_PoCs

[19] https://www.bleepingcomputer.com/forums/t/782193/esxi-ransomware-help-and-support-topic-esxiargs-args-extension/

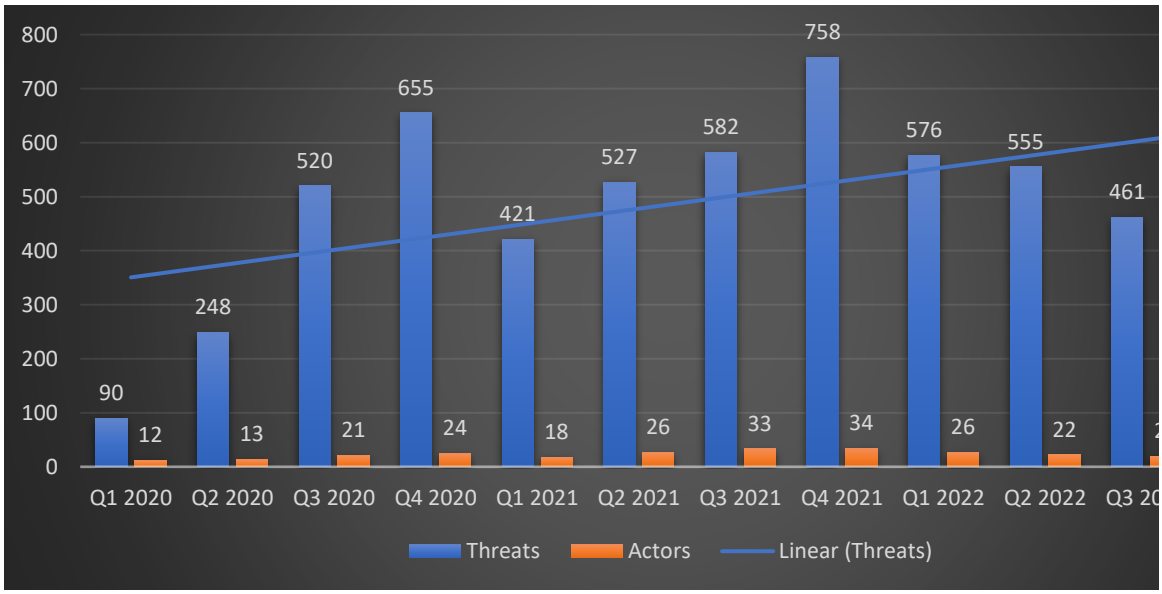
[20] https://www.bleepingcomputer.com/forums/t/782193/esxi-ransomware-help-and-support-topic-esxiargs-args-extension/page-31#entry5473353

There are hints at further extortion in the ransomware note shared on Bleeping Computer's forum post. In the days after the first wave of attacks, the modus operandi of the attackers changed[21]. They updated their ransom note by removing their Bitcoin wallet address and instead listing a TOR Onion (darkweb) Site.

Both versions of the ransom note threaten to share the stolen data if no ransom is paid. The first version lacked a typical negotiation site. The newer version of the ransom note with the TOR web address might indicate that the attackers are still developing their infrastructure to align with what has become the norm with typical Cyber Extortion negotiations.

There has been mention in some reports of a new ransomware group called 'Nevada', but no concrete evidence linking the mass exploitation of ESXi and the group has been presented yet. We do know, however, that Cyber Extortion groups evolve over time. Some fade out, while others morph into new groups.

In Q4 of 2022, we actually saw a relatively low number of threat actor groups extorting victim organizations around the world - a total of 19 threat actor groups victimizing 494 organizations. The last time we counted 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. During December, two new threat actor groups 'Play' and 'Royal' were added to our monitoring process, contributing to the sudden increase.



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

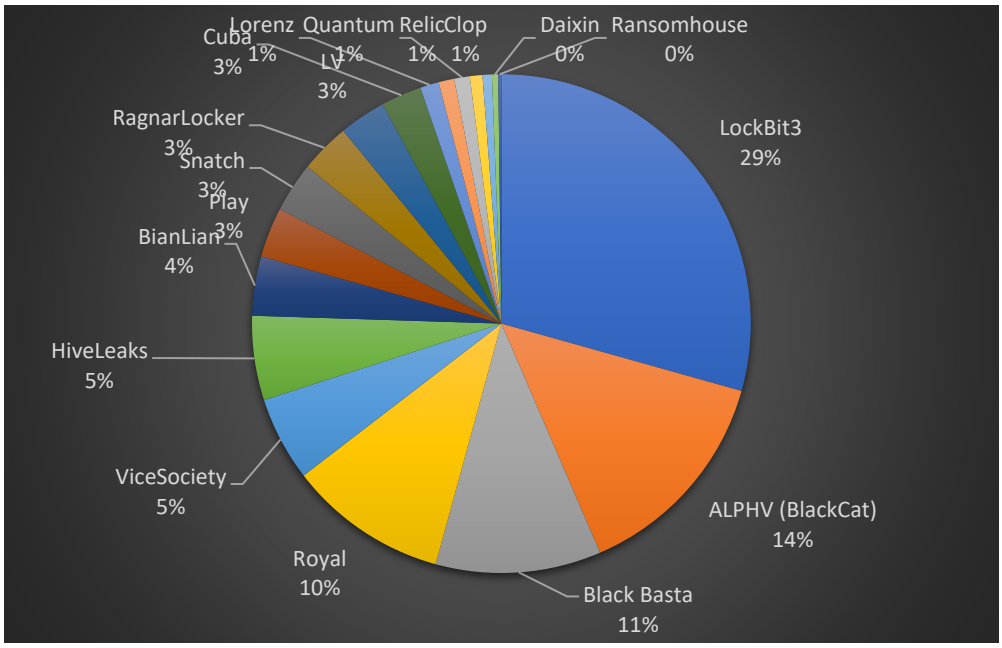
The group 'ViceSociety' also changed its TOR onion address during this period, which led to 19 victims being noted on the same day, so the data might not represent the actual date and time of the postings of these victims.

In mid-December, multiple sources reported on another new ransomware variant called 'Royal', which surfaced in November in our dataset but is said to have been

[21] https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

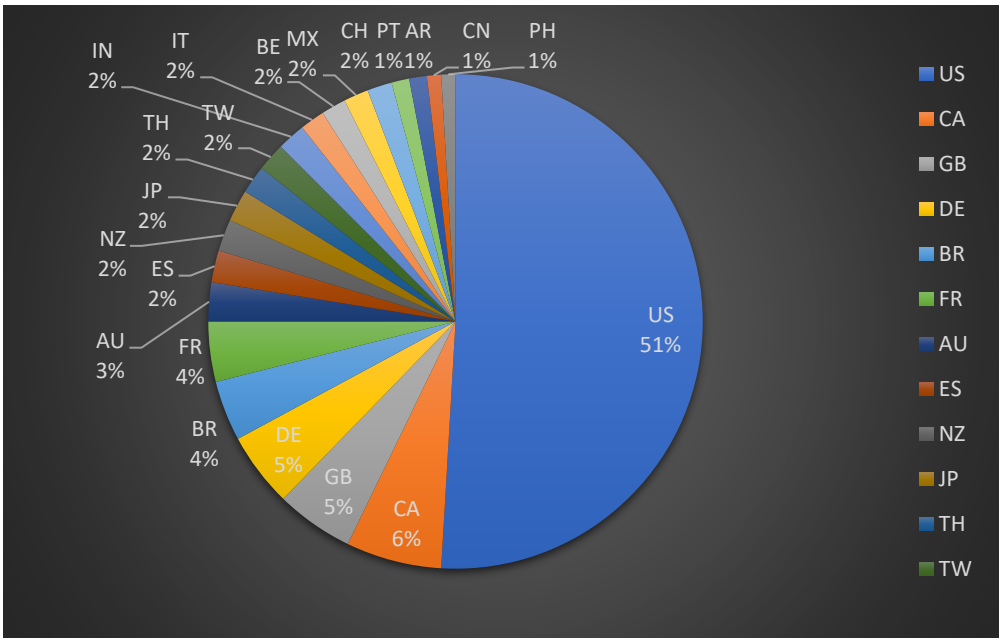
active already in early 2022. It is believed that some of the ex-Conti members are running this Cy-X operation. In November and December, we registered 51 businesses that have fallen victim to this group. Victims originated from countries such as U.S. (59%), Canada (8%), Brazil (6%), Germany (6%) and Austria (4%), showing 'the usual' mix of victim countries.

While the total number of victims increased again slightly 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.



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. In Q4 we saw that U.S. based victims rose to 51% of the total number of victims compared from 40% in Q3 2022. The second most impacted 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 in the fifth position. In Q4, and especially during December 2022, we registered the highest number of organizations from Brazil falling victim to Cyber Extortion.

Returning to the ESXiArgs malware. On a technical level it seemed at first that the encryption technique used by the attackers is cryptographically sound, but the extent to which the attackers encrypted the files could potentially result in data being recovered. A guide[22] was published by Turkish researchers to help with the possible recovery of virtual hosts. The guide does assume a high level of skill and experience with VMware and is not something a novice might be able to have success with. CISA have published resources to help with the recovery of data and should be easier to execute than the guide[23] [24].

However, it seems that the attackers realized that victims could recover their data and released a new version of the ransomware that encrypts up to 50% of the data if the VMware data file is larger than 128MB[25] . The reason for the 50% encryption is that the data files representing the virtual disk of the virtual computers can be gigabytes if not terabytes in size. Encrypting this can take very long. So, encrypting the disks selectively still renders the virtual discs unusable, but also leaves some of the data

[22] https://enes.dev/

[23] https://www.cisa.gov/uscert/ncas/alerts/aa23-039a

[24] https://www.hackread.com/cisa-esxiargs-ransomware-recovery-tool/

[25] https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

intact. It's a matter of luck whether the unencrypted data is usable. The updated version may render recovery per the guide and CISA tool less likely to be successful.

In conclusion. VMware and others have strongly urged users to install the latest security fixes for their supported ESXi hosts. If this is not possible, then at least disable the OpenSLP service and limit access to ESXi hosts and required services. Some versions of ESXi are no longer supported by VMware and thus no security fixes are available for known exploited vulnerabilities. Make backups of data as this can make restoring systems much easier. Ensure that backups are performed regularly and that backups are complete.

For more information on ransomware and how to approach this looming threat visit the Orange Cyberdefense website and read our whitepaper we published on the topic[26].

[26] https://www.orangecyberdefense.com/global/white-papers/beating-ransomware

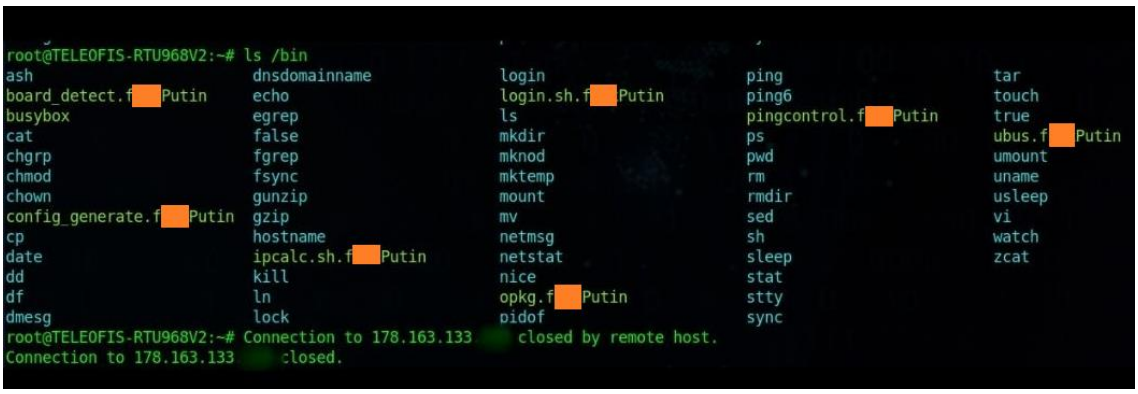
Ric

CSI: RTU

The arms race between defenders and adversaries in the cybersecurity domain has been accelerating for decades, and it has never been more ferocious. Moreover, since Stuxnet firmly cemented operational technology (OT) on the map of would-be adversaries in 2010, momentum has been gaining for it to become a viable target for less well-resourced and less capable adversaries. In response to this, OT-specific cybersecurity efforts have increased, thanks to a growing number of OT cybersecurity dedicated organizations and specialists.

2022 saw a few hacktivist groups displaying a dogged interest in OT, and perhaps even a growing capability – or so it initially seemed. Predatory Sparrow claimed that the physically devastating incidents at a number of Iranian steel mills was due to their attacks, the Cy-X gang Cl0p infiltrated South Staffordshire Water (although stopped at causing a physical impact), and we saw a number of nuisance attacks (basic, using existing functionality, and generally low impact) from the hacktivist groups OneFist and GhostSec. However, possibly most interesting of all was not actually an attack, but a display of capability by GhostSec.

Mid-January 2023, GhostSec made an announcement on Telegram that they had been “raising the bar” since they began attacking industrial control systems (ICS), and that they had made history with the first encryption attack on a remote terminal unit (RTU). GhostSec’s braggadocio was accompanied by screenshots showing a terminal of a TELEOFIS RTU968 v2, complete with encrypted files containing the suffix “.f***Putin”.



Unfortunately for GhostSec, such bold claims attracted the attention of security researchers and practitioners from OT cyber security organizations including Claroty and SynSaber. The analysis by the researchers revealed that the device in question was more like a router, running OpenWRT Linux, with some limited OT protocol and interface support, rather than a dedicated RTU. Researchers from the aforementioned organizations likened the technique to just hacking and encrypting Linux devices, which is not new. When viewed in this light, GhostSec's announcement appears to be considerably less novel than they originally purported. However, the fact that we are witnessing numerous attempts by adversaries to break into the OT space, including specifically targeting OT assets, is something to pay very close attention to – incidentally this is something which I address in a forthcoming blog post so watch out for that if you find this topic to be of interest.

On the opposite side of the arms race, defenders have been making OT-specific strides, too. Of note is a forensics tool created by researchers at Microsoft's Section 52 (https://github.com/microsoft/ics-forensics-tools). What is particularly interesting about this tool is that it is for programmable logic controllers (PLCs), which are the devices that sense and change the physical environment in OT. This is helpful because, while PLC configuration is mature when it comes to responding to engineering issues, it typically is not as mature when investigating issues that have been deliberately introduced by adversaries.

The PLC forensics tool first does a "full upload" of each function block on the PLC, which confusingly means it downloads each chunk of code on the PLC, complete with metadata such as when that code was uploaded and by what user. This stage can already provide the user with valuable data and potential forensic artefacts. After the "full upload", the tool can cross reference the downloaded code and metadata with the PLCs config file on the appropriate engineering workstation.

While we may not be currently seeing attacks directly targeting OT assets (save for the odd 'RTU' running OpenWRT), the fact that hacktivist groups are beginning to show an interest and trying to flex their capability is concerning. Without trying to sound like too much of a doomsayer, we might be needing tools such as Section 52's PLC forensics tool in the not too distant future.

Diana

On the question of 'why' – an exploration of reasoning of cyber extortionists conducting ransomware attacks and data extortion.

Why is it that threat actors continue victimizing organizations around the world with such a volume? Why do they almost seem to passionately do that and publicly advertise the results of their engagement in crime as if it was nothing to be ashamed of?

In 2022, we conducted research analyzing over 200 textual 'snippets'. The qualitative data varied between negotiations we observed between cyber extortionists and their victims, expressions shared on leak sites by the threat actors, ransom notes, content from threat actors' blogs on the darkweb such as 'About us' pages & announcements, forum posts and interviews some of the threat actors gave during our collection period.

We then applied a crime theory called 'Neutralization technique'. The theory looks at different forms of justifications threat actors install in order to make their criminal activities 'acceptable' and consequently let them engage in crime. By studying the phenomenon of cyber extortion, using our qualitative material, we looked for whether or not we would find specific neutralization techniques being actively applied. Sub-techniques we considered, were:

1.) **Denial of responsibility** – circumstances are to be blamed.

2.) **Denial of injury** – no one got hurt.

3.) **Denial of the victim** – through cyber space, victims are distant from the threat actors, making the criminal activities appear victimless.

4.) **Appealing to higher loyalties** – showing loyalty to sub-groups, e.g. hacker communities and 'their fight for better security practices'.

5.) **Condemning to condemners** – shift the focus of attention to the ones that disapprove, e.g. law enforcement agencies, 'corrupt' management, greedy negotiators etc.

We have published a blog series on our findings, you can start with the first initial introduction here, and jump to each blog from there.

Good News Cyber

In October 2020 we reported that cybercriminals were extorting Vastaamo, a Finnish psychotherapy center. At that time the data associated with 300 patients were already in the public domain and the criminals threatened to release the data of other patients unless a ransom is paid. Vastaamo refused to pay and the criminals uploaded all the patient information to the darkweb. A 25-year-old Finnish man was arrested in France for his role in the cyber-extortion. According to the latest reports the man error by including incriminating evidence in the files he uploaded to the darkweb, thus attracting the attention of Finnish law enforcement. The arrest in France also stemmed from a failure on the accused as he attracted attention to himself due to a domestic disturbance. Police arrested him when his backstory did not checkout and they matched his real identity.

European law enforcement agencies managed to shut down another encrypted chat app called Exclu that is used by criminals to exchange information. In 2021 we reported the success of the law enforcement agencies in shutting down the infamous SkyECC "secure" app that was also used by criminals groups. The latest shut down resulted in 42 arrests.

The United States (US) and United Kingdom (UK) issued joint sanctions on 7 persons the US and UK claim are members of Russian-base "Trickbot" cybercriminal group. The seven persons are named and each are specifically accused of their part in either developing the malware or contributing to the expansion of the cyber criminal activities. It is doubtful that these sanctions will have any direct impact on the current activities of the Trickbot malware, but it does send a clear message that the US and UK governments know the identities of those behind the criminal activities.