Threat Highlight Report

December 2023

WITH secure

Contents

Foreword

WithSecure's monthly threat highlights report contains our own proprietary data, as well as other carefully curated sources from the wider cybersecurity industry. It is designed to serve as a single-source product, delivering an overview of this month's cybersecurity news, the changing threat landscape, and relevant advice.

December is always a strange month for the THR due to the end of year break for people across the Infosec industry and beyond, but at the same time there have been several interesting events in various different areas.

Events surrounding Israel and Palestine continue, with associated hacktivist proxies active in the cyber arena for both sides. Ransomware attacks do, of course, continue as normal albeit in lower numbers than previous months. There have also been signs that Qakbot may be attempting to return after being taken down by Law Enforcement Agencies. We explore several incidents where threat actors are targeting identity to compromise organisations.

A number of interesting vulnerabilities have been in the news this month, both old and new, and we are exploring the data on these vulnerabilities in a slightly different way this month.

Stephen Robinson
Senior Threat Intelligence Analyst

1. Monthly highlights

1.1 Patched zero-click Outlook/Exchange exploit actively exploited by Russian APT

In March 2023, Microsoft stated that CVE-2023-23397 was being actively exploited by the Russian state sponsored actor known variously as APT28, Forest Blizzard, or Fancy Bear, identified by the US and UK as Unit 26165 of the Russian GRU.

In December 2023, they stated that this activity was still ongoing, and that they had worked with Polish Cyber Command to identify and mitigate the techniques used by the attacker.

CVE-2023-23397 is a vulnerability that allows an attacker to specify a location for a custom email notification sound, and by specifying an external location the attacker controls, they can then harvest the victim's NTLM hash when their Outlook client connects to the attacker's server to download the file. As long as this functionality is enabled at the Exchange server, this connection from the Outlook client will happen automatically, with no interaction required from the user, hence it is a zero-click vulnerability.

While originally patched in March, twice more bypasses to the original patch were identified, requiring further patches in May and October.

As if zero-click credential harvesting was not enough, in December researchers announced they had found that by chaining CVE-2023-23397 and CVE-2023-36710 it was possible to achieve zero-click remote code execution. This can be done by specifying a custom email notification sound and using a specially crafted WAV file of greater than 1GB in size to trigger a buffer overflow, resulting in code execution.

WithSecure™ Insight

This is a complex situation, but it shows that:

- A vulnerability that was first patched 9 months ago is still being successfully exploited by attackers.
- Not only that, but it took 3 patches over 7 months to (we hope) fully address the issue.
- And it is still being explored and further weaponized to increase its impact.

In WithSecure telemetry there has been a significant increase in detections of attempts to exploit CVE-2023-23397, with a 400% increase in detections in December compared to November.

What can you do?

Zero-click attacks can allow an attacker to compromise a user's device without the need for any user interaction, allowing for mass exploitation of user devices. Because no user interaction is required, user education and policies are totally bypassed. The only methods which can address a zero-click phishing attack are technical controls for phishing/spam detection, which will ideally prevent most attack emails from reaching a recipient, and, of course, the prompt application of security patches and mitigations. In this case, patching of the outlook client can remove the local vulnerability, while changing the configuration of the Exchange server to no longer allow custom email notification sounds can also prevent exploitation.

1.2 Mobile zero-click for Google, maybe zero-day for Apple?

Zero-click vulnerabilities are of great concern to any technical security function, and so are zero-day vulnerabilities. This month Google patched CVE-2023-40088, a vulnerability in a function in the Android operating system that is used for Bluetooth communication. This vulnerability could be abused to perform zero-click remote code execution by sending specially crafted Bluetooth messages. Because it is exploited via Bluetooth messages, the range is limited to that of Bluetooth connectivity, but a zero-click RCE that doesn't require physical access is still highly concerning.

At the same time, over on the Apple side of the playing field, an interesting piece of information came out through a lawsuit filed in a Russian court by one digital forensics company against another. The complainant, Elcomsoft, alleges that MKO-Systems stole code from them which can be used to extract passwords, photos, location and browsing history, and other sensitive data from an unlocked iPhone running iOS 16. The lawsuit claims an American company named Oxygen Forensics is using the same stolen code. Open-source reporting has found that Oxygen Forensics was founded by some of the same Russian businessmen who founded MKO-systems, and MKO-Systems was known as Oxygen Software until mid-2022. Both companies have also been linked to a Cyprus based entity named Oxygen Forensics Limited, which is of interest as recent reporting has indicated that many businesses that specialize in hacking mobile devices for government customers are based in Cyprus, as there is very little legal oversight of such technologies and services there.

Between them the reported customers of Elcomsoft, MKO-Systems, and Oxygen forensics include in the US:

- The FBI,
- Immigration Customs Enforcement,
- US Customs Border Control.

In Russia:

- The FSB,
- The Ministry of Internal Affairs

Apple has made no comment on these reports, but it does certainly appear as if there may be methods which are not publicly documented which allow access to what should be protected information on an unlocked iPhone.

WithSecure™ Insight

Mobile devices are so heavily embedded in our day to day lives, both professionally and personally, that they are an ideal target for a diverse range of attackers, all of whom may have wildly different goals which can be more easily achieved by accessing your mobile device. Unfortunately, mobile device patching is often not up to even the lack luster standards displayed in some Enterprise environments. The Android ecosystem especially is known to suffer from version fragmentation due to the diverse patching schedules and support lifetimes provided by device manufacturers.

What can you do?

Zero-days are as ever the bane of any security patching process, however they can be addressed and at least minimized through a defense in depth security model which applies a layered, belt and braces approach to security and monitoring.

1.3 Apache Struts into view again

This month CVE-2023-50164 was announced, a 9.8 CVSS vulnerability caused by case confusion in the file upload functionality in Apache Struts. This may have unpleasantly reminded some security professionals of CVE-2017-9805, which was used in the 2017 Equifax Breach where the PII of roughly 150 million people was stolen.

WithSecure™ Insight

Fortunately, analysis of the vulnerability has found that it is not well suited to mass exploitation, as it requires a number of specific conditions to be true, as well as requiring the attacker to be able to access a file upload endpoint in the application.

What can you do?

Because Struts is used as a part of so many other pieces of server software, this is definitely something to be aware of patch as a priority, but it appears unlikely that it will evolve into an Internet wide security phenomenon, like some of the other CVEs we have reported on this year.

1.4 Log4Shell Remains at Large

Speaking of the ghosts of Christmas past, Log4shell has once again been in the news as Andariel, part of the North Korean APT collective Lazarus Group, are reported to have been successfully exploiting a number of vulnerabilities for which patches exist, including Log4Shell. This campaign has been named Operation Blacksmith by Cisco Talos researchers.

WithSecure™ Insight

We might assume that because Log4Shell is over two years old and a patch has been available for most of that time, it is no longer widely exploitable, but apparently this is not the case. As well as the report on Lazarus Group activity, analysis of Internet exposed applications running Log4Shell by researchers at Veracode has found that 38% of them are still running vulnerable/unpatched software versions.

What can you do?

It's a simple message which is repeated often, but defenders need to identify and patch vulnerable software. To state that people do not patch their software, and they just need to start doing it is sometimes an overly simplistic view. The issue with Log4J is not that it is difficult to patch, but that it can be difficult to identify where Log4J is being included in/used by another application within a specific environment. This then is a situation where attack surface management can really come into play and help to direct the resources of the system administrators.

1.5 OAuth misuse

OAuth is an authorization framework that allows different applications to securely interact with each other without necessarily revealing an identity. Such a technology is important to enable access resources hosted by other applications across a network and has been cited as a key technology in securing APIs in a zero-trust model. Microsoft Threat Intelligence have detailed observations whereby threat actors have launched password spraying or phishing attacks to compromise accounts that “did not have strong authentication mechanisms and had permissions to create or modify OAuth applications”, and used those rights to create virtual machines. From these virtual machines a mix of activity was observed, including cryptomining, BEC attempts and other spamming activity from the impacted organizations legitimate domain name. Actors, among other things, were able to utilize OAuth as a persistence mechanism. The full, comprehensive, write up is available here.

WithSecure™ Insight

As organizations continue to deploy and use applications with a ‘thin’ computing architecture, the new network perimeter becomes a user’s identity. Exposure management is not simply limited to what services are routable to via the open internet but also limited to identities, accounts and (privileged) inter-application permissions. Complexity is often hidden from a user, so it is vital that understanding of cloud resources and their configuration is maintained, and security and access-control policies are continually evaluated.

What can you do?

As mentioned earlier, ensure security controls are audited and turned on where possible. Ensure policies are as secure as possible (e.g. a policy of least privilege) and security testing is undertaken. Because applications are hosted off-prem, one should not assume that security is also included. Cloud Detection and Response products/services can be deployed to protect these resources, just as xDR can be deployed on physical endpoints in a network.

1.6 SSH or just SH?

A vulnerability in the SSH protocol named Terrapin (CVE-2023-48795) was announced this month, along with two other vulnerabilities, CVE-2023-46445 and CVE-2023-46446, which are both vulnerabilities in the widely used Python SSH library, AsyncSSH's implementation of the SSH protocol.

Terrapin is a vulnerability in the handshake part of the SSH protocol and can be abused by a man in the middle attacker to downgrade certain security options as long as either the ChaCha20-Poly1305 cipher, or any CBC-EtM encryption mode is being used.

WithSecure™ Insight

SSH is incredibly widely used as a secure remote access protocol, so this could be extremely bad and may be causing network administrators to panic. However, the researchers themselves admit in their FAQ that it may not be that serious:

To exploit this vulnerability, an attacker needs to be positioned as a MiTM, and successful exploitation cannot make the connection insecure, it can simply make it less secure. The AsyncSSH vulnerabilities are implementation issues which, in combination with Terrapin, could allow an attacker to cause a victim to log into a different account on the destination server than they intended to, which could allow for credential harvesting and other shenanigans.

What can you do?

The main problem that Terrapin presents to defenders is that it appears to be a not particularly severe vulnerability that is difficult to exploit, however because SSH is so widely used, and there are so many implementations, the exact impact of the vulnerability is hard to assess. As ever, best practice is to promptly apply security patches and mitigations, as it is most definitely better to be safe than hacked.

2. Hacktivist Landscape

Iranian proxy Hacktivist groups target US due to Israel-Palestine conflict

Multiple reports have detailed the rise in hacktivist attacks which claim to be on behalf of one side or the other of the current major conflict in the middle east. Hacktivist groups sponsored by Iran, and effectively acting as Iran's political proxies, have claimed that they are targeting US entities which are using Israeli technology as a form of retaliation for the conflict. Reporting by Checkpoint finds that while there have been a number of attacks with real world impact attributed to these groups (as covered in last month's THR) they are also making exaggerated claims of their successes, claiming old attacks and leaks, as well as making falsified claims of successful attacks.

Killnet leader retires after being publicly identified

The leader of the Russian hacktivist group KillNet, known by the handle KillMilk, has announced their retirement, and handed the group over to another actor with the handle Deanon Club. This retirement comes only a few weeks after Russian journalists published what they alleged to be the true identity of KillMilk, naming him as Nikolai Serafimov, a 30-year-old Russian. It is not known what KillMilk or KillNet will do from now on, but it will most likely be more of the same DDOS and defacement activity.

70% of Iranian petrol pumps remotely disabled

It is not only Iranian backed hacktivists who are engaging in cyber attacks motivated by the current middle eastern conflict. A group named Predatory Sparrow which is believed to be Israeli state sponsored claimed to have taken down the majority of petrol pumps in Iran, and stated that while they could have taken down even more, they intentionally chose not to, so as not to interfere with emergency services. The group has previously successfully disrupted an Iranian steel plant and Iranian railways, and the simple fact of their obvious competence and professionalism makes them stand out from the crowd when compared to other hacktivist groups. As such, it seems likely that this group is actively operated, or at least heavily sponsored by the Israeli state.

3. Ransomware: Trends and Notable Reports

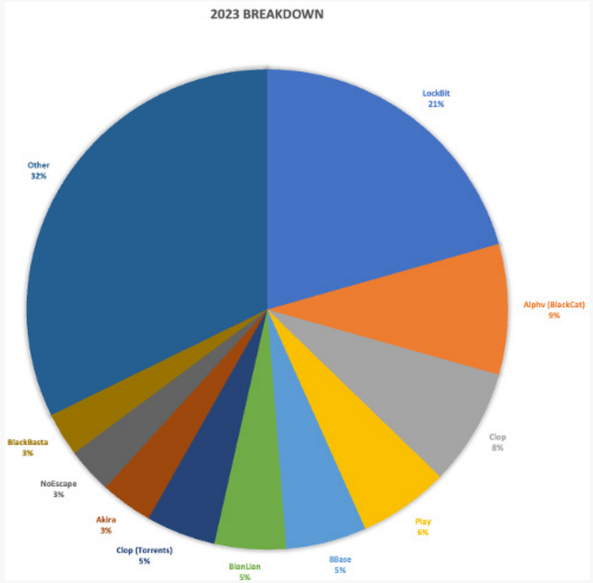
The following data is limited to ransomware and data leak groups who operate a leak site which is parseable. The following data was captured between 1st December – 31st December 2023.

Overall, there has been a sharp decrease in activity from Novembers' numbers with 152 fewer posts being made to leak sites. This is a drop of 30.22%. Of all Ransomware brands that posted victims (discounting 'new' brands) only four posted more victims in comparison to November 2023; CLOAK, STORMOUS, 3am and CACTUS.

We do not have evidence that can explain this drop (such a drop was not observed in 2022), however throughout December there were several law enforcement actions taken against Ransomware operations which may possibly have impacted numbers. This being said, tracked ransomware activity in December 2023 is still far higher than December 2022 with a 41.51% increase (+100 victims).

2023 in Brief

- Numbers of victims posted to leak sites have almost doubled from 2022 to 2023. From 2,635 to 5,079.
- Each month in 2023 saw higher numbers of victims from its respective month in 2022.
- Lockbit were responsible for 1,046 victims. This is greater than 1 in every 5 victims posted to leak sites (20.6%).
- 68 'brands' of multi-point extortion methods were observed in throughout 2023.
- WithSecure observed 35 new Ransomware brands over 2023.
- There remains no evidence to suggest that typical ransomware operators target specific industries in a discriminatory manner.



Groups	Dec	%	Change from Last Month
3am	4	33.33	1
8Base	23	-30.30	-10
Abyss Data	1	-75.00	-3
Akira	17	-10.53	-2
Alphv (BlackCat)	24	-53.85	-28
BianLian	12	-7.69	-1
BlackBasta	17	-58.54	-24
Black Suit	5	-28.57	-2
Cactus	17	70.00	7
Cloak	1	-	1
Clop	2	-81.82	-9
Daixin	1	-50.00	-1
Defray777	1	-50.00	-1
Dragon Force	21	**NEW**	21
Hunters International	5	-70.59	-12
INC Ransom	7	-53.33	-8
Knight	4	-33.33	-2
LockBit	81	-27.68	-31
Lorenz	1	-75.00	-3
MalekTeam	4	**NEW**	4
Medusa	10	-28.57	-4
Meow	6	-33.33	-3
MetaEncryptor	2	No Change	0
Monti	2	-60.00	-3
NoEscape	2	-91.67	-22
Play	33	-25.00	-11
Qilin	5	No Change	0
RA Group	5	-44.44	-4
Ransomhouse	2	-33.33	-1
Rhysida	10	-16.67	-2
SiegedSec	16	**NEW**	16
Snatch	2	-80.00	-8
Stormous	8	-	8

3.1 BlackCat/AlphV – Seized and unseized

BlackCat/AlphV were mentioned in last month's (November) Threat Highlights Report where we detailed a new tactic they were employing – reporting their victims to authorities. BlackCat have continued their interaction with authorities in December however probably not in a way they would have liked or anticipated. It appears that the FBI managed to compromise some of BlackCat's infrastructure – likely with the assistance of a cooperating insider, obtaining private keys the deep and dark web leak site, and repatriating decryption keys which enabled up to 300 victims to restore their systems. As they had a copy of BlackCat's private key, they were able to update their leak site with a seizure notice. Of course, BlackCat also had the key, and were able to update the blog themselves, proclaiming it 'unseized'. In response, BlackCat also made the following statement:

"Because of their actions, we are introducing new rules, or rather, we are removing ALL rules, except one, you cannot touch the [Commonwealth of Independent States], you can now block hospitals, nuclear power plants, anything, anywhere," according to a translation of the website that, hours before, showed the logos of law enforcement authorities around the world."

AlphV's move to cut the cost of working with them, widen the pool of available targets and ban discounts is likely in an attempt to retain its affiliates with financial incentive, as affiliate trust AlphV/BlackCat's operational security is almost certainly at an all-time low. It's possible that this posturing is an attempt to save face, as disruption such as this by the FBI can be an existential threat to a ransomware families brand – even if the affiliates themselves can still operate under a different banner.

3.2 Ransomware Newcomers

iTwo new ransomware leak sites have emerged this month, SiegedSec and DragonForce with 16 and 17 victims posted to leak sites respectively. Whilst there are no discernable patterns in victimology of DragonForce victims, it is readily apparent that SiegedSec are probably not operating primarily with a financial motivation.

SiegedSec first emerged in February 2023 posting to a telegram channel 'GhostSec' claiming to have hacked the organization Atlassian. The self-proclaimed 'furry' group reportedly compromised a number of other high-profile targets throughout summer 2023, before being referenced on 'Stormous's' redesigned leak site: "In collaboration with GhostSec, SiegedSec, ThreatSec, and Clop".

The victims posted on SiegedSec's shame site align with incidents claimed by SiegeSec, and also independently reported in media. It also appears that SiegedSec operate as a hacktivist, with two posts listed as 'Op Israel' and 'Op TransRights'. On this theme, other victims of note posted to the shame site in December are NATO, and an Israeli telecommunications company (of which the credit is shared between known Hacktivist Anonymous Sudan, and SiegedSec).

Another newcomer emerged in December – MalekTeam. Few victims have been posted and little is currently known about them, however.

4. Other notable highlights in brief

4.1 Breach Breach Breach

In December there were several significant data breaches, with the PII of 35 million people stolen from the US telecoms provider Xfinity (a brand of Comcast), 15 million from the US mortgage lender MrCooper, and 1 million from DonorView, a provider of a cloud based charitable donation platform. Each of these breaches is significant and interesting in different ways. The data stolen from MrCooper is that of every current and former customer of the company or its sister brands and could even include the data of anyone who has ever even applied for a loan from/through Mr Cooper. In the case of Xfinity, the breach appears to have come about after a server vulnerable to CitrixBleed was left unpatched for 2 weeks, giving attackers more than enough time to find and compromise it. In the case of DonorView, the data was simply accessible from an unsecured Internet connected database. The data exposed includes not only the information of donors (including payment information), but also the details of children, their medical conditions, and attending doctors.

4.2 DarkGate

WithSecure has reported a couple of times recently on Darkgate, with the latest blog released in December this year (covered in more detail in section 6.1), and industrial colleagues have also undertaken similar research. In December alone, Trellix reported on Darkgate's updated execution chain, and a new password exfiltration capability and Avast have documented DarkGate's nefarious use of DNS TXT queries.

Darkgate is a malware as a service, propagated by numerous threat actors, including but not limited to ransomware-associated Tramp/TA577, and actors operating in a Vietnamese nexus with a very similar distribution pattern to Ducktail. This is significant, as tooling like this is a key element of the 'as-a-service' industry that operates in the supply chain of ransomware affiliates. It demonstrates that tooling like this is still under active development and highlights the need for security companies such as WithSecure to continually expand detection capabilities to remain ahead of such adversaries.

4.3 Merry Leaksmas

On December 24th multiple dark web actors released large datasets of stolen PII for free. Reporting by Resecurity found that around 65 million records had been leaked, including 22 million records from Peruvian telecoms provider Movistar.

4.4 Qakbot still Twitching

On December 11th a phishing campaign delivering a Qakbot payload was identified by researchers at Microsoft. The campaign was described as small, and targeted the hospitality industry specifically, with a campaign code/identifier of tchk06. The Qakbot binary has a new version number of 0x500, as well as new features and new bugs, which suggests that it has been actively developed since the FBI take down earlier in the year. Other open-source reporting suggests that the infrastructure in the phishing campaign was used as early as November 28th, but that December 11th is the earliest time that Qakbot is known to have been the payload.

4.5 The second Polish train saga

A fascinating tale of corporate malfeasance and hacking was published in December 2023, even though the actual activity detailed happened in 2022. The contract to service 10 trains on the Lower Silesian Railway in Poland was won by SPS, a company which was a competitor to Newag, the manufacturer of those trains. Once SPS won the contract, for some reason the trains started to break down, but with no indication that anything physical was wrong with them. Nothing in the Newag provided documentation covered such a situation, although they claimed that it was a safety feature causing the issue. Eventually SPS brought in a group of Polish cybersecurity specialists to investigate. Modern trains are extremely complicated, computerized, electromechanical machines, essentially mobile ICS systems, and the specialists were able to reverse engineer the operating systems of the trains, finding multiple pieces of code which would intentionally disable the trains if they spent a certain amount of time at the GPS co-ordinates of SPS maintenance depots, or after a certain hard coded date. In one train a GSM modem was also identified, which appeared to have no practical function, except that information as to whether any software lockouts were active was being sent to this device, and presumably then on to an external destination. The cybersecurity experts were able to create a software tool which removed the artificial errors and allowed the trains to function, this tool was then used to unlock a total of 24 Newag trains which were otherwise non-functional.

4.6 Syrus4 IoT Gateway completely unsecured by default

CVE-2023-6248 was identified as affecting the Syrus4 IoT Gateway, a device used for remote management of fleet cars. The vulnerability is that the device uses a completely unsecured MQTT server to download and execute commands from the manufacturer's cloud service. As such an attacker can connect to this unsecured server and perform a number of serious actions on any vehicle connected to the cloud service, such as sending CAN bus messages on the internal car network, immobilize the vehicle, get live video feeds from the vehicle, and send audio messages to the driver. Researchers stated that they identified at least 4,000 cars that could be remotely controlled in this way, and that the only response they received from the manufacturer was that they did not consider it an issue.

4.7 Hardware based cryptocurrency security provider not that secure

Users of Ledger hardware cryptocurrency wallets were victims of a software supply chain attack that resulted in the theft of $600,000 of cryptocurrency. Typically, software supply chain attacks involve the compromise of an individual software developer at a larger organization, or of the organization itself. In this case however, the compromise began when a former employee was compromised via a phishing attack. The employee still had access to push code to the Ledger connect-kit repository, and since no MFA protections were in place the attacker was able to upload malicious code which included a crypto drainer, i.e., a piece of malware intended to identify cryptocurrency wallets and send their contents to an attacker-controlled wallet. Connect-Kit is the software/library that allows applications to connect to the Ledger hardware, and so can be used to read/modify the data that the hardware is intended to protect.

Three versions of the connect-kit app were uploaded by the attacker, two of them were configured to download a separate NPM package which contained a crypto drainer, while the final version incorporated the crypto drainer within the connect-kit code itself.

4.8 Set an LLM to jailbreak an LLM

Researchers from Robust Intelligence and Yale University have identified a way to optimize the process of jailbreaking an LLM. When an LLM has been configured to follow “guiderails”, essentially not giving harmful or toxic responses, it is known as an aligned LLM, and all the major LLMs such as ChatGPT and Bard are aligned.

However, it is possible to create your own unaligned LLM using open-source solutions, though such an LLM will not have the training data sets and optimizations of the leaders in the field, and so will probably not be as capable. What the researchers discovered however, is that a small/simple, unaligned LLM can be used to rapidly jailbreak other more complex, aligned LLMs though a method named Tree of Attacks with Pruning. What is most interesting about this is that the researchers found that the more complex/capable the LLM, the easier it was to break the guiderails. The researchers state that they do not know of any obvious method to protect against this type of attack.

4.9 Barracudas choke on Excel

Vulnerability CVE-2023-7101 was identified in the open-source Perl module Spreadsheet::ParseExcel. This Perl library is used in Barracuda email security gateway (ESG) appliances to screen Excel file attachments to emails for malware. An investigation by Barracuda and Mandiant has identified that this vulnerability has been exploited by unidentified attackers designated UNC4841 to target a small number of IT and Government entities, predominantly in the US and Asia Pacific. The attackers were able to use the vulnerability to perform remote code execution, specifically of attacker supplied Perl code on the Barracuda ESG appliances. The investigators stated that they believe the campaign began on or around 30th November 2023, and Barracuda deployed a remediating patch for the issue as it applies to their ESG appliances on 21st December, and the Spreadsheet::ParseExcel Perl library itself was updated to address the vulnerability on 29th December. Because this is an open-source library that may be used by/contained within other services and solutions, this could represent a software supply chain risk if the patched version is not pushed down the software supply chain.

5. Threat data highlights | Vulnerabilities & Exploits

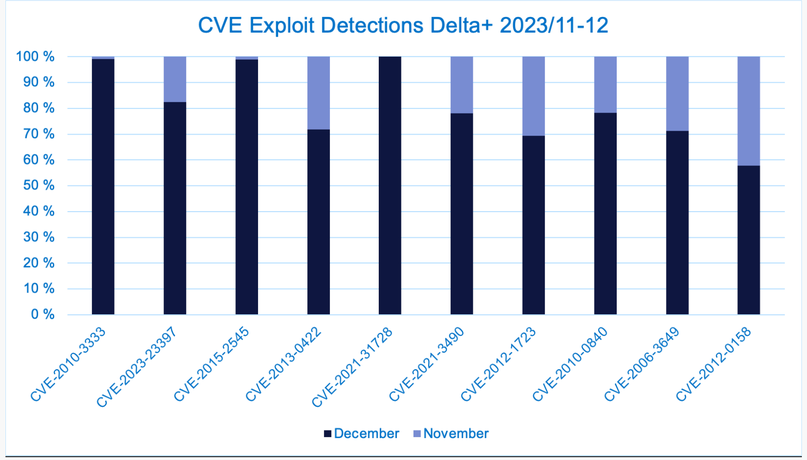
5.1 Exploits

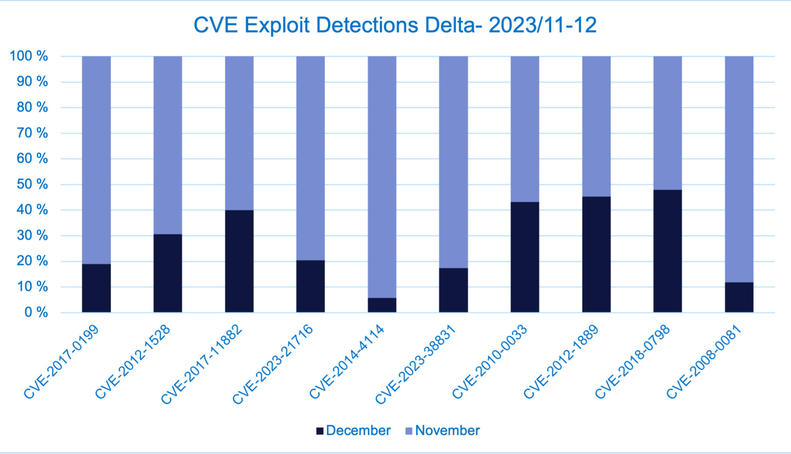
This month the exploit data is being analyzed in a slightly different way, putting the focus on changes over time in WithSecure and VirusTotal detection data.

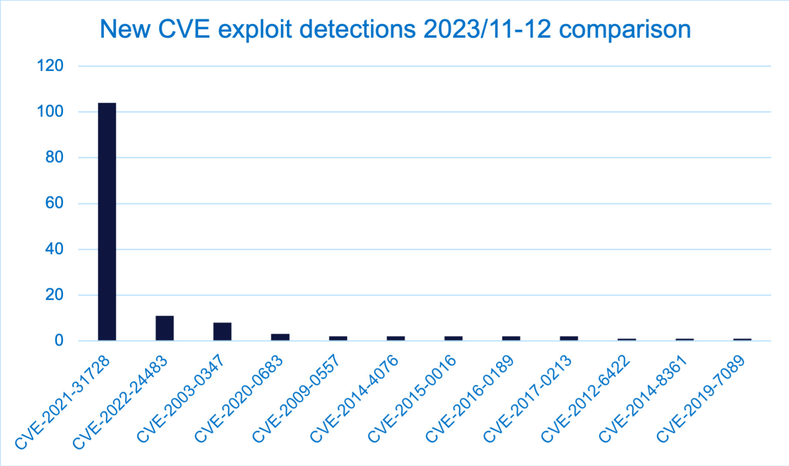
Looking at WithSecure detections specifically there are a number of CVEs which have fluctuated greatly in use when comparing data for November against data for December. The most significant increases were for vulnerabilities in Microsoft Office, Oracle Java JVM v, and a specific set of drivers from MalwareFox AntiMalware, which are used for BYOVD attacks.

Interestingly, only one of the vulnerabilities is from 2023, and that is CVE-2023-23397, which is mentioned in our Monthly Highlights section 2.1. At present we cannot say why detections of exploit attempts for that CVE have spiked in December, but it could be related to the activity described by Microsoft, or Microsoft's reporting may have caused other actors to begin using it again. As previously stated, there have been additional bypasses found for this CVE, with the most recent being re-patched in October, so in a way this is still a very recent exploit, and one that has been in the news repeatedly for various reasons.

Among the largest decreases in detections between November and December were two 2023 CVEs, CVE-2023-21716, the WinRAR RCE that has been used by state sponsored and financially motivated attackers alike, and CVE-2023-38831, the Office RTF Font Table buffer overflow which famously had a one-line POC that was tweeted by a security researcher. Considering the age of many of these CVEs, and their use in phishing campaigns, it is entirely possible that these changes are not necessarily to do with a significant change in the landscape, but instead simply indicate a change from the use of one old, yet reliable exploit to another by the operators of mass phishing campaigns.

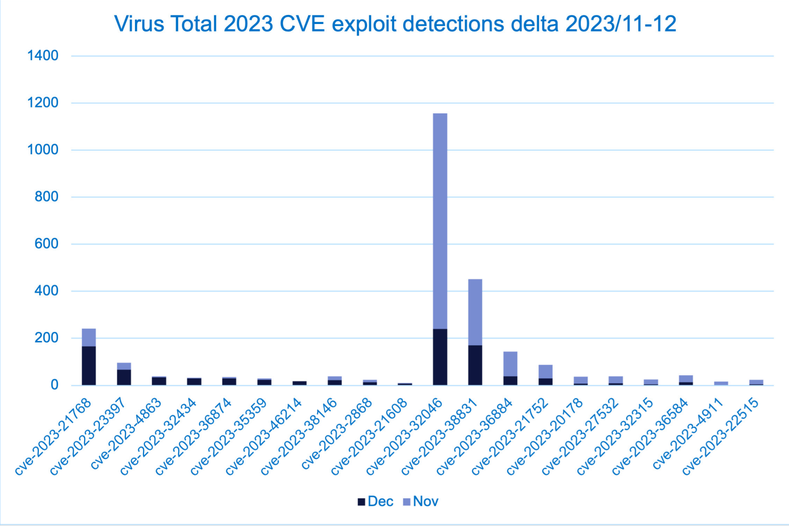






There are no 2023 CVEs being exploited this month that were not last month, however there is a significant spike in one CVE what was not exploited at all in November, that is CVE-2021-31728, relating to MalwareFox AntiMalware drivers which can be used for BYOVD/EDR Bypass attacks.

VirusTotal data is very noisy due to both the volume of data and the fact that anyone can submit any file, so patterns in the data are not necessarily new or relevant, however we can see some changes in the VirusTotal data between last month and this month that may be significant. CVE-2023-38831, the Office RTF Font Table buffer overflow, which was observed decreasing in WithSecure data, has also decreased in VirusTotal data.



CVE-2023-32046 Windows, an MSHTML Platform privilege escalation vulnerability also dropped significantly, from ~900 detected files to ~250.

There was also a significant increase in CVE-2023-21768 – a Windows Ancillary Function Driver for WinSock local privilege escalation vulnerability.

5.2 Newly Exploited Vulnerabilities

The following vulnerabilities have been added to CISA's Known Exploited Vulnerabilities catalogue in December:

CVE ID	Vendor	Product	Name	Date added	Description
VE-2023-42917	Apple	Multiple Products	Apple Multiple Products WebKit Memory Corruption Vulnerability	04/12/2023	Apple iOS, iPadOS, macOS, and Safari WebKit contain a memory corruption vulnerability that leads to code execution when processing web content.
VE-2023-42916	Apple	Multiple Products	Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability	04/12/2023	Apple iOS, iPadOS, macOS, and Safari WebKit contain an out-of-bounds read vulnerability that may disclose sensitive information when processing web content.
CVE-2023-33107	Qualcomm	Multiple Chipsets	Qualcomm Multiple Chipsets Integer Overflow Vulnerability	05/12/2023	Multiple Qualcomm chipsets contain an integer overflow vulnerability due to memory corruption in Graphics Linux while assigning shared virtual memory region during IOCTL call.
CVE-2023-33106	Qualcomm	Multiple Chipsets	Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset Vulnerability	05/12/2023	Multiple Qualcomm chipsets contain a use of out-of-range pointer offset vulnerability due to memory corruption in Graphics while submitting a large list of sync points in an AUX command to the IOCTL_KGSL_GPU_AUX_COMMAND.
CVE-2023-33063	Qualcomm	Multiple Chipsets	Qualcomm Multiple Chipsets Use-After-Free Vulnerability	05/12/2023	Multiple Qualcomm chipsets contain a use-after-free vulnerability due to memory corruption in DSP Services during a remote call from HLOS to DSP.
CVE-2022-22071	Qualcomm	Multiple Chipsets	Qualcomm Multiple Chipsets Use-After-Free Vulnerability	05/12/2023	Multiple Qualcomm chipsets contain a use-after-free vulnerability when process shell memory is freed using IOCTL munmap call and process initialization is in progress.
CVE-2023-41266	Qlik	Sense	Qlik Sense HTTP Tunneling Vulnerability	07/12/2023	Qlik Sense contains a path traversal vulnerability that allows a remote, unauthenticated attacker to create an anonymous session by sending maliciously crafted HTTP requests. This anonymous session could allow the attacker to send further requests to unauthorized endpoints.
CVE-2023-41265	Qlik	Sense	Qlik Sense Path Traversal Vulnerability	07/12/2023	Qlik Sense contains an HTTP tunneling vulnerability that allows an attacker to escalate privileges and execute HTTP requests on the backend server hosting the software.
CVE-2023-6448	Qlik	Sense	Qlik Sense HTTP Tunneling Vulnerability	07/12/2023	Qlik Sense contains an HTTP tunneling vulnerability that allows an attacker to escalate privileges and execute HTTP requests on the backend server hosting the software.
CVE-2023-49897	FXC	AE1021, AE1021PE	FXC AE1021, AE1021PE OS Command Injection Vulnerability	21/12/2023	FXC AE1021 and AE1021PE contain an OS command injection vulnerability that allows authenticated users to execute commands via a network.
CVE-2023-47565	QNAP	VioStor NVR	QNAP VioStor NVR OS Command Injection Vulnerability	21/12/2023	QNAP VioStar NVR contains an OS command injection vulnerability that allows authenticated users to execute commands via a network.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

Our latest reports: Threat-Research