Threat Highlight Report

July 2024

WITH secure

Contents

Foreword

This month we spent quite a lot of time talking about something that wasn't actually a cyber incident, the Crowdstrike outage. The impact of this was so great and it is of such importance to the sector as a whole that we chose to cover it in our Monthly Highlights.

The impacts of the ransomware attack on Kadokawa corporation and subsidiaries in Japan continues to be felt, and the wide variety of sectors in which it does business means that there are multiple ways that the impact of the attack is being felt. There are also multiple different types of data belonging to their diverse customers and partners that have been stolen. As ever, the impact of a ransomware attack is heavily reliant upon the victim's business.

There was also a high severity vulnerability in the very widely used SSH reference implementation, OpenSSH, which could open up a large number of victims to attacks from any attackers with the patience to launch an attack that could take over a week to bear fruit.

There is a significant volume of ransomware related news and activity this month, as well as both AI and Hacktivism stories. These sections include several good news stories, where international law enforcement have shut down criminal activities and automated online influence operations.

Finally, we know that not everyone has the time or inclination to read a report of this size. To address this, for several months now we have been producing a podcast where I and our Director of Threat Intelligence, Tim West talk through the contents of the THR report in a brief and light-hearted manner. The podcast is called Cyber Threats Xposed, and it is available from on YouTube, Spotify, or directly on the WithSecure site.

- Stephen Robinson, Senior Threat Intelligence Analyst, WithSecure

1 Monthly highlights

1.1 Crowdstrike software update causes largest ever computer outage

While we do not consider this to be a cyber incident, it had a staggering impact, and is important to the sector as a whole so we wished to cover it.

In July what was probably the largest computer outage of all time occurred when at least 8.5 million Windows computers began repeatedly crashing due to a flawed CrowdStrike software update. Any devices running Windows with CrowdStrike Falcon installed that were online between 04:09 UTC and 05:27 UTC on Friday 19th July were affected, including servers, PCs, and embedded computers such as point of sale devices and even billboards. As such, outages were first noticed in Oceania and East Asia, where due to the time difference, it was Friday afternoon. Microsoft state that at least 8.5 million devices were affected, but this number only includes devices with Windows Error Reporting enabled, which connect back to Microsoft servers to report issues that have caused them to bluescreen.

The error that caused the problem was in what Crowdstrike call a channel file. Crowdstrike explained that they deploy "template types", which are templated blocks of code that can be customized and implemented by later "rapid response" deployments of "template instances" to the Falcon software. Channel files contain template instances. In February 2024 Crowdstrike pushed a new template type to detect abuse of Named Pipes. Some Named Pipe instances were pushed successfully after that, but then on July 19th a channel file was pushed that contained a template instance with an error which caused the Falcon software to attempt an out-of-bounds memory read. Because Falcon runs as a kernel driver, when an exception such as this occurs the Windows kernel goes into a blue screen error state, as it can no longer guarantee the integrity of kernel memory.

In some cases, due to the slight variability in when the error would occur, it was possible to resolve the error by repeatedly rebooting a device whenever it blue screened. This was because eventually it would be online for long enough to download the updated channel file from Crowdstrike, however this could take upwards of 20 reboots and was not guaranteed to work. In addition, many devices which have Falcon installed also have BitLocker disk encryption enabled, requiring a centrally managed 48-character key in order to boot. These centrally managed keys are typically stored on a Windows server, and of course if that server had falcon installed it was also affected by the outage. As such, many organizations encountered additional roadblocks to resolving the issue.

Fortunately there are a lot of clever and inventive people out there who found ways around these issues, including creating barcodes of BitLocker keys and scanning them into devices to get them to boot.

When the cause of the outage had been identified and as Crowdstrike were being named on almost every news site and media channel, cybercriminals began launching phishing campaigns and scams claiming to be Crowdstrike support, or to simply have a fix for the issue.

After about a week the vast majority of devices were back online, and details are still emerging as to how the error occurred. Crowdstrike stated that their change update files are tested by an automated content validation process, and it appears that a bug in that process meant that the flawed data was not detected, and the update was pushed out to endpoints.

Microsoft and the Crowdstrike outage

While the outage was often called a Microsoft outage, it was not directly caused by Microsoft. There has been some criticism of Microsoft however, with some commentators questioning whether Microsoft were at fault for certifying a kernel driver which by design will dynamically load further, unverified code. Security software pretty much must have some level of kernel access in order to function correctly. If security software does not run with the highest of privileges, then it is not able to properly monitor the system or take action against malicious software, and could then be disabled or modified by malware itself. Microsoft have published a blog stating that best practice for security software is to run as little code as possible at kernel level for monitoring and enforcement only, while as much code and as many of the functions of the software as possible should be run outside of the kernel, where any failures will be less likely to cause a full system crash. Although, if that was the case, there is then a question as to whether those ancillary security software functions running at a lower privilege level would be vulnerable to modification by malware which could alter the behavior of the software or system.

Microsoft are reported to have since claimed that the outage is a result of the 2009 EU antitrust ruling against Microsoft which forced them to make Windows kernel functionality previously restricted to Windows Defender available in some form to other software vendors. However, that antitrust ruling did not specify how exactly Microsoft were to make the functionality available, and at no point states that they had to enable other security vendors to run their full security suites at the kernel level. They could instead have provided an interface which would allow security vendors access to the kernel functionality in some other way, such as a non-kernel API.

While this has already been a rather long section, it seems only correct to reproduce WithSecure's official message about the Crowdstrike outage:

> The unprecedented impact of the Crowdstrike and Microsoft issues over the last few weeks has been well publicized and the full fallout is yet to be established, with ongoing legal and commercial impact making the headlines. What we can talk about is how the events impacted WithSecure and our own approach to situations like this.
>
> We did see some impact to non-critical services, however we saw no impact to our customer facing business critical products and services.
>
> Through our 35 years of software development and customer engagement we have evolved our release and change processes to mitigate the risks of similar situations. We continue to review and learn lessons from events like this to make sure we remain vigilant and robust in our change, release, and development practices. Our own practices prevent any kind of customer software release without rigorous testing and a controlled, staged release approach. Where our software does instrument the operating system we can state with certainty that releases have been subjected to a battery of tests over extended periods across multiple operating system versions to ensure that there is no negative impact on stability or performance.
>
> We continue to be available to support all our customers and partners as people adjust to business after recovery, including supply chain management, continuity, and the constant challenge of efficacy of security versus speed of deployment.

1.2 Kadokawa corporation and subsidiaries suffer extensive outages and data theft from BlackSuit ransomware incident

On June 8th Japanese corporation Kadokawa group suffered a major cyber incident, the most visible indicator of which was an outage of the popular Japanese video sharing website, Niconico. Kadokawa announced that this was a ransomware attack on June the 14th, and the attack was then claimed by the BlackSuit ransomware group on June 27th, who threatened to publish stolen data if the ransom was not paid. In June and July Kadokawa have posted updates on the incident and their status. On June 27th they stated that most of their operations were still impacted in some way, including their accounting functions, physical media publishing, physical distribution, all Niconico services, and the account services for their online stores and portals. On July 3rd they posted an update regarding the data that was stolen, saying that there was a high possibility that data of the Kadokawa Dwango Educational institute had been stolen, meaning that personal information of some high school students and graduates was likely to have been leaked. Legal documents including contracts between the Kadokawa Group company Dwango and individual authors, content creators, and companies was likely to have been leaked. The personal information of all current and previous Dwango employees, and employees of Dwango affiliated companies is also believed likely to have been leaked.

In their statement, Kadokawa have said that they hope to have the investigation reports from the 3rd parties whom they have engaged, and considering how transparent they have been regarding the impact of the incident so far it is hoped that they will also share further technical details about the incident that others can learn from. In Kadokawa's most recent statement on the 3rd of July, they say that they do not intend to give in to the criminal acts, which seems to mean that they do not intend on paying whatever ransom has been demanded, which might explain why they described the stolen data as "likely to be leaked".

WithSecure Insight

Kadokawa is a major media corporation in Japan, and the Niconico video sharing website is often described as Japan's YouTube. This has been an extremely visible incident for Kadokawa from the very start due the outage of Niconico, but some of the other impacts that have come to light may even be more serious. There have been OT network impacts which have prevented them from printing/creating physical media and their distribution network was affected. It is possible that the most severe impact for the company could come from the impact on their accounting function. Not only does the loss of the accounting function leave an organization unable to invoice, it may also mean that the company could be unable to meet its regulatory and legal requirements.

In early June, before this incident, Kadokawa were valued at roughly JP¥465billion (USD$3 billion), but the share price has since dropped by 15% to JP¥395billion, knocking JP¥70 billion (USD$500 million) off the value of the company. While other factors have caused their share price to fluctuate over the past several years, it does appear that this most recent drop is entirely due to the very severe, and every public impact of this ransomware attack.

1.3 RegreSSHion unauthenticated RCE identified in OpenSSH servers

On July 1st researchers at Qualys disclosed CVE-2024-6387, a race condition vulnerability in OpenSSH which affects glibc-based Linux systems, though not OpenBSD-based systems. The researchers describe OpenSSH as one of the most secure pieces of software in the world, stating that it provides a near-flawless implementation of SSH, but the emphasis there is on the fact that it was near flawless. CVE-2024-6387 is in fact a regression of CVE-2006-2051 and was accidentally re-introduced in OpenSSH 8.5p1 from October 2020.
The vulnerability comes about because sshd's SIGALRM signal alarm handling function is called asynchronously, but the handler then calls functions which are not safe to call asynchronously, and which can introduce a race condition. That race condition can then be exploited to get a remote root shell on the target device. An apparent working exploit for RegreSSHion was discovered in the wild on July 3rd, only 2 days after the CVE was disclosed.

It is likely that this vulnerability affects a large number of servers and infrastructure devices from multiple vendors. Indeed, Cisco posted an advisory about the vulnerability which included a list of 150 different device series which are affected by the vulnerability, including desk phones, servers, switches, firewalls, and email gateways. In their advisory the scale of the problem is such that they have no current estimate of when fixes will be rolled out for some products, while the estimated patching date for other products is as far ahead as November 2024.

After RegreSSHion was disclosed, another researcher then discovered and disclosed CVE-2024-6387. This is a similar race condition, but it is triggered in a less privileged process, meaning that successful exploitation would only grant unprivileged/non-root access to a server. This would still provide a foothold into the network even so, and as the researcher notes, this is a separate vulnerability to RegreSSHion, which will need to be patched separately. In addition, it is possible that there will be different scenarios where one vulnerability will be more attractive/easily exploited than the other.

WithSecure Insight

Some reporting has suggested that this vulnerability is academic, as to successfully exploit it could take up to a week of repeated connection attempts, however exploitation attempts were observed within days of the vulnerability being announced. There are more than enough APTs, whether motivated by espionage or financial gain, who would be more than willing to leave a process running for a week if it would result in gaining root access to a high value victim. In fact, there is no reason why attackers couldn't perform multiple attacks in parallel against different devices or victims. As our next story makes clear, with the possible payouts available, it is very likely that some actors will be more than willing to reap the rewards of delayed gratification.

1.4 Fortune 50 company pays largest known ransom ever to Dark Angels ransomware group

In late July, Zscaler and Chainalysis each reported that in early 2024 they had observed a payment of USD$75 million, the largest known ransom payment ever, being made to a cryptocurrency wallet controlled by the Dark Angels ransomware group. In reporting such as this it is standard practice for companies not to name victims, and that was the case here. However, as the name suggests there are only 50 companies in the Fortune 50, and only one of those disclosed a ransomware incident in early 2024, Pharmaceuticals company Cencora. Cencora notified regulators that they had experienced a ransomware attack and data had been stolen in February 2024. Cencora are a USD$10 billion company who in 2023 had a revenue of USD$262 billion, so it is entirely plausible that they would pay a USD$75 million payment to remain operational and to attempt to stop the leaking of stolen data.

The actual impact of the attack and information on what data was stolen is quite hard to piece together as Cencora has a number of subsidiaries, and Cencora and at least two of its subsidiaries have each filed separately with regulators stating that data was stolen during the attack. The two subsidiaries that filed did so in May, 3 months after the attack, and in July Cencora updated its filing to say that more data had been stolen than previously known.

Cencora have stated that the stolen data was from its partners, which are other pharmaceutical companies, pharmacies, and healthcare providers. However, as this is a Fortune 50 company when they say partners, it is likely that they mean other very large companies, and in May 30 pharmaceutical related companies notified the State of California that they were affected by a data breach on 21st February 2024, including:

- Pfizer
- Johnson & Johnson
- GlaxoSmithKline
- Abbott Laboratories
- Abbvie
- Novartis
- Genentech
- Bayer
- Regeneron
- Takeda Pharmaceuticals US
- Sanofi US
- Bristol Myers Squibb

In a randomly chosen sample of the filings of these companies, each one listed the compromise of Cencora subsidiary Lash group as being the cause of the data breach.

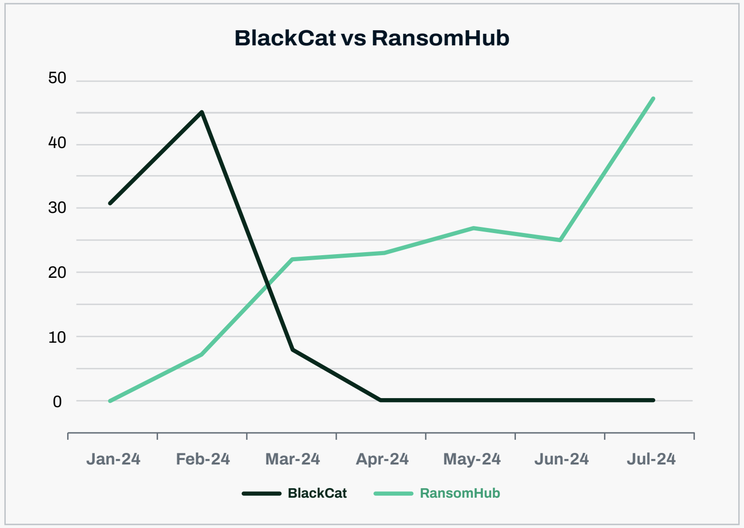
WithSecure Insight

The fact that a ransomware payment of this size was made truly illustrates just how profitable it can be for attackers. Dark Angels have never been one of the top Ransomware brands by numbers, however this single payment makes them a very significant actor based on profits made this year. We don't know if Dark Angels have an intentional strategy of big game hunting, performing small numbers of attacks on high value targets for big payouts, or if they just got lucky. Either way, it's clear that big game hunting in general can indeed be a legitimate strategy for patient, low volume actors. Something which should make everybody a bit more wary of vulnerabilities such as RegreSSHion. As well as what we can learn from the attacker in this incident, the breadth of impact of this attack is also quite breathtaking. While (as far as we know) there was not a significant operational outage, tens of companies with a combined turnover of trillions of USD$ were affected by this data breach.

2 Ransomware: Trends and notable reports

2.1 Ransomware data

For the second month in a row, and for the second month since we began recording, ransomware numbers for July 2024 are less than the numbers recorded in the same month the previous year (July 2023). There was a total of 413 new and unique organizations posted to leak sites throughout July, which is an increase of 94 from a relatively quiet June (in ransomware victim postings, at least). The increase is largely due to upticks in postings from Lockbit (+30), RansomHub (+22), Akira (+10) and Meow (+21).



Ransomhub was the most commonly observed ransomware family this month with 47 victims posted. This continues a near-constant increase since they first emerged in February 2024. In last month's Threat Highlight Report, WithSecure noted that a group known as ScatteredSpider had moved to working with RansomHub following the exit scam of AlphV/BlackCat.

WithSecure has noted several examples where TTPs previously observed in BlackCat incidents are now seen with RansomHub incidents. Comparing RansomHub's victim posts with BlackCat's it does appear that they are inversely proportional.

Group	Victims posted	Change from June
8BASE	0	-8
Abyss	3	-1
Akira	30	10
Arcus Media	1	-13
BianLian	13	4
BiteMe	0	0
BlackBasta	7	-8
Blackbyte	1	0
Blackout	2	2
Blacksuit	10	-4
Brain Cipher	6	6
Cactus	7	-11
Cicada3301	6	2
CL0P	1	-2
Cloak	7	1
Daixin	1	0
dAnon	1	-2
DarkVault	4	-6
Defray777	4	4
Dispossessor	6	6
Donut Leaks	5	5
DragonForce	14	7
Dunghill Leak (News)	1	1
Embargo	4	2
Eraleignews	0	-6
Everest	5	1
Fog	12	12
FSOCIETY	4	2
Hunters International	25	17
INC Ransom	11	-7
Kill Security	3	3
LockBit	39	30
Lynx	2	2
Mad Liberator	8	8
Mallox	2	-1
Medusa	16	-2
Meow	21	21
MetaEncryptor	1	0
Mogilevich	0	0
Money Message	0	-1
Monti	3	0
Play	21	-14
Pryx	2	2
Qilin	10	-5
Qiulong	0	-1
RA Group	5	5
Ransomcortex	4	4
Ransomhouse	11	8
RansomHub	47	22
Red Ransomware	0	-1
Rhysida	11	5
SenSayQ	0	-2
Space Bears	8	-2
Stormous	2	2
Trinity	0	-3
Underground	2	0
Vanir	3	3
WikiLeaksV2	1	-3

2.2 Lockbit Update

Lockbit's numbers continue to be unpredictable, as this month they posted 39 victims. This is a slight recovery from the 9 victims of last month, but should be compared to their activity levels from before law enforcement’s Operation Cronos disruption event. Prior to that, the group hadn't posted less than 50 victims per month since 2022.

PLAY ransomware posted 14 fewer victims in July than in June, which may be significant as PLAY has claimed to have teamed up with LOCKBIT. Several announcements were made on various channels to this effect, with LOCKBIT reportedly sharing knowledge and expertise. We are yet to see the impact of this partnership and how it may manifest.

WithSecure noted in June that Lockbit's infrastructure had been in a state of constant change throughout the month. This has continued into July with new contact details. Lockbit has claimed to be experimenting with Signal and Telegram and has a new TOX ID. Download servers are frequently being deliberately taken offline and new leak and chat sites were initialized in July. It is clear Lockbit is in a state of significant change, and it is possible that there has been a change in personnel, as well as tooling and infrastructure.

2.1.1 Lockbit Targeting Croatia Healthcare

In the last 90 days (at the time of writing), Lockbit's second most targeted sector is Hospitals and Healthcare. There have been a number of high impact attacks on the healthcare sector from various ransomware actors, and one of the latest is Lockbit's attack on the largest hospital in Croatia. This attack shut down the hospital's IT services for a day and "took us back 50 years — to paper and pencil".

While possibly unrelated, this event occurred the day after a large DDoS campaign by pro-Russian hacktivist group NoName057, who targeted multiple Croatian national organizations including the Ministry of Finance, Tax Administration, Croatian National Bank (CNB) and the Zagreb Stock Exchange. There is nothing to suggest any choreography between the attacks on Croatian institutions by these two Russian threat groups, but there is some coincidence.

2.3 New Groups

There were seven new ransomware data leak sites first seen in July 2024. Fog, Mad Liberator, Brain Cipher, Ransomcortex, Pryx, Vanir and Lynx.

2.3.1 Fog Ransomware

Fog has posted 12 victims throughout July, of which 8 are in the field of Education. This is an abnormally high proportion of victims in a single sector. Fog was first observed in June by Arctic Wolf, but at that time had no extortion portal or data leak site.

Fog was reported leveraging compromised VPN accounts to access their victims' networks. Commentators have noted an overlap in Fog's TTPs and those of Akira. Microsoft noted this month that Storm-0844, an actor known for distributing Akira had started deploying Fog more often than Akira. Developers behind Fog ransomware have also developed a Linux/ESXi variant, giving them the ability to target virtual instances.

2.3.2 Mad Liberator

Mad Liberator posted 6 victims in July, 4 of which was European and two African. There are no discernible patterns in victimology

2.3.3 Brain Cipher

Brain Cipher was first observed having compromised the Ministry of Communication and Informatics for the government of Indonesia. Posting 6 victims in July there does not to be any discernible patterns in victimology. Little is known about Brain Cipher, but it was reported by Sangfor that it is the latest in many ransomware variants built using Lockbit 3.0's leaked builder.

2.3.4 RansomCortex

Not to be confused with the now dormant MegaCortex ransomware variant, RansomCortex are new in July 2024 posting 4 victims, 3 of which are Mexican victims. Of note, RansomCortex have advertised a bounty program whereby they offer "freelancers" money if they can be employed to "help" companies in major cities decide to pay a ransom. They suggested that such actors should "have their own team for physical action, as well as stalkers, OSinters and 'swatters'." If this materializes this would represent a relatively new extortion lever employed by Ransomware actors, although in 2022 Brian Krebs reported on what was at the time a concerning new marketplace centered around 'Violence-as-a-Service.

2.3.5 Pryx

Pryx is a new 'group', which started operating in June 2024. There have been 3 posts to the leak site in July, 1 US county college, and 2 entries claiming a breach of the UAE government, and its 'wwwroot' (the web root folder, containing all static files of a project/website) directory.

Whether Pryx operates an encryption toolkit is unknown, however based on a dark web forum post by a rival of Pryx, it appears the actor found a bug in a college administration SaaS solution and exploited it to scrape data relating to school applications of its US victim – a county college.

2.3.6 Vanir

Vanir has posted 3 victims in July and no patterns in victimology are discernible.

2.3.7 Lynx

Lynx has posted 2 victims in July and no patterns in victimology are discernible.

2.4 Ransomware Highlights

2.4.1 Scattered Spider hacker linked to MGM Resorts attack arrested in UK

Scattered Spider were publicly attributed to the 2023 compromise of networks of MGM Resorts, a USD$14 billion gambling and entertainment enterprise. It was reported that services were taken offline for multiple days and a ransom was paid to hackers who had threatened to leak its data. In July the National Crime Agency of the UK arrested a 17-year-old male accused of being involved with Scattered Spider, more specifically "targeting large organizations with ransomware and gaining access to computer networks". This comes a month after another man suspected of being the 'ringleader' of Scattered Spider was arrested in Spain.

2.4.2 Meow

After 21 postings this month the group MEOW is worthy of a closer look. While they were active in 2022 and early 2023, MEOW appeared to cease operations when a decryptor was publicly released for their encryption tool. They re-emerged in November 2023, and since then they have never posted more than 9 victims in any single month. Indeed, before July they had only posted 9 victims throughout the entirety of 2024. WithSecure has not observed any encryption malware related to MEOW and therefore it is possible MEOW operate solely as a data theft operation. Reviewing some of the posts it does appear that Meow are simply seeking to sell stolen data with varying list prices.

While there is no discernible pattern in victimology, the victim numbers are unusual. WithSecure do not have insight into the cause of the data leaks, but it is possible MEOW have found a method that has enabled them to steal data across victims at a larger scale than usual. Such an increase can happen when actors discover a single but fruitful exposure in externally facing services - vulnerable managed file transfer services, or cloud services without sufficient authentication controls, for example.

2.4.3 Volcano Demon pressures victims through phone calls

Researchers at Halcyon have described 'Volcano Demon', a ransomware operator utilizing LukaLocker attempting to mount pressure on victims to encourage them to pay a ransom. LukaLocker was not a ransomware family known to WithSecure, and it is likely the actor is relatively rudimentary in its capability. It is not unheard of for ransomware actors to directly contact victims to attempt to convince or intimidate them to collect payment, but it does not frequently happen with the more capable ransomware variants.

2.4.4 Ransomware attack continues to impact South Africa’s national lab service

Hospitals and Healthcare was the fourth most targeted sector in July; however, one could argue it is the most impactful on society and on individuals. In yet another highly impactful attack on laboratory services this year, South Africa's National Health Laboratory Service (NHLS) was impacted by ransomware. While the attack occurred on 22nd of June, in July the NHLS was still not fully operational, with physicians across the country unable to access test results through a portal. This is quite a critical impact as South Africa is in the midst of an outbreak of the disease mpox. This is another example (if one were needed) of the real-world impact of ransomware to global citizens everywhere.

3 Other notable highlights in brief

3.1 Kaspersky leaves US after government ban

In response to the US government ban on Kaspersky providing cybersecurity software and services in the US, it has announced that it will be shutting down US operations and laying off the <50 employees remaining in the US at this time. Kaspersky are also offering 6 months of free products to customers in the US.

3.2 URL protection services abused by attackers to hide phishing links

Researchers at Barracuda identified a trend of attackers abusing legitimate URL protection services to conceal malicious phishing campaign URLs, with the activity they identified beginning in May 2024. URL protection services wrap links in outbound emails within a “safe” link, then if an email recipient clicks on the wrapped link the service scans the original URL to check it is safe. If the URL appears safe, the user is redirected to the true destination. The researchers observed multiple services being abused, and believe the attackers are leveraging access to compromised accounts to send phishing links to themselves and are then using the re-written links in their phishing campaigns. Researchers from Cofense also saw this surge in activity and note that such behavior was seen previously, but increased drastically in May 2024. Cofense believe that the abuse of URL protection services is possible as Email Security Gateways are not correctly vetting rewritten, “safe” URLs.

WithSecure Insight

Historically, URL shorteners were abused for their ability to obfuscate the true destination of a link, something with Email Security Gateways (ESGs) and URL protection services tried to address. As such, it is slightly ironic to see these services being abused in a similar way. The key thing however, is that it seems these services seem to be struggling to properly vet phishing URLs in outbound emails. In light of the apparent increasing trend of BEC and onward attacks from compromised accounts, this is hopefully something that can be effectively addressed.

3.3 The core Python Project Github repository token left publicly accessible

Researchers at JFrog found that a GitHub token that granted elevated access to the GitHub repositories of the Python language itself, PyPi, and the Python Software Foundation was accidentally made public in a public Docker container hosted on Docker Hub. It is possible that if an attacker had found this token they would have been able to perform a supply chain attack against the actual source code of the Python programing language or the PyPi package manager. The token was not present in the source-code within the Docker image, but instead in a compiled python (.pyc) format from which it could then be decompiled and accessed. Once it was reported, PyPI responded to the researchers within 17 minutes, the token was revoked, and all uses of that user account reviewed and verified. A full write up of how this token came to be made public was written by the owner of the token, PyPi’s Director of Infrastructure.

WithSecure Insight

Control of the Python language’s repository would have been a huge thing for a malicious actor. It would be hoped that malicious changes to such a heavily watched, critical open source repository would be rapidly picked up, but as previous software supply chain attacks exploiting leaked tokens have shown, it only takes a short while for large numbers of downstream victims to be impacted. It is however very good to see such absolute transparency being displayed by Python, with a clear and thorough explanation for exactly what happened, how, and why.

3.4 Void Banshee exploited Zombie Internet Explorer vulnerability

Microsoft Windows vulnerability CVE-2024-38112 was exploited as a zero-day by APT group VoidBanshee to deploy Atlantida Stealer malware. When exploited the vulnerability allows an attacker to force a victim to open a link in the legacy Internet Explorer browser, even if IE is not the default browser, or is in fact disabled on the machine. As lures for the campaign, Void Banshee used zip archives disguised as e-book PDFs distributed through cloud file sharing services, discord servers, and online libraries.

WithSecure Insight

Internet Explorer has been legacy software for some time now, and even when it was current software it was considered extremely insecure. As such it is an incredibly dangerous thing for an attacker to be able to force a victim to open a URL in Internet Explorer.

3.5 UK government to introduce diluted version of mandatory reporting for ransomware attacks

The new UK government announced a Cyber Security and Resilience Bill they intend to pass into law which will update cybersecurity regulations and include a mandatory ransomware incident reporting requirement for “regulated entities”, i.e. CNI organizations. A statement from the NCSC has indicated that the proposed bill will also apply to parts of CNI supply chains. This is a less ambitious, but most likely more achievable version of the legislation proposed by the previous UK government, which would have required all victims of ransomware incidents to report incidents to the government and get a license from the UK’s sanction authorities before making any extortion payments.

3.6 Novel OT malware that targets any ModBus devices linked to sabotage of communal heating in Ukraine

Researchers at Dragos have identified a malware they have named FrostyGoop which is reportedly the first known malware able to interact directly with OT systems via the Modbus protocol. As such, unlike other OT malware in the past, which has targeted specific types of hardware/systems, FrostyGoop presents a threat to almost any system that uses Modbus. Dragos identified 46,000 Internet exposed devices communicating over Modbus. The Ukrainian CERT have confirmed that FrostyGoop is the malware that was deployed in January 2024 to target a local energy company in Lviv. Attackers used it there to turn off the communal heating system for 600 apartments.

WithSecure Insight

It seems like it would be best practice not to expose ModBus interfaces to the public Internet, but even when these interfaces are internal facing if there is not clear IT/OT network segregation then the ability for a piece of malware to communicate directly with a ModBus compatible OT device is significant. All an attacker would need to do is compromise a device which can reach the OT network, then drop this malware to begin reconnaissance and/or destructive attacks.

3.7 Multiple DoS vulnerabilities identified and patched in Bind 9 DNS server

The Internet Systems Consortium (ISC) who maintain the DNS server software BIND, have released patches to address multiple newly identified vulnerabilities that could be used in denial-of-service attacks against DNS servers. CISA also issued an advisory about the vulnerabilities. Exploitation of other BIND server vulnerabilities was noted in VirusTotal exploit data in the June Threat Highlight Report.

3.8 Philippines closes entire offshore gambling industry linked to organized crime and cyberfraud

The Philippines government has decided to close its entire offshore gambling industry due to the high volume of illegal activity associated with the sector. Philippines Offshore Gambling Operators (POGOs) were licensed in the Philippines to offer gambling to users outside of the Philippines, most often China, where online gambling is illegal.

WithSecure Insight

Huge amounts of international cyberfraud have been perpetrated by POGO entities, supported by human trafficking of thousands of workers forced to work in online scam sweatshops. While removing the license of POGOs may simply drive some of this activity further underground, it will also remove any possible veneer of legitimacy from these organized crime entities. As such it is hoped that this may reduce the volume of cybercrime coming out of the Philippines.

3.9 New warnings about password protected archives introduced to Google Chrome

Google Chrome has introduced new warnings and protections when users download password-protected archives. Warnings are based upon AI generated malware verdicts, and may warn that files are suspicious or dangerous, depending on the verdict. In addition, users with Enhanced Protection mode enabled will be prompted to enter the password for the file so that the file can be submitted to Google's Safe Browsing service to have its contents scanned. Google state that all files and passwords submitted to this service will be deleted promptly and any collected data will only be used for download protection of Chrome users. Users who use Standard Protection mode instead of Enhanced Protection mode will still be prompted for the password, but only the metadata of the archive contents is sent to Google, the file and password remain locally on the device.

WithSecure Insight

Password protected archives are regularly abused by malicious actors because they can prevent security software from examining the contents, while allowing the recipient victim to open the archive and execute the contents. While at first glance it may seem that people are unlikely to simply submit their passwords to Google servers, the passwords they would be submitting would not be their own, they would often have been sent in plaintext via email, and typically would not be very strong anyway. As such, it is possible that users would be willing to use this service. Even if take up is relatively low, and limited to files from unknown senders which users are already suspicious of, it could still be effective. Those are, after all, the exact archives that should have their contents scanned.

3.10 Evolve Bank and Trust compromised leading to PII theft and downstream financial impact

In June Lockbit claimed to have breached the US Federal Reserve, however it turned out to have in fact compromised Evolve Bank & Trust. In July Evolve confirmed this came from a successful phishing attack, and that while the attackers could not access any money, they were able to download customer information. Evolve however are not just a private bank, but also a business-to-business, Banking as a Service and payment processing technology provider. As the Change Healthcare hack recently illustrated, a cyber-attack on such a provider can have a greatly increased scope and impact. In the case of Evolve, they provided USD account services to London based international money transfer company Wise, buy now pay later credit provider Affirm, payment processor Stripe, e-commerce and Point of Sale (PoS) platform Shopify, and the start-up focused fintech company Mercury. Extensive data belonging to customers of these other companies has been found in the stolen, and now publicly leaked Evolve data.

In a filing on the 9th of July with US regulators, Evolve stated that 7.6 million individuals were affected by the data theft.

Shopify user data was also leaked in a separate incident this month, which Shopify blames on an as yet unnamed third-party app that integrates with its platform. Third-party apps such as these can provide extra functionality to users, but also require access to the data of users.

WithSecure Insight

The financial industry is particularly vulnerable to supply chain attacks because there are so many financial services and fintech services which are used by multiple large financial organizations. Many financial organizations process the financial data and transactions of other organizations, and as such both data theft and service interruption can have much impacts that reach far beyond the initial victim.

3.11 Frankfurt University of Applied Sciences latest victim in a spate of similar attacks against Hochschules

In early July the Frankfurt University of Applied Sciences announced that it had experienced a severe hacking attack leading to the total shutdown of its IT systems. This is the latest in a series of cyber-attacks on German engineering/applied science institutes known as hochschules. Other Hochschules (or similar institutes) that have experienced such attacks in the past year include Kempten, Kaiserslautern, Harz, Ruhr West, EUFH, Duisberg-Essen, Hannover, and Hamburg. Some attacks have been claimed by Russian ransomware groups including BlackSuit and Vice Society.

WithSecure Insight

This is an interesting targeting trend, however it is not presently possible to say whether this indicates a specific intent to target these types of institutions by attackers, or instead a shared security posture failure by these organizations or their suppliers.

3.12 New GhostScript remote code execution vulnerability reported to be under exploitation

CVE-2024-29510 has been disclosed in GhostScript, the open-source PostScript and Adobe PDF file format interpreter which is used under the hood of vast numbers of image file conversion software and services. This vulnerability was patched in April 2024, however significant concerns remain because GhostScript is in the software supply chain of so many different solutions.

WithSecure Insight

Vulnerabilities in GhostScript are problematic because it is a library that is intended to provide functionality to other pieces of software, and GhostScript itself is so successful that it is the go-to solution for the functionality it provides. As such the right vulnerability could well present a significant software supply chain issue.

Of particular concern is that one of the places GhostScript is commonly used is OCR, or optical character recognition, something that is often used when parsing training data for AI models.

3.13 Snowflake enables admins to enforce MFA, but not before the call logs of every AT&T user were stolen

Snowflake have now provided administrators at their customers with the ability to make MFA mandatory for all user accounts within their tenants. The announcement does not mention the compromises of Snowflake victims, however when Mandiant were engaged to investigate the breaches of Snowflake victims they stated that every single compromised account did not have MFA enabled. Also in July, the US telco AT&T announced that the phone records of “nearly all” of their customers have been stolen from their Snowflake account. The stolen records contain phone numbers, call and text records, and some geolocation information for devices at the time of the calls and texts between May-October 2022, and also from January 2023, for an unspecified subset of customers. This data also includes customers of any mobile/cell phone providers who also use AT&T’s network. In total, AT&T have stated that they will be notifying 110 million people that they have been affected by the data breach. The CEOs of AT&T and Snowflake have been issued with a series of questions about the breaches by the US senate’s Judiciary Committee privacy subpanel.

WithSecure Insight

This is a welcome move on the part of Snowflake as it is vital to empower organizations to enforce and audit their security policies, functionality which it appears Snowflake administrators did not previously have.

3.14 Another critical Gitlab CVE allows users to run pipelines as any other user

Gitlab has released new versions of its Community and Enterprise editions which fix a number of CVEs, including 9.6 CVSS CVE-2024-5655. This vulnerability enables an attacker to trigger a pipeline as another user, which could give an attacker the ability to access private repositories and change or steal code and data from them. Gitlab state they are unaware of it being exploited in the wild at this time.

WithSecure Insight

While this may not seem like a huge issue as it can only be exploited by an authenticated user, this represents a compliance risk as well as a security risk. Companies may be required to prove or attest that they meet certain requirements regarding their software development security, such as having MFA and conditional access to their build environments and processes. If users can run pipelines and perform build actions as other users, then such requirements are not met.

3.15 Indonesian government data center ransomware attack gets worse, then better

After the ransomware attack on Indonesia’s National Data Centers in June, it has now come to light that 98% of all data stored in one of the two data centers was not backed up. While backup capacity was made available to the government agencies using the datacenters, using it is optional, and so most agencies chose not to use it due to budgetary constraints. The Communications and Informatics minister has stated that in future, backing up such data will be made mandatory. This issue was described to parliament as a governance issue, to which the Chair of the First Commission of the People’s Representative council responded, “This is not a governance issue, it is a stupidity issue”.

Fortunately for all involved, Brain Cipher, the ransomware gang behind the attack appear to have apologized for the attack and handed over the encryption key for the data. Brain Cipher have suggested that the public should be grateful for the release of the encryption key, and even provided an account at which people could make donations in gratitude for their actions.

WithSecure Insight

This is quite an interesting outcome to this ransomware incident, and definitely not one that we would have predicted. It seems that the Brain Cipher group may have been spooked by the scale of the impact they had on the country of Indonesia, which suggests that either they are not particularly experienced attackers, or they became concerned that the level of impact could become a problem for them. This raises the possibility that they could be local to Indonesia, as it seems likely that Russian ransomware operators would not be particularly concerned about the level of impact to a Southeast Asian country.

3.16 Juniper networks releases out of band critical security update for perfect 10 router vulnerability

Juniper Networks have released an out of band security update for their Session Smart Router, Session Smart Conductor, and WAN Assurance Router devices to address 10.0 CVSS CVE-2024-2973. Successful exploitation allows an unauthenticated remote attacker complete control of the device. The CVE only applies to devices configured in a High Availability (HA) configuration with redundant peers. The vulnerability was found during internal testing and Juniper are unaware of the vulnerability being exploited in the wild. There are no mitigations, the only resolution is to apply the patch.

3.17 Almost every Apple device vulnerable to CocoaPods software supply chain security flaws

CocoaPods is an open-source dependency manager developed and run by a volunteer team, and used in more than 3 million Swift and Objective-C packages, or “pods”, which are either applications themselves, or dependencies of other down-chain applications. As such it is believed that almost every single Apple device has software installed that either directly uses CocoaPods or is dependent on software that uses it.

Researchers identified multiple critical vulnerabilities affecting Cocoapods, beginning with the 9.3 CVSS CVE-2024-38368. That CVE has existed for the last 10 years and allows anybody to claim ownership of (and thus modify and completely control) one of almost 2,000 unclaimed libraries, or “pods”, some of which are used by apps from Meta, Microsoft, TikTok, Amazon, and even Apple. A second vulnerability, CVE-2024-38366, which has a CVSS 10.0 severity, allows for remote code execution against CocoaPod’s custom GitLab replacement “Trunk” thanks to the use of a vulnerable Ruby package. Finally, there is also CVE-2024-38367, a CVSS 8.2 severity session validation token theft vulnerability which exploits the fact that when a new device attempts to authenticate to a Trunk account, Trunk sends an authentication link to the registered email address for the account. Researchers discovered that it was possible for an attacker to create a spoofed XFH header and use it to construct a valid verification URL which they could then send to the owner of the account. If the link is clicked, then due to the spoofed XFH header it will send a session token directly to the attacker. In fact, if the victim is behind an Email Security Gateway, the gateway’s link checking process essentially “clicks” the link to check that it is not malicious, essentially turning it into a conditional zero-click vulnerability.

CocoaPods patched these vulnerabilities at some point in 2023, and while there was no evidence of exploitation of the CVEs, the blogpost also noted that there was no evidence they had not been exploited either, and so all user session tokens were reset.

WithSecure Insight

Once again, software supply chain issues can have far reaching impacts on so many different organizations, in this case there was the possibility of affecting all 1 billion Apple devices. As Cocoapods communications about these vulnerabilities makes clear, the software and service is run by a group of volunteers who, it turns out, are a key, foundational part of a significant, international software ecosystem.

3.18 Researchers demonstrate that AiTM can completely remove ability to use passkeys to securely authenticate

Researchers at eSentire have identified and demonstrated an attack against passkey authentication that they call a Passkey Redaction Attack. This attack is similar to a standard Attack in The Middle (AiTM) proxy attack but takes advantage of the fact that even when passkeys are in use, there are often less secure fallback authentication methods available. In an AiTM attack an attacker can modify the content that is presented to the target, and as such they can remove the option to use a passkey to authenticate from the login page, forcing the target to instead use a less secure authentication method. The researchers were able to demonstrate this by using Evilginx to successfully remove the ability to authenticate to both GitHub and Microsoft with a passkey.

The attackers describe this not as an implementation flaw or a bug, but instead as a result of what they call “authentication immaturity”, i.e. the fact that users are not familiar enough with passkeys and other authentication methods to understand the security implementations of the different options, or to identify when the authentication flow may have been modified or doctored.

WithSecure Insight

AiTM attacks are growing in popularity as they can directly defeat the security improvements brought by Multi-Factor Authentication (MFA), allowing attackers to compromise a victim’s sessions in a way that is transparent to the user and is only detectable in cloud security logs. Passkeys are intended to address some of the limitations of MFA, so this ability for attackers to simply remove the option for passkey authentication is significant.

3.19 Zero Day Initiative raises concerns over lack of coordination in vulnerability disclosure processes

In a blog post on July 15th, shortly after Microsoft’s July Patch Tuesday, Dustin Childs of vulnerability reporting and bug bounty program Zero Day Initiative (ZDI) described his concerns around the integrity of the process of coordinated vulnerability disclosure between vendors and security researchers. In the blogpost it was observed that a number of serious zero-days have recently been patched by vendors without any advance warning to researchers, and without any acknowledgement of the work of the researchers who discovered and reported them. He also raised issues around the CVSS rating of CVEs, highlighting the case of a vulnerability which was fully weaponized and used at Pwn2Own by Valentina Palmiotti. However, when that vulnerability was patched by Microsoft they stated that the exploit code was unproven, unavailable, or only theoretical. Differences in CVSS rating may seem minor, but organizations will often roll out patches for Critical CVEs quicker than High CVEs, and so a disagreement over severity could lead to totally different security postures for millions of people and their data. While these examples related to Microsoft, it was made clear that security researchers and the ZDI feel this is a wider industry problem affecting coordinated vulnerability disclosure.

The blogpost also raised the issue that if security researchers feel that a vendor is not clearly communicating and collaborating with them, they could stop working with that vendor, or simply release exploits without co-ordination as a zero-day, guaranteeing that they will be credited, and the vendor will be forced to respond rapidly to address the vulnerability.

WithSecure Insight

Co-ordinated vulnerability disclosure is an important process and principle when dealing with vulnerabilities. There have been well documented disagreements between security researchers and vendors in the past over the balance between silent patching and full transparency, such as between Rapid7 and JetBrains earlier this year. This can be a complicated decision space, and the impact of the choices that different organizations make can interact in unpredictable ways, as with the Progress/WatchTowr/IPWorks situation in June.

4 Hacktivism

4.1 US sanctions two members of Cyber Army of Russia_Reborn hacktivist group

The US government has named and sanctioned two members of Cyber Army of Russia_Reborn (CARR), a Russian government aligned hacktivist or influence operation, depending on your definition. The two individuals are described as the group's leader, Yuliya Vladimirovna Pankratova and the primary hacker, Denis Olegovich Degtyarenko. CARR has been carrying out unsophisticated, low impact DDoS attacks against Ukraine since 2022, but in 2023 began performing attacks against industrial control systems in the US and Europe. The sanctions state that in May 2024, Degtyarenko was known to be developing training materials on how to compromise industrial control systems, and that he may have been looking to distribute those materials to other groups.

WithSecure Insight

Many hacktivist groups are believed to simply be sock puppets for nation states. In the case of CARR, they appear to be closely aligned with NoName057, and in reporting from Q2 2024 Mandiant described CARR as operating closely with the Russian military intelligence APT, Sandworm.

4.2 Spanish authorities arrest three individuals for use of DDoSia hacktivist platform

Spanish authorities arrested three individuals and seized multiple computers and mobile devices from Seville, Huelva, and Manacor in relation to use of the DDoSia platform in attacks against governments and other organizations in NATO countries. DDoSia is controlled by Russian government aligned hacktivist group NoName057. DDoSia was released in August 2022 and allows people who sign up to the platform and allow their devices to be used for DDoS attacks to be paid based on the quantity of traffic they generate.

WithSecure Insight

DDoSia functions in a similar way to crypto mining, allowing people to make money from running code on a computer. Cyber criminals who have compromised devices into a botnet can install DDoSia and abuse the bandwidth of the compromised devices to earn money. As such, the individuals arrested in Spain are unlikely to be individuals who have signed up their home computers to DDoSia. Instead, they are much more likely to be criminal botnet operators.

4.3 UK shuts down DDoS-for-hire site digitalstress.su and arrests suspected admin

The UK National Crime Agency (NCA), the Police Service of Northern Ireland (PSNI) and the US FBI announced that after a law enforcement operation named Operation Power Off (not a hugely inventive name) the DDoS platform digitalstress.su has been taken down and the suspected administrator arrested somewhere in the UK. DigitalStress is described as a DDoS for hire platform that allows criminals to select a destination and pay for a DDoS attack to be launched, and it is described as being responsible for tens of thousands of attacks per week. The .su domain is the former Soviet Union TLD, which some cybercriminals use as they believe it is more difficult for Western law enforcement to investigate. As with the Lockbit takedown, LE used the messaging function of the site to contact its users and inform them that the site had been taken down by law enforcement. In addition, the NCA stated that for some time they were mirroring the site, and that they have details of the activities of anyone who used the site while it was being mirrored, which we can hope will lead to further investigations and arrests.

WithSecure Insight

While DigitalStress was hosted on a former Soviet Union TLD, that doesn't necessarily indicate that it is aligned with Russian (or former Soviet) interests. In fact, while it is a DDoS site, and so may have sold services to hacktivists from time to time, it appears to be operated solely on a commercial basis, not for geopolitical or ideological motivations. Attacks launched through DigitalStress may have been targeted at commercial businesses and websites by competitors or Internet trolls, or even just a Minecraft server that has earned the ire of an unscrupulous player.

4.4 Hacktivist group SiegedSec claim hack of US think tank The Heritage Foundation, then disband

The US hacktivist group SiegedSec, who appear to be quite unique in that they may actually be the hacktivists they claim to be, have leaked 2 Gigabytes of data which they claim to have stolen from the Heritage Foundation, a rightwing US think tank. SiegedSec say that they released the data in response to Heritage Foundation's Project 2025, a set of right-wing policies intended for Donald Trump if he wins the upcoming US election. The data appears to contain blogs ad material related to a website called The Daily Signal, a rightwing media site affiliated with the Heritage Foundation. A Heritage Foundation spokesperson claimed that they were not hacked, and that instead the leaked data was from a 2-year-old archive of The Daily Signal which was left publicly accessible on a contractor's server. The Heritage Foundation then said they were contacting the FBI about getting a legal order to identify the operator(s) of SiegedSec's social media accounts, and while it seems unlikely that SiegedSec used any real contact information when creating those accounts, they have since announced that they have disbanded "for our own mental health, the stress of mass publicity, and to avoid the eye of the FBI".

WithSecure Insight

SiegedSec have been of interest because they have appeared to actually be a hacktivist group motivated by ideology, not simply a sock puppet for a nation state actor. While the group may now be disbanding, it is likely that any law enforcement efforts to identify and prosecute them will continue, so this may not be the last we hear of them.

5 AI

5.1 Concerns raised over lack of AI/ LLM vulnerability reporting and tracking structures for coordinated disclosure

A researcher who found a method to reliably crash multiple major LLMs recently published a follow-up article about their experience disclosing that vulnerability to vendors. They state that when they initially notified Microsoft, they were informed that the denial-of-service vulnerability was a “bug/ product suggestion” and that it did not meet the definition of a security vulnerability. The researcher then had an article published in The Register, after which Microsoft chose to re-assess. After the publishing of the article, they were then informally contacted by the employee of an unspecified major tech company who operate multiple LLMs. They provided the exploitation method, and demonstrated that it worked as described, after which they heard nothing more. Except, a number of the LLMs that would previously crash when given this prompt then suddenly stopped crashing, though there was no acknowledgement that anything had been done to address the vulnerability found by the researcher. After this, the Microsoft vulnerability team responded again to conclude that the denial-of-service issue was instead a performance limitation, not a vulnerability. From this reporting experience the researcher concludes that there is a distinct lack of vulnerability/bug reporting infrastructure for LLMs, and seemingly a lack of ability for security researchers, LLM developers, and LLM infrastructure providers to collaborate.

WithSecure Insight

These are the same coordinated disclosure concerns that have been raised about other, non-AI software this month. In this case, the lack of coordination and transparency, and the apparent silent patching of vulnerabilities is very reminiscent of the state of the standard software vulnerability reporting process 10+ years ago. Hopefully it will not take as long for a collaborative process that is acceptable to all involved parties to develop in the AI sector.

5.2 Law Enforcement seize Russian AI bot farm

It has been something of an ongoing joke that social media accounts online are being operated by LLM chat bots, and there have been screenshots of unknown authenticity which appear to show prompt injection attempts and successes against twitter accounts. However, a recent law enforcement statement has disclosed an operation by US, Canadian, and Dutch agencies that really blows the lid of this kind of activity, showing that it is indeed being performed at volume to influence online discourse. As part of the operation, US authorities have seized two domains and 968 social media accounts which they state were being operated as part of a covert influence operation initiated at the behest of a senior executive of Russian state agency, Russia Today. The domains were registered by somebody who was identified by law enforcement as the lead developer of a software package named “Meliorator”, which uses LLM chat bots to operate large numbers of social media accounts and fake online personas to push propaganda and influence online discourse. The tool was used by affiliates of RT to push disinformation about the US, Poland, Germany, the Netherlands, Spain, Ukraine, and Israel. The tool was only identified in use on X, however LE analysis of the tool indicates an intent by its developers to expand the functionality to other social media platforms.

6 Threat data highlights

6.1 Exploits

In WithSecure detection increases this month there was a very significant increase in a 2017 Microsoft Office Equation Editor CVE, which increased roughly 5 times over. Reporting in June stated that this vulnerability was being exploited by DPRK actors Kimsuky in attacks targeting aerospace and defense that distributed a keylogger, though that may not be the sole direct cause of this increase in detections.

The second highest increase, though far smaller, was also a 2017 Microsoft Office RCE, followed by a 2010 Adobe RCE, and a 2008 Excel RCE. Detection numbers fell off quite rapidly after that point however, possibly due to the time of year meaning that far fewer people are currently actively using their devices (and clicking on phishing links).

In WithSecure detection decreases there was a huge drop in the 2006 Office VBA Macro RCE from 2,463 detections last month to only 1 detection this month. The second largest drop was in the 2018 Equation Editor RCE. An interesting contrast to the large rise in the 2017 Equation Editor RCE. The last change of any significant volume in the graph is the 3rd value, a 2023 MS Word RTF parsing RCE, which dropped from 450 to 230 hits.

Figure 1: WS Detections - Any year CVE exploits - biggest increase

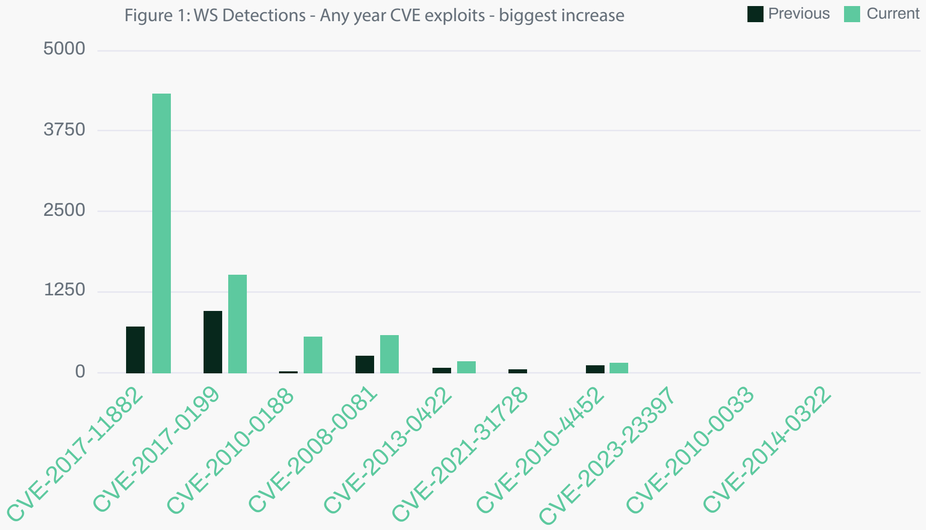
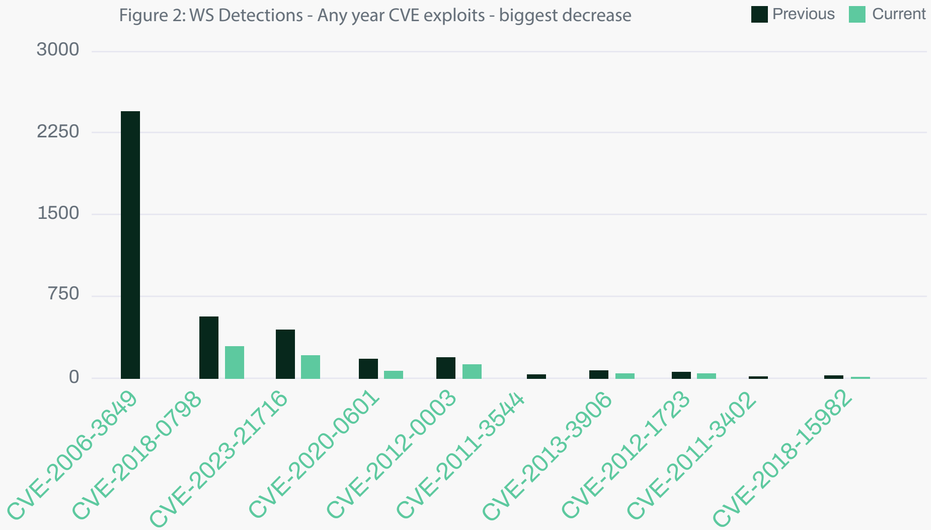


Figure 2: WS Detections - Any year CVE exploits - biggest decrease



In purely 2023/24 WS detections there were very small increases in some detections of Windows and Office CVEs, then towards the bottom of the graph a 2024 Jenkins arbitrary file read for Mac dropped from 11 detections to 0, and the 2023 MS Word RTF parsing RCE is at the bottom of the graph with a much larger drop. Indeed, the drop in detections of this CVE was large enough that it actually came in 3rd on the previous graph of all WS detections of all CVEs.

Any new WS exploit detections this month are very low in volume, so do not appear to be significant.

Figure 3: WS Detections - CVE Exploits - 2023/24

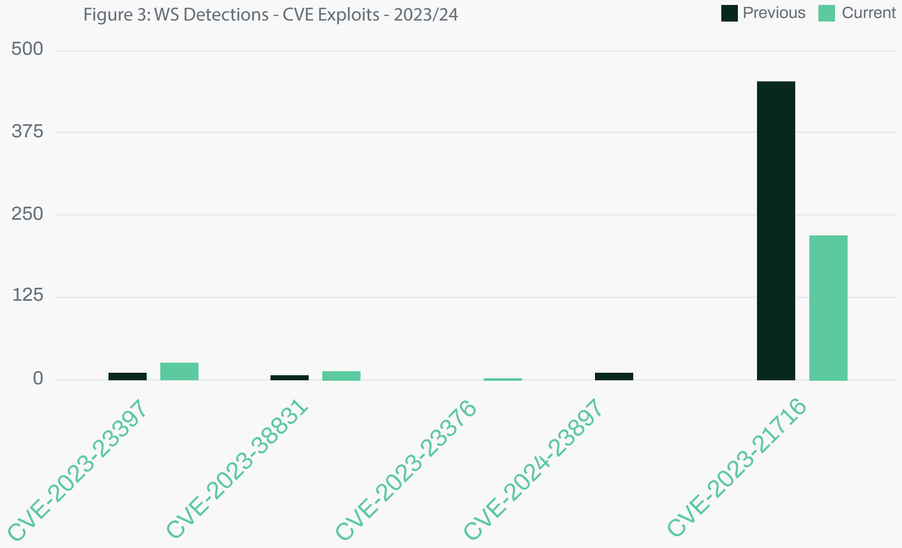
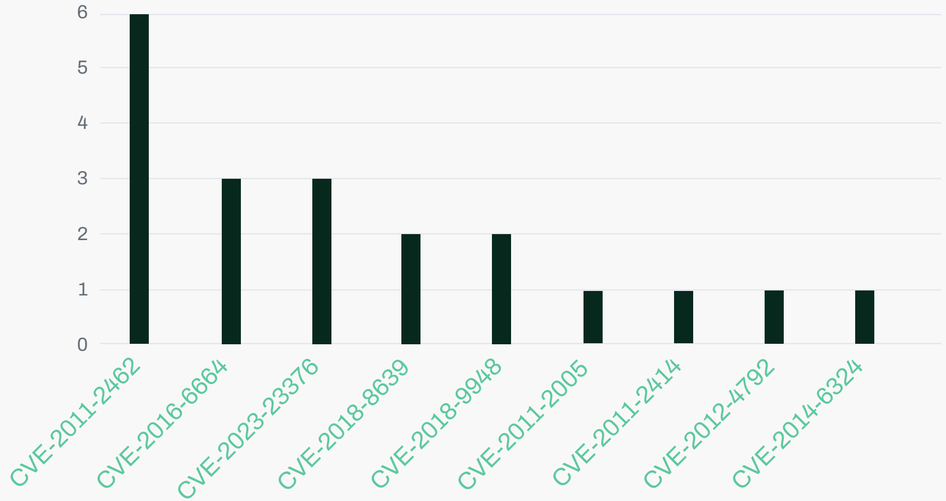


Figure 4: WS Detections - New - Monthly

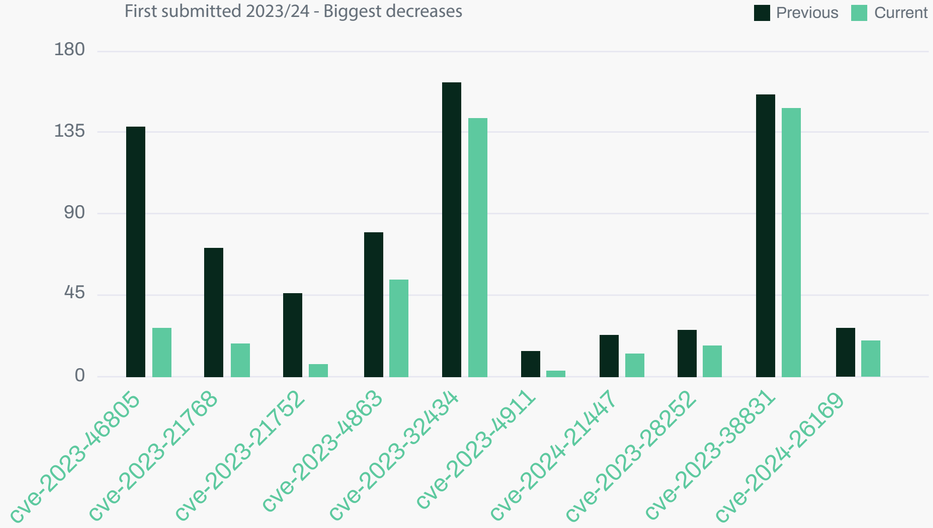


Moving on to VirusTotal exploit detections for 2023/24 CVEs, 5 vulnerabilities, including 1st place, are Windows privilege escalation vulns. There are also 3 different 2024 detections that have increased from less than 10 detections to greater than 100. At 2nd and 3rd are Windows Kernel and Visual Studio privilege escalation vulnerabilities, while at 6th is 38112, the Zombie IE bug which allows attackers to force the use of Internet Explorer to open a specified URL. At the very bottom of the graph is the XZ backdoor, once again highlighting that the presence of a CVE in this data is down to the interest not only of attackers, but also of researchers.

Looking at the biggest decreases in the 2023/24 CVE exploit detections we see a proportionately large fall for an Ivanti ICS auth bypass at 1st place. The other drops are much smaller, but throughout this graph there are 4 Windows privilege escalation vulnerabilities. In the previous graph we saw that multiple Windows privilege escalation vulnerabilities also increased this month, though none of the changes in either graph were particularly large. This could imply that such vulnerabilities are so widely used by different actors right now that they form a lightly fluctuating background noise of exploitation. Once again, apart from the 1st place vulnerability, the changes in volume of the rest of the graph are not very significant.

Figure 5: VirusTotal 2023/24 CVE Exploit Detections - First submitted 2023/24 - Largest increases

Figure 6: VirusTotal 2023/24 CVE Exploit Detections - First submitted 2023/24 - Biggest decreases



In VirusTotal detections of exploits of any CVE we finally see some very large changes. The top 4 vulnerabilities each show an increase of around 45,000, and they are all ICMP DoS vulnerabilities. 1st and 2nd place have the exact same numbers, and so are probably duplicate detections, however 3 and 4, which are both ICMP Path MTU Discovery vulnerabilities (albeit from 11 years apart) have slightly different detection numbers. At 5th place is a 2016 Windows Media player RCE which has more than doubled from 12,000 to 25,000, then interestingly at 8th place there is a SQUID DoS CVE. While the increase is proportionally small, it is yet another DoS vulnerability with over 50,000 detections and an upward trajectory this month.

Looking at the biggest fall in VirusTotal exploit detections, the top two places are both Microsoft Office Equation Editor RCEs. The drop in the 2nd place Equation Editor RCE mirrors WithSecure's detection data. At 3rd and 4th place are two CVEs with identical detection numbers. This appears to be a generic, TLS/SSL use of RC4 weakness, and a CheckPoint firewall specific IKE weakness. What is most interesting about this is that as they are triggering the same detections, and so are either the same vulnerability or at least very similar, one is from 2002, and the other is from 2013. Further down, with highest number of detections on this graph is the exact MS Office Equation editor CVE which increased so dramatically in WithSecure detections. In contrast to the WithSecure data however, it shows a fall of roughly 4%. Finally, at the very bottom of the graph with only a slight downwards fluctuation is the Huawei HG532 router RCE that we have been observing for several months now, however most detections now are coming from Chinese submissions. While previously most submissions were coming from Japan, they are no longer even in the top 10.

Figure 7: VirusTotal CVE Exploit Detections - First submitted 2023/24 - Biggest Increase

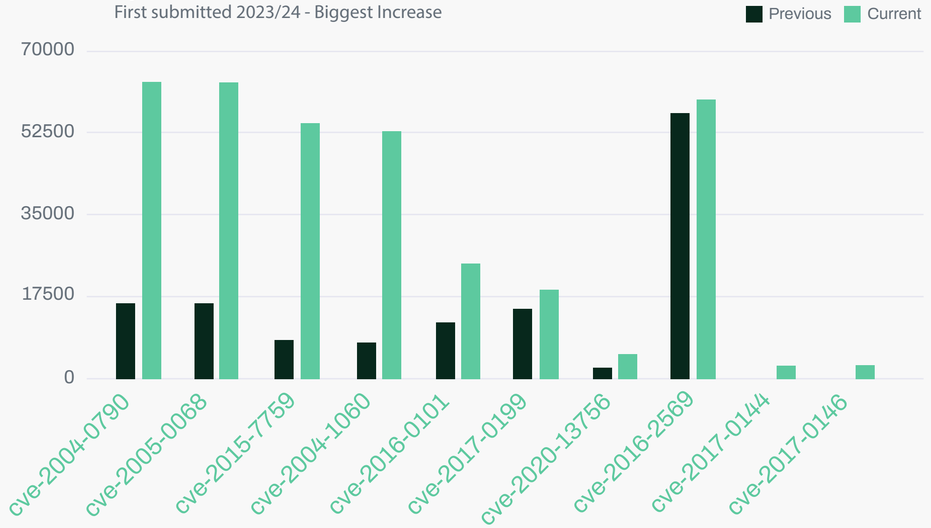
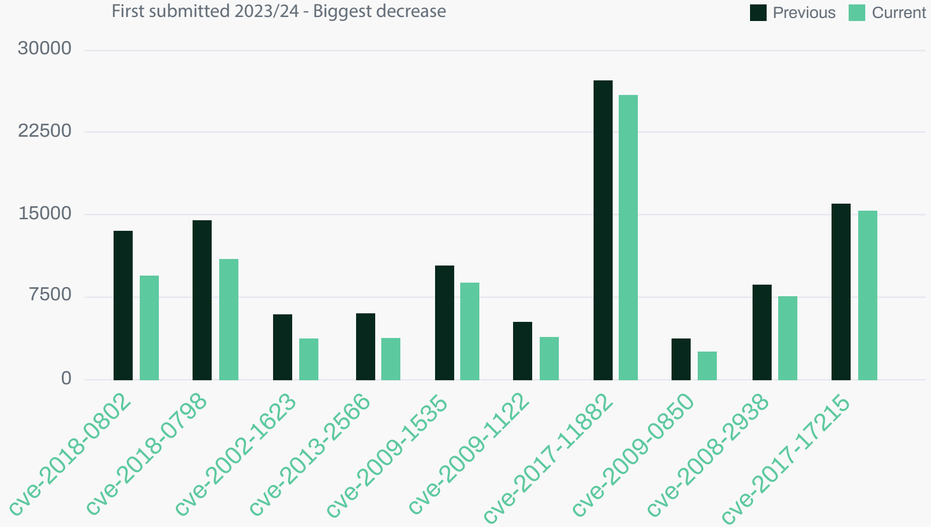


Figure 8: VirusTotal CVE Exploit Detections - First submitted 2023/24 - Biggest decrease



6.2 Newly exploited vulnerabilities

Looking at the additions to the KEV this month, we can see the CrushFTP and Cisco ASA zero-days that we discuss this month.

CVE ID	Vendor	Product	Vulnerability	Date added	Description
CVE-2024-20399	Cisco	NX-OS	Cisco NX-OS Command Injection Vulnerability	02/07/2024	Cisco NX-OS contains a command injection vulnerability in the command line interface (CLI) that could allow an authenticated, local attacker to execute commands as root on the underlying operating system of an affected device.
CVE-2024-23692	Rejetto	HTTP File Server	Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability	09/07/2024	Rejetto HTTP File Server contains an improper neutralization of special elements used in a template engine vulnerability. This allows a remote, unauthenticated attacker to execute commands on the affected system by sending a specially crafted HTTP request.
CVE-2024-38080	Microsoft	Windows	Microsoft Windows Hyper-V Privilege Escalation Vulnerability	09/07/2024	Microsoft Windows Hyper-V contains a privilege escalation vulnerability that allows a local attacker with user permissions to gain SYSTEM privileges.
CVE-2024-38112	Microsoft	Windows	Microsoft Windows MSHTML Platform Spoofing Vulnerability	09/07/2024	Microsoft Windows MSHTML Platform contains a spoofing vulnerability that has a high impact to confidentiality, integrity, and availability.
CVE-2024-36401	OSGeo	GeoServer	OSGeo GeoServer GeoTools Eval Injection Vulnerability	15/07/2024	OSGeo GeoServer GeoTools contains an improper neutralization of directives in dynamically evaluated code vulnerability due to unsafely evaluating property names as XPath expressions. This allows unauthenticated attackers to conduct remote code execution via specially crafted input.
CVE-2022-22948	VMware	vCenter Server	VMware vCenter Server Incorrect Default File Permissions Vulnerability	17/07/2024	VMware vCenter Server contains an incorrect default file permissions vulnerability that allows a remote, privileged attacker to gain access to sensitive information.
CVE-2024-28995	SolarWinds	Serv-U	SolarWinds Serv-U Path Traversal Vulnerability	17/07/2024	SolarWinds Serv-U contains a path traversal vulnerability that allows an attacker access to read sensitive files on the host machine.
CVE-2024-34102	Adobe	Commerce and Magento Open Source	Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability	17/07/2024	Adobe Commerce and Magento Open Source contain an improper restriction of XML external entity reference (XXE) vulnerability that allows for remote code execution.
CVE-2024-39891	Twilio	Authy	Twilio Authy Information Disclosure Vulnerability	23/07/2024	Twilio Authy contains an information disclosure vulnerability in its API that allows an unauthenticated endpoint to accept a request containing a phone number and respond with information about whether the phone number was registered with Authy.
CVE-2012-4792	Microsoft	Internet Explorer	Microsoft Internet Explorer Use-After-Free Vulnerability	23/07/2024	Microsoft Internet Explorer contains a use-after-free vulnerability that allows a remote attacker to execute arbitrary code via a crafted web site that triggers access to an object that (1) was not properly allocated or (2) is deleted, as demonstrated by a CDwnBindInfo object.
CVE-2023-45249	Acronis	Cyber Infrastructure (ACI)	Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability	29/07/2024	Acronis Cyber Infrastructure (ACI) allows an unauthenticated user to execute commands remotely due to the use of default passwords.
CVE-2024-5217	ServiceNow	Utah, Vancouver, and Washington DC Now	ServiceNow Incomplete List of Disallowed Inputs Vulnerability	29/07/2024	ServiceNow Washington DC, Vancouver, and earlier Now Platform releases contain an incomplete list of disallowed inputs vulnerability in the GlideExpression script. An unauthenticated user could exploit this vulnerability to execute code remotely.
CVE-2024-4879	ServiceNow	Utah, Vancouver, and Washington DC Now	ServiceNow Improper Input Validation Vulnerability	29/07/2024	ServiceNow Utah, Vancouver, and Washington DC Now releases contain a jelly template injection vulnerability in UI macros. An unauthenticated user could exploit this vulnerability to execute code remotely.
CVE-2024-37085	VMware	ESXi	VMware ESXi Authentication Bypass Vulnerability	30/07/2024	VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.

7 Research highlights

7.1 Analysis of cyber threats to Paris 2024 Olympics

In this research paper Tim West, W/Intelligence's Director of Threat Intelligence and Outreach, has looked into the cyber threats facing the Paris 2024 Olympics. As one of the world's greatest and most watched events, there is always going to be unwanted interest, but how much should we worry and who are the main antagonists?

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