Threat Highlight Report

May 2023

W/TH secure

Contents

1 Monthly highlights 3
2 Ransomware: Trends and
notable reports 8
3 Other notable highlights in brief 11
4 Threat data highlights 12
5 Research highlights 14

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, providing an overview of this month's cybersecurity news, the changing threat landscape and relevant advice.

This month we look at the dangers of newly introduced top-level domains, how attackers are bypassing a patched vulnerability in Outlook, and some actively exploited vulnerabilities in common WordPress plugins. We also examine the state of the growing infostealer marketplace and provide a brief update on the state of so-called hacktivist groups.

This month's look at the ransomware landscape includes identification of several newcomers, showing that the barrier for entry into ransomware is low, thanks to the professionalization of the cybercrime ecosystem and easy access to leaked locker code (LockBit and Babuk).

- Ziggy Davies, Intelligence Analyst

1 Monthly highlights

1.1 zip, a file extension or a domain?

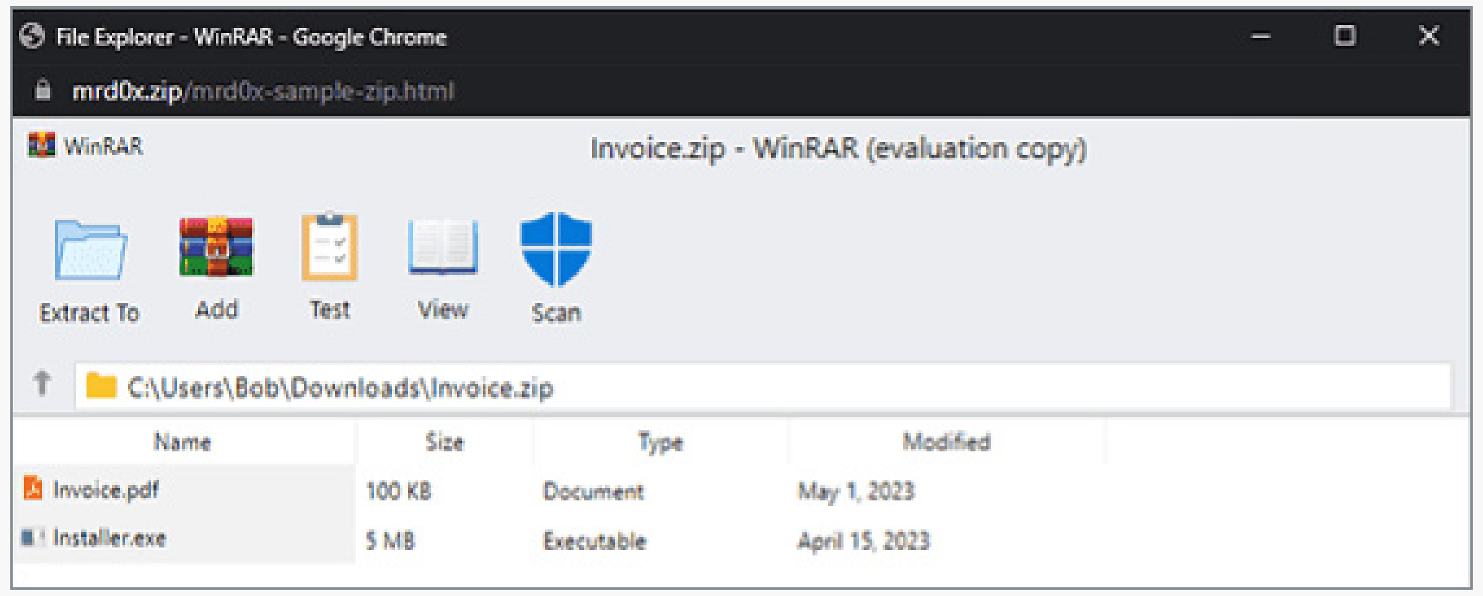
This month Google have launched 8 new top-level domains, which include:

- .dad
- .phd
- .prof
- .esq
- .foo
- .zip
- .mov
- .nexus

The security community has instantly identified the risk of domains which could easily be mistaken for file extensions such as zip archives or video files.

This has been excellently demonstrated by security researcher mr.d0x who has created a proof-of-concept that demonstrates how a file archive software like WinRAR can be emulated in the browser, to create a highly convincing malicious website.

This technique would be highly compelling for the typical end-user, and would undoubtably lead to interaction at a greater level than a standard phishing email or malicious site.



File Explorer - WinRAR - Google Chrome

mrd0x.zip/mrd0x-sample-zip.html

Invoice.zip - WinRAR (evaluation copy)

C:\Users\Bob\Downloads\Invoice.zip

Name	Size	Type	Modified
Invoice.pdf	100 KB	Document	May 1, 2023
Installer.exe	5 MB	Executable	April 15, 2023

There is already evidence of threat actors seeking to exploit the new TLDs with many suspicious domains being registered, suggesting that infrastructure aligned with common phishing themes is being built.

Some malign examples include:

- microsoft[.]zip
- microsoft-windows-update[.]zip
- chromeupdatex64[.]zip
- browser-update[.]zip
- attachment[.]zip

This issue is further aggravated by some websites/services such as YouTube automatically converting prior mentions of zip files into new hyperlinks. An example of this issue is an innocuous mention of a file called 42[.]zip on a four year old comment, which is now a clickable link that directs to a malicious domain.

This issue isn't limited to the .zip domain, and you can certainly imagine similar tactics and techniques being used to exploit the new .mov domain with video file style themes and lures.

WithSecure™ Insight

Phishing domains are often hard to detect, with threat actors going to a lot of effort to disguise them, often making them indistinguishable from a legitimate domain. The addition of new TLDs that can be easily confused with file extensions is only going to add to this problem; exploitation is already evident, with over 45k suspicious .zip domains and 2k .mov domains being identified on VirusTotal since their introduction (about 1,000 have detections on VirusTotal).

These links are often so convincing that even experienced and security-conscious users can be tricked, and training will not be enough to stop every potential incident. The onus is therefore on defenders to come up with mitigations to prevent these attacks from being successful. Very soon after public registration of .zip domains became possible, WithSecure™ telemetry detected instances of outbound requests to .zip domains where it was almost certain that filenames were being misinterpreted as domain names. This presents an issue for network monitoring teams as it decreases the fidelity of rules based on domain name matching, and analysts risk alert fatigue when investigating high risk TLDs where a lot of false positives are expected.

What can you do?

There are not many legitimate reasons for an organization to use these domains. Most companies and providers make use of the common gTLD's (General Top Level Domains) such as .com, .org, and nation specific (ccTLDs) examples such as .co.uk and .fi.

We therefore suggest that defenders consider the business need for allowing communication to domains in the zone of these new top level domains, especially .zip and .mov, and provide awareness training to end users about the dangers of file extension imitation within domains.

1.2 Outlook patch bypassed by attackers

The patch of a recent "zero-click" CVE in Microsoft Outlook (CVE-2023-23397), fixed in March 2023, was able to be circumvented due to a bug in the HTML platform (CVE-2023-29324). Defined as a security feature bypass exploit rather than a user interaction vulnerability, as per the original, researchers at Akamai found that the March patch could simply be circumvented by adding a single character to change how a function executed, thus nullifying the existing patch.

This vulnerability is present due to an issue with Universal Naming Convention (UNC) paths, which are a standard way to locate and access shared resources. In this attack, attackers can specify a UNC path that causes the Outlook client to retrieve audio files from any SMB server. To address this issue, Microsoft added an API function, called "MapUrlToZone", that verifies the security zone of a UNC path. The initial patch ensured that if an external location was used, then a default sound would be used instead of the custom sound. However, by simply adding a '\' to the UNC path, it would assess it as being in a local security zone, allowing the custom file to be downloaded from an external SMB server on port 445.

As this negates the initial patch, this also means that the attacker could still access a user's Net-NTLMv2 hash, which was the initial issue, and use it to launch NTLM Relay attacks against another service, or recover credentials.

WithSecure™ Insight

While we recommend the patching of any networked system to the best of any organization's ability, this bypass is an example of how a rigorous patching process doesn't always equal absolute safety, and a defense in depth approach is required to effectively mitigate security risks. Determined threat actors and attackers will often seek to bypass known vulnerability patches, as it is likely less resource intensive and far more likely to work than any attempt to develop a new exploit for a zero-day.

It is also an example of how simple features like the inclusion of custom audio files for alerts can be an issue, when the feature is hijacked for launching malicious code. Superfluous features like these can present more risk than benefit.

What can you do?

Microsoft has produced guidance for defenders on detecting and investigating exploitation of this vulnerability. It stresses the importance of having a good patch management process, detecting potential exploitation, limiting SMB traffic on certain ports, and disabling NTLM as appropriate.

1.3 Wordpress woes

There are currently three actively exploited vulnerabilities present in common WordPress plugins, these include:

Advanced Custom Fields (CVE-2023-30777)
This plugin is highly prevalent, with over two million active installs, presenting a cornucopia of opportunity for threat actors. The vulnerability is a high-severity reflected cross-site scripting (XSS) flaw that allows unauthenticated attackers to steal sensitive information and escalate their privileges on impacted WordPress sites, and potentially deliver malicious code/redirects to visitors.

Researchers at Akamai have noted a surge in exploitation following the release of proof-of-concept (PoC) code.

Beautiful Cookie Consent Banner
While less common, this plugin is still present on 40,000 active WordPress instances, and outdated versions feature a XSS vulnerability that can allow attackers to install redirects to malicious websites and malware. Security company Wordfence have noted a sudden uptick in exploitation during May, despite a patch being available since January.

Elementor (CVE-2023-32243)
Elementor is a WordPress builder, that is commonly used to aid the creation of websites and is used on over eight million websites.

This escalation of privilege vulnerability means it is possible to reset the password of any user as long as an attacker knows their username, thus being able to reset the password of the administrator and log in to their account. The vulnerability occurs because this password reset function does not validate a password reset key and instead directly changes the password of the given user. PoC code is available and this vulnerability will likely be heavily targeted by opportunistic threat actors.

WithSecure™ Insight

The web content management system (CMS) WordPress is highly popular and prevalent across the web, accounting for over 40% of all websites. This is because of its ease of use, capability and the vast array of plugins and add-ons which make it suitable for a wide array of use cases.

Unfortunately, this also means that WordPress is heavily targeted by threat actors, and presents a massive attack surface for vulnerabilities and exploits.

What can you do?

Patch management is key to maintaining a secure WordPress instance, thankfully many plugins can be set to update automatically from within the WordPress admin panel, ensuring that the most current version is always in use.

The discussed vulnerabilities have all been patched in the following versions:

- Advanced Custom Fields 6.1.6
- Beautiful Cookie Consent Banner 2.10.2
- Elementor 5.7.1

1.4 Spoilt for choice: infostealers

‘Infostealers’ are a type of malware designed to quietly steal and exfiltrate credentials, cookies, tokens, secrets and occasionally banking/crypto wallet data. There are titans of this space such as Redline, Raccoon and Vidar which dominate the landscape. There are also many newcomers to the scene, seeking to capitalize on the needs of threat actors needing valid credentials for initial access. The following infostealers are currently advertised for hire on dark and deep web marketplaces as part of a growing cybercrime ecosystem:

Titan
A highly regarded stealer amongst the cybercriminal community that is written in Go and is capable of stealing browser credentials, crypto wallets, FTP client details, taking screenshots, and exfiltrating files. It is advertised within channels on the instant messaging platform Telegram.

LummaC2
A typical infostealer that is advertised and sold on Telegram and hacking marketplaces for a monthly fee.

Stealc
An infostealer which can exfiltrate data automatically, and was reported to be distributed via malicious YouTube videos advertising cracked software.

WhiteSnake
This infostealer can target both Windows and Linux machines, something which is uncommon.

Pureland
A little-known stealer that targets MacOS.

MacStealer
Another MacOS stealer that is distributed via malicious .DMG files.

Atomic Stealer
A newer and fully-fledged MacOS stealer that is advertised and sold via Telegram, and often distributed via fake “cracked” software, a common tactic with infostealers.

RecordBreaker
The successor to the veteran stealer Raccoon, which dominates the market and is distributed by malicious YouTube activity and “cracked” software.

Bandit Stealer
This infostealer is capable of targeting secrets and credentials from various internet browsers, and also cryptocurrency wallets. Bandit Stealer is written in the programming language Go, making it possible the malware will be deployed cross-platform in the near future.

WithSecure™ Insight

The rise of the infostealer is an important part of the continued professionalization of the cybercrime ecosystem, with sophisticated threat actors like ransomware groups seeking massive volumes of easy initial access for their campaigns. A topic discussed in our recent report “The professionalization of Cyber Crime”.

All of these infostealers share capability, so why so many? Supply, demand and every criminal wants to take advantage and cash in on a credential-theft gold rush.

What can you do?

Endpoint protection security solutions can detect infostealer malware behavior, but prevention also relies on the education of end users to avoid phishing, malicious websites and the dangers associate with downloading software of unknown provenance.

As always, it is vital to use complex passwords, a password manager, and make use of multi-factor authentication, such as hardware solutions or number matching prompts in authenticator applications.

1.5 “Hacktivist” update

The last month has seen a big shake up with Killnet, a sub-group of pro-Russian hacktivist group Kill Milk, making a statement that they are now switching their operation and renaming to PMC Killnet, essentially becoming ‘hackers for hire’. This obviously caused some tension within the wider Kill Milk community, as a statement quickly emerged, saying that the current roster of KillNet personnel was being disbanded and new members were being recruited.

Anonymous Sudan is continuing its DDoS campaign and has targeted Scandinavian Airlines (SAS), demanding a $3 million dollar ransom to cease the attack, which seems to be increasing every few days. The group appears to be favoring targets within the transportation sector, with several small airlines and also train operators being targeted.

WithSecure™ Insight

The legitimacy of these groups and whether they are truly “hacktivists” has always been a point of contention. Killnet’s shift to being an out-and-out financially motivated actor is a sign of how complex the landscape is, and how the true motives of these groups are complex.

Anonymous Sudan demanding a ransom from SAS is a similar shift, suggesting the group are becoming financially motivated, rather than propelled by ideology or politics.

2 Ransomware: Trends and notable reports

The following data is limited to multi-point of extortion ransomware leak sites which are parseable and were captured between 28th April 2023 and 30th May 2023. There has been a moderate increase in overall ransomware attacks this month (+41%), which can be largely attributed to a surge of activity from newcomers 8base and Akira. While 8base have dumped a massive 67 victims on their leak site this month, the group has alluded to the fact that these attacks occurred over a longer period of time, but are now being leaked, which skews our statistics slightly.

Group	Number of attacks	Percentage	Change
LockBit	76	17 %	-31%
8base	67	15 %	N/A
BianLian	52	11 %	+160%
Alphv	44	10 %	-14%
Akira	30	7 %	+233%
Royal	26	6 %	-13%
Nokoyawa	25	5 %	+213%
Play	25	5 %	+127%
Medusa	16	4 %	+46%
Trigona	12	3 %	+100%
Stormous	11	2 %	+10%
BlackBasta	10	2 %	-47%
Snatch	9	2 %	+200%
Qilin	8	1 %	+300%
Vice Society	6	1 %	+50%
Ragroup	6	1 %	N/A
Other	36	8 %	N/A
Total	**459**		**+41%**

2.1 Newcomers

8Base
8Base are newcomers to the ransomware landscape. This group has a presence on Twitter designed to name/shame victims, along with a .onion leak site. Little is known about the group's TTPs at this stage, but with 67 victims listed, the group appears to be capable and one to watch.

Rapture
This group is reported to be using a new variant of an old locker called Paradise, and like many ransomware groups is heavily reliant upon Cobalt Strike.

GazProm
These newcomers have named themselves after the Russian gas company Gazprom, and are making use of the leaked Conti locker. Their ransom note also includes an ASCII depiction of a certain Mr. Putin...strange!

CrossLock
Information on this new group is scant, but it has an active .onion leak site, and its locker is written in the cross-platform language, Go.

RA Group
This group has been targeting organizations throughout May, and have so far posted six victims to their leak site. The group are making use of the leaked Babuk locker.

Cactus
This group is using a complex custom locker, which is itself delivered encrypted to help evade security solutions. The group is known to target vulnerable Fortinet VPN instances for initial access.

MichaelKors
This group is reported to be targeting ESXi instances, but are is capable of targeting Windows machines.

CryptNet
A new variant which is one (of many) variants of the veteran Chaos ransomware.

Malas Locker
This new group appears to be using the Spanish language and targeting vulnerabilities within Zimbra. The group's motto? Somos malas, podemos ser peores...a phrase associated with social justice.

Rhysida
Newcomers Rhysida is marketing itself as a security company, and operating a .onion leaksite. There are reports that the group has struck the networks of the Chilean armed forces.

2.2 Akira ransomware goes retro

Akira is a new ransomware group active since April. The group appears to be channelling a 1980s aesthetic, naming itself after a 1988 cult Japanese Manga/Anime and running a CLI-style leak site on the dark web. The group has been prolific since its emergence, and at the time of writing has struck at least 31 organizations, posting them to its leak site on the Tor network.

The group has impacted organizations across multiple sectors, suggesting it is purely opportunistic, but this does include a children's daycare provider, indicating a lack of moral code that is present in some groups.

A report by Sophos has provided insight into how the group works and we can examine their attack process:

Initial Access
The group has accessed networks through VPN credentials and a legitimate account, suggesting the use of initial access brokers and likely prior infection with commodity malware such as infostealers. Notably, MFA was not enabled on either service.

Credential Access
Gathering credentials by dumping LSASS memory, a common tactic used by threat actors.

Discovery
Akira is using the tools PCHunter64 and Advanced IP Scanner to discover system information, and is also using a scheduled task to gather remote directory listings.

Lateral Movement
Akira is utilizing RDP to move across compromised networks, thanks due to a lack of restrictions on RDP usage.

Command and Control
Much of Akira's activity appears to be 'hands-on keyboard', and they are heavily leveraging the RMM software AnyDesk, but also making use of a free tunnelling tool available from Cloudflare.

Impact
Akira is executing locker binaries that encrypt the compromised hosts, and drops ransom notes named "FN.txt" in the C: drive.

All of these TTPs are well-known and are considered part of the standard ransomware playbook, and are detectable by modern security solutions such as EPP/XDR/MDR.

2.3 Royal

Conti successor Royal is a successful and prevalent ransomware group that strikes dozens of organizations each month. A recent development with the group is the use of its own custom loader, instead of commodity options such as Qakbot.

The loader is a lightweight (<250kb) file, with a primary goal of deploying Cobalt Strike on the infected host, and beginning C2 communications. Research suggests that there is similarity with the loader and QakBot and IcedID, commodity malware strains that were commonly used by Royal/Conti.

The loader is reported to be under active development, but has been deployed by Royal during a social engineering campaign dubbed "midnight", in which the group used callback phishing and a pretext of a ransomware attack by "midnight" to gain access to systems.

2.4 Money Message leaks MSI keys

A recent attack on computer hardware manufacturer MSI by the ransomware group Money Message has snowballed into a potential supply chain issue. This has happened as part of the data stolen by Money Message during their ransomware attack on MSI, contained two private encryption keys, which are used to sign firmware updates and as a UEFI boot guard key.

This is alarming as the keys could be used to sign fake firmware/updates and deliver malware to devices, with them appearing entirely legitimate. This is a significant issue, but the boot guard key could also be abused to infect certain devices using MSI motherboards . This risk is mitigated slightly, as UEFI updates would normally be installed by a device admin, but threat actors are resourceful and social engineering pretexts imitating MSI or tech support would likely drive user interaction. The issue is further aggravated as it appears that MSI has no easy way to revoke the key across all devices, and MSI isn't being as transparent or communicative as the manufacturer perhaps could. It is also not limited to MSI devices, but also includes third parties devices that use certain MSI hardware.

2.5 Buhti switches it up

The ransomware group Buhti, who have recently exploited vulnerabilities in PaperCut (CVE-2023-27350) have reportedly begun to use a lightly modified version of both LockBit and Babuk's leaked locker code as part of their attacks.

It's not the first time a group has taken advantage of the leaks, with it offering groups the opportunity to have a proven locker with little development effort. It also means that Buhti can now target multiple platforms, despite the group originally targeting Linux systems, they now have lockers which can work on Windows, Linux and virtual environments.

3 Other notable highlights in brief

3.1 Goodbye CryptBot, NodeStealer and Snake

The past few weeks have involved action by the security community and law enforcement in combatting organized crime groups and the greater cybercrime ecosystem.

Firstly, Google began legal action against the Pakistan based operators of the infostealer CryptBot, allowing them to seize and takedown infrastructure being used by the malware, disrupting its operations. Google has taken the lead on this operation, likely due to the fact that the operators of CryptBot were distributing their malware via fake updates and versions of Google Earth and Google Chrome.

Meta has also taken action to disrupt another infostealer called NodeStealer, issuing takedown requests to malicious domains hosting the malwares C2 infrastructure. The action has seemingly wiped out all activity associated with the Vietnam-based NodeStealer operators since late February.

CISA has shone a light on the sophisticated Snake implant, a vital part of Russia's security services arsenal, and has previously been used to target NATO nations and for wide reaching cyber espionage operations. CISA's report is highly detailed, and provides valuable insight for defenders on the malware's operation and infrastructure, allowing defenses to be put in place and Snake infections to be mitigated.

3.2 Does this Android look infected?

An organized criminal network called 'Lemon Group' is reportedly behind the mass pre-infection of cheap Android devices, giving attackers the ability to spy on users, intercept their information and be abused for spam campaigns. This campaign involved devices which have an OS tainted with Guerilla malware, and while this tactic is not new, the scale of this operation is shocking, with nearly nine million devices involved.

3.3 Brute Print

Passwords, especially those short in length can be guessed through a technique called brute forcing, which is essentially just guessing the alphanumeric combinations recursively until a credential is accepted. Biometric readers on smartphones have been widely adopted by manufacturers, and help solve this problem, as you can have a complex password/passphrase, while still being able to unlock your phone quickly with the touch of a finger.

This is an ideal security solution as unique and physical characteristics are required to unlock the device, but researchers have unveiled a new technique that could give an attacker with access to the device a way to brute force the fingerprint reader. The technique works by fuzzing (guessing) the possible combinations of unique fingerprint identifiers, while also bypassing attempt limits. At current, the technique is limited to certain hardware options, and is obviously limited to attackers who have physical access to the phone. Of course, you could just use a high enough resolution photo of someone's fingerprint and some glue to achieve the same result (results may vary).

4 Threat data highlights

4.1 Vulnerabilities & Exploits

What is everyone talking about? The following is a list of the top five discussed vulnerabilities on social media across May. *Data is provided by cvetrends.com*

1. CVE-2023-27350
PaperCut
As discussed in last months report, this vulnerability in PaperCut is being actively exploited by various threat actors, including ransomware groups. Make sure to patch!

2. CVE-2023-24932
Windows
This vulnerability was recently patched by Microsoft, but is being actively exploited and can allow an authenticated attacker to bypass secure boot.

3. CVE-2023-29336
Windows
Another actively exploited vulnerability that was recently patched by Microsoft, this one is an escalation of privilege vulnerability, that can give an attacker SYSTEM level access.

4. CVE-2023-32409
Apple
This vulnerability has been patched along with a handful of others by Apple, but could allow a remote attacker to escape from a web content sandbox.

5. CVE-2023-29324
Windows
This security bypass vulnerability is related to a different vulnerability in Microsoft Outlook (CVE-2023-23397), which allows an attacker to craft an Outlook event/reminder that can result in NTLM credential theft. Microsoft's Threat Intelligence team have assessed that a Russian threat actor has used the vulnerability in targeted attacks against several organizations in the European government, transportation, energy, and military sectors, for approximately a year.

What have we seen?

The following observations are based on telemetry data available to WithSecure™:

There has been a significant increase in **CVE-2023-28274** exploitation, which is a Windows Win32K vulnerability, that can allow an attacker to escalate their privilege to the SYSTEM level. This vulnerability was only introduced in April, but has quickly been weaponized and exploited by threat actors.

There has been a notable increase in **CVE-2023-21716** exploitation, which is a Microsoft Word vulnerability, that can be abused by attackers delivering a specially crafted RTF file that can result in the execution of malicious code.

What vulnerabilities are being newly exploited?

The following are additions to CISA’s known exploited vulnerability catalog. Six have received a “CRITICAL” CVSS rating.

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-28771	Zyxel (Firewalls)	Critical	Zyxel ATP, USG FLEX, VPN, and ZyWALL/USG firewalls allow for improper error message handling which could allow an unauthenticated attacker to execute OS commands remotely by sending crafted packets to an affected device.
CVE-2023-2868	Barracuda Email Security Gateway	Critical	Barracuda Email Security Gateway (ESG) appliance contains an improper input validation vulnerability of a user-supplied .tar file, leading to remote command injection.
CVE-2023-25717	Ruckus Wireless	Critical	Ruckus Wireless Access Point (AP) software contains an unspecified vulnerability in the web services component. If the web services component is enabled on the AP, an attacker can perform cross-site request forgery (CSRF) or remote code execution (RCE). This vulnerability impacts Ruckus ZoneDirector, SmartZone, and Solo APs.
CVE-2016-3427	Oracle Java SE, Jrockit	Critical	Oracle Java SE and JRockit contains an unspecified vulnerability that allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Java Management Extensions (JMX). This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.
CVE-2016-8735	Apache Tomcat	Critical	Apache Tomcat contains an unspecified vulnerability that allows for remote code execution if JmxRemoteLifecycleListener is used and an attacker can reach Java Management Extension (JMX) ports. This CVE exists because this listener wasn't updated for consistency with the Oracle patched issues for CVE-2016-3427 which affected credential types.
CVE-2021-45046	Apache Log4j2	Critical	Apache Log4j2 contains a deserialization of untrusted data vulnerability due to the incomplete fix of CVE-2021-44228, where the Thread Context Lookup Pattern is vulnerable to remote code execution in certain non-default configurations.
CVE-2016-6415	Cisco IOS, IOS XR, IOS XE	High	Cisco IOS, IOS XR, and IOS XE contain insufficient condition checks in the part of the code that handles Internet Key Exchange version 1 (IKEv1) security negotiation requests. contains an information disclosure vulnerability in the Internet Key Exchange version 1 (IKEv1) that could allow an attacker to retrieve memory contents. Successful exploitation could allow the attacker to retrieve memory contents, which can lead to information disclosure.
CVE-2021-3560	Red Hat Polkit	High	Red Hat Polkit contains an incorrect authorization vulnerability through the bypassing of credential checks for D-Bus requests, allowing for privilege escalation.
CVE-2010-3904	Linux Kernel	High	Linux Kernel contains an improper input validation vulnerability in the Reliable Datagram Sockets (RDS) protocol implementation that allows local users to gain privileges via crafted use of the sendmsg and recvmsg system calls.
CVE-2023-29336	Microsoft Win32k	High	Microsoft Win32k contains an unspecified vulnerability that allows for privilege escalation up to SYSTEM privileges.
CVE-2023-1389	TP-Link Archer AX21	High	TP-Link Archer AX-21 contains a command injection vulnerability that allows for remote code execution.
CVE-2023-21839	Oracle WebLogic Server	High	Oracle WebLogic Server contains an unspecified vulnerability that allows an unauthenticated attacker with network access via T3, IIOP, to compromise Oracle WebLogic Server.
CVE-2004-1464	Cisco IOS	Medium	Cisco IOS contains an unspecified vulnerability that may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases, Hypertext Transport Protocol (HTTP) access to the Cisco device.
CVE-2023-21492	Samsung Devices	Medium	Samsung mobile devices running Android 11, 12, and 13 contain an insertion of sensitive information into log file vulnerability that allows a privileged, local attacker to conduct an address space layout randomization (ASLR) bypass.
CVE-2014-0196	Linux Kernel	Medium	Linux Kernel contains a race condition vulnerability within the n_tty_write function that allows local users to cause a denial-of-service or gain privileges via read and write operations with long strings.
CVE-2015-5317	Jenkins UI	Medium	Jenkins User Interface (UI) contains an information disclosure vulnerability that allows users to see the names of jobs and builds otherwise inaccessible to them on the ""Fingerprints"" pages.
CVE-2023-32409	Apple OS's	Under Review	Apple iOS, iPadOS, macOS, tvOS, watchOS, and Safari WebKit contain an unspecified vulnerability that can allow a remote attacker to break out of the Web Content sandbox.
CVE-2023-28204	Apple OS's	Under Review	Apple iOS, iPadOS, macOS, tvOS, watchOS, and Safari WebKit contain an out-of-bounds read vulnerability that may disclose sensitive information.
CVE-2023-32373	Apple OS's	Under Review	Apple iOS, iPadOS, macOS, tvOS, watchOS, and Safari WebKit contain a use-after-free vulnerability that leads to code execution.

5 Research highlights

WithSecure™ Intelligence identified attacks which occurred in late March 2023 against internet-facing servers running Veeam Backup & Replication software. Research indicates that the intrusion set used in these attacks has overlaps with those attributed to the FIN7 activity group. It is likely that initial access and execution was achieved through a recently patched Veeam Backup & Replication vulnerability, CVE-2023-27532.

FIN7 is a financially motivated cybercrime group with roots dating back to mid-2010s. The group has been involved in several high-profile and large-scale attacks over the years. The group's tradecraft and modus operandi have evolved over its multi-year history, developing new tools, expanding their operations, as well as affiliating with other threat actors.

The full WithSecure™ blogpost provides an analysis of intrusions we have observed, along with a timeline of these attacks.

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.