Threat Highlights Report

October 2022

WITH secure

Contents

Foreword

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

This month's report contains a look at attacks against organizations in the the US Defense Industrial Base sector, likely committed by the China-backed threat actor APT27. As well as the widespread exploitation of a critical vulnerability in 3 Fortinet products, and look at the evolution of Ducktail.

We assess the ransomware threat landscape, which includes high-profile attacks on the automobile showroom owner Pendragon by LockBit and attacks on Ukrainian and Polish organizations by "Prestige". We also examine updates to both BlackByte and Black Basta, who continue to expand their tactics, techniques and procedures.

We also take a brief look at several issues, including a study examining the prevalence of malicious code on GitHub, new Microsoft Exchange vulnerabilities, new efforts by LinkedIn to combat fake profiles, the abuse of Chromium's application mode for phishing, and other reports and advisories from the cybersecurity community.

Ziggy Davies, Threat Intelligence Analyst.

1 Monthly highlights

1.1 Military targets attacked

The United States (US) Cybersecurity and Infrastructure Security Agency (CISA) have released an alert regarding attacks on a target within the Defense Industrial Base (DIB). The DIB sector includes organizations and companies that conduct research and development, design, production, delivery, and maintenance of weapon systems and associated technology for the US military.

CISA and a private third party were tasked with investigating intrusions into the network of the DIB organization, with the response occurring between November 2021 and January 2022. The first signs of compromise relate to the organization's Microsoft Exchange Server, though CISA explains that the "*initial access vector is unknown*". The attack involved various elements:

- Compromise of an admin account and access to the EWS API
- Use of command shell to enumerate the network and discover sensitive data ready for exfiltration
- Use of the open-source toolkit Impacket on another system, in an attempt to achieve lateral movement
- Exploitation of numerous Microsoft Exchange vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) to install the well-known web shell "China Chopper" and Remote-Access Trojan (RAT) HyperBro

Regarding the usage of Impacket, CISA state:

"*The APT cyber actors used existing, compromised credentials with Impacket to access a higher privileged service account used by the organization's multifunctional devices. The threat actors first used the service account to remotely access the organization's Microsoft Exchange server via Outlook Web Access (OWA) from multiple external IP addresses; shortly afterwards, the actors assigned the Application Impersonation role to the service account by running the following PowerShell command for managing Exchange…*

```
powershell add-pssnapin *exchange*;New-
ManagementRoleAssignment
- name:"Journaling-Logs"
-Role:ApplicationImpersonation
-User:<account>
```

This command gave the service account the ability to access other users' mailboxes".

Regarding the usage of the customer tool CovalentStealer, CISA state:

"*CovalentStealer is designed to identify file shares on a system, categorize the files, and upload the files to a remote server. CovalentStealer includes two configurations that specifically target the victim's documents using predetermined files paths and user credentials. CovalentStealer stores the collected files on a Microsoft OneDrive cloud folder, includes a configuration file to specify the types of files to collect at specified times and uses a 256-bit AES key for encryption*".

CISA has produced a separate report on the custom exfiltration tool, CovalentStealer.

The alert goes on to provide a detailed Mitre ATT&CK framework relating to the compromise, as well as detailed advice regarding mitigation and best practices.

WithSecure™ Insight

While CISA has not attributed this attack to a specific threat actor, they have described them as an Advanced Persistent Threat (APT). The targeting of a DIB organization is indicative of an APT that is acting in the interests of a nation-state, and one who is interested in uncovering data related to the development of military assets and weapon systems. This, in combination with the usage of China Chopper and HyperBro, are indicators that this compromise was possibly carried out by APT27 (aka TG-3390, Emissary Panda, BRONZE UNION), a Chinese group who have been active since 2010 that target organizations in the aerospace, government, defense, technology, energy, manufacturing and gambling sectors.

The use of the new custom exfiltration tool CovalentStealer is novel, and the analysis performed by CISA is invaluable. Of note, however, is the lack of prevalence related to this malware, with it seemingly being used only on this occasion, with very few samples being publicly available, and no intelligence to suggest its wider adoption.

What can you do?

CISA has provided a long list of useful mitigation advice and recommendations, most of which focus on the technical aspect of this incident and the detection of anomalous activity. From an organizational perspective, we suggest:

- Ensure that vulnerabilities are patched, especially those which are known to be actively exploited.
- Continually assess your attack surface, and monitor for the necessity of patching or mitigations, either through an in-house process or the employment of an attack surface monitoring service/provider.
- Make use of endpoint protection services, that are effectively able to detect anomalous and suspicious activity.
- Consider the information security CIA triad (confidentiality, availability, integrity), when storing data, and assess what the result and risk will be if data is compromised.

1.2 Fortinet vulnerability under active attack

On the 10th of October Fortinet produced an advisory regarding a known vulnerability in its FortiOS, FortiProxy and FortiSwitchManager products, which is tracked as CVE-2022-40684 and scores a 9.8 CRITICAL CVSS score.

The vulnerability, which is defined as an authentication bypass using an alternative path or channel can "*allow an unauthenticated attacker the opportunity to perform operations on the administrative interface via specially crafted HTTP(S) requests*". Fortinet state that the vulnerability is being actively exploited, and numerous proof-of-concept (POC) exploits are available in the wild, including the ability to add SSH keys to the admin account, allowing SSH access and therefore compromise of the system.

Fortinet has released patched versions of the vulnerable products, which include:

- FortiOS version 7.2.2 or above
- FortiOS version 7.0.7 or above
- FortiProxy version 7.2.1 or above
- FortiProxy version 7.0.7 or above
- FortiSwitchManager version 7.2.1 or above
- FortiSwitchManager version 7.0.1 or above
- FortiOS version 7.0.5 B8001 or above for FG6000F and 7000E/F series platforms

WithSecure™ Insight

This vulnerability is gaining a lot of attention and is currently the second most discussed vulnerability on Twitter, and internet traffic monitoring/security company GreyNoise have tracked an increase in IPs mass scanning for the vulnerability, indicating threat actor activity, seeking to map out possible targets.

Fortinet products are prevalent throughout the IT sector, and previous Fortinet vulnerabilities have been widely exploited and targeted by threat actors, due to the wide array of organizations using the products. As above, there is growing evidence that threat actors are seeking to add CVE-2022-40684 exploits to their arsenal, and this is likely to develop into a bigger issue, if systems fail to be patched.

While patched versions are available, it is possible that many systems will take time to rectify and remain vulnerable while patch management plans are enacted.

What can you do?

If you or a trusted third party are using Fortinet products, you must first assess whether you are using a vulnerable system, these include:

- FortiOS : 7.2.1, 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0
- FortiProxy : 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, and
- FortiSwitchManager : 7.2.0, 7.0.0

If a vulnerable system is present, then Fortinet is recommending that you search for the following indicator of compromise in the devices logs, as well as checking for the presence of malicious admin accounts:

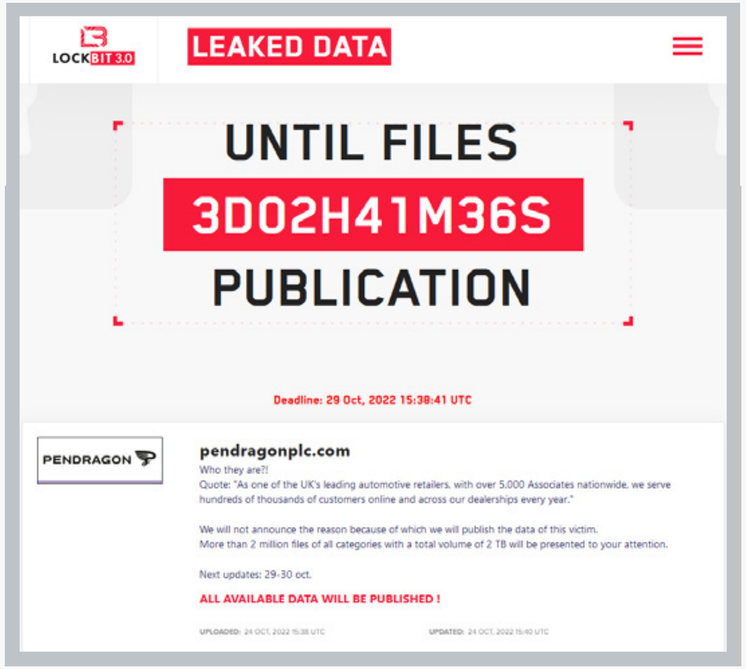
```
user="Local_Process_Access"
```

As detailed above, patches are available for all vulnerable products, if a product cannot be updated, then the HTTP(S) administrative interface should be disabled, until a time when the product can be patched.

2 Ransomware: Trends and notable reports

2.1 Automobile dealer group Pendragon held to $60m ransom

Pendragon, who own about 160 automobile showrooms across the United Kingdom (UK) have reportedly been compromised by ransomware titans LockBit 3.0.



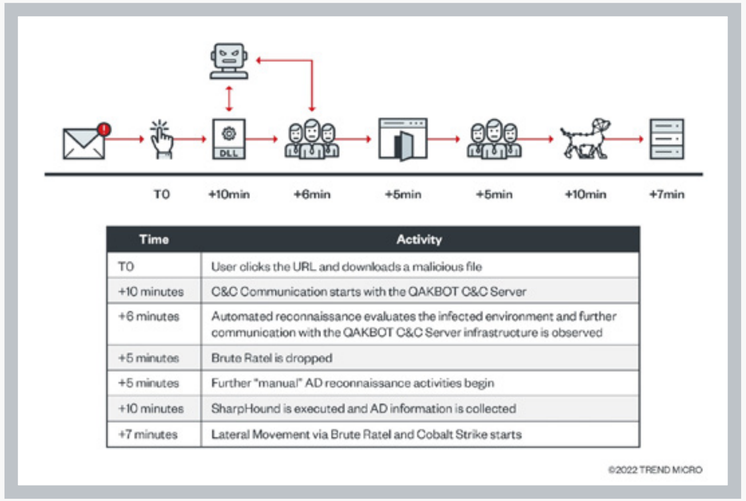
Reports suggest that Pendragon is refusing to pay the ransom and negotiate with the criminal group, with LockBit's leak site detailing that 2TB of data belonging to the firm will be released on the 29th of October 2022. Pendragon are working with law enforcement, the UK NCSC and their own IT security services to resolve the breach.

2.2 Black Basta ransomware utilizes Qakbot, Brute Ratel and Cobalt Strike

A recent case involving Black Basta ransomware has been analyzed by researchers at Trend Micro, with the incident beginning with Qakbot malicious file user interaction, and involving Brute Ratel as a secondary payload.

The adoption of the adversary emulation framework Brute Ratel by threat actors has dramatically increased in the past month, due to the unfortunate leaking and sale of cracked versions on hacker forums/marketplaces.

Trend Micro have mapped the attack timeline as follows:



Time	Activity
T0	User clicks the URL and downloads a malicious file
+10 minutes	C&C Communication starts with the QAKBOT C&C Server
+6 minutes	Automated reconnaissance evaluates the infected environment and further communication with the QAKBOT C&C Server infrastructure is observed
+5 minutes	Brute Ratel is dropped
+5 minutes	Further "manual" AD reconnaissance activities begin
+10 minutes	SharpHound is executed and AD information is collected
+7 minutes	Lateral Movement via Brute Ratel and Cobalt Strike starts

2.3 “Prestige” ransomware hits Poland and Ukraine

Microsoft’s Threat Intelligence Center (MSTIC) has identified a new ransomware variant dubbed “Prestige” that has struck organizations in the transportation and logistic sectors within Poland and Ukraine.

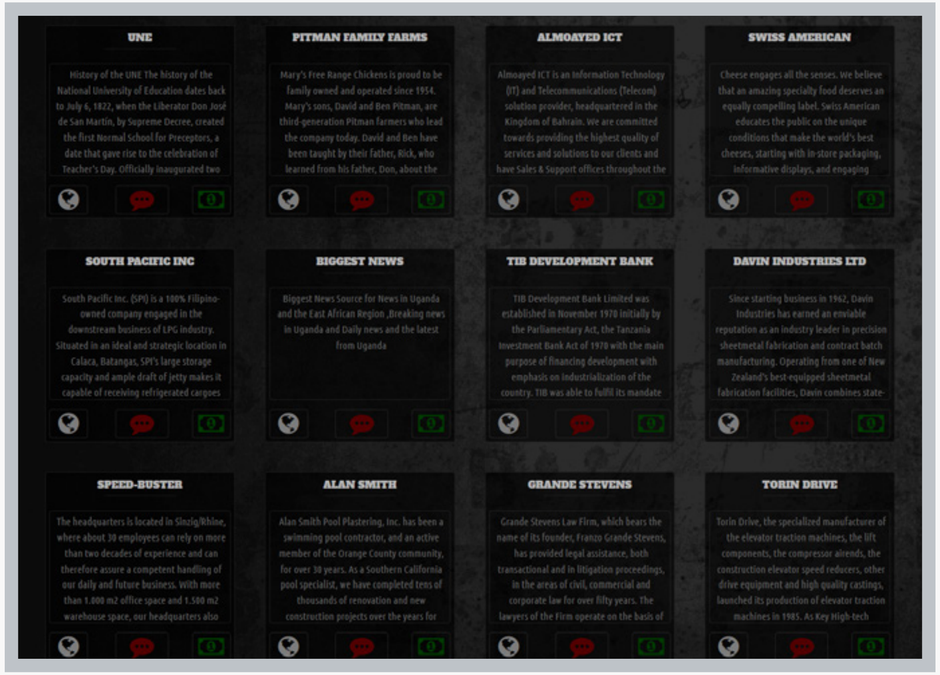
MSTIC has not attributed the campaign to a specific group or nation, but it appears that in all cases, the threat actor had prior access to high-level credentials, likely gained in earlier compromise and the victimology overlaps with the interests of Russian-backed threat groups.

MSTICS report contains useful information regarding recommended customer actions and mitigation, which include adopting defenses against the open-source tool Impacket, which was used in many instances.

2.4 BlackByte abuse vulnerable drivers to bypass security

BlackByte, a group active since October 2021, took a brief hiatus but are apparently back and now operate a leak site that imitates LockBit’s, whereby victims can interact with the group and pay varying ransom amounts to delay the leaking of data, download the data or destroy it.

Sophos are reporting the use of the “bring your own vulnerable driver” (BYOVD) technique by BlackByte, an attack technique which has recently been abused by threat actors to evade/bypass security products and Sophos’ report goes into technical detail on how BlackByte attempt to bypass EDR and aggravate analysis by exploiting CVE-2019-16098, a vulnerability within MSI Afterburner.



3 Other notable highlights in brief

3.1 GitHub rife with malicious code

A study by academics at Leiden University in the Netherlands has examined 47313 repositories on GitHub that claim to contain POC exploit code for known vulnerabilities, and has found that about 10% contain some form of malicious code.

The study concentrated on code which:

- Could connect with known malicious IPs
- Contains obfuscated hexadecimal or base64
- Contains known trojanized binaries

While many of the examples found were innocuous and contained jokes, others were designed to infect the user with RATs, infostealers, crypto-miners and Cobalt Strike.

3.2 Two new Microsoft Exchange vulnerabilities being actively exploited

The team at Vietnamese cybersecurity company GTSC recently detected 2 new vulnerabilities in Microsoft Exchange and subsequently submitted them to Trend Micro's Zero Day Initiative bug-bounty reporting platform.

Microsoft have subsequently responded and the vulnerabilities have been assigned CVE-2022-41040 and CVE-2022-41082, and described the in-the-wild exploitation as being "*limited*" and say:

"*CVE-2022-41040 can enable an authenticated attacker to remotely trigger CVE-2022-41082. However, authenticated access to the vulnerable Exchange Server is necessary to successfully exploit either vulnerability, and they can be used separately*".

While prior access is required to exploit these vulnerabilities, the level of authentication does not have to be elevated, and low-level credentials such as these can be gained through techniques such as password spraying and purchase of previously compromised credentials on hacker marketplaces, meaning future exploitation of these exploits is likely, if not mitigated against.

3.3 FBI issue Iran hack-and-leak warning

The FBI have issued a Private Industry Notification (PIN) regarding an ongoing hack-and-leak campaign conducted by an Iranian cyber group called Emennet Pasargad, who have previously been linked to election interference and the spread of disinformation in the Israel and the US.

The report describes Emennet Pasargad's activity as being:

"*...targeted (against) entities primarily in Israel with cyber-enabled information operations that included an initial intrusion, theft and subsequent leak of data, followed by amplification through social media and online forums, and in some cases the deployment of destructive encryption malware*".

The group also make use of false-flag tactics, and leak data under the names of fake organizations and individuals, in an attempt to aggravate attribution and create a narrative in-line with their interests.

Iran have been in the cyber-news a lot lately, especially because if their recent attacks against Albania (discussed in last month's THR), and this report by the FBI further highlights Iran's ongoing hostile cyber activity.

3.4 LinkedIn addresses fake profiles

LinkedIn has become a popular platform for threat actors, who often create networks of fake profiles, which are then used for social engineering campaigns. These profiles are often quite convincing, and either involve the imitation of genuine people, or entirely fictional personas that use AI generated profile pictures.

LinkedIn is now taking steps to better detect these profiles, and combat this problem. There efforts include:

- "About this profile" feature, that allows other users to check on profile creation dates and whether the account is using a verified phone number or work associated email address.
- Creation of a deep-learning-based model to help detect the usage of AI generated profile images, that are often associated with fake/malicious accounts.
- Adding warnings to certain direct messages, so that users are aware of potential risks, such as communicating outside of LinkedIn and also alerted to suspicious content.

3.5 Abusing Chromium's application mode to phish

Security researcher mr.d0x has released research on a novel phishing attack technique which involves the abuse of Chromium browsers application mode. Mr.dox says:

"*Chromium-based browsers such as Google Chrome and Microsoft Edge support the --app command line flag. This flag will launch a website in application mode which does several things*:

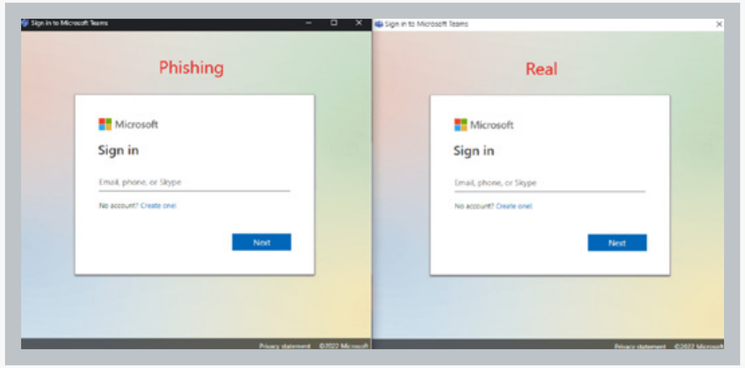
- *Causes the site to be launched in a separate browser window.*
- *The launched window is given a desktop application appearance r.ather than a browser appearance.*
- *The Windows Taskbar displays the website's favicon rather than the browser's icon.*
- *Launches the website while hiding the address bar".*

Example commands are provided:

```
# Chrome
C:\Program Files\Google\Chrome\Application>-
chrome.exe --
app=https://mrd0x.com

# Microsoft Edge
c:\Program Files (x86)\Microsoft\Edge\
Application>msedge.exe --
app=https://mrd0x.com
```

Mr.dox goes on to suggest that this technique could be used to deliver .lnk shortcut files via phishing, which could trick users into inputting credentials as they will imitate legitimate services such as Microsoft office login prompts or application login portals.



3.6 Healthcare sector report on commonly abused tools

The US Department of Health and Human Services (HSS) have released a slide deck discussing some commonly abused tools, that are often used in attacks against the health-care sector (among others). The report discusses:

- Cobalt Strike
- Powershell
- Mimikatz
- Sysinternals
- Anydesk, and
- Brute Ratel

This report is very useful, and describes at both a strategic and technical level, how each tool can be abused by threat actors, as well as providing insight in to some of the threat actors leveraging the tools.

NB: This pdf has since been removed from the HHS site without reasoning, the hyperlink included is provided via a capture on the Wayback Machine. The report is TLP:White, so we are unsure why the file was pulled, but believe it is valuable and are therefore grateful that it has been immortalized by the internet archive.

3.7 Joint report outlines top vulnerabilities exploited by China

A joint report by the NSA, CISA and FBI has collated the top vulnerabilities that are known to have been exploited by China-backed threat actors since 2020. These include:

Table I: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitrary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Execution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitrary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution
Apache HTTP Server	CVE-2021-41773	Path Traversal

The reports appendix does an excellent job of breaking down each vulnerability, explaining how it can be exploited and suggesting mitigation, and in particular highlights the importance of having and maintaining a patch management process.

3.8 Zimbra vulnerability widely exploited

The critical vulnerability CVE-2022-41352 in popular software suite Zimbra is reportedly being actively exploited. The vulnerability occurs due to a loophole in the CPIO file archiver utility used by Zimbra on some installations, which allows malicious .cpio, .tar and .rpm files to be sent by threat actors as a way to plant files and achieve RCE on vulnerable systems.

CISA have previously reported that Zimbra is an attractive target for threat actors, and is under active exploitation. On the 11th of October 2022, Zimbra released a security patch to address the issue, and also highlighted that systems using PAX would not be vulnerable.

4 Threat data highlights

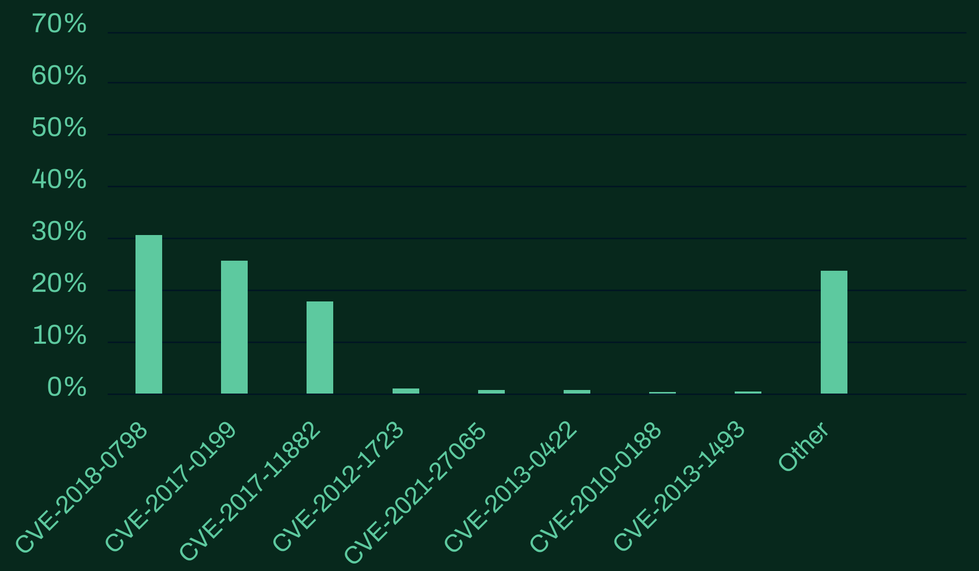
4.1 Exploits

This month, we will make a comparison of vulnerability exploitation telemetry/data across the following data points for October:

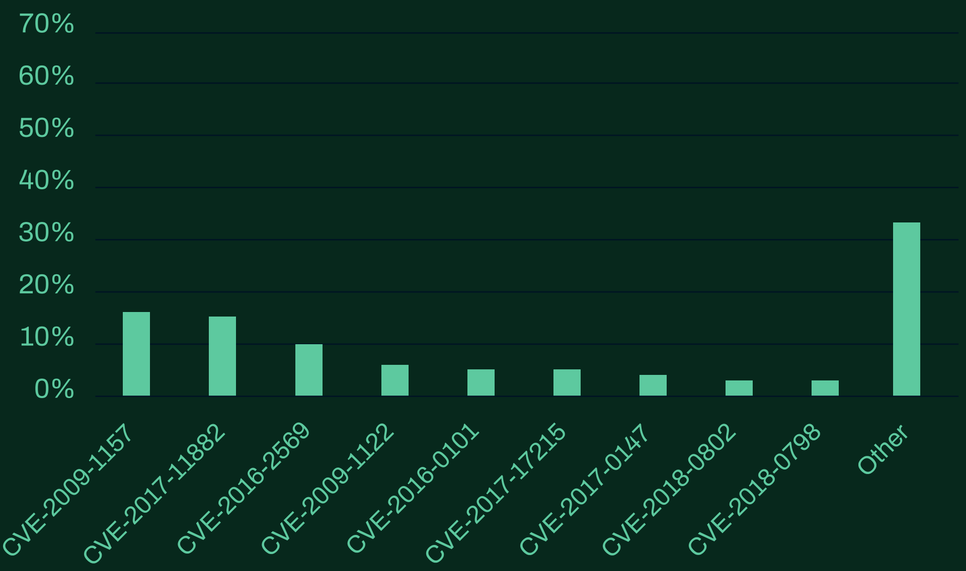
- Prevalence of vulnerabilities regardless of year of CVE origin
- Prevalence of vulnerabilities which originate from 2022 CVE's

We include WithSecure's own proprietary data, and data available from VirusTotal's file submission data.

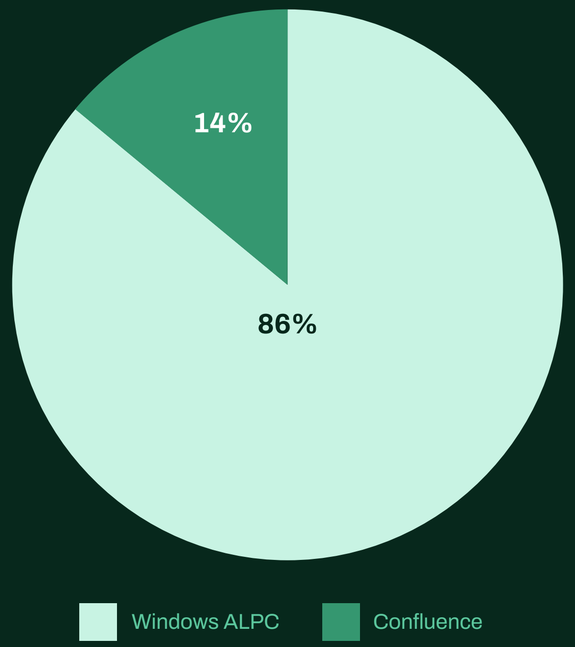
Internal Telemetry –
October vulnerabilities regardless of year of CVE



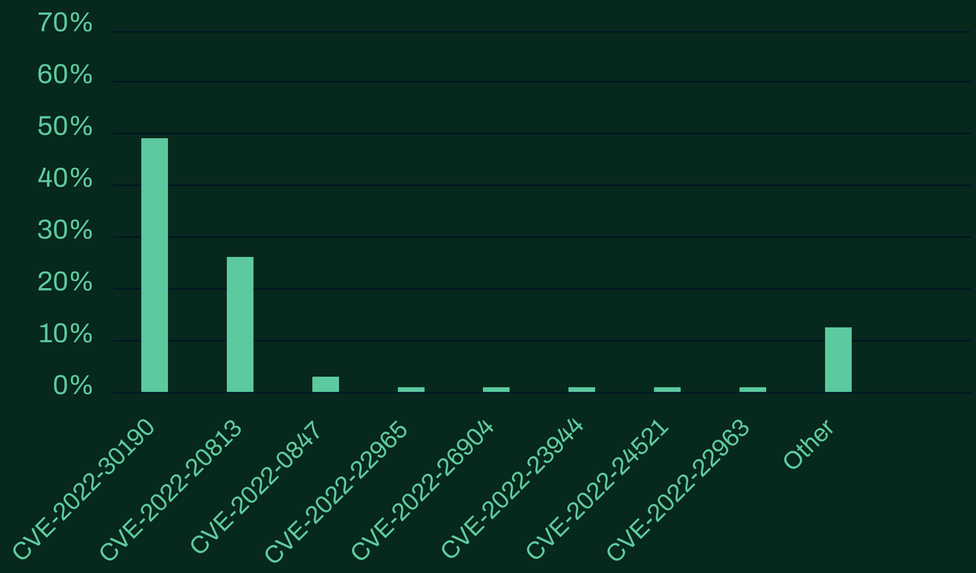
Expanded Telemetry –
October vulnerabilities regardless of year of CVE



Internal Telemetry – October vulnerabilities with CVE's from 2022



Expanded Telemetry – October vulnerabilities with CVE's from 2022



Top CVE's from October telemetry breakdown TAGS

CVE-2018-0798: An old but very popular vulnerability, that involves the use of weaponized .doc and .rtf files to achieve RCE. `Initial Access` `RCE`

CVE-2017-11882: An even older, but still very popular vulnerability, once again it involves the use of weaponized office files that when executed can achieve RCE. `Initial Access` `RCE`

CVE-2022-30190: This vulnerability, which is also known as "Follina" made big waves when exploits first appeared. It involves specially crafted office files, and can result in RCE with little user interaction. `Initial Access RCE`

CVE-2022-20813: A vulnerability in some CISCO products, which can be exploited to intercept sensitive data. `MITM`

CVE-2021-27065: One of many Microsoft Exchange vulnerabilities that is often used in a chain with CVE-2021-26855 to achieve RCE. `RCE`

CVE-2021-44228: The chaos caused by this vulnerability, which is often referred to as log4shell was immense. This is due to the prevalence of the library in various java products, making it widespread. Exploits are trivial and can result in RCE. `Initial Access RCE`

CVE-2021-40444: A Microsoft Office MSHTML Remote Code Execution Vulnerability, that doesn't make use of macro's to achieve RCE, making it quite unique and a particularly useful way to gain initial access. `Initial Access RCE`

CISA's known exploited vulnerabilities catalog

For October, CISA have added 12 vulnerabilities to their known exploited vulnerabilities catalog. These include:

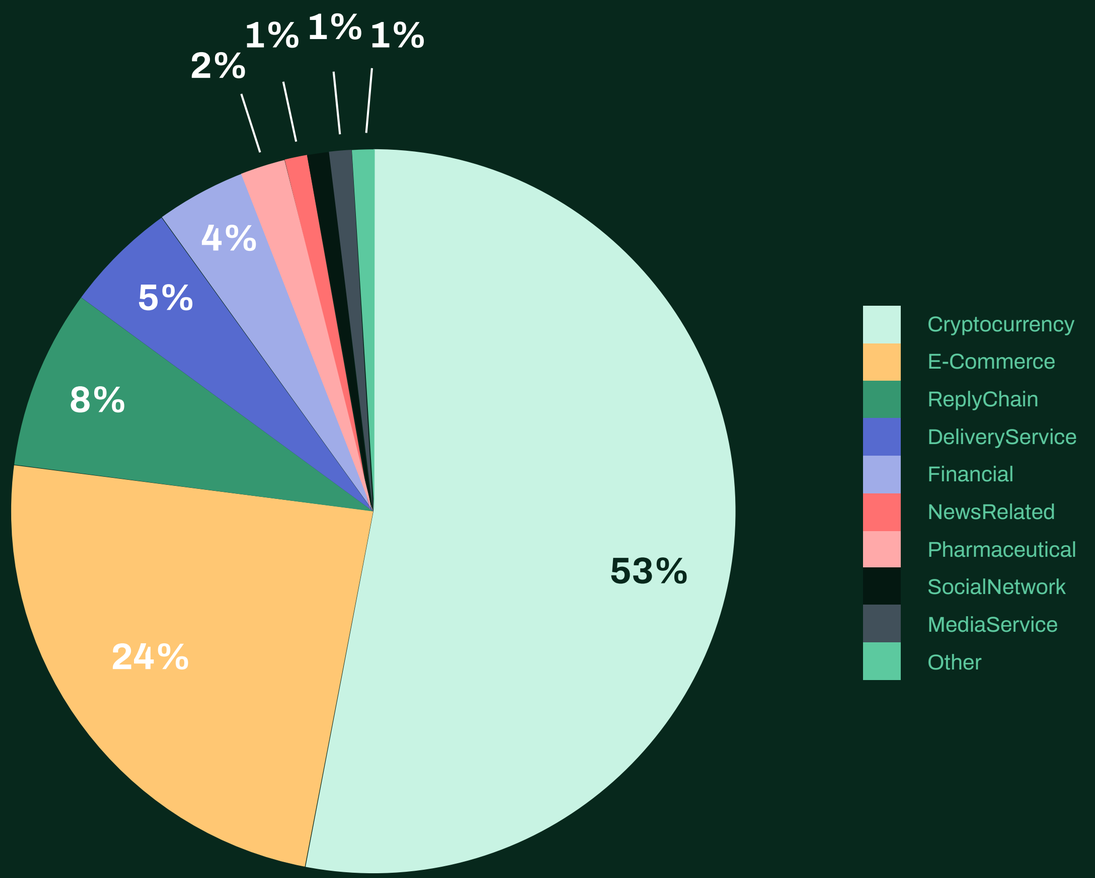
CVE ID	Vendor / Product	What's the vulnerability?
CVE-2022-40684	Fortinet	Multiple Products Authentication Bypass Vulnerability
CVE-2022-41033	Microsoft	Microsoft Windows COM+ Event System Service Privilege Escalation Vulnerability
CVE-2022-41352	Zimbra	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability
CVE-2021-3493	Linux	Linux Kernel Privilege Escalation Vulnerability
CVE-2020-3433	Cisco	Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability
CVE-2020-3153	Cisco	Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability
CVE-2018-19323	GIGABYTE	GIGABYTE Multiple Products Privilege Escalation Vulnerability
CVE-2018-19322	GIGABYTE	GIGABYTE Multiple Products Code Execution Vulnerability
CVE-2018-19321	GIGABYTE	GIGABYTE Multiple Products Privilege Escalation Vulnerability
CVE-2018-19320	GIGABYTE	GIGABYTE Multiple Products Unspecified Vulnerability
CVE-2022-42827	Apple	Apple iOS and iPadOS Out-of-Bounds Write Vulnerability
CVE-2022-3723	Google	Google Chromium V8 Type Confusion Vulnerability

4.2 Email threats

In October, cryptocurrency themed spam mail has seen a resurgence being responsible for 53% of all spam messages in our data.

All other types remain typical, with no real movement since last month.

Spam Email themes



WithSecure™ spam data collection

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.

WITH secure