Threat Highlight Report

December 2022

W/TH 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 we look at the breach of LastPass (change your passwords), the US and UK bans on Chinese tech over concerns relating to China's National Intelligence Law, a new commercial spy group called Variston, a threat actor called SCATTERED SPIDER who are targeting telecommunication companies and a problematic vulnerability in Windows.

We look at the ransomware landscape, including a highlight on newcomers Trigona, analysis on a wiper called Ransom-BOGGS that has hit Ukraine, and look into the ransomware attack by the Play ransomware group that took down Rack-Space's exchange hosting.

We also discuss the sale of data harvested from Twitter, critical vulnerabilities in Citrix and Fortinet, a new backdoor used by APT37 and the breach of the FBI's intelligence sharing platform Infraguard.

As ever, we look to WithSecure's telemetry for insight into malware observed, and the top vulnerabilities exploited in the wild as seen by WithSecure™ and CISA's telemetry.

- Ziggy Davies, Threat Intelligence Analyst

1 Monthly highlights

1.1 LastPass security incident

On the 22nd of December, password management company LastPass updated their customers and released a statement saying a "*threat actor copied information from a backup that contained basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service.*"

The breach relates to an earlier compromise that occurred in August, when the threat actor was able to steal source code and some credentials/technical data that was then later abused to further compromise a cloud storage service.

The cloud service reportedly stored the following customer data elements:

- Names
- Billing addresses
- Email addresses
- Telephone numbers
- IP addresses
- Website URL's
- Website usernames (encrypted)
- Passwords (encrypted)
- Secure notes (encrypted)
- Form data (encrypted)

LastPass are keen to point out:

"*These encrypted fields remain secured with 256-bit AES encryption and can only be decrypted with a unique encryption key derived from each user's master password using our Zero Knowledge architecture. As a reminder, the master password is never known to LastPass and is not stored or maintained by LastPass. The encryption and decryption of data is performed only on the local LastPass client.*"

WithSecure™ Insight

The compromise of LastPass is highly problematic as the platform is used by over 25 million people as a password and secret manager, with those passwords now being in the hands of an unknown threat actor, albeit in an encrypted format.

Because the decryption of a LastPass vault is carried out client-side using a user's master password, whether an account should be considered compromised is simply down to the strength of that master password, and whether it can be guessed, brute forced or sprayed using previously leaked credentials. As such, we would suggest that any password stored on LastPass should now be assumed compromised and those passwords reset and never reused. If any other information was stored on LastPass, in the form of secret notes, those should also be considered breached, and you should take steps to remedy the issue. In addition, please always remember to use complex and long passwords, especially your "master" password, and utilize MFA methods such as pattern/number matching authenticator apps or hardware solutions.

1.2 Bans on Chinese equipment

The US and UK are taking action to ban Chinese equipment and technology, over fears that it "*presents a risk to national security*".

The US Federal Communications Commission has adopted new rules which limits the licensing and import of new equipment from the Chinese companies, Dahua, Hikvision, Huawei and ZTE, all of whom have previously been connected with allegations of espionage and cooperation with the Chinese intelligence services.

The UK's position is not as broad and only covers the installation of "*video surveillance cameras" within government estates and sensitive sites, though they have also advised, "to consider whether there are sites outside of the definition of sensitive sites to which they would wish to extend the same risk mitigation*".

WithSecure^{TM} Insight

There have been concerns regarding the use of Chinese technology, hardware, and services since the introduction of China's National Intelligence Law in 2017, article 7 of which allows the Chinese intelligence services to compel businesses registered in China to cooperate and hand over data upon request, regardless of their actual area of operation. This can potentially be used to turn companies like Huawei into intelligence collection conduits. These concerns have been investigated in the past by the FBI, especially with regard to telecommunications equipment in proximity to sensitive locations.

These recent bans issued by the US and UK follow an ongoing trend of treating Chinese companies and their tech with suspicion, especially with regard to their installation in critical national infrastructure and sensitive sites. The companies involved, Dahua, Hikvision, Huawei and ZTE are all highly popular, with Huawei phones accounting for a large proportion of Android mobile phones sold in Europe and Hikvision cameras being widespread in both commercial and consumer applications.

Concerns over the state of relations between the West and China have been raised by analysts who have noted the possibility of enormous geopolitical and economic turbulence in the event of an increase in Chinese hostility towards Taiwan. Almost two thirds of the worlds Microchips are manufactured in Taiwan and disruption of these exports would have severe global ramifications. As any significant geopolitical event ramps up, cyber activity does also.

1.3 Google expose Variston spy group

Google's Threat Analysis Group (TAG) have shared findings relating to the likely development, sale and usage of spyware called Heliconia by Spanish company Variston IT.

TAG claim that the Heliconia framework is able to utilize vulnerabilities in Google Chrome, Mozilla Firefox and Windows Defender and is fully capable of launching payloads to target devices. TAG report that they became aware of Heliconia thanks to an anonymous submission to its bug reporting program, which contained 3 items:

- Heliconia Noise: a web framework for deploying an exploit for a Chrome renderer bug followed by a sandbox escape
- Heliconica Soft: a web framework that deploys a PDF containing a Windows Defender exploit
- Files: a set of Firefox exploits for Linux and Windows

TAG's report goes into deep detail regarding the functionality of Heliconia and an analysis of the frameworks code, which is what leaks the connection between Heliconia and Variston IT, a company that describes itself as offering "*tailor made Information Security Solutions.*" Google have investigated several cases involving commercial spyware operators and consider them a "*harmful ways to conduct digital espionage against a range of groups.*"

WithSecure™ Insight

This investigation by TAG is unfortunately just the tip of the commercial spyware/espionage iceberg and Heliconia (Variston) joins the likes of Pegasus (NSO), Candiru, Quadream, CyberRoot, Paragon and Predator (Intellexa).

These groups often operate in a legal grey area, but the growth of the commercial spyware industry is worrying and something which needs to be closely monitored and guarded against, especially as it appears to be growing more and more each day.

What's most worrying is the use of 0-day exploits by these companies, making defense problematic, though, in this instance, the vulnerabilities in Chrome, Windows, and Firefox have fixes/patches available.

1.4 SCATTERED SPIDER targets Telcos

Researchers from the cybersecurity firm CrowdStrike have released an analysis of a campaign that is directed at telecommunication and business process outsourcing (BPO) companies, for which the end goal appears to be "*to gain access to mobile carrier networks and, as evidenced in two investigations, perform SIM swapping activity.*"

CrowdStrike's report goes into detail regarding the attack pathway of several known intrusions:

Initial Access:
Often gained through social engineering techniques such as the imitation of IT employees, followed up with instructions which navigated targets to credential harvesting pages or to download remote monitoring and management (RMM) software. Attackers would also overcome MFA by tricking targets to divulge one-time passes (OTP) or by using MFA fatigue. Though the attacker has also been seen to leverage an exploit for CVE-2021-35464 a ForgeRock OpenAM application server vulnerability.

Persistence:
Attackers gained access to the organizations MFA console, and added their own devices, associated with the accounts of individuals who had been compromised during initial access. The most common tactic for persistent access, was the use of off-the-shelf remote access tools, with a myriad of different versions being abused.

Reconnaissance and lateral movement:
CrowdStrike state that the attacker is able to operate across Windows, Linux, Google Workspace, AzureAD, M365 and AWS environments as well as accessing cloud environments, with the purpose being to perform reconnaissance and search for information on MFA, VPN and items useful in gaining further access/exploitation. Furthermore the report states that attackers used other techniques to laterally move such as "*domain replication, lateral movement via Windows Management Instrumentation (WMI) using Impacket, SSH tunneling and various remote access tools.*"

CrowdStrike's report also includes a full list of comprehensive indicators of compromise (IOCs).

WithSecure™ Insight

This report by CrowdStrike is of particular interest, as it demonstrates how adversaries can take a fairly simple and non-technical approach to compromise. There have been many instances of high-profile attacks using similar tactics, techniques and procedures (TTPs), such as those perpetrated against Uber, Rockstar, Okta, etc.

A recent high-profile breach of Twitter reportedly released names and associated phone numbers of potentially 400 million accounts. This will almost certainly be of interest to threat actors with intent to perform SIM swap attacks to gain access to high value individuals.

Sometimes 0-day vulnerabilities, custom malware and masses of resources aren't necessary, and adversaries like LAPSUS$ or the unnamed attackers investigated by CrowdStrike know this and are instead using social engineering and coercive psychology to gain initial access, and then abuse legitimate off-the-shelf tooling to carry out their attack, something which can be problematic to defend against. In response to these tactics we recommend:

- Providing all employees with training on phishing, social engineering and the correct use of MFA.
- Enforcement of alternative MFA methods such as number matching or more preferably hardware keys.
- Limiting employee access to sensitive files, systems, etc (principle of least privilege).

1.5 Windows vulnerability is worse than initially thought

In September Microsoft patched a vulnerability tracked as CVE-2022-37958, which is an information disclosure vulnerability in SPNEGO NEGOEX. At the time, Microsoft rated the vulnerability as simply "important", but unfortunately new information has come to light, and this has vulnerability has been recategorized as a "critical" vulnerability, suggesting exploitation is more likely, and that the impact/damage would be higher than initially thought.

A researcher from IBM has released a thorough write up on CVE-2022-37958, which identifies the fact that numerous Windows application protocols make use of SPNEGO NEGOEX such as SMB and RDP, but also potentially SMTP and HTTP, making it a widespread issue. IBM have compared this vulnerability to CVE-2017-0144, a similar vulnerability associated with the NSA developed EternalBlue exploit and infamous WannaCry attacks due to the fact it can utilize SMB, is potentially wormable and can be used to achieve remote code execution (RCE).

WithSecure™ Insight

IBM are not alone in making the comparison between CVE-2022-37958 and CVE-2017-0144, with other reports and online discussions making the comparison to EternalBlue. There are however some important differences to consider as well, such as the fact that EternalBlue was an exploit that was based off a 0-day vulnerability and developed by a nation-state group, whereas this new vulnerability has already been fixed and exploitation is described as requiring a "*high complexity.*"

There are however videos of proof-of-concept exploits surfacing and it will likely not be long before this vulnerability is being adopted by a wide range of adversaries as part of their arsenal. Thankfully, the issue was patched in September, but as always, this will only be the case if patch management plans are being followed and updates are installed in a timely manner, as such, we would recommend:

- Ensuring that you have a thorough patch management plan, that is enacted in a timely and risk averse manner.
- Prioritize this and other "critical" vulnerabilities, due to the elevated risk they present.
- Conduct an assessment of your attack surface, and ensure that any services such as SMB and RDP are properly protected.
- Make use of security products, such as endpoint protection.

2 Ransomware: Trends and notable reports

December has been a typical month for ransomware incidents, with 224 ransomware related incidents occurring during the month (based on ransomware group leak site data). With the most prevalent groups being; LockBit 3.0, Royal, Alphv (BlackCat), Snatch, Play, BianLian, Hive, Cuba, Ragnar Locker and BlackByte. BianLian's activity is of specific interest, as the group have conducted almost half (45%) of their attacks in December, a rapid uptick since their origin in July.

2.1 RansomBOGGS

The war in Ukraine rages on, and so does the cyber campaign against the nation with a new "ransomware" variant emerging called RansomBOGGS. This campaign was detected and reported by ESET, who have suggested the group responsible is Sandworm a Russian adversary connected to the GRU, who have continually attacked Ukraine, both pre and post the 2022 invasion.

The ransomware is written in the .NET framework, and code used in the attack reportedly bears a striking resemblance to previous attacks involving Industroyer2 by Sandworm, suggesting this malware has been developed by the same team and is simply part of the ongoing cyber warfare campaign against Ukraine orchestrated by Russia. The use of a ransom note with numerous mentions of the film Monsters Inc. is somewhat unusual though, perhaps they're just fans of the franchise but we doubt Pixar will appreciate the link!

2.2 Ikea struck by Vice Society

The flatpack furniture titan Ikea have reported that their franchises in Kuwait and Morocco have been struck by the Vice Society ransomware group. Ikea appear keen to note that these franchises are independent from the rest of the company, and the wider Ikea network is not part of the attack.

Vice Society have been highly active in the ransomware landscape since June 2021, with 130 victim profiles appearing on their dark web leak site since that time. The groups victimology is somewhat unusual, and their focus is ordinarily on educational establishments, something which makes them fairly unique within the landscape, and suggests that the attack on Ikea is opportunistic, rather than particularly targeted.

2.3 Guatemala hit by Onyx

Onyx, a ransomware variant built using the widely available Chaos ransomware builder has reportedly been used against Guatemala's foreign ministry. Onyx are a group who have been active since late April 2022, and have attacked 28 organizations, across different nations and sectors, suggesting they are a purely opportunistic threat actor.

2.4 Trigona launch leak site

A ransomware group who had previously gone unnamed have recently created a website on the dark web and branded themselves "Trigona". The ransomware has reportedly been in usage since early 2022, and while further details regarding the operation are scant, the group are clearly investing a lot in their infrastructure, so expect to hear more in the coming months!

2.5 Rackspace attack causes widespread issues

The San Antonio cloud computing company Rackspace have experienced a ransomware attack which brought down the Microsoft Exchange hosting for those customers using the service. Unfortunately, it took quite some time for Rackspace to recover from the attack, and they are still working on recovering the data of those customers who may need it. An investigation by CrowdStrike, has concluded that the initial access was a gained through a new method called OWASSRF, which involves the chaining of two exploits (CVE-2022-41080 and CVE-2022-41082) to trigger remote code execution (RCE) via Outlook Web Access (OWA), and apparently is able to bypass the mitigations provided by Microsoft regarding ProxyNotShell exploits. CrowdStrike have also attributed the attack and technique to ransomware newcomers Play, who despite only appearing in December 2022, have managed to strike at least 35 organizations.

3 Other notable highlights in brief

3.1 Twitter data breach exposed 5-400 million phone numbers

A vulnerability in the social media platform Twitter, which was first reported via HackerOne in January 2022, is reportedly much worse than initially thought with multiple hackers/groups having accessed the data.

The vulnerability involved an error in searching which enabled an attacker to associate phone numbers and email addresses with their respective Twitter ID and therefore an individual, despite their privacy settings restricting access to that data. The data was initially offered for sale by a single actor on Breach Forums, stating it related to "*5.4 million users*", but now appears to be being sold by multiple different entities across hacker forums and marketplaces, with some sources describing the data as relating to as many as 400 million users.

While Twitter patched the vulnerability, it is still important that you check your privacy settings and ensure that you are not indexed on the platform via your personal contact information.

3.2 Citrix and Fortinet patch actively exploited vulnerabilities

Two critical 0-day vulnerabilities in Fortinet (CVE-2022-42475) and Citrix (CVE-2022-27518) are reportedly under active exploit, allegedly by an unnamed ransomware group(s).

Additionally, the NSA has released a report which details the exploitation of the Citrix vulnerability by APT5, a Chinese group who are motivated by espionage. With the report containing relevant IOCs and have asked for further insights from the wider cybersecurity community.

Both vulnerabilities have patches, so please ensure you are making use of a patch management plan and completing updates in a timely and risk averse manner.

3.3 Dolphin backdoor used by APT37

Researchers from ESET have attributed a new piece of malware called "Dolphin" to the DPRK-backed APT37 (ScarCruft).

Dolphin, which is a backdoor with the ability to monitor drives, exfiltrate data, conduct keylogging, take screenshots and steal credentials, has reportedly been under "*continued development*" since April 2021. ESET's report contains a full technical breakdown and in-dept analysis of Dolphin's components, but a key point is the malware's ability to modify a targets Google and Gmail account settings, lowering their level of security and allowing greater access to the attacker.

APT37 have a long history of using malware of this type with TTPs which align with the activity witnessed by ESET. They also have a specific focus on targets which would be of interest to North Korea's military, such as those within South Korea and the defense sector.

3.4 InTheBox, a web-inject marketplace

Researchers from Resecurity have released intelligence on a new dark web criminal marketplace called “InTheBox” which focuses on web-injects for mobile malware platforms such as Ermac and MetaDroid.

The market has allegedly existed since 2020, and specializes in web-injects designed to imitate legitimate applications and login pages, so that an attacker can harvest credentials/sensitive data relating to financial applications/payment services, etc.

InTheBox’s market is well organized and contains a plethora of options for cyber-criminal customers, including over 400 web-injects, that are sorted by the nation of the target company, with 43 countries being listed. It is likely that these web-injects are being well utilized, and offer an unsophisticated attacker an easy way to harvest credentials, payment data, and sensitive information.

3.5 Infraguard breach

Infraguard, which is a project and platform run by the FBI has been compromised and details of the networks 80,000 members have been offered for sale on the criminal marketplace/forum Breached.

The platform, which is essentially an intelligence sharing hub for companies and industry figures, is limited to vetted parties, and the FBI has described the incident as originated from a “*false account*”, and is looking into the matter.

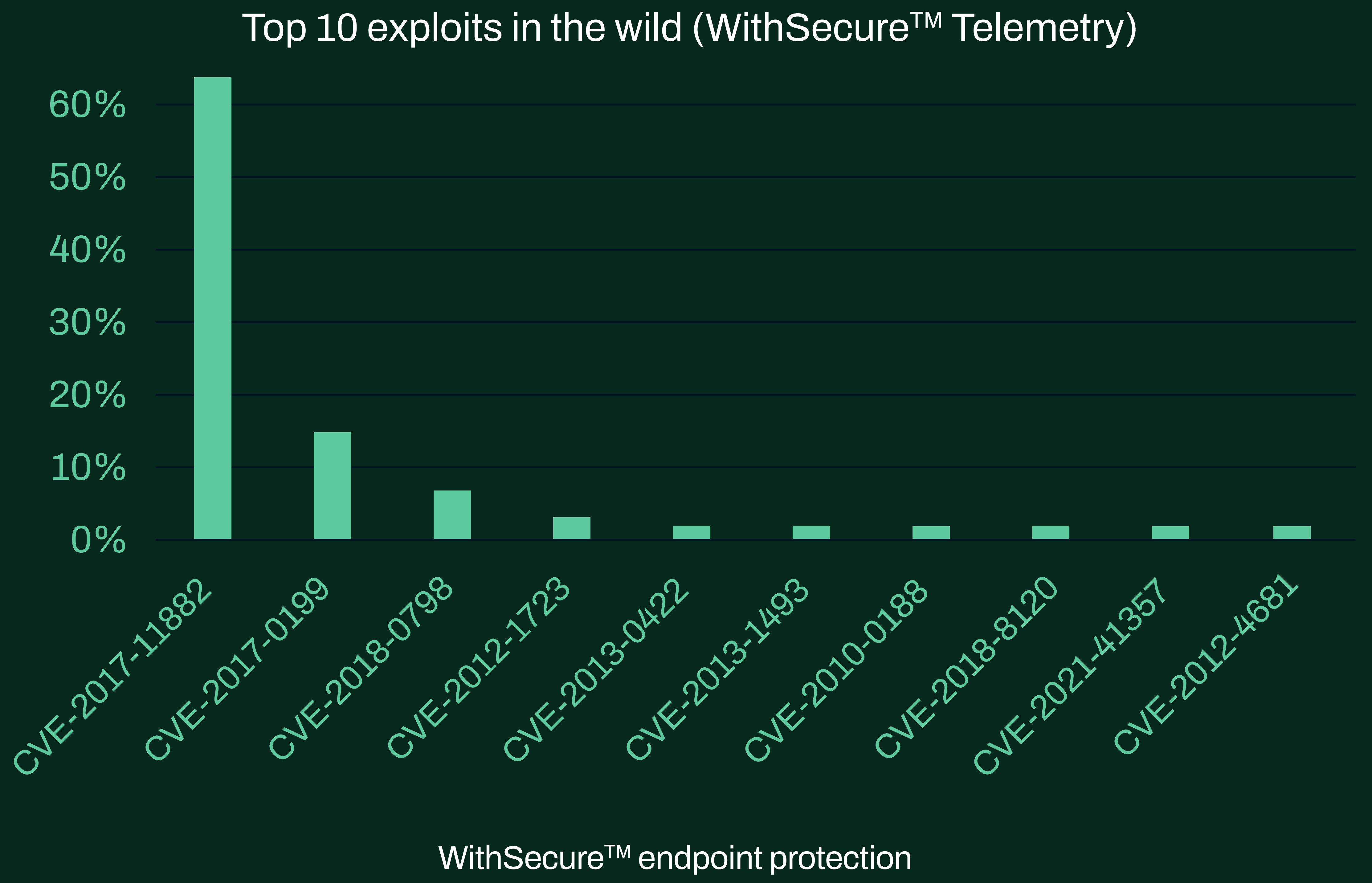
The sale of data from Infraguard is problematic though, as it will likely contain contact information for key persons in elevated positions in organizations and companies responsible for maintaining critical infrastructure. Such information could be abused by threat actors, likely through social engineering, and there are reports that Infraguard members have already received malicious contact via the platform.

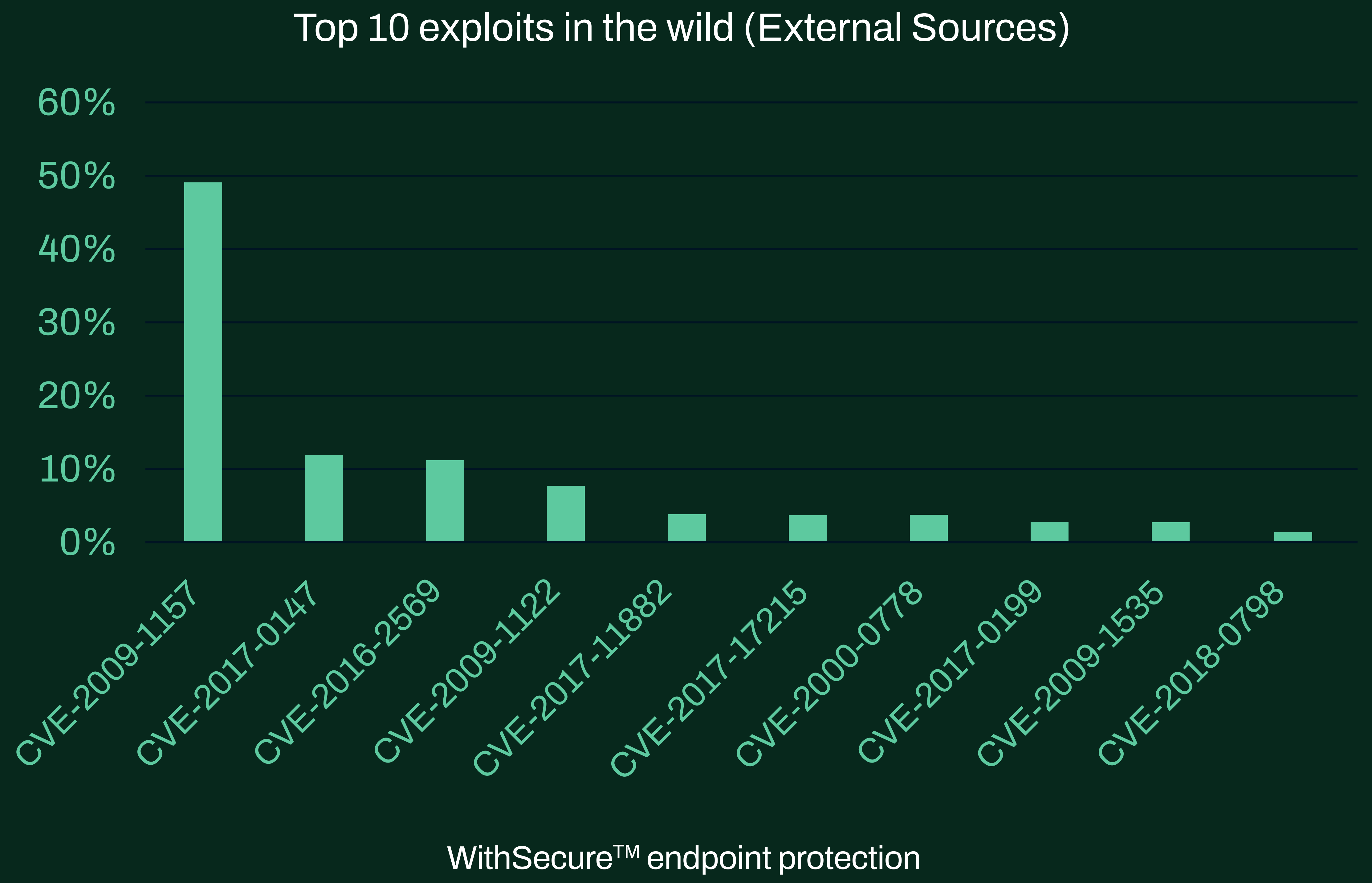
.

4 Threat data highlights

4.1 Exploits

There’s little change across the vulnerability exploitation landscape this month, with old favorites such as CVE-2017-1182, CVE-2017-0199 and CVE-2017-0147 all continuing to score highly, which are all vulnerability relating to Windows/Microsoft Office.





CISA’s known exploited vulnerabilities catalog

In December CISA added 9 vulnerabilities to their known exploited vulnerabilities catalog. 3 of which are rated “critical”.

CVE ID	Vendor / Product	What's the vulnerability?
CVE-2018-5430	TIBCO	TIBCO JasperReports Server contains a vulnerability which may allow any authenticated user read-only access to the contents of the web application, including key configuration files.
CVE-2018-18809	TIBCO	TIBCO JasperReports Library contains a directory-traversal vulnerability that may allow web server users to access contents of the host system.
CVE-2022-42856	Apple	Apple iOS contains a type confusion vulnerability when processing maliciously crafted web content leading to code execution.
CVE-2022-42475	Fortinet	Multiple versions of Fortinet FortiOS SSL-VPN contain a heap-based buffer overflow vulnerability which can allow an unauthenticated, remote attacker to execute arbitrary code or commands via specifically crafted requests.
CVE-2022-44698	Microsoft	Microsoft Defender SmartScreen contains a security feature bypass vulnerability that could allow an attacker to evade Mark of the Web (MOTW) defenses via a specially crafted malicious file.
CVE-2022-27518	Citrix	Citrix Application Delivery Controller (ADC) and Gateway, when configured with SAML SP or IdP configuration, contain an authentication bypass vulnerability which allows an attacker to execute code as administrator.
CVE-2022-26500	Veeam	The Veeam Distribution Service in the Backup & Replication application allows unauthenticated users to access internal API functions. A remote attacker can send input to the internal API which may lead to uploading and executing of malicious code.
CVE-2022-26501	Veeam	The Veeam Distribution Service in the Backup & Replication application allows unauthenticated users to access internal API functions. A remote attacker can send input to the internal API which may lead to uploading and executing of malicious code.
CVE-2022-4262	Google	Google Chromium V8 contains a type confusion vulnerability. Specific impacts from exploitation are not available at this time.

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.