Threat Highlights Report

November 2022

W / T H secure

Contents

1 Monthly highlights 3
2 Ransomware: Trends and notable reports 6
3 Other notable highlights in brief 9
4 Threat data highlights 10
5 Research highlights 13

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 another high-profile data leak in Medibank, as well as sharing research conducted by Group-IB into the rise in information stealer malware – particularly common in high-profile ransomware and hack-and-leak attacks. While on the topic of info-stealers, we also highlight updates to our own research into Ducktail.

We assess the ever-changing ransomware landscape with a particular look into the 'Royal' and 'BlackBasta' variants, and examine new assessment into links between Russian state, criminal and hacktivist groups.

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. We also explain the much-hyped vulnerability in OpenSSL and why, in this case, it perhaps did not have the impact as expected prior to its release.

Tim West – WithSecure Threat Intelligence

1 Monthly highlights

1.1 Ukraine attributes somnia ransomware to russian hactivists

The Computer Emergency Response Team of Ukraine has released a blog post highlighting the claims made by pro-Russian hacktivist groups FRwL (aka Z-team, UAC-0118) that they are responsible for a new 'Ransomware' variant 'Somnia'. The report details IOCs and TTPs utilized by the actors.

Initial compromise occurred through the download of a file that mimicked "Advanced IP Scanner" which in fact contained the Vidar malware. Vidar, an information/credential stealer, took Telegram session data which was used to transfer VPN connection configuration files to users. This was then used to gain unauthorized connections into the corporate network. Cobalt Strike post-exploitation framework was deployed throughout the network before Somnia was executed.

Somnia was first observed in the summer of 2022, with actors FRwL removing the ability to decrypt data in August, essentially rendering the malware a wiper.

"*We removed the decryption function especially for hohloreiha, now the process is irreversible, and the encryption algorithm is just insane! We gave a chance to change their minds and stop the bloodshed by leaving messages on encrypted hosts, here's an example...*"

WithSecure^{TM} Insight

At the start of the Ukraine conflict, a number of wiper samples emerged targeting Ukrainian and Polish organizations. Hacktivist groups observed operating with a clear anti-Ukraine sentiment have evolved their TTPs since February. DDoS attacks, while generally low impact, are common and do appear to have limited success. Killnet - a pro-Russian hacktivist group was reported to have launched an effective DDoS attack against the EU parliament website in response to their labelling of Russia a state sponsor of terrorism.

Researchers have noted possible links between Russian state, and criminal groups. This month, researchers from the Stanford Internet Observatory have provided assessment on the links between Russian domiciled ransomware organizations and state:

"*Based on the findings, we theorize that Russia maintains loose ties with ransomware groups,*" Nershi said. "*These Russian based groups operate as independent criminal organizations who occasionally perform favors for the government. And in exchange, Russia gives these groups a safe harbor from prosecution.*"

This assessment comes in the same month as ESET attributes RansomBoggs ransomware to Russia and have noted similarities to destructive attacks on Ukraine energy sectors which was reportedly undertaken by Russian GRU Main Centre for Special Technologies (GTsST) in the initial months of the Russian invasion of Ukraine in 2022.

WithSecure's previous Threat Highlights Reports also contained comment upon research into ties between Russian state and hacktivist groups, and a possible state sponsored ransomware variant targeting Ukraine and Poland.

1.2 Information stealers as a service

Group-IB released research of information stealers sold in the darkweb via stealer-as-a-service model. 34 distinct Russian-speaking groups were identified distributing various information stealers as a service.

The most typically used malware were Racoon or Redline stealers which are used to steal information such as steam and roblox accounts, credentials for Amazon and Paypal as well as payment records and cryptocurrency wallets. These attacks are conducted through Russian-language telegram groups.

The majority of the victims were located in the United States, Brazil, India, Germany and Indonesia. The associated Telegram groups and bots first appeared in 2021. Out of these, 34 distinct scam groups were identified. The most popular stealer used by the cybercriminals is RedLine (23 out of 34 groups) Racoon being in the second place with eight groups while three others use custom stealers.

The data which cybercriminals collected throughout 2021 included passwords, cookie files, payment records, and cryptocurrency wallets and details of bank cards. Groub-IB estimates the underground market value of the data stolen during last 10 months of 2021 to be around $5.8 million.

WithSecure™ Insight

Information stealers continue to be a prevalent threat. According to the WithSecure™ telemetry, information stealers are the third most prevalent malware type identified throughout November.

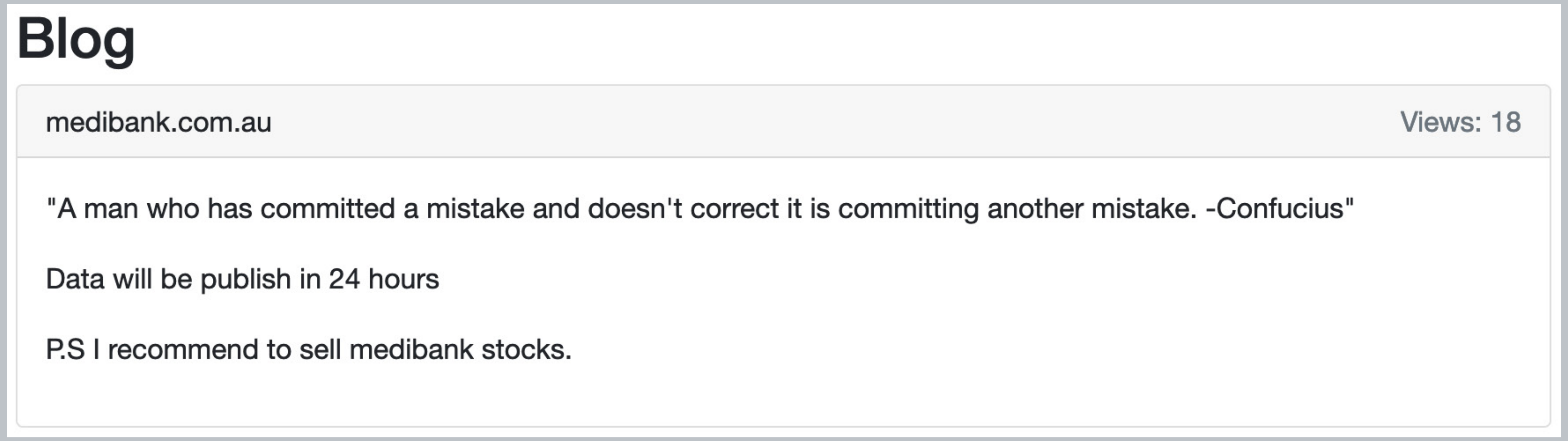
Information stealers are delivered using common methods such as malicious download links in social media, trojanized software downloads or (the most common method): phishing emails. Many incidents that WithSecure™ deal with, and report on, begin with compromised or leaked credentials. The use of information stealers is almost synonymous with ransomware events and utilizing stolen credentials is almost certainly more common in cyber events than the exploitation of zero-day vulnerabilities.

While information stealers are prevalent and can cause an impact against organizations as well as individuals, the main way to protect against them is simply having a good anti-malware solution. It can detect information stealing malware via signatures or behavioral patterns.

Additional protective layers can be added on the network level as a browsing protection for endpoints as well as against email-based attacks with email security solutions. Detection on erroneous use of credentials may provide an extra mitigative layer.

1.3 Medibank data posted on dark web

Following October's news that Medibank had become the latest victim of a spate of high-profile cyber-attacks, data started to emerge on Deep and Dark Web blogs controlled by actors likely behind the attack. BlogXX posted the victim with the following message:



Blog

medibank.com.au Views: 18

"A man who has committed a mistake and doesn't correct it is committing another mistake. -Confucius"

Data will be publish in 24 hours

P.S I recommend to sell medibank stocks.

Medibank later admitted that actors accessed the data of almost 10 million people, stating the following:

"*Medibank is one of the largest Australian private health insurance providers with approximately 3.9 million customers. Based on our investigation to date into this cybercrime we currently believe the criminal has accessed: Name, date of birth, address, phone number and email address for around 9.7 million current and former customers and some of their authorised representatives. This figure represents around 5.1 million Medibank customers, around 2.8 million ahm customers and around 1.8 million international customers.*"

Medibank have stated that they will not pay the ransom to the attackers.

WithSecure™ Insight

BlogXX is a ransomware leak blog that has been linked to REvil ransomware, a once prolific RaaS service behind multiple high-profile attacks, through a redirect in REvil's 'Happy' blog to BlogXX. It is highly unlikely that BlogXX represents a simple rebrand of REvil. Attackers claimed they utilized compromised credentials and possibly connected through a service called 'Redshift', an Amazon data warehousing product. Attackers also claimed to access Medibank's confluence server and Stash – a source code repository. The fact Medibank initially incorrectly stated that no data had been accessed is a likely indication that organizations still struggle with comprehensive log consumption and event visibility across their entire estate, particularly when dealing with destructive attacks and/or cloud/third-party infrastructure.

Medibank is the latest victim of a high-profile data leak, following Optus whereby an unprotected API was accessed and Uber whereby compromised credentials and an MFA fatigue approach gave attackers initial access. What is common across these (and many other) data leaks is the utilization of technically uncomplex attack vectors. This should not be a source of confidence for organizations as it highlights that there is no single silver-bullet technology or solution for blue teams and that human factors are also important when considering a holistic defensive approach.

2 Ransomware: Trends and notable reports

2.1 Quantum locker targets cloud environments

Researchers at Computerland have observed Quantum Locker operating ransomware extortion on cloud environments such as Microsoft Azure against organizations across northern Europe. Quantum actors demonstrated the ability to hunt and delete data stored in cloud buckets and blobs. Researchers observed targeting of IT administrators and networking staff, particularly with a view to compromise Microsoft cloud services through the root account. Comprehensive compromise of cloud accounts is likely to have an increased impact on business operations, but also ability for an organization to quickly respond to an incident as it unfolds.

2.2 The rise of royal ransomware

Royal Ransomware, a ransomware variant that emerged in September 2022 has been active throughout November 2022 posting 43 victims to their leak site(s) throughout the month. Victims are distributed across sectors with notable inclusions in the energy and legal sectors.

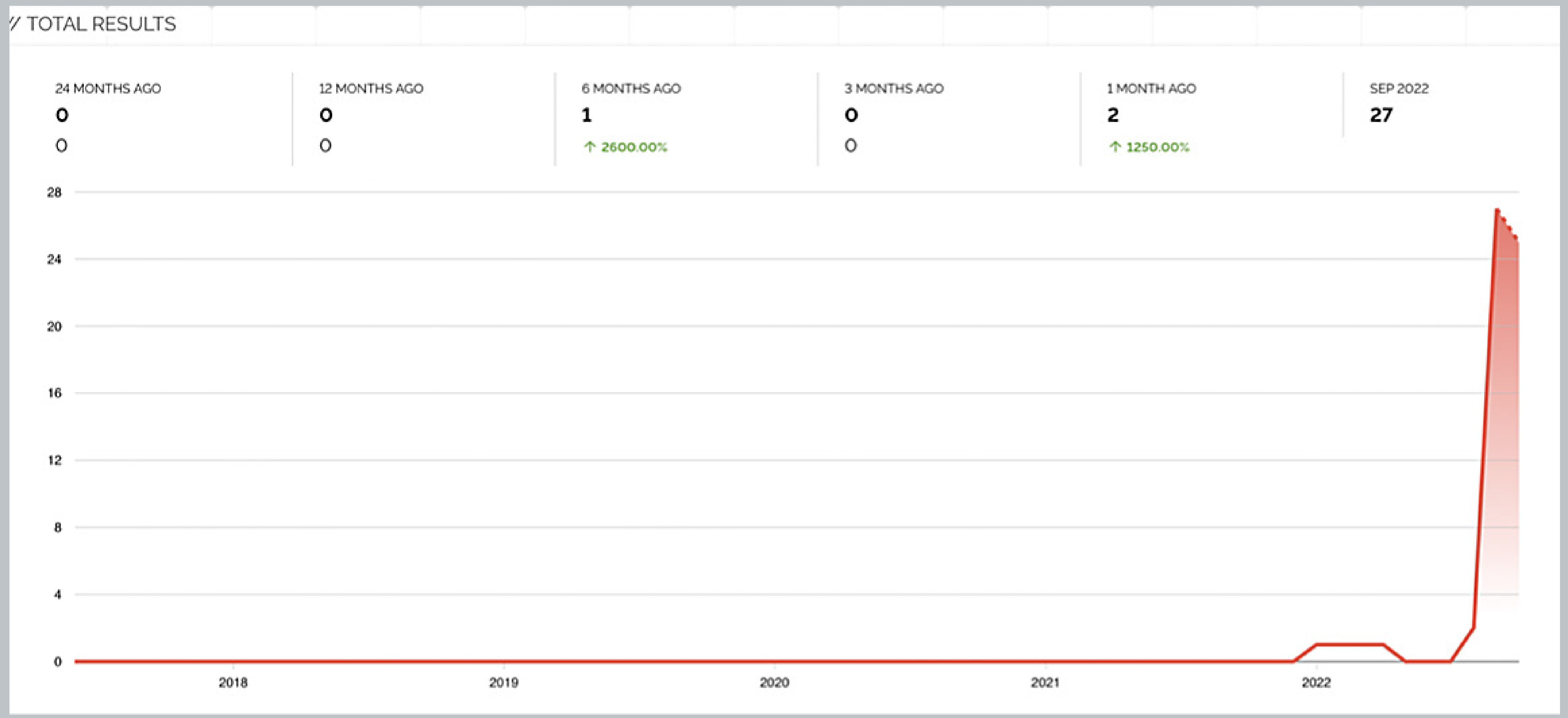
Microsoft track the actors behind Royal Ransomware as DEV-0569 and have released a report detailing observed delivery tactics of Royal Ransomware.

Royal actors have been observed making extensive use of signed MSI or VHD files spoofing legitimate remote administration software containing ‘BATLOADER’. Actors were also observed installing commodity malware payloads (QBot, Gozi, Vidar etc) and utilizing PowerShell and batch (.bat) files to perform administrative tasks, such as disabling AV and delivering additional payloads. Researchers at VMWare have this month released an advisory on BATLOADER and highlighted it’s use in multiple malware campaigns “*including a banking Trojan, an information stealer, and the Cobalt Strike post-exploitation toolkit on victim systems.*”

WithSecure™ Insight

Microsoft's insight into Royal Ransomware correlates with the findings of WithSecure™ Incident Response teams. WithSecure™ have observed extensive misuse of legitimate remote administration tooling (AnyDesk, ScreenConnect, Remote Access WinLauncher and RDP) for persistence and lateral movement, and the subsequent use of Cobalt Strike. Batch and PowerShell files utilized by the Royal actor match Sigma rules for activity related to Ryuk and Conti ransomware. TTPs and commands issued are consistent with the leaked 'Conti' playbook and historical reports of Conti intrusions, notably the post-exploitation activity as detailed in this Sophos report.

WithSecure™ were able to retrieve the Cobalt Strike configuration details for the beacon utilized in the attack and noted several other hosts in the wild that had been created with the same watermark.



- 2022-09-24 –Webshell observed
- 2022-09-24 –Cobalt Strike server discovered
- 2022-09-27 – 24 replicated Cobalt Strike Servers initialized
- 2022-09-29 – Cobalt Strike executed
- 2022-10-11 – Royal Ransomware execution attempted
- 2022-11-04 – 20 Victims uploaded to Royal Portal
- 2022-11-05 -> 2022-11-20 – 18 further victims added

Actors have been reported utilizing a variety of initial access techniques to gain access to a victim network, including call-back social engineering, phishing emails, fake updates and malvertising campaigns.

Noting the diversity of potentially time-consuming initial-access techniques with batched initialization of Cobalt Strike infrastructure, and synchronization of victims released to Royal's blog, WithSecure™ assess that it is likely that Royal actors are purchasing developed access to organizations from one or more Initial Access Brokers.

2.3 BlackBasta linked to FIN7 threat actor

The team at SentinelLabs have discovered links between BlackBasta operators and the FIN7 intrusion set. Pivoting on a custom defence impairment tool used exclusively by BlackBasta, researchers were able to discover a service that spoofed a ‘healthy’ Windows Defender dashboard. Pivoting on this highlighted packed samples of BIRDDOG backdoor, which connects to an IP address hosted on “pq.hosting”, a known bulletproof hosting provider favored by FIN7. FIN7 have also been observed utilizing BIRDDOG (aka SocksBot) on multiple occasions.

SentinelLabs assess the impairment tool used by BlackBasta is developed by the same actor who has access to the packer source code used in FIN7 operations, thus establishing a possible connection between the two groups.

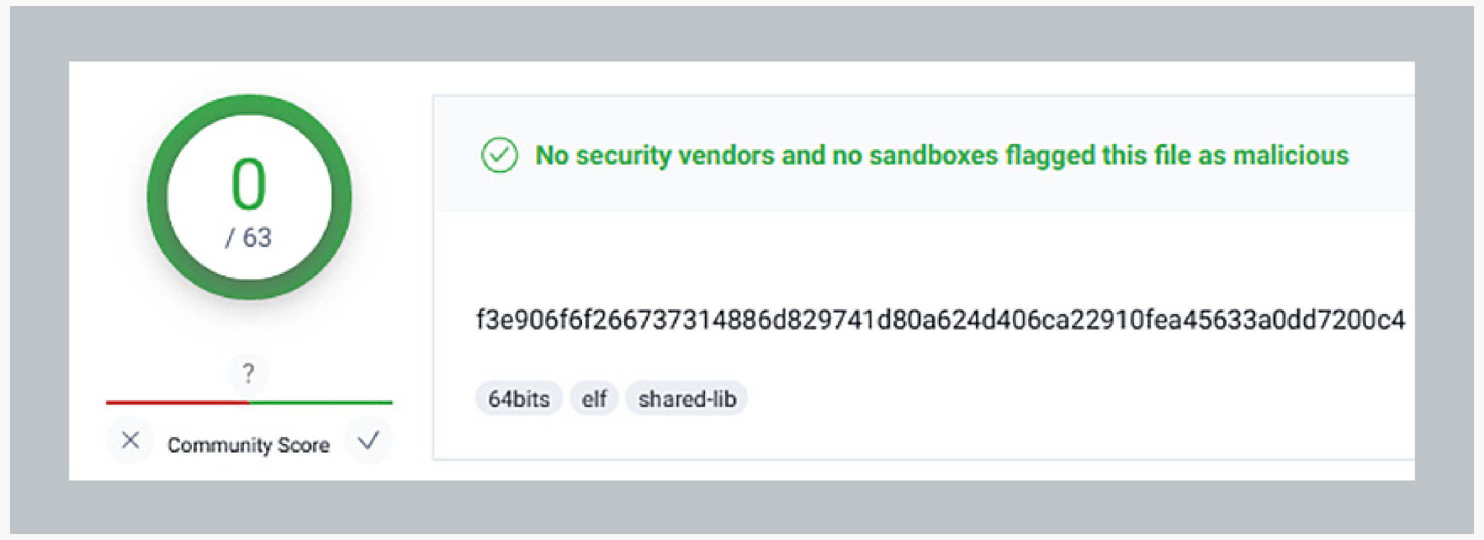
WithSecure™ Insight

FIN7 are financially motivated and capable cyber criminals who have historically targeted financial organizations and Point of Sale (PoS) devices. Black Basta was first discovered in February 2022, where it quickly rose to prominence, posting the third most victims throughout the period of April – September of all known Ransomware families engaged in double extortion techniques. The actors behind BlackBasta are capable actors and it is no real surprise to see competent financially motivated cyber criminals joining or creating ransomware affiliate programs.

WithSecure™ has observed extensive QBot activity throughout Q3 2022 likely driven, at least in part, by BlackBasta. QBot is observed being delivered through malspam containing a download link to a .zip file containing an ISO image of QBot. As has been reported by colleagues across the industry, PrintNightmare vulnerability is utilized in BlackBasta attacks (CVE-2021-34527) in order to undertake privileged actions. BlackBasta actors also extensively utilize SystemBC, a tool that establishes SOCKS5 traffic proxying.

2.4 US Govt issue HIVE ransomware advisory

The US DoJ, CISA and DoHHS have issues a joint advisory into Hive ransomware. Through to November 2022, Hive have targeted a number of organizations in Government, IT and Healthcare sectors. As with many other prominent malware families (BlackBasta, Lockbit, Babuk etc), Hive ransomware contains a variant designed to target ESXi servers. Of particular note, it is likely that Hive ransomware developers are working to reduce the detectability of their ESXi variants, with a researcher noting a sample uploaded to VirusTotal with zero detections. NB. At the time of writing this report, the sample provided is now well detected across multiple AV vendors.



0 / 63

No security vendors and no sandboxes flagged this file as malicious

f3e906f6f266737314886d829741d80a624d406ca22910fea45633a0dd7200c4

3 Other notable highlights in brief

3.1 DTrack activity targeting Europe and Latin America

Researchers at Kaspersky have released a report on observed DTrack backdoor activity, a tool used by Lazarus Group. Lazarus group have been attributed to the government of DPRK. Kaspersky's telemetry highlights activity across Latin America, Europe, India, Saudi Arabia, Turkey and the United States. WithSecure's telemetry has also detected the DTrack sample highlighted by Kaspersky in Austria.

Lazarus Group is traditionally known as a financially motivated intrusion set, however has morphed to become a 'catch-all' term for actors operating out of DPRK. This campaign as highlighted by Kaspersky is reported to target "*Education, Chemical Manufacturing, governmental research centers and policy institutes, IT service providers, utility providers and telecommunications.*"

3.2 Emotet botnet operational after 5-month hiatus

The Emotet banking trojan has become operational again after a five-month hiatus, discovered when researchers observed malspam spamming victims worldwide. Emotet botnets utilize 'reply-chain' phishing, whereby email threads are included in the message body to increase the likelihood of a victim interacting with the malicious elements of the email. In this case, encrypted .xls (Microsoft Excel) and .lnk (Link) files. To bypass Microsoft's 'Mark of the Web' protection, victims are instructed to copy the file into the 'Templates' folder, a trusted location whereby opening documents will bypass 'Protected view'. Emotet infections often result in subsequent malware being deployed, including but not limited to, Cobalt Strike and Trickbot. In campaigns observed by ProofPoint in November, IcedID and Bumblebee malware were dropped.

3.3 ProxyNotShell exchange exploits available

Microsoft's November patch Tuesday contained fixes for two vulnerabilities in Microsoft Exchange dubbed 'ProxyNotShell' (Initially reported in October THR). While few exploits for ProxyNotShell were observed in the prior months, now exploit code has been made available. Many ransomware actors were observed exploiting vulnerabilities in Microsoft Exchange, namely ones dubbed 'ProxyShell'. Patching Microsoft Exchange servers is not always a quick process, and as authentication is needed to exploit the vulnerability, it is highly likely there is still a large threat surface available to this vulnerability.

3.4 OpenSSL vulnerability downgraded

Two vulnerabilities were released in OpenSSL this month and were initially reported as CRITICAL. OpenSSL is an opensource software package used in many enterprise software packages. As the Log4j vulnerability had highlighted the difficulties associated with vulnerabilities in ubiquitous open-sourced software libraries to many network administrators, these vulnerabilities attracted a lot of attention.

Two buffer overflow attacks were downgraded from CRITICAL to HIGH, a denial of service and a remote code execution bug respectively. The downgrade occurred due to difficulties in triggering the exploit conditions to achieve RCE. While the vulnerabilities were not as severe as expected, it did serve a reminder to organizations that third party software libraries do form part of an attack surface, and there are inherent difficulties with identification and mitigation of associated risks – particularly where open-sourced software is maintained by volunteers.

4 Threat data highlights

4.1 Exploits

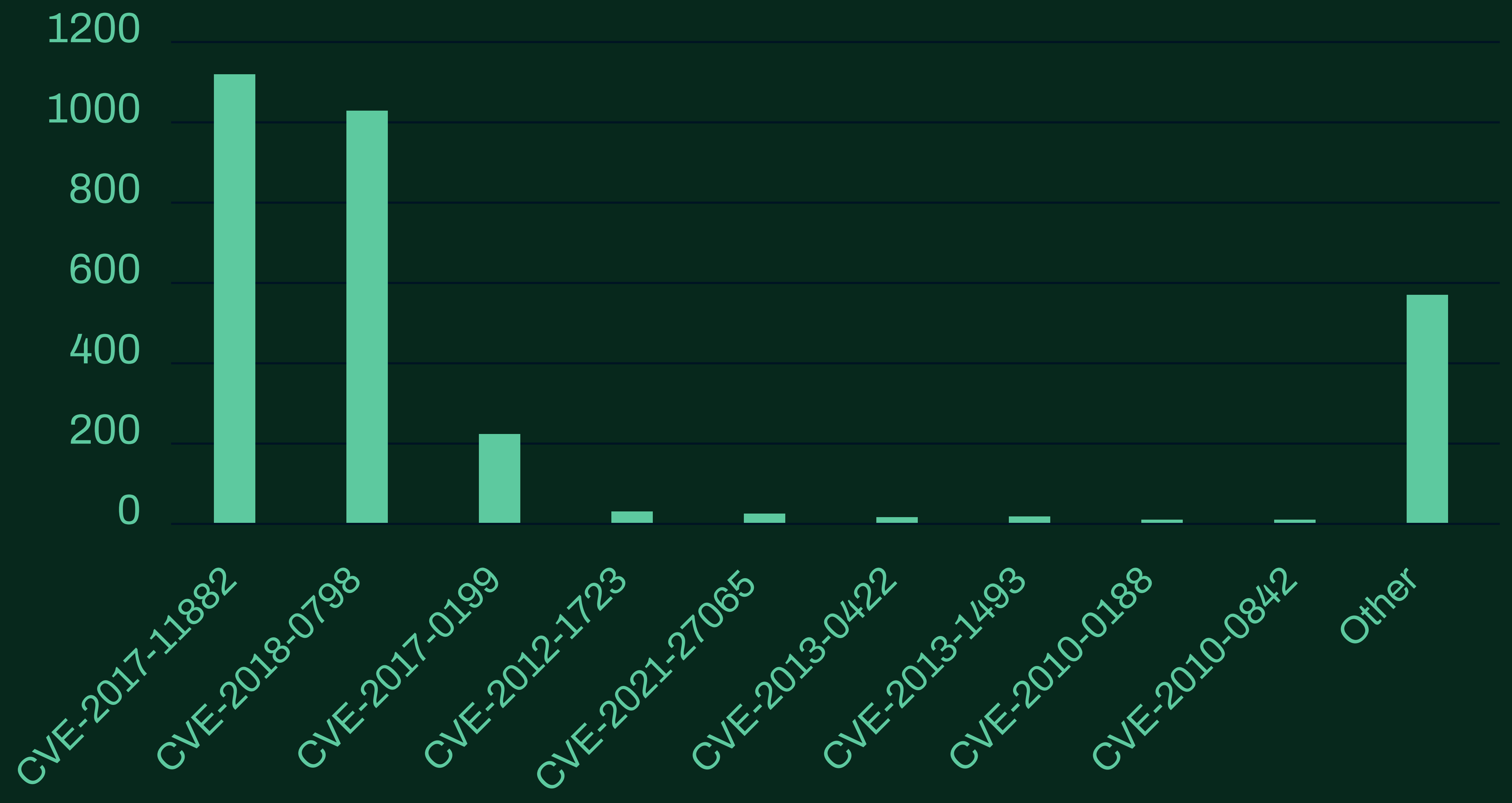
Top CVE’s from November telemetry breakdown

CVE-2017-11882: Old, but still very popular vulnerability, that involves the use of weaponized .doc and .rtf files to achieve remote code execution.

CVE-2018-0798: A bit more recent and very popular vulnerability, once again it involves the use of weaponized office files that when executed can achieve remote code execution.

CVE-2017-0199 is a RCE (remote code execution) vulnerability in MS Office and Wordpad, it is exploited with specially crafted RTF documents.

Exploits in the wild



Prevalence across all detected vulnerabilities.

CISA's known exploited vulnerabilities catalog

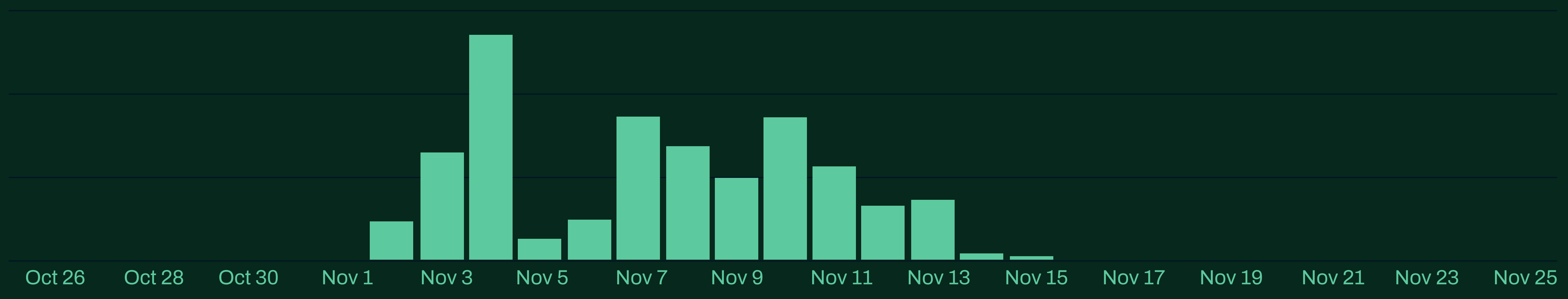
In November, CISA added eight vulnerabilities to the catalog of known vulnerabilities. These include high and medium severity vulnerabilities in windows components as well as Samsung mobile devices.

CVE ID	Vendor / Product	What's the vulnerability?
CVE-2022-41049	Microsoft Windows Mark of the Web (MOTW)	Microsoft Windows Mark of the Web (MOTW) contains a security feature bypass vulnerability resulting in a limited loss of integrity and availability of security features.
CVE-2022-41091	Microsoft Windows Mark of the Web (MOTW)	Microsoft Windows Mark of the Web (MOTW) contains a security feature bypass vulnerability resulting in a limited loss of integrity and availability of security features.
CVE-2022-41073	Microsoft Windows Print Spooler	Microsoft Windows Print Spooler contains an unspecified vulnerability which allows an attacker to gain SYSTEM-level privileges.
CVE-2022-41125	Microsoft Windows CNG Key Isolation Service	Microsoft Windows Cryptographic Next Generation (CNG) Key Isolation Service contains an unspecified vulnerability which allows an attacker to gain SYSTEM-level privileges.
CVE-2022-41128	Microsoft Windows Scripting Languages	Microsoft Windows contains an unspecified vulnerability in the JScript9 scripting language which allows for remote code execution.
CVE-2021-25337	Samsung Mobile Devices	Samsung mobile devices contain an improper access control vulnerability in clipboard service which allows untrusted applications to read or write arbitrary files. This vulnerability was chained with CVE-2021-25369 and CVE-2021-25370.
CVE-2021-25369	Samsung Mobile Devices	Samsung mobile devices using Mali GPU contains an improper access control vulnerability in sec_log file. Exploitation of the vulnerability exposes sensitive kernel information to the userspace. This vulnerability was chained with CVE-2021-25337 and CVE-2021-25370.
CVE-2021-25370	Samsung Mobile Devices	Samsung mobile devices using Mali GPU contain an incorrect implementation handling file descriptor in dpu driver. This incorrect implementation results in memory corruption, leading to kernel panic. This vulnerability was chained with CVE-2021-25337 and CVE-2021-25369.

4.2 Emotet

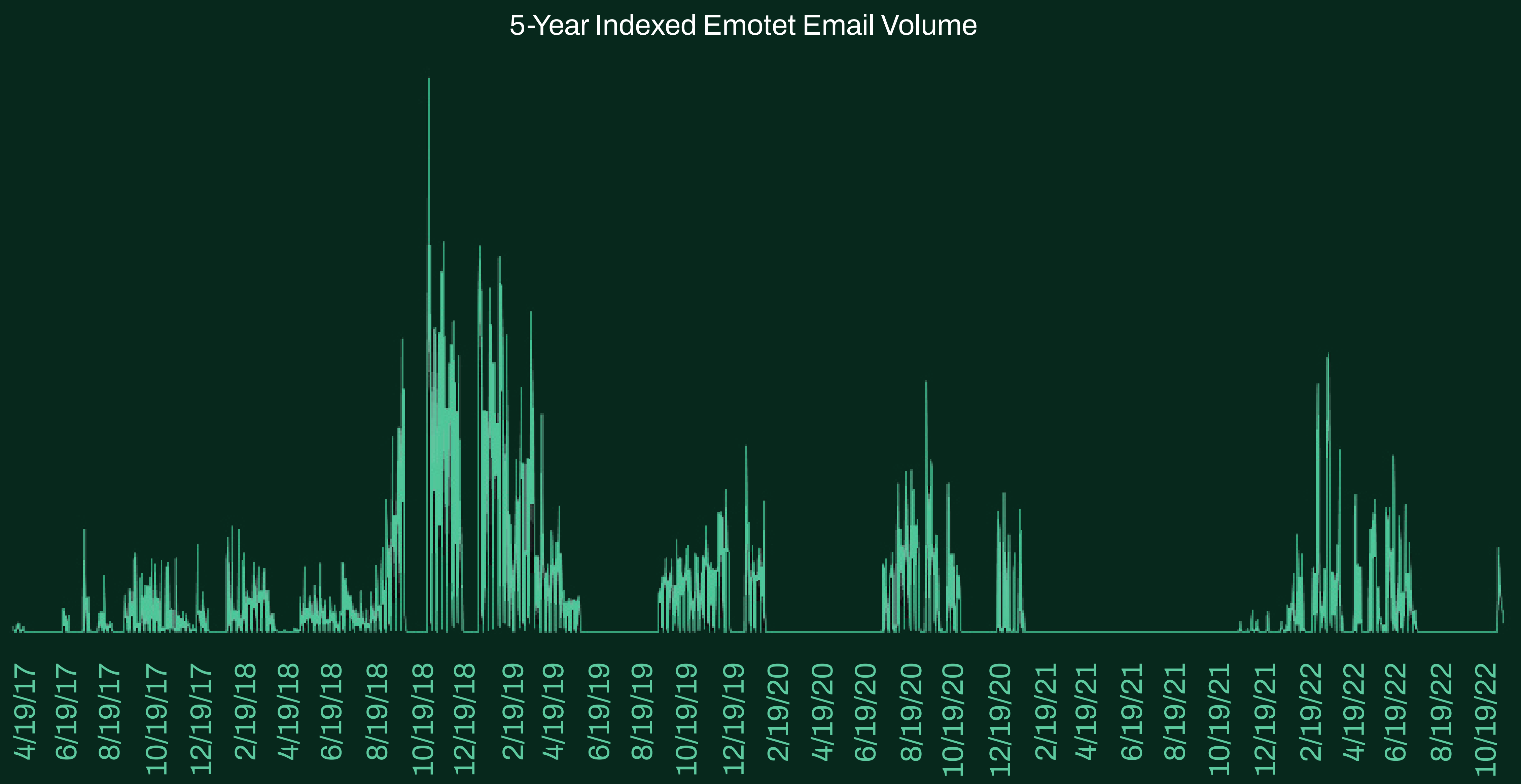
At the beginning of November, there has been an uptick in the amount of Emotet samples observed in the wild, the payloads as well as email lures have changed since the last campaign during the summer.

Based on the samples in the wild, the campaign has not been a long lived and died down towards the end of November.



Volumes of Emotet samples observed in the wild throughout November

Based on the following data by proofpoint, the volume of November campaign was rather low in the grand scheme of Emotet but it might be followed by more activity towards the end of the year:


5-Year Indexed Emotet Email Volume

Indexed volume of email messages containing Emotet, TA542's signature payload

(from April 19, 2017 – November 10, 2022)

5 Research highlights

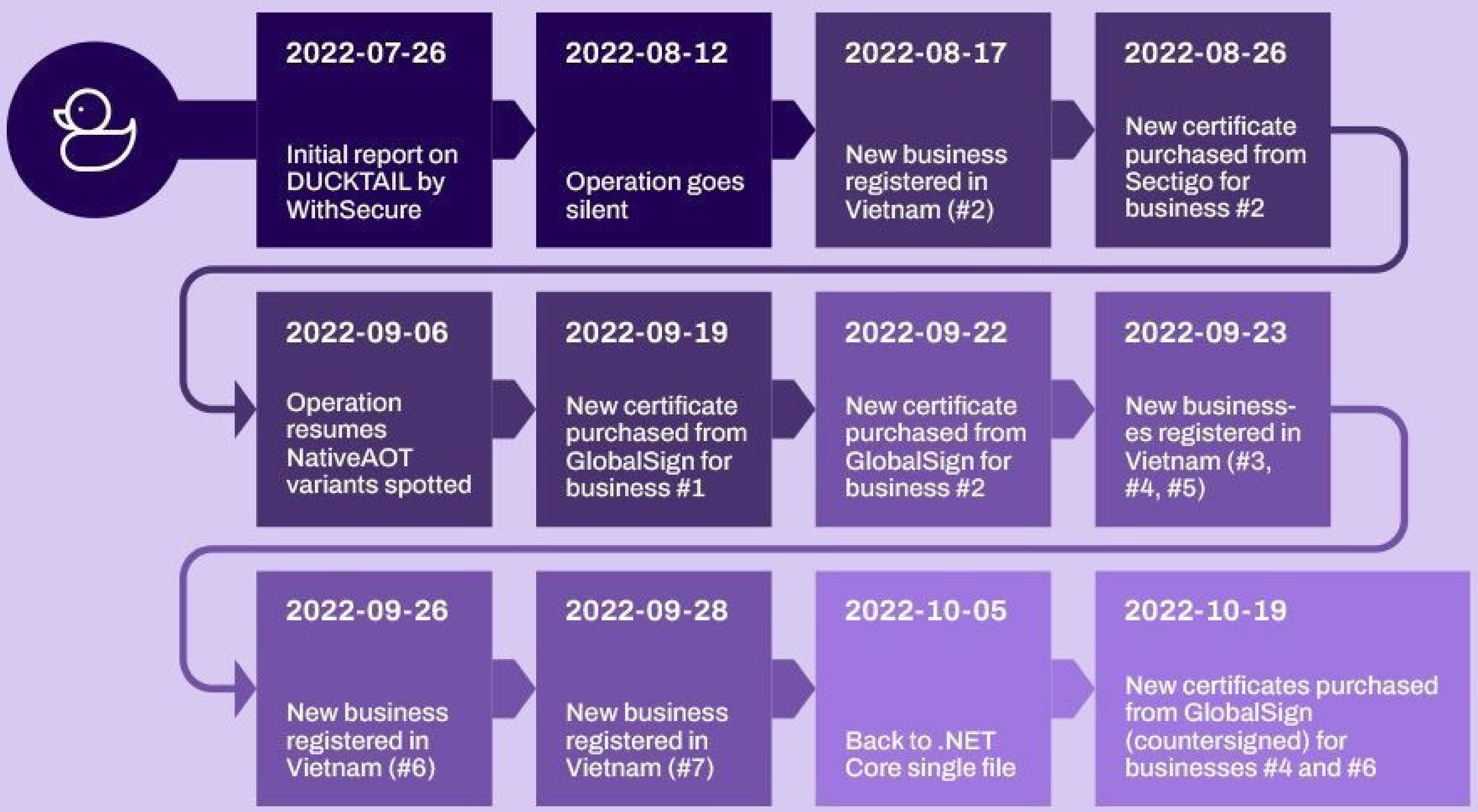
5.1 DUCKTAIL, continued

DUCKTAIL, a financially motivated cybercrime operation first discovered and analyzed by WithSecure™ is still ongoing. The operation targets widespread individuals and organizations making use of Meta's business/ads platform. The evidence strongly suggests that the goal of this operation is to gain access to business accounts and use the advertising credit and payment methods to run fraudulent ads.

Recent DUCKTAIL activity observed since early September featured several changes to their mode of operation, including:

- New avenues to spear-phish targets through messaging apps such as WhatsApp.
- Changes to malware capabilities with a more robust way of retrieving the attacker-controlled email addresses, and making the malware look more legitimate by opening dummy documents and video files upon launch.
- Continuous efforts at defense evasion by changing file format, compilation, and countersigning certificates.
- Further resource development and operational expansion by setting up additional fake businesses in Vietnam and onboarding affiliates into the operation.

Figure 14. Overview of DUCKTAIL's current activities



2022-07-26 Initial report on DUCKTAIL by WithSecure

2022-08-12 Operation goes silent

2022-08-17 New business registered in Vietnam (#2)

2022-08-26 New certificate purchased from Sectigo for business #2

2022-09-06 Operation resumes NativeAOT variants spotted

2022-09-19 New certificate purchased from GlobalSign for business #1

2022-09-22 New certificate purchased from GlobalSign for business #2

2022-09-23 New business-es registered in Vietnam (#3, #4, #5)

2022-09-26 New business registered in Vietnam (#6)

2022-09-28 New business registered in Vietnam (#7)

2022-10-05 Back to .NET Core single file

2022-10-19 New certificates purchased from GlobalSign (countersigned) for businesses #4 and #6

Companies operating in the advertisement vertical which are targeted by DUCKTAIL and similar attacks reported direct financial damage fluctuated between $100,000 to $600,000.

WithSecure™ has released detailed analysis of the latest activities:

What can you do?

Defenders can take the following steps to protect themselves from DUCKTAIL and similar threats:

- Raise awareness on spear-phishing among users with access to Facebook/Meta business accounts.
- Your Facebook Business administrator should review users added under Business Manager > Settings > People and revoke access for unknown users that were granted Admin access (with finance editor role).
- Use EDR/EPP solutions to prevent and detect malware in the earlier stages of the attack lifecycle.
- Ensure managed or personal devices used with company Facebook accounts have basic hygiene and protection in place.
- Use private browsing to authenticate each work session when accessing Facebook Business accounts (so the session is forgotten after finishing, which prevents cookies from being stolen and abused).
- Follow Meta's recommended security practices.

5.2 Machine learning accuracy forecast

In November, Mark van Heeswijk published in WithSecure™ labs blog about machine learning model performance over time and how to sustain the performance on expected level.

Mark looks into a host classification system, a system which uses information about the host activity as input, e.g., processes launched, domains accessed and extensions of files opened, to classify the host as technical, non-technical or server.

The host classification system is used as an example to study how to assess the performance of the model with couple of techniques.

The key takeaways from the research are:

- Predicting model performance by looking at data drift is not always effective, since data drift can be harmless.
- The average model uncertainty metric can act as a good proxy for the actual model performance, and it can be used as an additional tool to monitor models in production, using only unlabeled data.
- In response to detected model deterioration, the model can be retrained, and specific samples can be investigated and correctly labeled based on either model uncertainty (for unlabeled data), or loss (for labeled data).

This work has been partially supported and funded by Business Finland as part of the Eureka ITEA3 IVVES project.

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