Threat Highlights Report

May 2022

WITH secure

Contents

Foreword

This month's threat landscape includes a useful advisory from the United States (US) Cybersecurity and Infrastructure Security Agency (CISA) regarding initial access, something that every organization can learn from and use to harden their first-line defenses. As well as a look at an analysis of Emotet's resurgence and the group's new tactics, techniques and procedures (TTPs) which appear to be changing to counter efforts by defenders to overcome phishing attacks. We also take a look at an espionage tool linked to China called BPFdoor which uses unusual command and control techniques to reduce its likelihood of detection.

There are reports this month that the ransomware group Conti is shutting down some of its infrastructure and reorganizing its personnel and resources, likely in response to insider leaks and extra attention from security researchers, as well as a high-value bounty placed on the group's leaders by the US Department of State. Elsewhere in the ransomware landscape, we look at the potential return of the prominent REvil group, which was dismantled in January following arrests.

We are also looking at the poisoning of packages within the Python Package Index (PyPI) with malware, a .NET post-exploitation framework called IceApple, a step towards a password-less future thanks to Apple, Microsoft and Google, as well as other interesting highlights across the wider threat landscape.

As always, we hope you enjoy this month's report, and we welcome any feedback you may have.

Ziggy Davies, Threat Intelligence Analyst

1 Monthly highlights

1.1 Advisory on initial access techniques

The United States (US) Cybersecurity and Infrastructure Security Agency (CISA) has released a joint advisory, which has been co-authored with cyber-security agencies from across the globe. The advisory identifies the tactics, techniques, and procedures (TTPs) which are currently being used by threat actors to gain initial access.

The advisory seeks to aid organizations in bolstering their defenses, by both identifying common attack TTPs and explaining common misconfigurations or weak security practices. The TTPs discussed are mapped to the Mitre ATT&CK framework and include:

- The exploitation of public-facing applications [T1190]
- Leveraging of external remote services [T1133]
- The use of phishing [T1566]
- Breach via trusted relationship [T1199]
- Use of valid accounts [T1078]

The advisory explains “malicious cyber actors often exploit the following common weak security controls, poor configurations, and poor security practices to employ the initial access technique…” and lists:

- Multifactor authentication (MFA) is not enforced
- Incorrectly applied privileges or permissions and errors within access control lists
- Software is not up to date
- Use of default login usernames and passwords
- Remote services such as VPNs lack sufficient controls to prevent unauthorized access
- Strong password policies are not implemented
- Cloud services are unprotected
- Open ports and misconfigured services are exposed to the internet
- Failure to block or detect phishing
- Poor endpoint detection and response

The advisory then details ways in which these issues can be resolved or mitigated, discussing how to improve control access, implementing credential hardening, establishing log management, maintaining a rigorous patch management program, and employing anti-virus programs and detection tools.

WithSecure™ Insight

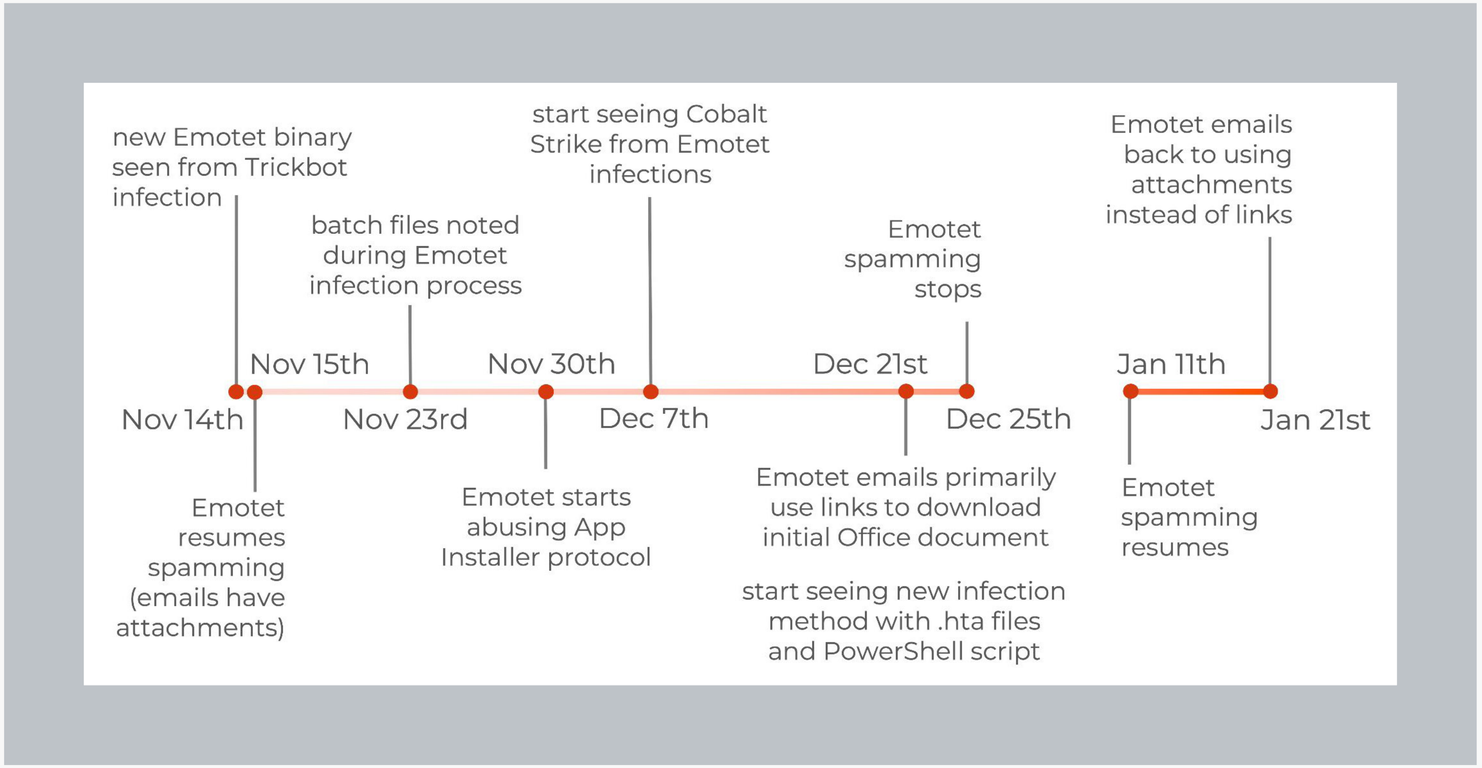
The content of this advisory by CISA is generic but very useful as it is applicable to a broad spectrum of cyber-attacks and are TTPs used by a variety of threat actors. Initial access is the third part of the ATT&CK matrix (after reconnaissance and resource development) and often the first opportunity for an attack to be detected and stopped. Following the suggestions and mitigations within this advisory will strongly improve an organization’s defenses, making them far harder to compromise and a less-attractive target for many opportunistic threat actors.

1.2 Emotet back at full power

Emotet, a prominent trojan and threat actor which has existed since 2014, was shut down in January 2021, due to a joint law enforcement operation. Since that time Emotet has been rebuilding and has steadily grown, with many media sources reporting that it is back to being a prolific malware family and major threat.

Researchers at Unit 42 have released an analysis on Emotet's presence and development between November 2021 and January 2022. This article describes how Emotet is still being heavily distributed through spam email and has rebuilt its botnet infrastructure, dubbed Epoch 4 and 5, as well as employing new delivery techniques, such as the use of email thread hijacking, malicious app installers and .hta files, with researchers at ASEC also reporting the use of malicious .lnk files.

Unit 42 researchers have created the following timeline of Emotet activity:



This timeline shows the development and adaptation of Emotet by its operators, with analysis by Proofpoint concurring that Emotet is testing new techniques and delivery methods.

WithSecure™ Insight

Assessing the analysis, we can infer that Emotet is being delivered in the following ways:

- Malicious email attachments, often office documents (maldocs) containing VBA/XL4 macro code which either directly installs Emotet or does so via dropped .bat file.
- Malicious links with an email that leads to a compromised website which imitates a file download service such as Google Drive. Interacting with the website leads to the download of a malicious file (app installer, .appx, .lnk, .zip, .xll) which installs Emotet.

Traditionally Emotet was solely deployed by malicious macro code and the shift to using alternative methods is likely due to Microsoft recently disabling XL4 macros by default, as well as better user education surrounding phishing and the enabling of macros.

Due to Emotet's email delivery, effective defenses include anti-phishing filtering, email filtering and detection mechanisms provided by EDR data for the occasions preventative measures are ineffective.

1.3 BPFDoor, an insidious backdoor

As part of PricewaterhouseCoopers' (PwC) annual "Cyber Year in Retrospect" report, they have shared a case study involving a China-based threat actor they are tracking as "Red Menshen". They state "this threat actor has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors using a custom backdoor we refer to as BPFDoor".

PwC explain "this backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant". With researcher Kevin Beaumont describing the malware as "highly evasive" due to the fact "BPFDoor doesn't open any inbound network ports, doesn't use an outbound C2, and it renames its own process in Linux". It appears that BPFDoor has been in used for at least 5 years, with Kevin Beaumont highlighting historic samples being uploading to VirusTotal (2019) and Pastebin (2018) and reporting that scanning suggests the malware is in use "across the globe".

Crowdstrike have released a blog post detailing their own research into the threat actor, who they are tracking as "DecisiveArchitect", and the backdoor which they name "JustForFun". Their analysis highlights that the "adversary (is) targeting global entities, in particular telecommunications companies, to obtain targeted personal user information" and specifically using an exploit in Solaris systems (CVE-2019-3010) to escalate privileges.

WithSecure™ Insight

BPFDoor uses techniques that are stealthy and almost undetectable, being able to operate without opening new ports or changing firewall rules by abusing BPF packet filtering. This is something that has previously been seen in BVP47, a backdoor attributed to the NSA. While PwC has attributed BPFdoor to a China-based threat actor, Crowdstrike state they are "not currently attributing (the malware) to a specific country-nexus".

It is however noteworthy that PwC monitored the threat actor's activity to be operating between Monday-Friday and conforming to office hours (0100-1000), suggesting a nation-state or at least organized threat actor, located in Asia (+8 hours UTC). This is reinforced by Crowdstrike's mention of the threat actor targeting "personal user information — for example, call detail records (CDRs) or information relating to specific phone numbers", data which would be targeted in espionage, rather than by financially motivated criminals.

2 Ransomware: Trends and notable reports

2.1 Is this the end of Conti?

AdvIntel are reporting that the ransomware group Conti are reorganizing and shutting down much of their infrastructure, with their report stating:

> **“The Conti brand, and not the organization itself, was in the process of the final shutdown. As of May 19, 2022, our exclusive source intelligence confirms that today is Conti’s official date of death”.**

AdvIntel have not explained who or what their source is, only describing it as “sensitive”, but the report outlines the shutdown of much of Conti’s infrastructure, including their leak site admin panel, negotiation site and a “reset” of their chatrooms, messengers and servers. With the group apparently diving its resources and personnel across other extortion groups, or starting new ones, with the report saying:

> **“For over two months, Conti collective had been silently creating subdivisions that began operations before the start of the shutdown process. These subgroups either utilized existing Conti alter egos and locker malware, or took the opportunity to create new ones”.**

This news follows a high-profile attack by Conti on the government of Costa Rica, which led to the nation’s president declaring a national emergency, while at the same time the US Department of State offered a $10,000,000 reward for information leading to the arrest of any leaders of Conti. The group was also recently exposed in a recent publication by Prodaft which examined the inner workings of the group, as well as shining a light on their tooling and infrastructure, which in combination with the chat logs and source-code leaked by @ContiLeaks highlights issues with data leakage and insider threat amongst the group.

Despite the claims by AdvIntel, Conti have subsequently published data for 25 victims on their leak site, whether this is historic data that was queued, or proof that the group is still operational will likely be revealed in the coming weeks.

2.2 Iran is carrying out ransomware attacks

Secureworks has released an analysis of ransomware activity which they are attributing to an Iran-based threat actor they are tracking as COBALT MIRAGE. The analysis states that the group is operating in two clusters, one that is using ransomware for financial gain, and another that is concentrated on gaining initial access and the collection of intelligence.

With regards to the group's victimology, Secureworks state; "COBALT MIRAGE has demonstrated a preference for attacking organizations in Israel, the U.S., Europe, and Australia", and believes a previous alert published by CISA is related to the same group.

COBALT MIRAGE is believed to be using a scan-and-exploit model, targeting systems that are vulnerable to exploits such as those in Fortinet (CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591), Microsoft Exchange (CVE-2021-26855), ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) and Log4j. The operators are installing a Fast Reverse Proxy client (FRPC) and gaining remote access to their victim's systems, then going on to enumerate the wider network and laterally moving, before deploying Bitlocker as a form of ransomware. In an unusual step, the attackers are sending their ransom notes to a local printer.

2.3 Operator of Thanos builder charged

The United States Attorney's Office (USAO) has reported an unsealed criminal complaint that relates to the creator of a popular ransomware builder called "Thanos". The builder's mastermind Moises Luis Zagala Gonzalez (aka Zagala, Nosophoros, Aesculapius, Nebuchadnezzar) is a citizen of France and Venezuela and is believed to be residing in Ciudad Bolivar, Venezuela. They are reported to be working also as a cardiologist, whilst building and operating a large criminal network.

"As alleged, the multi-tasking doctor treated patients, created and named his cyber tool after death, profited from a global ransomware ecosystem in which he sold the tools for conducting ransomware attacks, trained the attackers about how to extort victims, and then boasted about successful attacks, including by malicious actors associated with the government of Iran," said U.S. Attorney Breon Peace.

If caught, Zagala could face up to 5 years in prison.

2.4 The return of REvil?

In January 2022 14 members of the REvil ransomware group were arrested by Russia's Federal Security Service, following the October shutdown by law enforcement of some of the groups infrastructure. REvil had been one of the most prolific and high-profile ransomware operators/variants and this news was welcomed, but it would appear that REvil are reemerging and some of their infrastructure is back online.

Though at time of writing it is now offline and displaying an nginx error, for a brief period the groups old leak site was redirecting to a new one, which was listing new victims. This was also detected by researcher Catalin Cimpanu, and suggests that a member of REvil with access to the old infrastructure is rebuilding. This is backed up by analysis by Secureworks who have had access to samples of REvil used in recent (post-arrest) attacks, they state "these samples indicate that the developer has access to REvil's source code, reinforcing the likelihood that the threat group has reemerged".

REvil were a formidable threat and this potential return is worrying, and whether this activity is indicative of the group returning to the same standing and ability, will likely only be revealed in time.

3 Other notable highlights in brief

3.1 PyPI packages compromised

The popular “ctx” package and “phpass” framework on PyPI have been compromised. It is reported that both have been altered with malicious code designed to collect environmental variables, encode them in base64, and upload them to an attacker-controlled domain.

PyPI have confirmed:

> **“If you installed the package between May 14, 2022 and May 24, 2022, and your environment variables contain sensitive data like passwords and API keys (like AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY), we advise you rotate your passwords and keys, then perform an audit to determine if they were exploited”.**

PyPI have removed the ctx package and frozen the compromised account involved in the attack.

3.2 IceApple

The Crowdstrike Falcon OverWatch team has uncovered a .NET-based post-exploitation framework, which they have called “IceApple”. Crowdstrike notes that IceApple is being deployed to compromised Microsoft Exchange instances, but could be deployed on any IIS web application. They describe the framework’s functionality as including:

> **“IceApple is a post-exploitation framework – this means it does not provide access, rather it is used to further mission objectives after access has already been achieved. OverWatch’s investigations have identified 18 distinct modules with functionality that includes discovery, credential harvesting, file and directory deletion, and data exfiltration”.**

3.3 Russia reroute Ukraine’s internet

Russia has reportedly severed existing fiber-optic connections within occupied regions of Ukraine and has rerouted their traffic through Russia’s own Miranda and Rostelecom networks.

Ukrainian sources believe that Russia is “attempting to leave Ukrainians without access to the true information on developments in the war waged by Russia against Ukraine, and to make their false propaganda an uncontested source of information”.

3.4 Gootloader

The DFIR Report has released excellent analysis on Gootloader (GootKit), a payload distribution framework. The analysis demonstrates how the operator behind Gootloader, is employing SEO poisoning to push their malicious domains to the top of common Google searches. A Twitter account called GootLoader sites is currently identifying and tracking malicious domains involved in Gootloader.

3.5 Apple release patches

CISA are encouraging users and administrators to apply updates to any Apple systems within their estates. This is due to Apple releasing security updates addressing multiple vulnerabilities in their products that are being actively exploited.

3.6 North Korea create insider threat risk

The FBI, Treasury Department and State Department have released an unclassified alert relating to the risk of unwittingly employing North Korean teleworkers. The alert states:

> **“There are thousands of DPRK IT workers both dispatched overseas and located within the DPRK, generating revenue that is remitted back to the North Korean government. DPRK IT workers are located primarily in the People’s Republic of China (PRC) and Russia, with a smaller number in Africa and Southeast Asia. These IT workers often rely on their overseas contacts to obtain freelance jobs for them and to interface more directly with customers”.**

It is believed that this campaign is designed to both generate income for North Korea and is also being used to gain initial access to company environments and networks. The alert contains advice for companies seeking to employ freelance/remote IT workers and developers, and specific red-flags to be aware of that may indicate a candidate is a North Korean hostile actor.

3.7 Facestealer malware on app stores

Trend Micro have released analysis on Facestealer, malware variants within fake Google Android applications which are available on the Google Play store. The malware functions as a password-stealer designed to compromise victims’ Facebook accounts, which would then be used as part of a wider campaign. The report also highlights similar malicious applications imitating cryptocurrency miners which are designed to steal wallet credentials.

3.8 Say goodbye to passwords

Apple, Google and Microsoft have announced that they will soon be supporting alternative authentication methods that avoid passwords, which include the use of smartphones as the user’s key. The companies are active contributors to a password-less sign-in standard created by the Fast Identity Online (FIDO) alliance, who state “this new approach protects against phishing and sign-in will be radically more secure when compared to passwords and legacy multi-factor technologies such as one-time passcodes sent over SMS”.

3.9 Crypto mixer Blender.io sanctioned

The US Department of Treasury has released a statement regarding the world’s first sanctions against a cryptocurrency mixing service. The service offered by firm Blender, seeks to obfuscate and disguise the true source of cryptocurrency transactions, by mixing it amongst others, and is allegedly being used by the North Korean-backed Lazarus crime-group. The press release accuses Blender of processing $20.5 million of illicit proceeds linked to a crypto-heist carried out by Lazarus, and the sanctions seek to block Blenders presence and activity within the US.

3.10 A vulnerability in Zyxel is being exploited

It is reported that “a widespread, critical vulnerability affecting Zyxel firewalls is being exploited by hackers, according to several researchers and the director of cybersecurity for the NSA”. The vulnerability which is tracked under CVE-2022-30525 and was first discovered and reported by researchers at Rapid7, and allows an attacker to “modify specific files and then execute some OS commands on a vulnerable device”. Zyxel have patched the vulnerability, but have been faced with criticism for their handling of the issue and for failing to communicate with Rapid7.

3.11 ICO fine Clearview AI 7.5 million GBP

The UK Information Commissioner's Office (ICO) has "fined Clearview AI Inc £7,552,800 for using images of people in the UK, and elsewhere, that were collected from the web and social media to create a global online database that could be used for facial recognition". Clearview had collected more than 20 billion images of people's faces from social media and public websites, as part of a database which it sells to other entities such as law enforcement. The ICO's complaint and fine relates to the fact that Clearview never asked permission for this data or informed users that their data would be harvested and used in this way, a breach of UK law and privacy rights.

4 Threat data highlights

4.1 Exploits

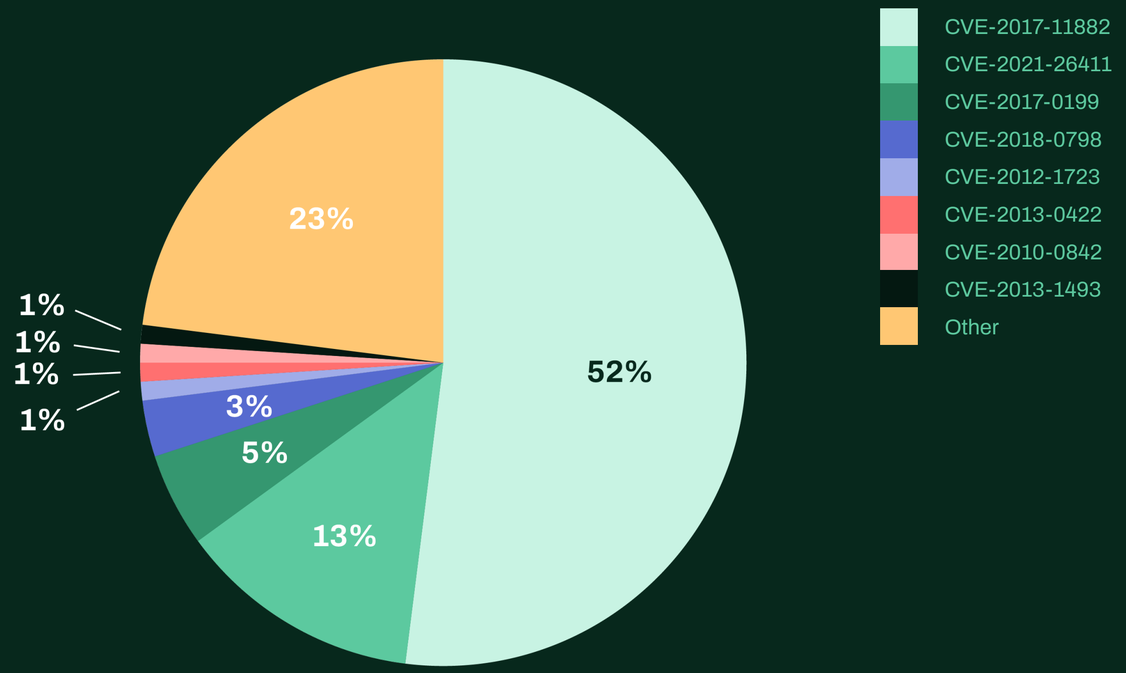
CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker, it is exploited by malicious office documents.

CVE-2021-26411 an internet explorer memory corruption vulnerability follows at the second place. This vulnerability is exploited by malicious websites.

CVE-2017-0199 is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted RTF document.

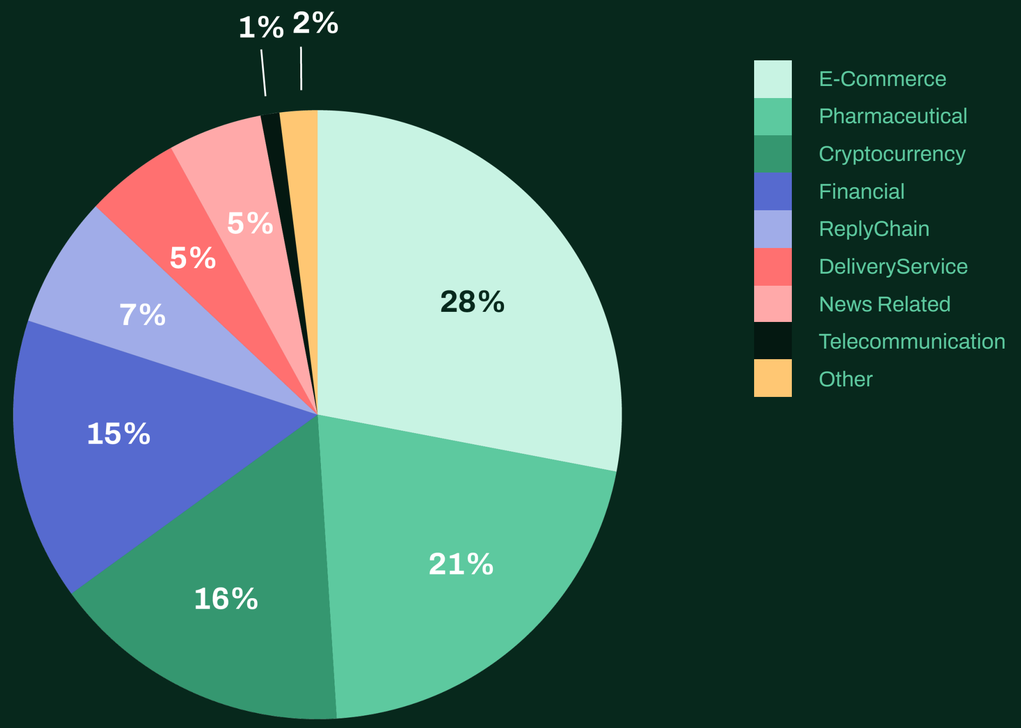
In May, CISA added 83 CVEs to the list of vulnerabilities exploited in the wild. These vulnerabilities affect multiple applications on various operating systems, ranging from internet explorer on windows to network access storage systems and linux kernel.

In May, a remote code execution vulnerability in F5 Networks BIG-IP was disclosed: CVE-2022-1388. Proof of concept exploit is publicly available and used in the wild by threat actors. This vulnerability affects the management interface and self IP addresses of the BIG-IP.

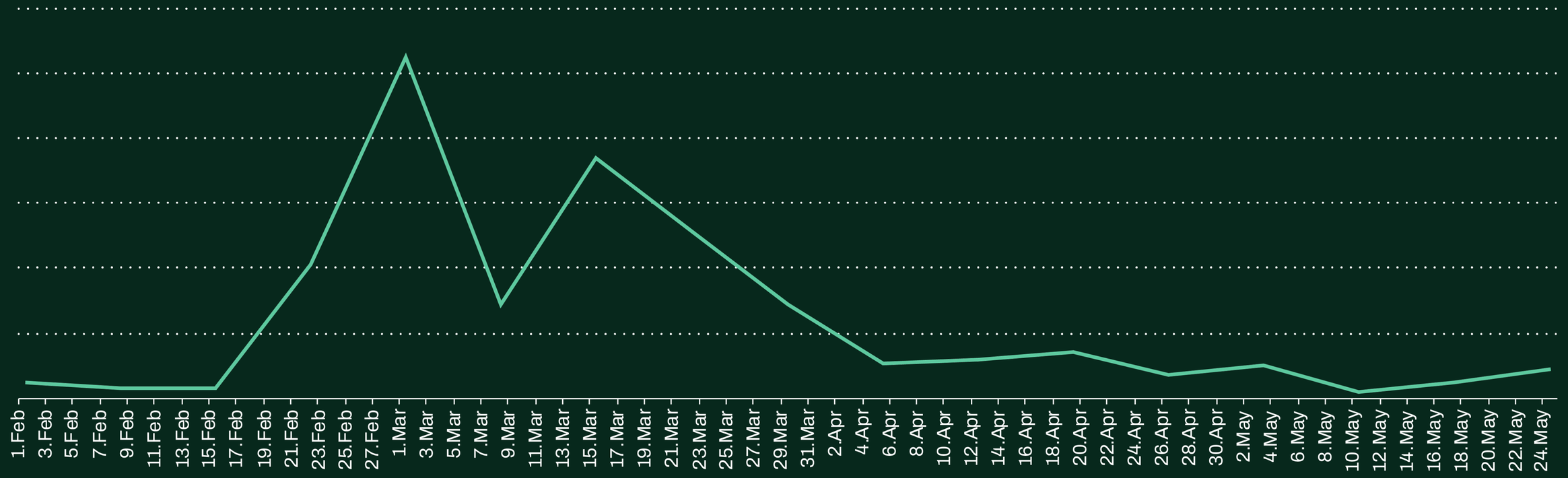


4.2 Email threats

E-commerce theme dominates the spam landscape. Interestingly in May we saw an uptick on the amount of pharmaceutical spam in our data, this was due to a more widespread spam campaign at the beginning of May. Cryptocurrency and financial spam remain popular.



Ukraine themed spam emails have died down. Since the peaks in February and March, the amount of Ukraine themed spam emails is close to the levels before the Russian attack in Ukraine.



Who We Are

WithSecure™ 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 & response is 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™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure