MONTHLY TRT REPORT

Threat Intelligence Summary

Fidelis Security

Threat Research Team

November 2022

Overview | November 2022

It's no secret that cyber criminals are continuously updating and evolving their attack techniques to try and stay one step in front of the cyber defenders. As a result, traditional prevention models that rely on detecting known threats must also keep pace. Because the cybersecurity industry trends towards a focus on resiliency over prevention, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) formalized this concept in their latest **Strategic Plan**. By keeping up with the findings highlighted in this report and applying Fidelis Security's proactive defense capabilities, you'll learn how to identify potential security weaknesses in your IT systems and ensure your organization remains protected against the latest and greatest threats.

In this month's Threat Intelligence Summary, the Fidelis Security Threat Research Team (TRT) outlines CISA's new strategy. We also examine the return of an old botnet, supply chain attacks leveraged against news organizations, ongoing data breaches, and more. And we present updated metrics on the most prevalent and urgent vulnerabilities and malware threats affecting the global cyber community.

Security News and Findings

CISA Outlines New Strategy Document for 2023-2025

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) laid out a new **Strategic Plan** for 2023-2025. This new document is a first of its kind for the 4-year-old agency, and it calls for a "whole of nation" approach to protecting critical infrastructure from cyber-attacks. The plan lays out goals in four critical areas: cyber defense, risk reduction and resilience, operational collaboration, and agency unification. The overall theme calls for an evolution beyond traditional prevention strategies to new approaches that revolve around decreasing risk and improving resiliency. This approach signifies a distinct pivot away from the methods used for cyber-defense since the dotcom era. It also recognizes the need for cross-collaboration between federal, state, local, and tribal governments, along with private sector companies that often own and operate the critical infrastructure that CISA defends.

CISA's plan places particular emphasis on proactive strategies that can detect, triage, and quickly respond to new threats and attacks. The plan calls out the importance of full visibility of IT environments and continual risk assessment as foundational elements. At Fidelis Security, we fully support the CISA strategy, and we provide proactive capabilities that accelerate network and endpoint-based detection and response. We also offer game-changing deception technology that bolsters resiliency by giving defenders a distinct advantage over adversaries.

Emotet Botnet Returns to Life

Mirroring our report from November of last year, the Emotet botnet has once again returned to life just in time to spread malware for the holiday season. After a four-month long break in Emotet activity, security researcher Cryptolaemus discovered Emotet distributing phishing emails on November 2, 2022. Emotet is designed to deliver malware through malicious Microsoft Excel or Word attachments that contain DLL loader macros. Once Emotet infects a system, the DLL finds emails to spoof and downloads additional malicious payloads. **BleepingComputer** reported email distribution campaigns targeted at users worldwide utilizing Microsoft Excel files posing as forms, invoices, scans, and other document types.

Microsoft Accuses Chinese Government of Abusing 0-Day Laws

In the **Digital Defense Report 2022**, Microsoft notes that since the advent of the September 2021 law requiring Chinese companies to report vulnerabilities to government authorities, China has been particularly adept at identifying and weaponizing zero-day vulnerabilities. For instance, four days prior to the public disclosure of CVE-2022-26134, Microsoft discovered exploit code for the vulnerability used by a threat actor that is most likely affiliated with China. As Microsoft notes: "The increased use of zero days over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority."

News Websites Compromised in Supply Chain Attack

An unnamed media content provider's infrastructure has been compromised in such a way to infect hundreds of U.S. news websites in a supply-chain attack according to Proofpoint. This compromised infrastructure infects the news websites with the SocGholish malicious JavaScript, which is injected into benign files to push fake browser updates delivered as zip archives.

Twitter Data Breach Affects 5.4 Million Accounts

User records for 5.4 million Twitter users were compromised via a now-patched zero-day vulnerability from December of 2021. A threat actor utilized a vulnerability that allowed anyone to submit an email address or phone number, verify the associated Twitter account, and retrieve the associated account ID. From there, the actor scraped publicly available information to create profiles on users, including phone numbers, email address, locations, and follower accounts. While there was no exposure of login credentials, Twitter recommends that users enable two-factor authentication and is sending out notifications to affected users.

LastPass Data Breach

The password manager service LastPass announced that it suffered a second data breach by same threat actor that compromised its internal development environments in August. The first breach did not impact customer data, but upon return, the actors accessed “certain elements” of customer data. LastPass notes that user passwords remain securely encrypted, and that the company launched an investigation into the issue. This compromise demonstrates how attacks continue against third-party services and supply chains to gain access to intended victim networks. It also shows that threat actors can persist through initial discovery and remediation, highlighting the need for tools that provide detection and response at any point along the kill chain. Furthermore, this finding bolsters CISA’s message regarding the urgency of zero trust adoption and proper cyber hygiene that promotes network and asset resiliency over mere prevention techniques.

Use of Impacket Tool Suite

Last month, we highlighted a government report detailing the use of the open-source Python toolkit Impacket. This tool suite contains a variety of scripts allowing for lateral movement across a network in compromises in the Defense Industrial Base. Fidelis Security’s Threat Intelligence Team continues to see Impacket use in a variety of recent compromises. The team verified that our existing protections can detect and mitigate the threat, and it additionally added several new rules to refine and improve our detections.

Emerging Vulnerabilities

Each month, Fidelis Security tracks emerging vulnerabilities through open-source intelligence and our proprietary tools, and it assigns a weighted score based on the scope, severity, and usage of the vulnerability. In November 2022, Fidelis Security tracked more than three thousand of these vulnerabilities. The chart below shows the relative weight of each Common Vulnerability and Exposure (CVE) tracked as part of this Vulnerability Quotient metric. We summarize the top 10 vulnerabilities that all organizations should be tracking.

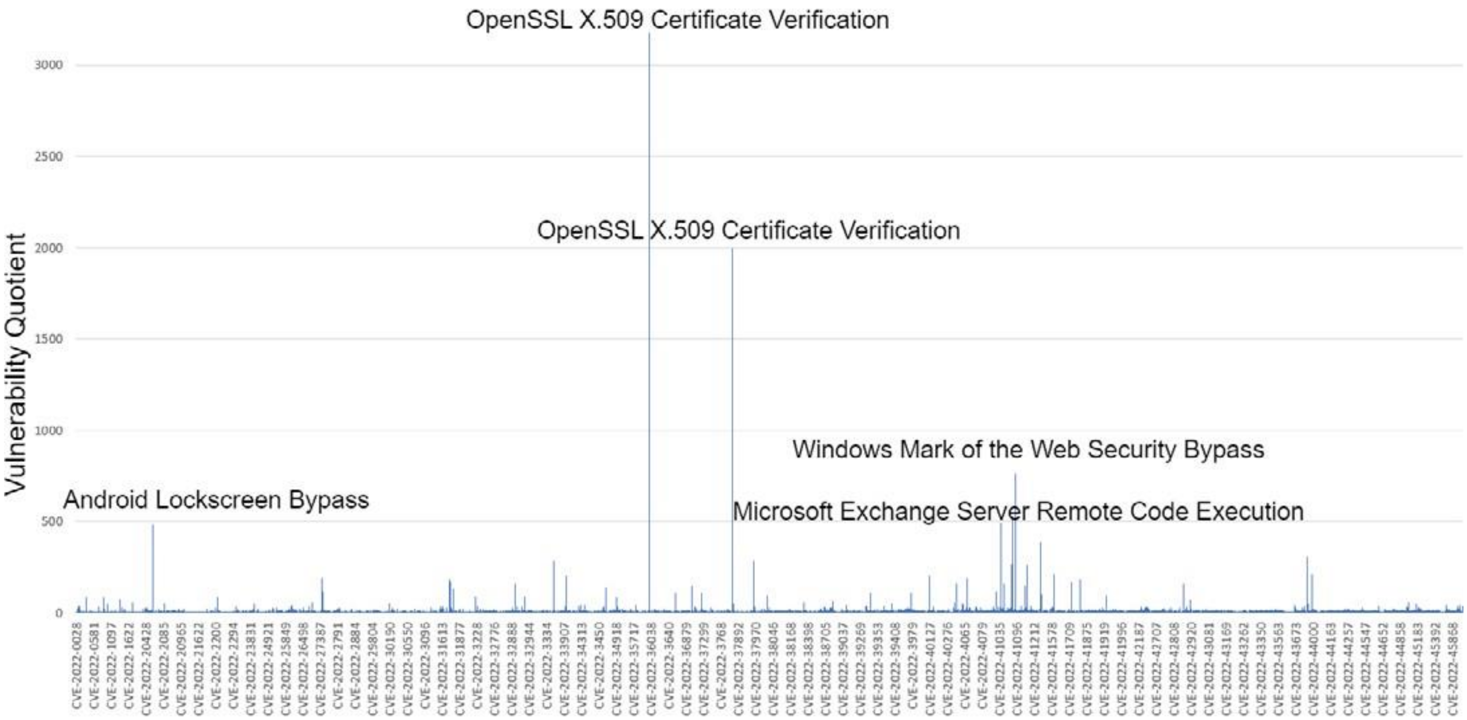

Figure 1: Emerging Vulnerabilities for November 2022

Top 10 Vulnerabilities in November

#1 and #2 OpenSSL X.509 Certificate Verification Buffer Overflow (CVE-2022-3602 and CVE-2022-3786)

Name constraint checking in the X.509 certificate verification is vulnerable to buffer overrun. Note that this occurs after certificate chain signature verification and requires either a certificate authority (CA) to have signed the malicious certificate, or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack or overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially lead to remote code execution. While initially reported as a critical vulnerability, it has since been downgraded to a ranking of "high" due to the implementation of mitigating factors across many platforms. As of publishing, this CVE does not appear to be actively exploited in the wild, but mitigations should be implemented as soon as possible.

#3 Windows Mark of the Web Security Feature Bypass (CVE-2022-41091)

An attacker can craft a malicious file that would evade Mark of the Web (MOTW) defenses, resulting in a limited loss of integrity and availability of security features such as Protected View in Microsoft Office, which rely on MOTW tagging. This vulnerability is being actively exploited in the wild.

#4 and #5 Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2022-41082 and CVE-2022-41040)

Microsoft Exchange Server 2019, Exchange Server 2016 and Exchange Server 2013 are vulnerable to a server-side request forgery (SSRF) attack and remote code execution. An authenticated attacker can use the combination of these two vulnerabilities to elevate privileges and execute arbitrary code on the target Exchange server. Microsoft is aware of active exploits of these zero-day vulnerabilities in limited, targeted attacks.

#6 Android Lockscreen Bypass (CVE-2022-20465)

Android devices have a vulnerability allowing a local attacker to bypass the lockscreen by inserting a SIM card with a PIN code enabled, incorrectly entering the code 3 times, and then entering the PUK code for the SIM. This exploit stems from a logic error in the code for the dismiss function in KeyguardHostViewController.java and related files. This could lead to local escalation of privilege with no additional user interaction needed. A proof of concept is readily available, and success with this attack requires little technical skill.

#7 Google Chrome Sandbox Escape (CVE-2022-4135)

A heap buffer overflow in Google Chrome prior to version 107.0.5304.121 allowed a remote attacker who had compromised the GPU renderer process to potentially perform a sandbox escape via a crafted HTML page. It was assigned a critical vulnerability score as this exploit has been seen in the wild.

#8 Bitbucket Command Injection (CVE-2022-43781)

There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup.”

#9 Windows Kerberos Elevation of Privilege (CVE-2022-33679)

An unauthenticated attacker could perform a man-in-the-middle network exploit to downgrade a client’s encryption to the RC4-md4 cypher, followed by cracking the user’s cypher key. The attacker could then compromise the user’s Kerberos session key to elevate privileges. The attacker must inject themselves into the logical network path between the target and the resource requested by the victim to read or modify network communications. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.

#10 Windows Kerberos RC4-HMAC Elevation of Privilege (CVE-2022-37966)

An unauthenticated attacker can leverage cryptographic protocol vulnerabilities in RFC 4757 (Kerberos encryption type RC4-HMAC-MD5) and MS-PAC (Privilege Attribute Certificate Data Structure specification) to bypass security features in a Windows AD environment. Successful exploitation of this vulnerability requires an attacker to gather information specific to the environment of the targeted component. A successful exploit could lead to privilege escalation to administrator.

CVE Telemetry

Fidelis detected 274 unique exploitation attempts of critical vulnerabilities across our sensor network in November 2022. As is normal, the bulk of these attempts were against older vulnerabilities, with the top two being consistent month-to-month, highlighting the need to keep all software systems up to date with the latest patches. Staying up to date is your best defense in the remediation of long-standing vulnerabilities.

Cyber Threat Analysis Highlights

In November 2022, Fidelis Security enabled clients to defend their networks and clouds from more than:

53K

high-severity malware threats (e.g. Ransomware, Trojans, Backdoors, Exploit Kits, Loaders, Droppers)

274

critical vulnerability exploitation attempts

Cyber adversaries continue to use what works, and pivot only when necessary. Last month featured the same top two attempted exploits that we also saw in November. This means that attackers still gain traction and reliable results exploiting these unpatched vulnerabilities. Meanwhile, another “old, but new again” vulnerability—first witnessed in 2017—took the third spot in our top three most-attempted exploits for November.

The top three most attempted exploits for November were:

Microsoft Office Equation Editor Remote Code Execution Vulnerability (CVE-2018-0802)

Due to a mishandling of objects in memory, Equation Editor in Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, and Microsoft Office 2016 allow for remote code execution. This vulnerability, known as the “Microsoft Office Memory Corruption Vulnerability”, is unique from CVE-2018-0797 and CVE-2018-0812.

Apache Struts Remote Code Execution (CVE-2018-11776)

The open-source framework for Java web applications, Apache Struts 2, suffers from a possible unauthenticated remote code execution vulnerability. This vulnerability presents when the alwaysSelectFullNamespace option is enabled and an ACTION tag is specified without a namespace attribute (or when the attributed is wildcarded). Oracle notes that products incorporating Struts 2 are not necessarily vulnerable. They provide a list of products and status on their webpage so that users can verify their systems. A proof of concept for the vulnerability is publicly available and it is believed there is active use of this exploit in the wild.

Microsoft Office Memory Corruption Vulnerability (CVE-2017-0199)

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory.

Malware

Each month, Fidelis Security tracks the most prevalent malware threats and maps each threat to industrial sectors. This analysis provides defenders with a model for the most pressing threats in their industry. In November 2022, Fidelis Security detected and defended clients against more than 53 thousand high-severity malware threats. In the graph below, we see the mapping of observed threats across the hardest hit industrial, commercial, and governmental sectors that we monitor.

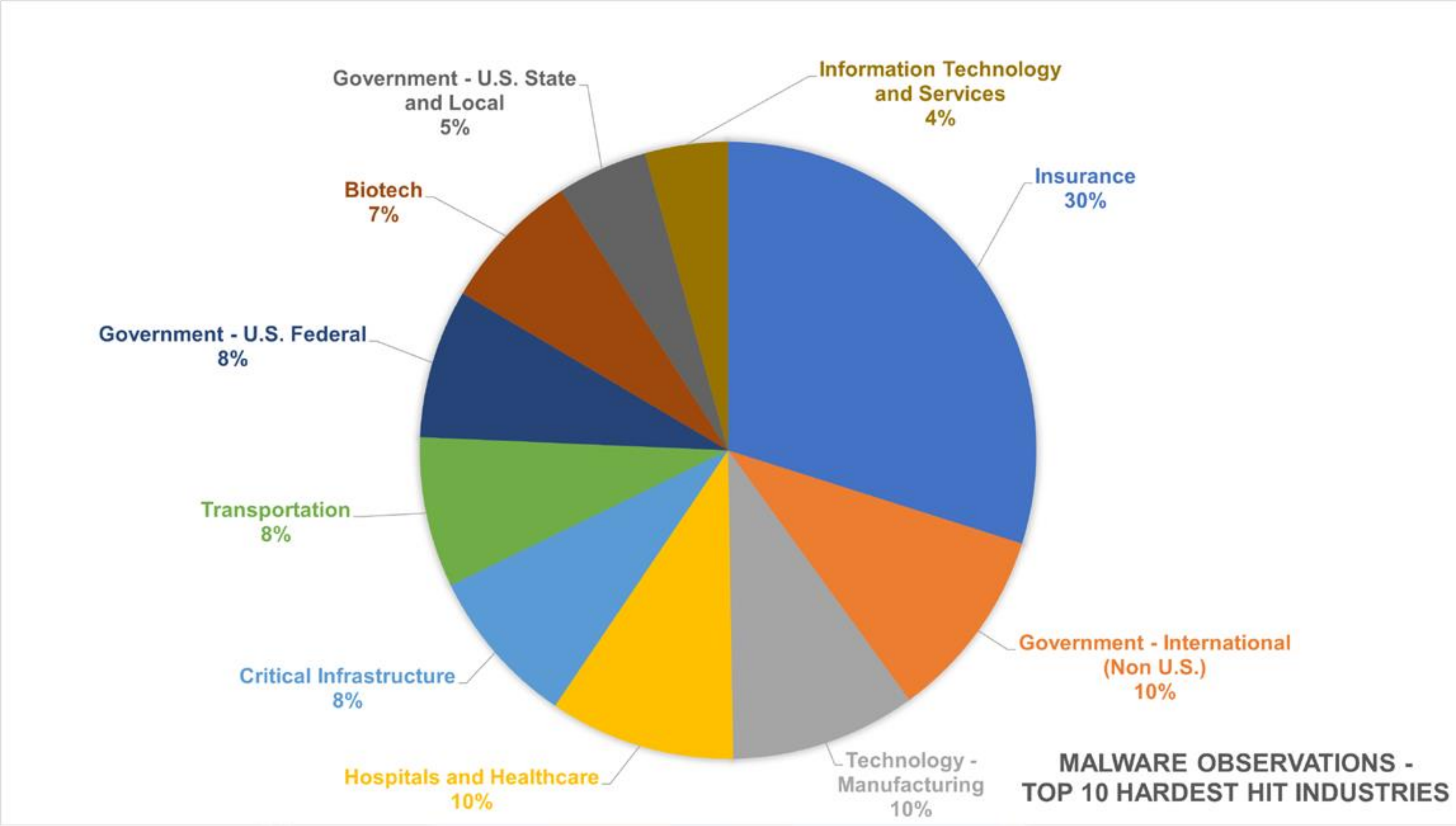

Figure 2: Top 10 Hardest Hit Industries

We also breakdown each sector to examine the top trending malware families in each of the hardest hit sector s. While we only call out our top 10 hardest hit industries, we also curate data across nearly every industry segment. Similarly, the figures in the charts below represent the top threats in each of the represented industries. Some sectors experienced attacks across up to 100 known and unknown attack vectors. In some cases, those “unknowns” make up a significant portion of the observed threats. These observations are based on files pushed to our sandbox malware analysis environments that were deemed suspicious but did not hit directly against any known samples. These findings are critical in the fight against cybercrime, as they suggest a pivot in adversary tactics to previously unknown attack techniques. They also point to the importance of constant vigilance, and the need for having a highly capable threat research team on your side to stay ahead of emerging threats.

Most Observed Malware by Industry

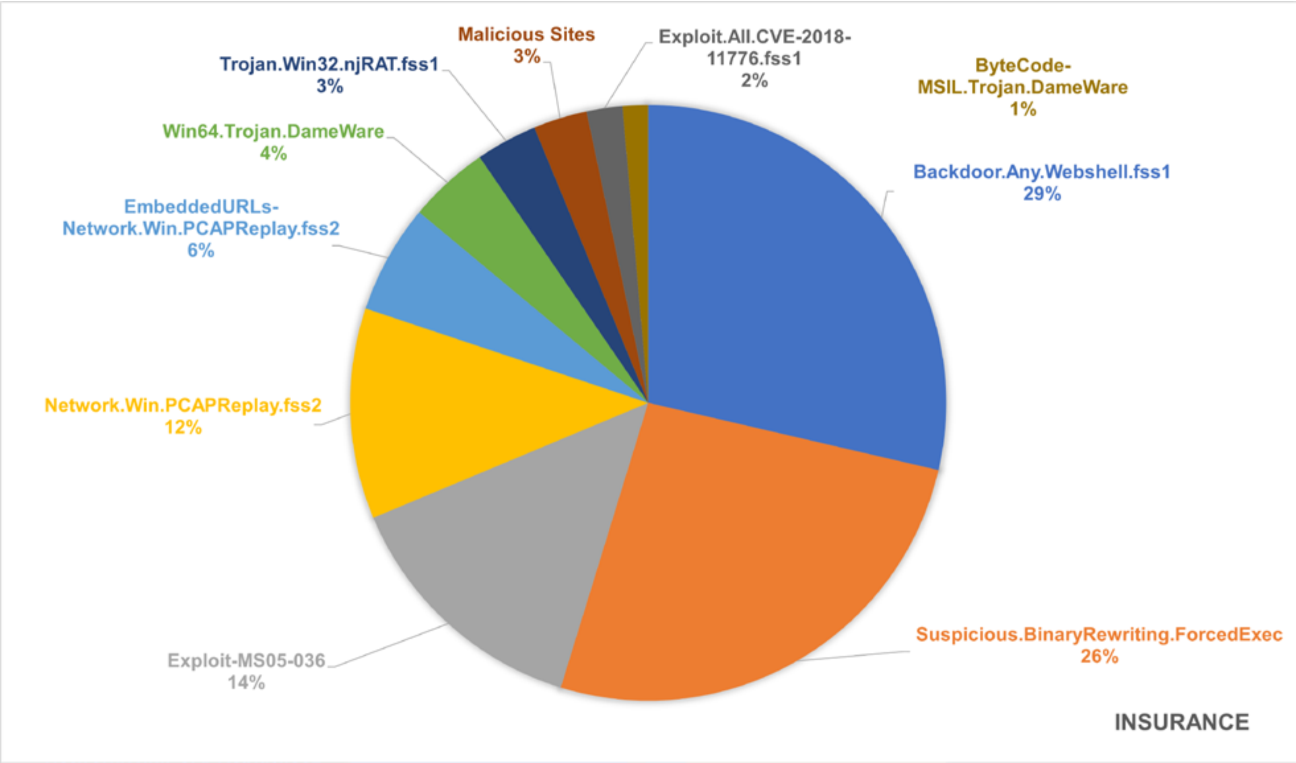

Figure 3: Insurance

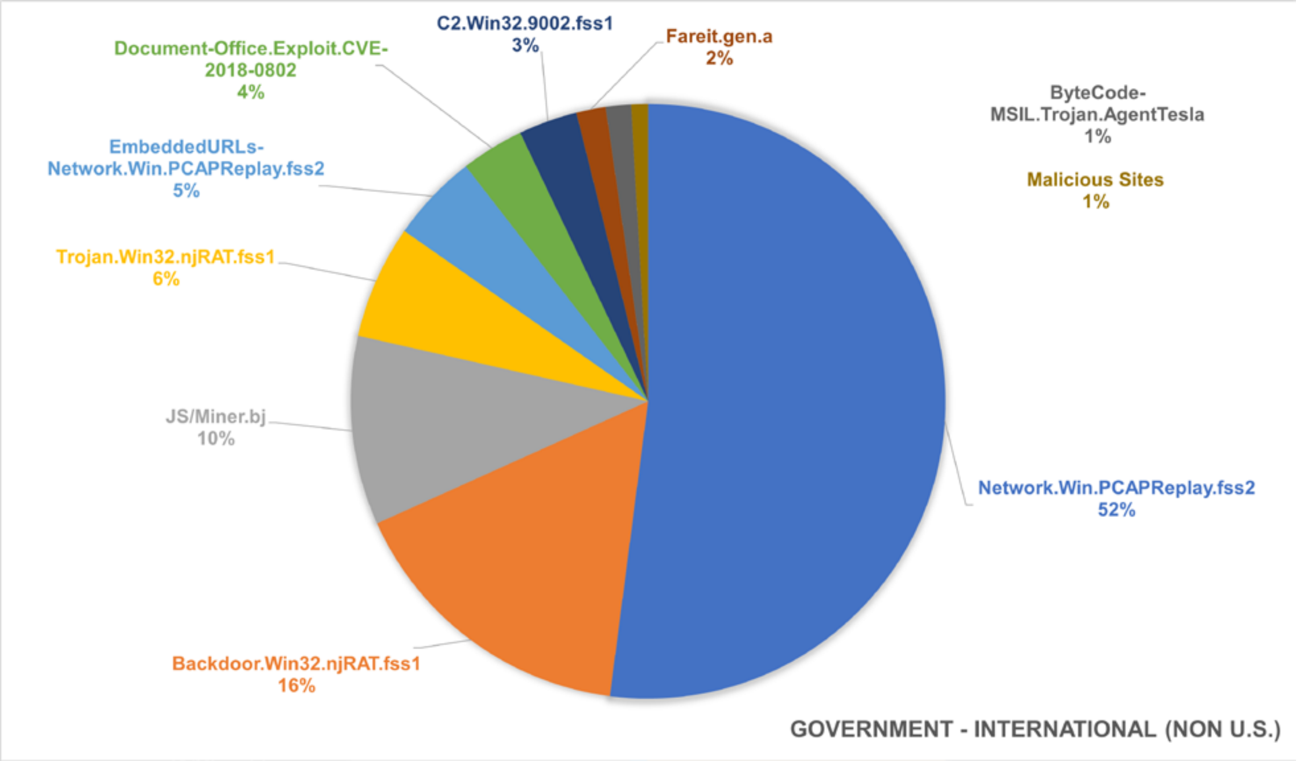

Figure 4: Government - International (Non U.S.)

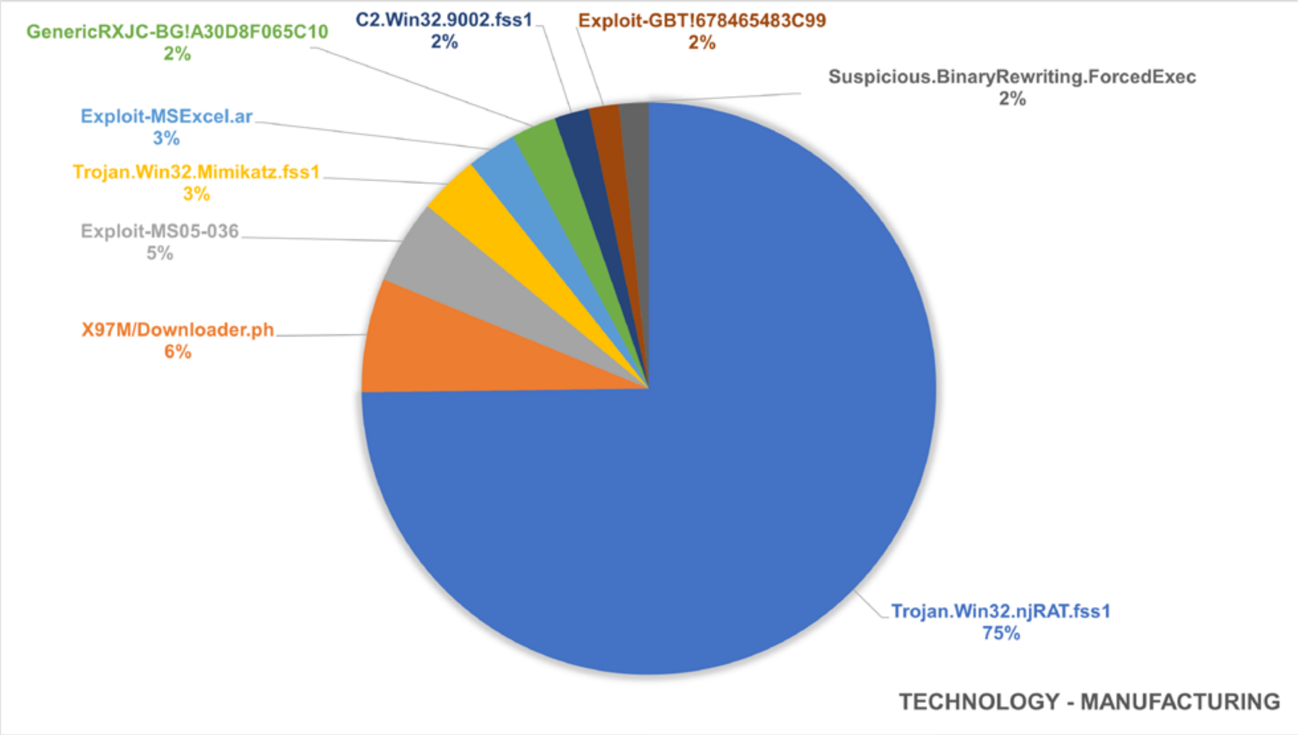

Figure 5: Technology - Manufacturing

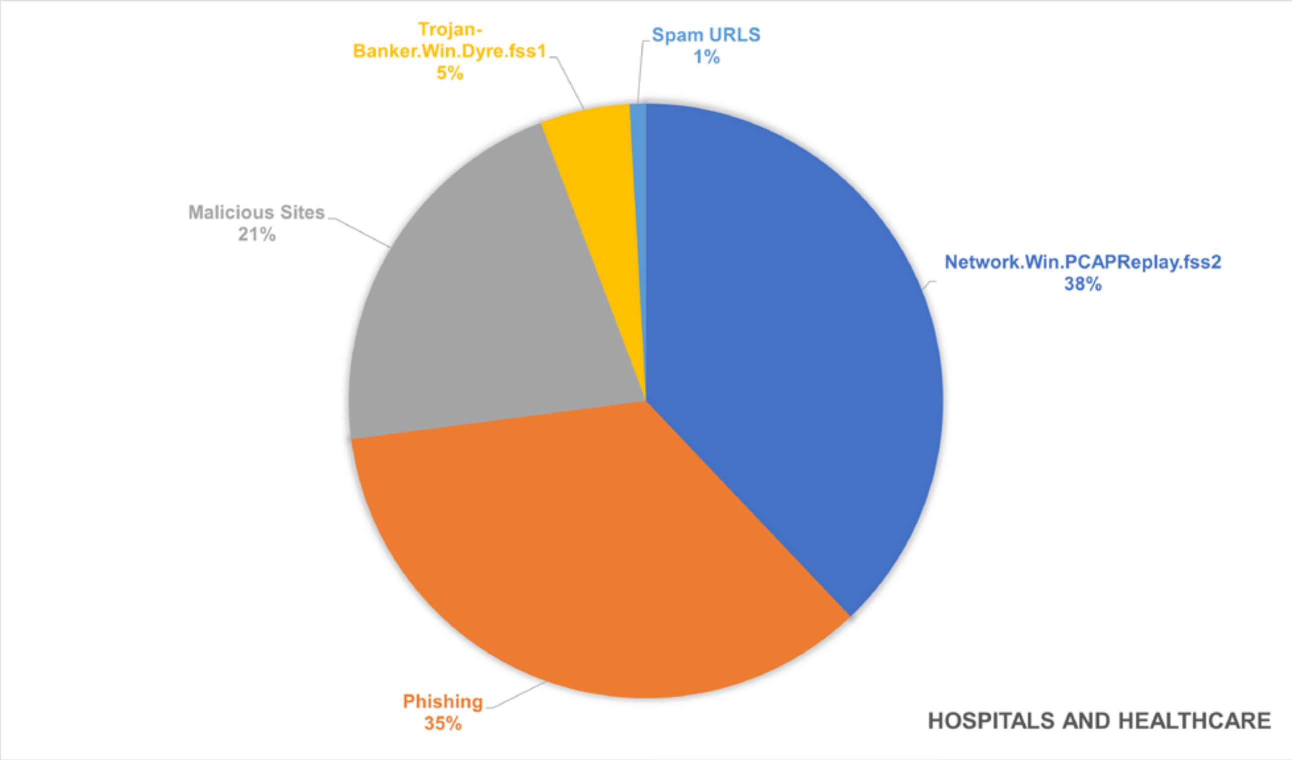

Figure 6: Hospitals and Healthcare

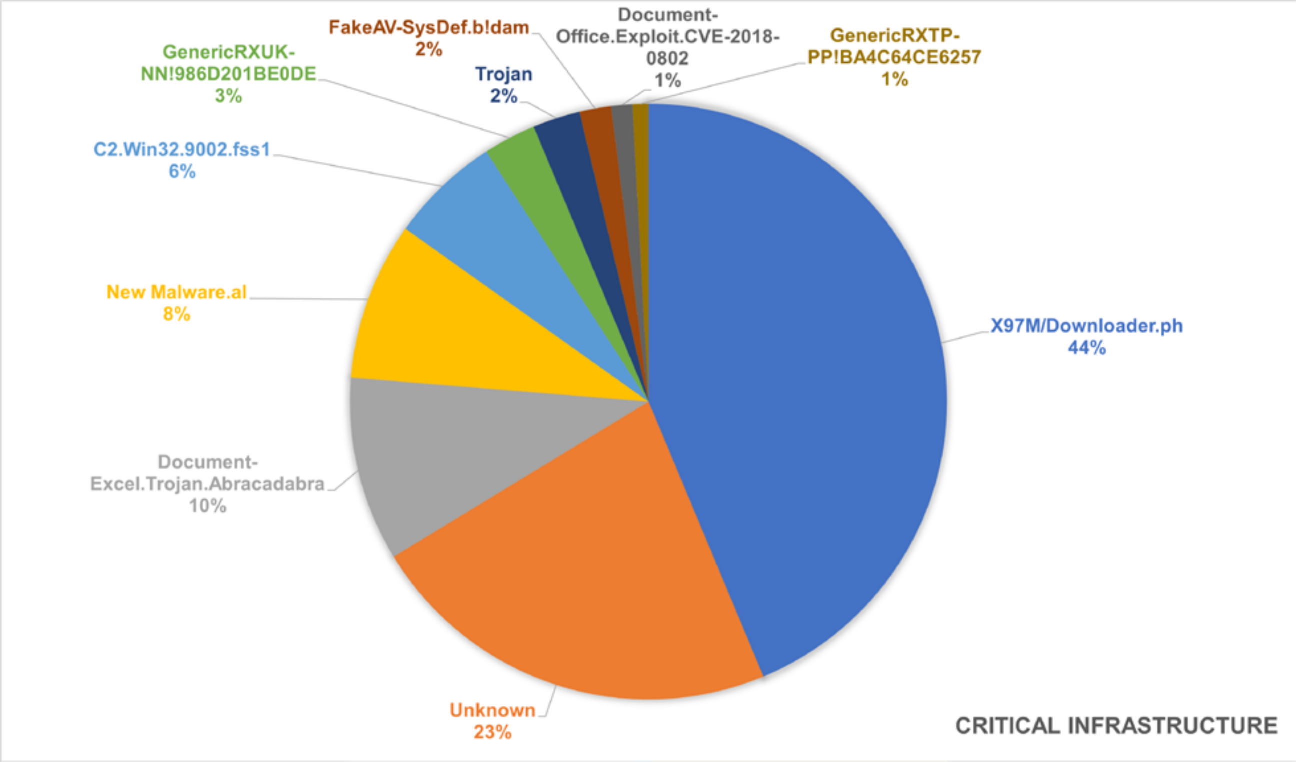

Figure 7: Critical Infrastructure

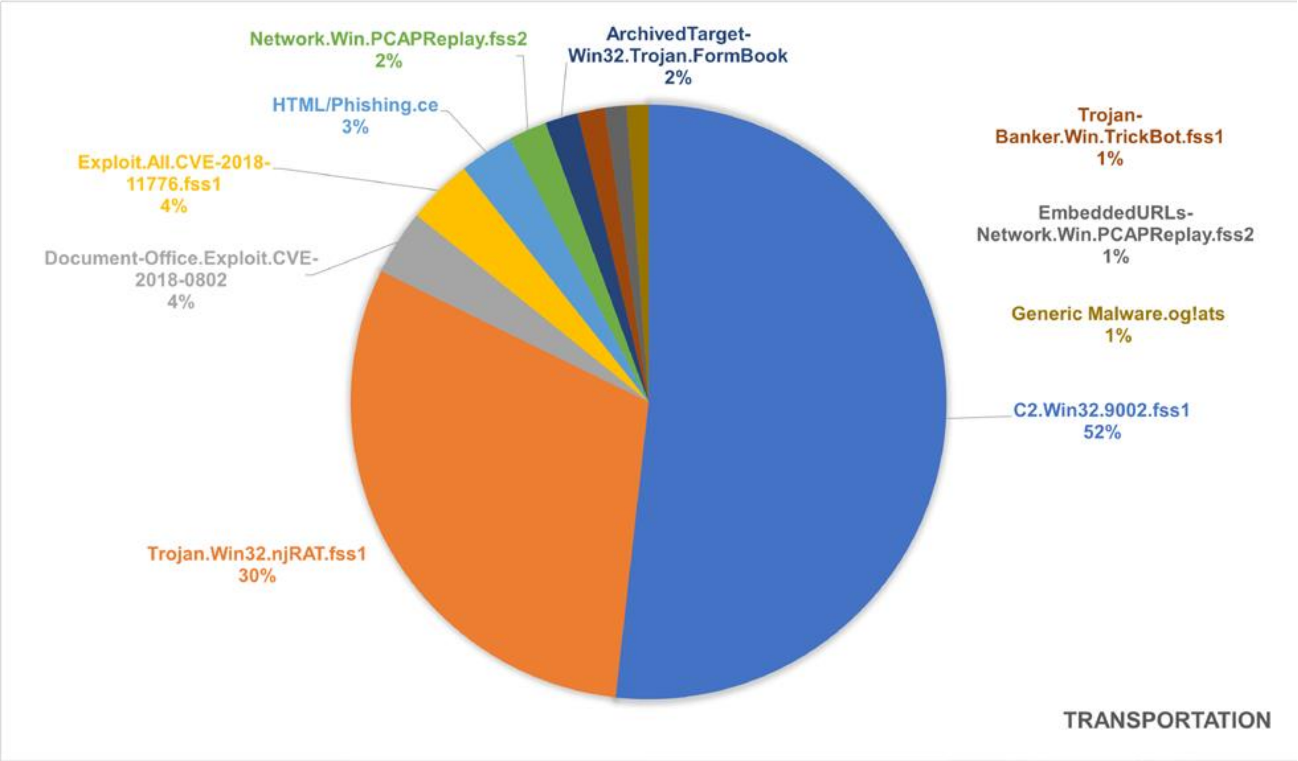

Figure 8: Transportation

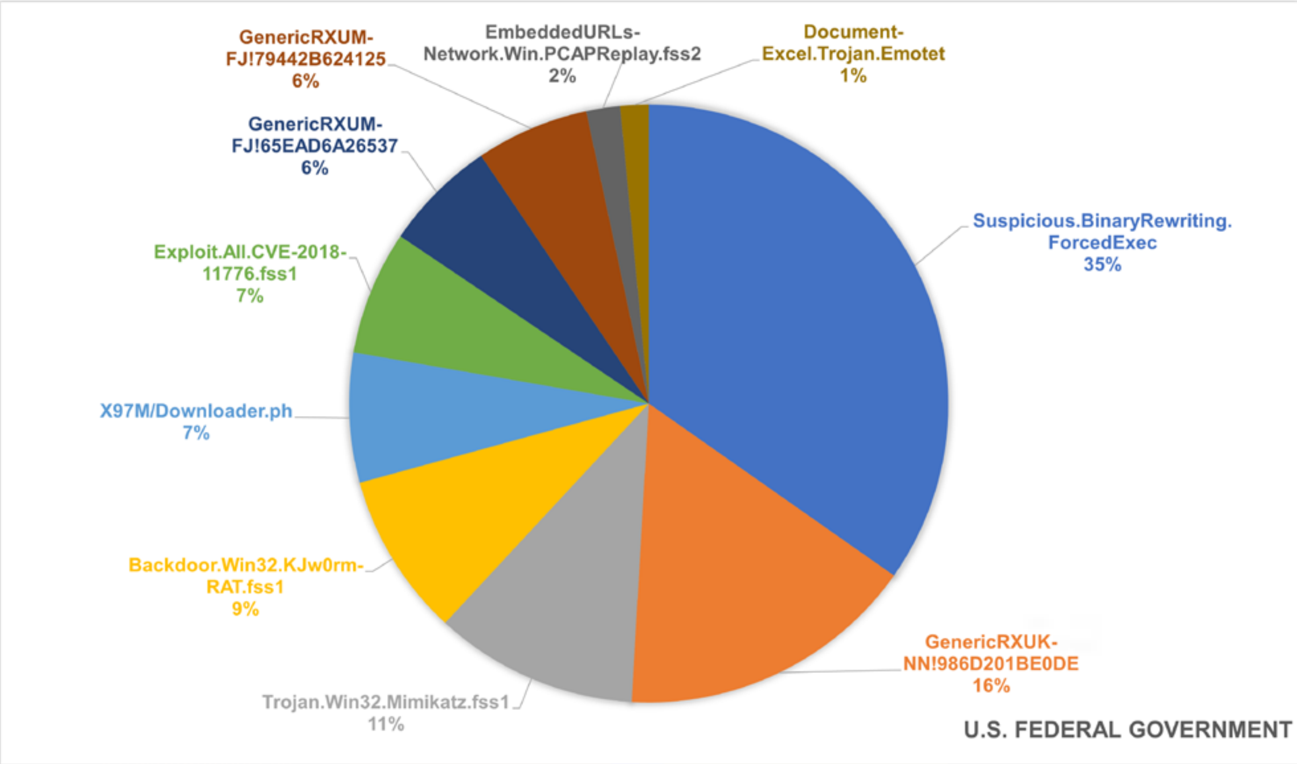

Figure 9: U.S. Federal Government

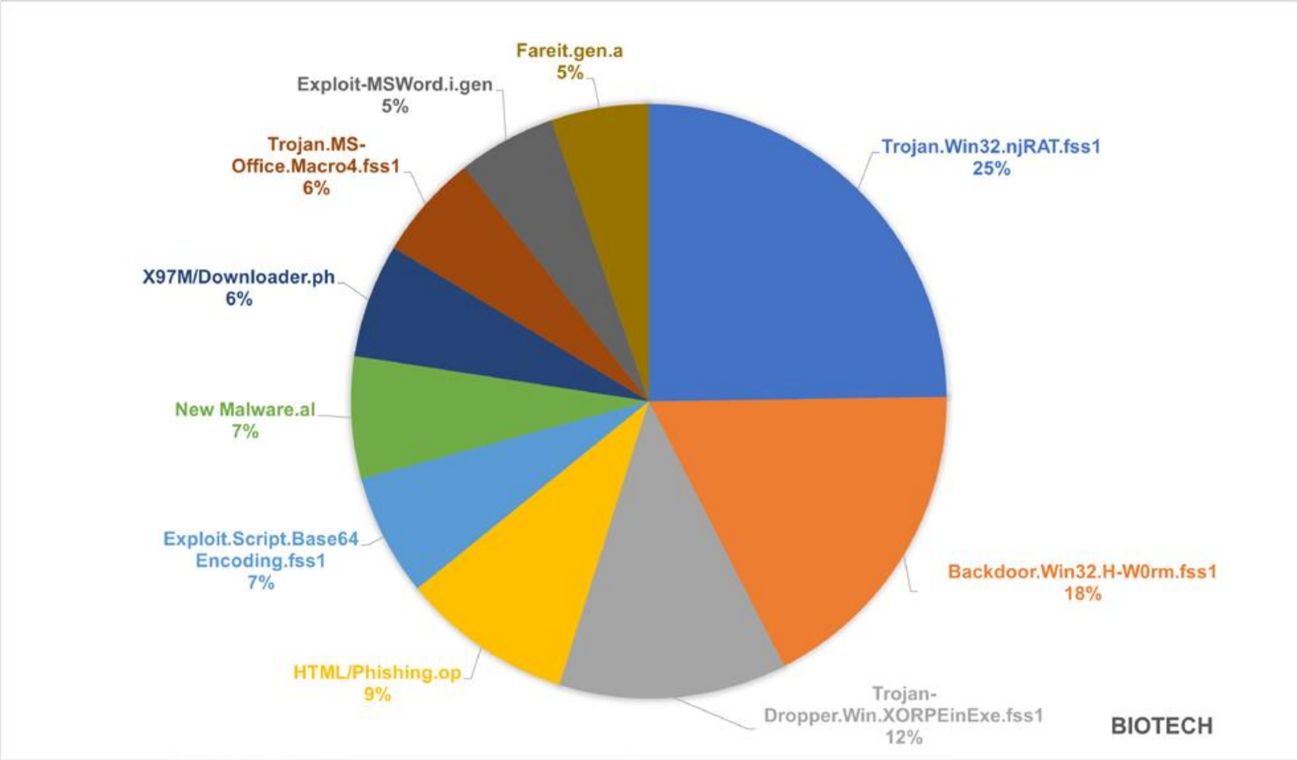

Figure 10: Biotech

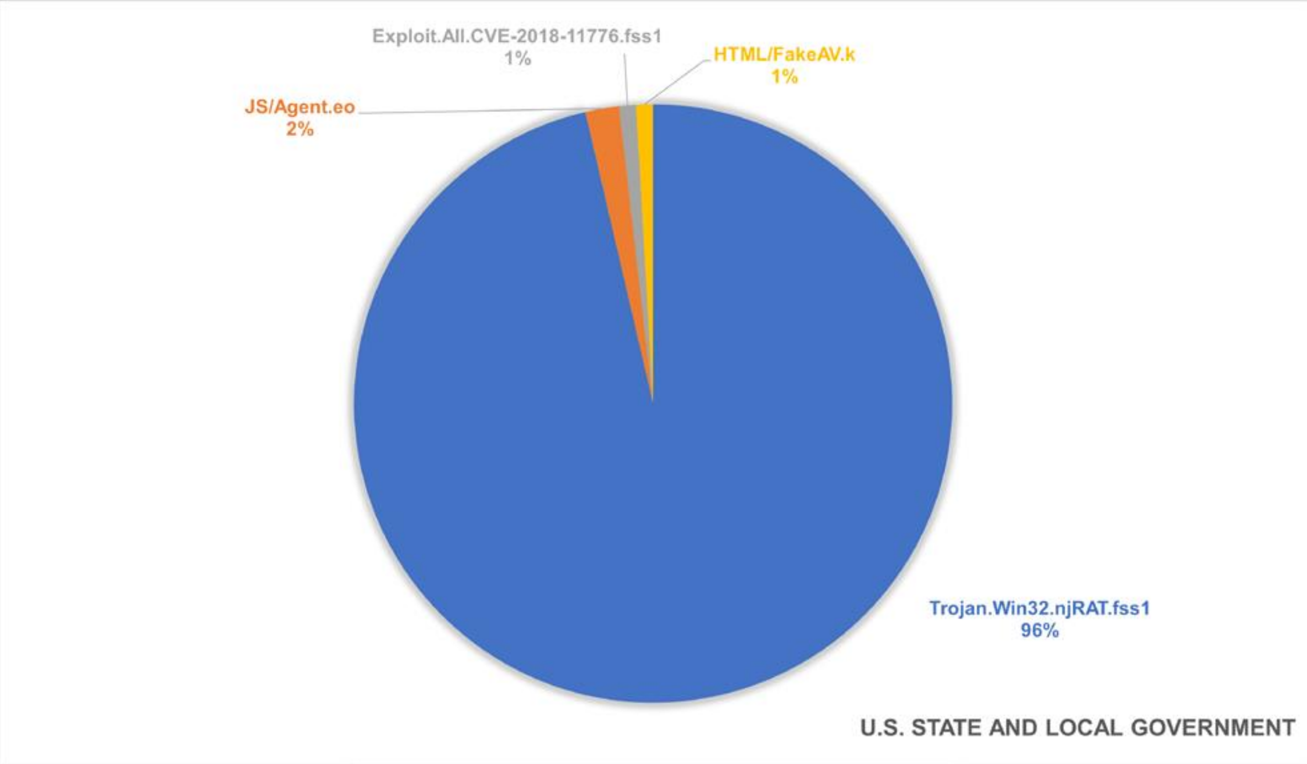

Figure 11: U.S. State and Local Government

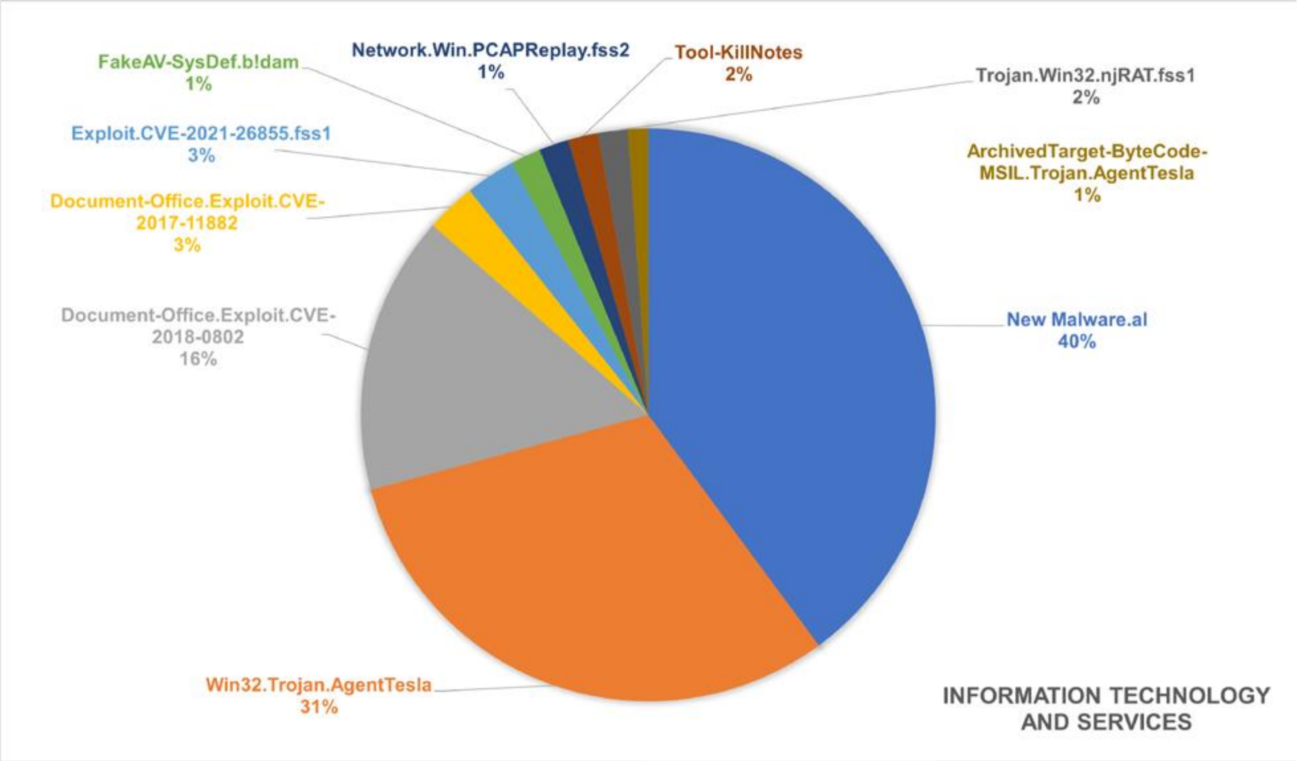

Figure 12: Information Technology and Services

Top 5 Active Malware Families

#1. NjRAT

This month the njRAT remote access tool continues to hold the crown as one of the most popular malware families. First surfacing in 2012, NjRAT makes regular appearances in our telemetry. It has also spawned many derivatives due to multiple leaks of its source code. Capabilities include keystroke logging, camera monitoring, credential theft, reverse shell, upload/download files, and more.

#2. Keyloggers

A category containing several different utilities designed to monitor and record the keystrokes typed on a machine, Fidelis Security sees a sharp increase in the number of keyloggers that were attempted to be deployed against monitored systems.

#3. Blacole

An old malicious javascript file, originally dating back to 2011, Blacole serves as a loader for other malicious tools. Part of the Blackhole family of malware.

#4. X97M
A Windows Trojan downloader often sent as an attachment to email messages sent by other malware samples.

#5. Victy Worm

A worm that tries to spread via removable media by using Windows auto-run functionality.

Summary

At Fidelis Security, the Threat Research Team (TRT) provides day-to-day insight into the functions of threat actors around the globe and works to ensure that our customers are always provided with the most up to date detections and threat feeds.
This month, we examined highlights from open-source reporting about supply chain compromises, governmental actions, the return of a prevalent botnet, and breaches of social media information. We examined new and emerging vulnerabilities that all organizations should keep a close eye on. Finally, we looked at some metrics for the active threats and vulnerabilities seen in the wild for the month of November 2022.

Subscribe to the Threat Geek blog for the latest updates, threat research, and industry insights from the professionals at Fidelis Security. To see first-hand how the Fidelis Security platforms help security teams worldwide protect, detect, respond, and neutralize even the most advanced cyber adversaries across network, endpoints, and cloud, schedule a free demo.

About Fidelis Security

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms.
Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure.
Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.