MONTHLY TRT REPORT

Threat Intelligence Summary

Fidelis Security®

Threat Research Team

October 2022

Overview | October 2022

Cyber actors continually invest in new and inventive tools and technologies. They use their skills to attack enterprises throughout the world, steal intellectual property and sensitive data, ransom data for profit, and deny and degrade critical IT services. Attackers continue to exploit unpatched vulnerabilities and use Phishing and Social Engineering as their “go to” techniques for gaining initial access to systems. Anyone can be a target, making it critically important to stay abreast of current trends and tactics used by these bad actors in their quest to compromise your data and systems.

In this month’s Threat Intelligence Summary, we present newsworthy events and highlights gleaned from open-source reporting and Fidelis’ threat research. You’ll see the types of data our threat research team references to track Advanced Persistent Threat (APT) actor’s tools and techniques. We present the trends of the most exploited vulnerabilities and provide insight into the most pervasive malware threats so you’ll know what to look for as you fortify your own cyber defenses.

APT Reporting Highlights

Advanced Persistent Threat (APT) actors typically represent the most insidious threats that an organization’s network can face. These are an obvious concern for our governmental customers, but this reporting has broader applicability to all sectors. APTs dig for intellectual property, advanced technologies, and data that furthers their intelligence gathering missions. In this section we present a sampling of recent government reporting that highlights the tools and tactics these APT actors use to target organizations.

Joint NSA/FBI/CISA Report on China State Sponsored Actor TTPs

In October, the United States National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity & Infrastructure Security Agency (CISA) published a joint report detailing the most exploited vulnerabilities utilized by the People’s Republic of China (PRC) state-sponsored cyber actors. These attacks targeted American and US ally networks and technology companies to steal valuable intellectual property. It should come as no surprise that many of the most prominent exploits listed include those previously reported by Fidelis Security, including Apache Log4j (CVE-2021-44228), Microsoft Exchange Vulnerabilities (CVE-2021-26857, CVE-2021-26857, and CVE-2021-27065), and a F5-Big-IP remote code execution vulnerability (CVE-2020-5902). For a full list of the most commonly seen vulnerabilities, Fidelis Security recommends all customers follow the joint reports at **media.defense.gov**.

FBI Report Detailing Iranian Cyber Actor Group “Emennet Pasargad” Hack and Leak Operations

The US FBI provided an advisory concerning Iranian cyber actor group “Emennet Pasargad” performing hack-and-leak operations of primarily Israeli and US organizations. These attacks aimed to cause reputational damage and financial loss for targeted organizations. Emennet tends to amplify and exaggerate the level of success that is achieved against victims’ networks to increase the reputational damage that an organization suffers. The FBI lays out several Tactics, Techniques, and Procedures (TTPs) used by Emennet, calling special attention to vulnerabilities in Drupal, Wordpress, Ckeditor, and of course Apache’s Log4j. The report also details two alternate personas used by Emennet, identified as the “Hackers of Savior” and “Deus”. For further information related to this actor, please see the FBI report available at **ic3.gov**.

Joint CISA/FBI/NSA Report on Use of Impacket Scripts in Compromise of Defense Industrial Base

In early October CISA, the FBI, and NSA published a joint report detailing the use of the open-source Python toolkit “Impacket”. This toolkit enabled lateral movement across a compromise of a Defense Industrial Base (DIB) partner organization, likely initiated by multiple APT actors. The reports primarily detail two Impacket modules which are used to invoke the Windows Management Instrumentation (WMI) and Server Message Block (SMB) protocols. These tools provide remote access by leveraging previously compromised account credentials. The report provides an in-depth look at the chain of compromise and exploits used in this attack. It also provides a list of actionable mitigations. For more information, please reference the report at **media.defense.gov.**

Emerging Vulnerabilities

Attackers constantly change tactics and shift to vulnerabilities and exploits most likely to succeed. For October 2022, Fidelis Security tracked almost six thousand unique and emerging vulnerabilities and assigned a weighted score to each based on its scope, severity, and usage. The chart below shows the relative weight of each Common Vulnerability and Exposure (CVE) tracked as part of this Vulnerability Quotient metric.

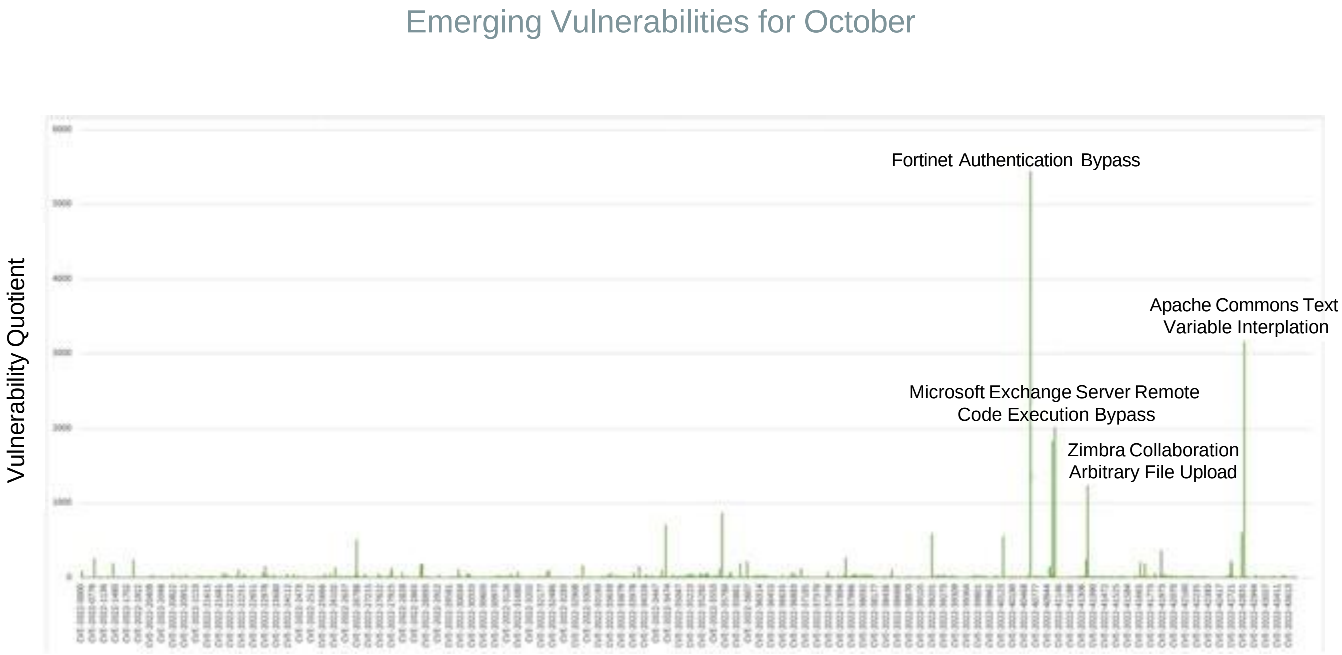

Figure 1: Emerging Vulnerabilities for October 2022

Top 10 Vulnerabilities in October

Our Threat Research Team (TRT) works diligently to keep customers current with the latest trending CVEs and protected from the most pressing threats. Here are the top ten CVEs observed during October.

#1 Fortinet Authentication Bypass (CVE-2022-40684)

An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS, FortiProxy, and FortiSwitchManager allows an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. Evidence suggests active exploitation in the wild by threat actors via a Metasploit module.

#2 Apache Commons Text Variable Interpolation (CVE-2022-42889)

Apache Commons Text is a library of focused string-manipulation algorithms. A flaw discovered in library versions 1.5 through 1.9 allows an attacker to exploit a variable interpolation process. The exploit can cause dynamic definition of properties, leading to potential remote code execution, as well as unintentional contact with remote servers.

#3 and #4 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.

#5 Zimbra Collaboration Arbitrary File Upload (CVE-2022-41352)

An issue discovered in the Zimbra Collaboration (ZCS) open-source email platform that allows an attacker to upload arbitrary files through amavisd via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public). This provides unauthorized access to any user account in the system. Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavisd automatically prefers it over cpio. A Metasploit module exists for this exploit.

#6 SQLite Array Bounds Overflow (CVE-2022-35737)

SQLite 1.0.12 through 3.39.2 sometimes allows an array-bounds overflow. On vulnerable systems, this CVE can be exploited by passing billion-byte string argument to certain C API calls. While this vulnerability was only recently discovered, the issue has existed in the SQLite code base since the year 2000.

#7 Windows TCP/IP Remote Code Execution Vulnerability (CVE-2022-34718)

This Windows TCP/IP Remote Code Execution Vulnerability allows an unauthenticated attacker to send a specially crafted IPv6 packet to a Windows node where IPSec is enabled. A successful exploitation of this vulnerability could enable remote code execution on an impacted machine.

#8 Apple iOS Application Arbitrary Kernel Code Execution (CVE-2022-42827)

Apple recently addressed an out-of-bounds write issue by improving bounds checking. An application running on an unpatched system may be able to exploit this vulnerability to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.

#9 Cobalt Strike Cross Site Scripting Vulnerability (CVE-2022-39197)

A Cross Site Scripting (XSS) vulnerability in HelpSystems Cobalt Strike through 4.7 allows a remote attacker to execute HTML on the Cobalt Strike teamserver. To exploit the vulnerability, one must first inspect a Cobalt Strike payload, and then modify the username field in the payload. Alternately, this vulnerability can be exploited by creating a new payload with the extracted information and then modifying the username field to a malformed value.

#10 Trend Micro Apex One Origin Validation Vulnerability (CVE-2022-40140)

An origin validation error vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to cause a denial-of-service (DDoS) on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. Trend Micro states that they observed at least one active attempt at exploitation in the wild.

CVE Telemetry

In October 2022, Fidelis Security detected 262 exploitation attempts of critical vulnerabilities across our sensor network. As is normal, the bulk of these attempts were against older vulnerabilities, highlighting the need to keep all software systems up to date with the latest patches. Staying up to date on updates and patches is your best defense in the remediation of long-standing vulnerabilities.

Cyber Threat Analysis Highlights

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

84K

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

262

critical vulnerability exploitation attempts

The top three most attempted exploits for October were:

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.

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.

Microsoft Office Specially Crafted Document (CVE-2017-0199)

By exploiting the “Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API”, remote attackers can execute arbitrary code via crafted documents. This vulnerability affects Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8.1.

Malware

Over the past 30 days, Fidelis Security detected and enabled clients to defend against more than 84-thousand high-severity malware threats. In last month's Threat Intelligence Summary report, we looked at malware samples across all monitored systems, broken down by industry. For October, we examine the top five malware samples and take a deeper look at two of the industry sectors that we touched on last month. As is the norm, we observe that the most utilized malware samples are quite dated, demonstrating that threat actors readily reuse tools that Fidelis Security actively detects.

Top 5 Trending Malware Families

#1. NjRAT

Continuing the theme of what is old is new again, we continue to see the njRAT remote access tool 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. FAREIT

Another classic from 2012, the Fareit malware family has changed continuously throughout its years of use. While it is primarily used for credential theft, Fareit can also include a DDoS component.

#3. Fakesysdef

A trojan targeting Microsoft Windows, Fakesysdef was first discovered in 2010. It is a family of malware that claims to scan a PC for hardware defects, fabricates claims of errors, attempts to "fix" them, and informs the user that they must pay to receive the fix for the detected errors.

#4. TrickBot

A banking trojan dating back to 2016, TrickBot includes capabilities that attempt to steal account credentials, personally identifiable information (PII), and Bitcoin. TrickBot has evolved, and now primarily functions as a loader for other malware strains. It has been associated with intrusion chains involving Conti ransomware, Wizard Spider, UNC18178, and TA505. For a historical perspective, Fidelis Security performed a deep dive analysis of an early strain as seen **here**.

#5. Dyre

Also identified as Dyreza, Dyre is a modular Banking Trojan seen in the wild since at least 2014. Dyre is associated with the cybercriminal threat group Wizard Spider. Now primarily functions as a loader for other malware, often leading to intrusions which result in ransomware deployment.

Sector Specific Malware Trends

In this section we will examine two of the industrial sectors that we presented metrics for last month: retail and financial services. Each comparison provides some interesting insight into the types of malware threats observed in the wild for the month of October. You'll also see data that demonstrates how threat actors dig into what works best in different industries.

#1 Retail

The retail sector provides customer-facing point of sale access to consumer goods through both in-person and online stores. As we see in this breakdown, the Dyre family of malware represents by far the largest portion of the malware threats seen within the sector at nearly 59%. Continuing to align with our overall highest trending samples we see NjRAT taking 11.77% of the sample space. Rounding out the sector we see various machine learning based heuristics flagging suspicious files, Trojans exfiltrating data via DNS, malicious PDF files with malformed hyperlinks to phishing websites, and a small sampling of Microsoft Excel malicious macro files.

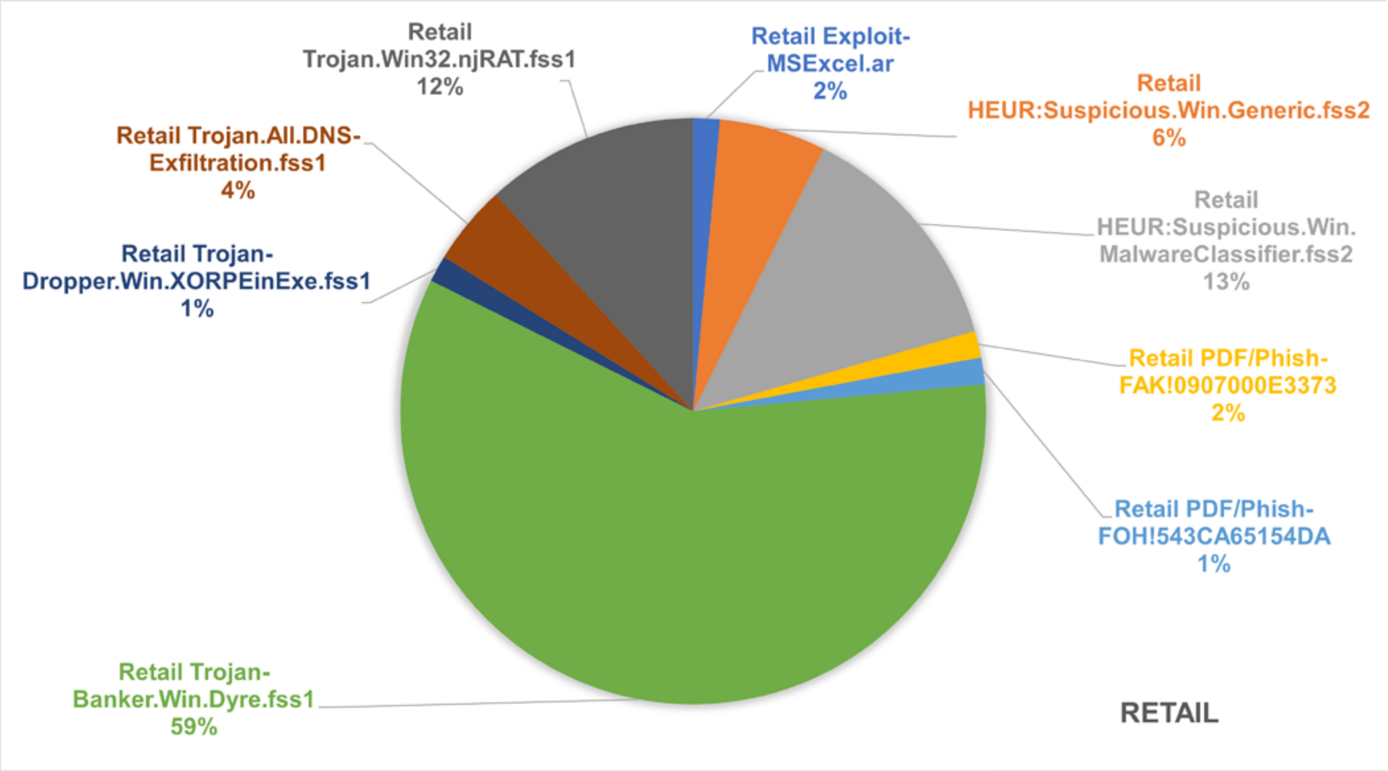

Figure 2: Malware Threats Observed in the Retail Market

#2 Financial Services

The financial services sector consists of businesses such as banks, investment firms, tax preparation companies, etc. Unlike the retail space above, none of our top trending malware families make the cut in this segment. Instead, note that Fidelis Security flagged nearly 37% of malicious detections as files containing digital certificates known to be used by APT actors associated to Deresbi, Sakula, and FF-RAT malware families. We also see the prevalence of attacks against Microsoft Office products, with nearly 29% of the market makeup being malicious Microsoft Word documents (Exploit-MSWord.I.gen), 10.5% as follow-on Office macro downloader utilities (W97M/Downloader.asx) utilized in likely phishing attempts, and nearly 8% of the detections being related to a vulnerability that allows a denial of service (crash) attack against clients running Word 2000. Rounding out this collection we see smaller segments made up of two Remote Access Trojans (RATs), Gh0st (10.5%), and Alienspy (5%).

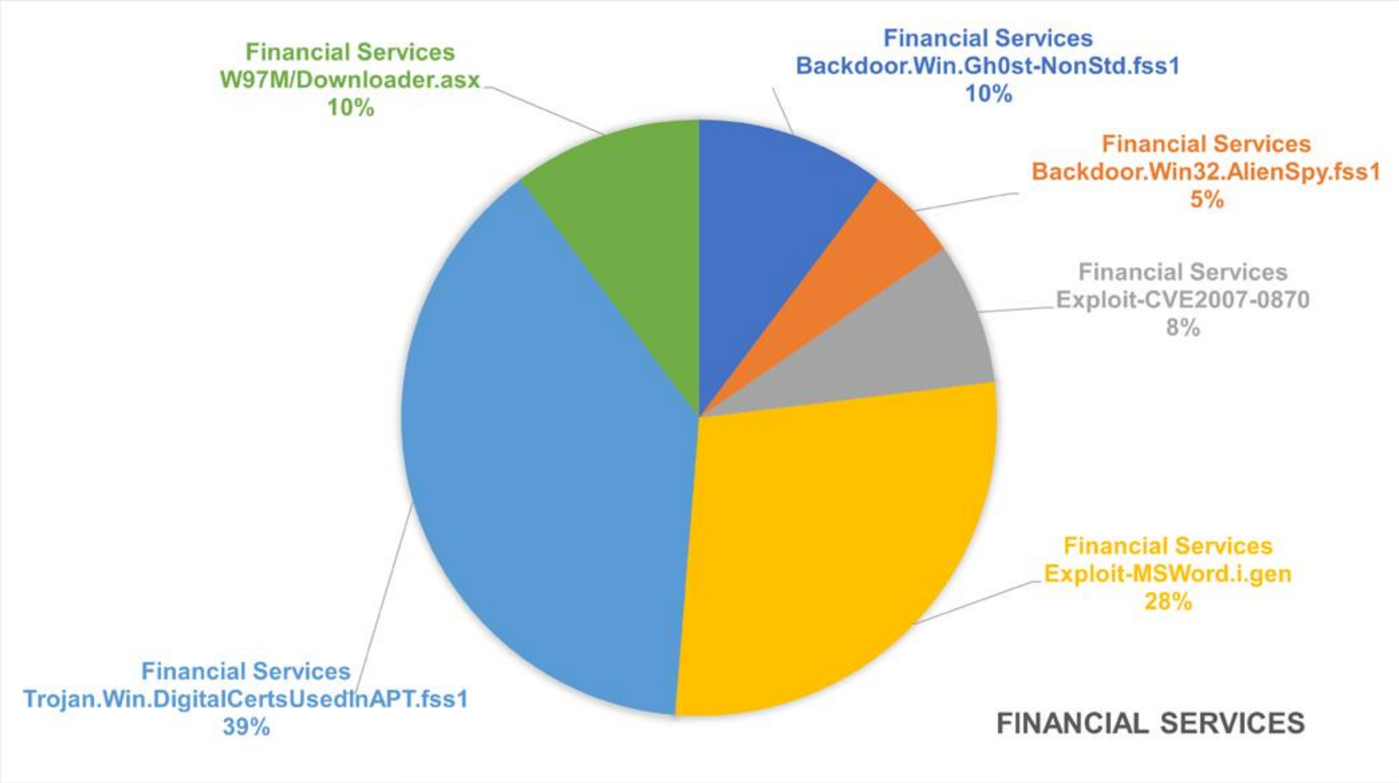

Figure 3. Malware Threats Observed in the Financial Services Market

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 several governmental agencies' reporting that highlighted the tactics and vulnerabilities utilized by nation state APT actors. 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 October 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.

Fidelis Security