Metrics | January 2022

Malware
Fidelis enabled clients to defend their networks from **585K** instances of malicious and potentially malicious software (includes Adware/Bloatware) traversing the Internet in January 2022.

High Severity
Fidelis Cybersecurity helped clients defend their networks from **582K** malware threats of high severity (e.g., Ransomware, Trojans, Backdoors, Exploit Kits, Loaders, Droppers) encountered in January 2022. The following are the top malware variants (by volume) that Fidelis Cybersecurity detected through telemetry for December 2021:

[1] **Andromeda**
- A modular Trojan; active in the wild since at least 2011.
- Also identified as Gamarue or Wauchos.
- Primarily used as a loader for other malware, including ransomware.
- There is likely a ‘cracked’ builder in circulation for v2.06.

[2] **Chanitor**
- Downloader; active in the wild since at least 2013.
- Also identified as Hancitor; historically associated to threats such as Pony and Vawtrak.
- Commonly delivered through phishing (e.g., GoogleDoc Links & DocuSign/Invoice Themes).

[3] **KJw0rm**
- Remote Access Trojan (RAT); active in the wild since at least 2014.
- Also identified as NJW0rm; derivative of njRAT (source code leaked).
- Use historically associated with threat actors in Southwest Asia.

[4] **njRAT**
- Remote Access Trojan (RAT); active in the wild since at least 2012.
- Also identified as Bladabindi; use historically associated with Southwest Asian state-sponsored actors (e.g., Gorgon Group, APT41, Transparent Tribe).
- Likely to be many derivative variants in circulation (various source code leaks).

[5] **vW0rm**
- JavaScript-based Remote Access Trojan (RAT); active in the wild since at least 2016.
- Also identified as Vengeance Justice Worm; authorship attributed to v_B01 (aka Sliemerez) who likely associated with the DevPoint Arabic-language malware development community.
- Other known variants include VisualBasic-based (Vengeance Worm), an AutoHotkey-based variant (Vengeance Rise Worm), and a PowerShell-based variant (Vengeance Depth Worm).
Vulnerabilities

Our tailored and community integrated detections helped clients to orient and respond to over 3.5K critical vulnerability exploitation events in January 2022. The Equation Editor vulnerability (CVE-2017-11882) has taken lead breaking into the new year – see Figure 1 below.

Active Exploitation

We continue to observe significant exploitation activity for much older vulnerabilities indicating that threat actors will continue taking advantage of opportunities presenting an optimal return on their investment. Vulnerabilities in user-software such as Microsoft Office and Internet Explorer provide a unique opportunity for threat actors to gain a foothold, when network perimeter posture is hardened. Threat actors are almost certainly keen to the notion that the mitigation of vulnerabilities in user-software may also take less priority, especially when contrasted against critical vulnerabilities which are remotely exploitable and public facing.

The following vulnerabilities represent 95% of the observed vulnerability exploitation attempts for January 2022 and customers should ensure that their systems are properly updated and patched against these vulnerabilities.

**CVE-2017-11882**

(Microsoft Office – Remote Code Execution) accounted for approximately 75% of the observed vulnerability exploitation attempts for January 2021. Infamously known as the 'Equation Editor' vulnerability, allows user-assisted (e.g., opening the file) arbitrary code execution against Microsoft Office v2007SP3, v2010SP2, v2013SP1, and v2016. This specific vulnerability highlighted the inherent risk in the porting of legacy code libraries as the equation editor module in these Microsoft Office versions allowed actors to side-step modern anti-exploitation mitigations (e.g., ASLR – Address Space Layout Randomization) and achieve remote code execution through buffer-overflow. Most likely to be leveraged by threat actors delivering phishing lures.

**CVE-2014-1776**

(Internet Explorer - Remote Code Execution) accounted for approximately 10% of the observed vulnerability exploitation attempts for January 2021. This vulnerability allows remote attackers to execute arbitrary code against Internet Explorer v6-v11. Actively exploited in the wild since April 2014 and likely to exploit the end-user, through a drive-by-download (e.g., Exploit Kit).
Threat Intelligence Summary

MONTHLY TRT REPORT

CVE-2021-44228
Apache Log4j2 – Remote Code Execution accounted for approximately 5% of the observed vulnerability exploitation attempts for January 2022. This vulnerability allows arbitrary code execution against public facing infrastructure (web-based and embedded systems/software) which leverage Apache’s Log4j2 v2.0beta9 - 2.12.1 and 2.13.0 - 2.15.0. This vulnerability is actively exploited in the wild by a multitude of threat actors of various skill and motivation.

CVE-2017-0199
Microsoft Office/Wordpad – Remote Code Execution accounted for approximately 4% of the observed vulnerability exploitation attempts for January 2022. This vulnerability allows remote attackers to execute arbitrary code against Microsoft Office and Wordpad (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, Windows 8.1) and is mostly likely to be leveraged by threat actors delivering phishing lures.

CVE-2018-11776
Apache Struts – Remote Code Execution accounted for approximately 1% of the observed vulnerability exploitation attempts for January 2022. This vulnerability allows arbitrary code execution against Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 and is most likely to be leveraged by threat actors seeking to gain a foothold in the enterprise, through compromise of external facing web resources.

Emerging
The following (weighted) emerging vulnerability threats this period, derived from our proprietary vulnerability tracking and scoring system – enhanced with context.

[1] CVE-2021-44228
- Remote Code Execution (RCE) – 10.0 Critical
- Impacts Log4j2 v2.0beta9 - 2.12.1 and 2.13.0 - 2.15.0
- Proof-of-Concept (PoC) code available.
- Exploitation in the wild by actors of various sophistication and motivation.

[2] CVE-2021-4034
- Local Privilege Escalation (LPE) – Rating Not Currently Assigned by NVD.
- Memory corruption leading to local privilege escalation in Polkit (PolicyKit) pkexec utility.
- Pkexec is a SUID-privileged program installed by default on popular Linux distributions.
- Allows any local unprivileged user to gain full root privileges.
- PoC exploit code is available.

- Local Privilege Escalation (LPE) – Rating Not Currently Assigned by NVD.
- Vulnerability allows heap-based buffer overflow in Linux Kernel.
- Impacts Red Hat Enterprise Linux 8.4 GA onwards and almost certainly additional Linux variants.
- Likely allows container breakout of containerized applications (e.g., Kubernetes)
- PoC exploit code is available.

- Improper input validation leading to SQL injection – 7.5 High
- Impacts WordPress versions 3.7.0-3.7.37 and v5.0.0-5.8.3, wherein plugins that leverage WP_Query function are abused to trigger an SQL injection.
- PoC exploit code is available.

[5] CVE-2021-40444
- Remote Code Execution (RCE) – 7.8 High
- Microsoft asserts that Application Guard and Protected View for Office mitigates exploitation, but likely won’t prevent user-assisted execution.
- PoC exploit code is available.
Key Findings | January 2022

The New Year brought with it no relief to the onslaught of cybersecurity threats each of us face. None were excused from having to defend their networks against advanced adversaries, whether they be state-sponsored or cybercriminal - it’s become increasingly more difficult over the last few years to discern the difference. Fidelis Cybersecurity enables our clients to fight smarter, not necessarily harder, demonstrating how defenders leveraging our technology and the right mindset can nip toss the adversary in each of the following real-world instances:

- Destructive malware attacks impacted the government of Ukraine, which resurrected dormant fears of another NotPetya - a 2017 destructive malware campaign attributed to Russia which directly impacted the Ukraine, producing significant and perhaps unforeseen bleed over impact into other global regions due it’s lateral movement capability (e.g., integrated EternalBlue SMB exploitation) across modern globally integrated networks.

- An advanced cyber threat actor who’s techniques and tools bare similarity to Russian state-sponsored threat APT28, reportedly abused Microsoft’s infrastructure (e.g., OneDrive, Graph APIs) for Command and Control (C2) of it’s unique payloads.

- Emotet, a pernicious advanced cybercriminal threat has literally resurrected itself from the dead, following a swift multi-national takedown effort last year. Having rebuilt through distribution partnerships with TrickBot, the botnet resumed self-powered phishing campaigns in full force throughout January.

WhisperGate

Closely following recent geo-political events in Ukraine and Eastern Europe, it was revealed this month that Ukrainian government organizations suffered destructive attacks involving malware pretexting as ransomware. The destructive attacks were carried out in three distinct stages and have not been attributed, though there are strong circumstantial indications that intent was to cause irreparable damage. Motivations for the attacks point toward nationalism echoing ongoing tensions between Russia and Ukraine.

- The first stage involved deployment of a Windows native executable which overwrote the entire 512 bytes of the victim host Master-Boot-Record (MBR) with static bytes (no encryption key) leaving a ransom message on next boot, with Bitcoin wallet address and a Tox ID through which to contact the actor. Tox is a messenger application commonly utilized by ransomware actors.

- The second stage comprised of a .NET executable which functioned as a loader, retrieving, and executing an obfuscated executable (.jpg extension) staged on a Discord file server.

- The third stage is loaded into memory by the .NET loader and executes file encryption of select host files, overwriting the first 1MB of each file with static bytes (again no encryption key).

- The Fidelis Network malware detection engine detects all three stages of the attack referenced in public reporting. The malware used in this attack, was minimally obfuscated and incredibly simple, almost brutish (offering a myriad of detection opportunities). It was likely meant to be used for a limited instance and discarded; meant to send a nationalistic message. Anecdotally, this malware screams ‘Quick and Dirty’ lacking the professionalism of an advanced cybercriminal or state-sponsored actor, and evoking the notion of a nationalist partisan activity.

Figure 2. Static Characteristics of WhisperGate Stage2
Source: Fidelis Cybersecurity
It is quite clear that certain static elements observed such as expired certificates (Figure 2 above) would immediately signal potentially malicious content.

The static Unicode Cyrillic, especially that in the description field (provodnik – Leader), also lends itself well to mitigations filtering out executables from regions wherein certain organizations wouldn’t ordinarily conduct their business. Another file descriptor in the version field (Tbopbh) is likely a transliteration of the Slavic word for creation.

Mitigations around static Cyrillic Unicode file attributes may be problematic for organizations within Eastern Europe or the Mediterranean who share a Cyrillic alphabet, but it presents opportunities for Judo hip tossing (simple mitigations) outside of the impacted region.

Upon execution, the .NET loader (second stage) launches PowerShell twice with a base64 encoded sleep command, as part of a hardcoded evasion mechanism (Figure 4 below). In doing so, it exposes an operational weakness in that this type of activity (using PowerShell as a sleep mechanism) can be readily identified through inherent process relationships discovered during behavioral analysis – see Figures 4 and 5 below.
After sleeping for 20 seconds, the .NET loader (second stage) calls the WebClient method (Figure 6 above) to request the third stage. Note the loader dynamically de-obfuscates its request parameter of ‘DxownxloxadDxatxxax’ to DownloadData.

The binary content requested from the Discord server is deliberately mislabeled a JPG (image file type) and there are no corresponding JPG headers (e.g., FF D8 FF). The binary content is in reverse order (Figure 7 above – Note reversed MZ header [ZM] at end of file) and the .NET loader performs a simple Reverse method to properly orient the content so that it can be dynamically loaded. Yet another evasion technique which presents yet another opportunity to hip-toss the threat actor, as Fidelis Cybersecurity incorporates detections for files that don’t match extension to content/structure.

We assess with high confidence that these attacks were meant to be destructive and that they were most likely directed specifically at Ukraine, underpinned by nationalist motivations. That said, cyberattacks can bleed over from their intended victim to other organizations so there is some risk of this attack (or copycat actors) expanding the use of this malware.

- Overwriting the MBR with static bytes is not indicative of ransomware, as there is no way to recover the original boot record.
- Overwriting the 1st MB of designated host files with static bytes is not indicative of ransomware, as there is no way to recover the file headers, perhaps only remaining data streams.
Graphite

Advanced threat actors leveraged a relatively recent remote code execution (RCE) vulnerability in MSHTML and leveraged OneDrive along with Microsoft Graph API for Command and Control (C2), during a sophisticated 6-stage intrusion campaign that likely targeted government entities in Western Europe. Researchers assert with low to moderate confidence that APT28 is responsible for the campaign – given timing, targeting, and cited code similarities to previous APT28 tools.

- A recent vulnerability in MSHTML (CVE-2021-40444) embedded in an Excel document, served as part of the initial access vector to launch the intrusion. CVE-2021-40444 is a remote code execution vulnerability allowing code execution from a remote resource (e.g., malicious HTML). This is an emergent vulnerability (see Vulnerability section) which we are presently tracking.

- Threat actors leveraged OneDrive and Microsoft Graph API for C2 at stage 3 of their intrusion. OneDrive and Microsoft’s Graph API would be trusted resources in most environments and thus offer substantial evasion capability for the threat actor.

Sensationalism aside, this intricate intrusion chain can be detected using a behavioral mitigation strategy geared towards knowing the adversaries’ strengths and weaknesses.

As we can very easily identify through sandbox analysis, the initial Excel document phishing lure (Figure 8 above) contains an embedded malicious macro which makes a call to the Windows Management Interface (WMI), and it also invokes long sleeps.

Evasion, as revealed (Figure 7 above), is the threat actor’s operational requirement demonstrated through behavior, thus exposing a weakness. We can presume that if this is state-sponsored tooling, they certainly don’t want it easily analyzed. WMI allows the caller to collect environment variables and thus useful to threat actors in determining if their malicious payloads are executing in an analysis environment (e.g., sandbox or analyst’s virtual machine). This is not a new technique and is certainly well documented.

Simply stated, it is not normal for a document file to call WMI – a system management tool. In their zealous guarding of a simple lure document, threat actors expose indicators of intent. Legitimate organizations simply have no need to place anti-analysis measures in their daily business documents.

We assert that process relationship chains involving Microsoft Office applications and WMI are a strong basis (one of many) for applied mitigation, and we implement such protections regularly for our clients.
Emotet

The Emotet crimeware botnet regrouped last Fall, initially leaning on their partnership with TrickBot for distribution. In 2022, Emotet continues to pursue its former capability and size, now distributing itself through self-powered phishing campaigns. Emotet has a lineage inherited from banking trojans (e.g., Cridex/Dridex) but these days it primarily serves as a loader for other malware, facilitating intrusion chains that often culminate in ransomware.

The [latest Emotet phishing lures](#) incorporate string obfuscation techniques, which are likely intended to thwart static detection of the malicious-macro laden droppers used to deliver payloads.

- While creative, such obfuscations are ineffective against adept behavioral analysis. Threat actors must work in a finite space and rely upon additional operating system features and tools (e.g., mshta.exe) to carry out their malicious tasks. Use of such functionality in the OS is powerful and enables significant capability for the adversary while also exposing natural weaknesses such as those inherent to process relationships.

- Fidelis Cybersecurity provides coverage for Emotet and similar threats by building key choke-points around threat actor operational requirements which naturally elicit select actions on the endpoint, anticipating that static detections will most certainly fail at some point.

- Fidelis Network also provides broader static coverage on the wire against the types of lures (e.g., Macro4) favored by threat actors so that string obfuscation techniques leveraged by Emotet and others aren’t as consequential to evading detection.

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in Active XDR and proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic asset discovery, multi-faceted context, and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. Fidelis Cybersecurity is dedicated to helping clients become stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit [www.fidelissecurity.com](http://www.fidelissecurity.com)