MONTHLY TRT REPORT

Threat Intelligence Summary

Fidelis Threat Research Team

March 2022

Overview | March 2022

As the Russo-Ukrainian conflict continued to unfold in March, Fidelis Security remained vigilant in defense of our clients, facing off against notable threats such as CaddyWiper - one of the latest iterations of destructive malware that impacted Ukraine. Government agencies in Ukraine are reporting that they are facing continuous onslaught of DDoS since the invasion began on 24 February 2022. State-sponsored actors operating on behalf Russia (APT28) and Belarus (UNC1151) continue their offensive cyber operations through phishing campaigns against public and private Ukrainian networks. Russian authorities published a staggering list of 17,576 IP addresses and 166 domains that it claims are responsible for participating in a series of DDoS attacks targeting Russian domestic infrastructure. While the Anonymous collective and Ukraine-backed IT Cyber Army continue to launch offensive operations against Russian media and government infrastructure. Given the unprecedented confluence of belligerents, the risks for spill-over effects and misattribution in this conflict are at an all-time high.

Key Findings | March 2022

CaddyWiper

CaddyWiper is one of the **latest iterations** in a series of destructive '**Wiper**' malware campaigns impacting Ukraine. CaddyWiper dispenses with the 'ransomware act' demonstrated by previous wiper malware (e.g., WhisperGate, HermeticWiper), forgoing a ransom note or Bitcoin wallet address, and instead gets right down to business.

- CaddyWiper enumerates mapped drives, overwrites user-owned files with static bytes and destroys the Master Boot Record (MBR) of the primary drive on victim host machines running Windows.
- CaddyWiper has no 'safety latch' concerning region or language with which to limit its deployment, and as demonstrated below, functions uninhibited against virtual machines the same as it would against physical hosts.

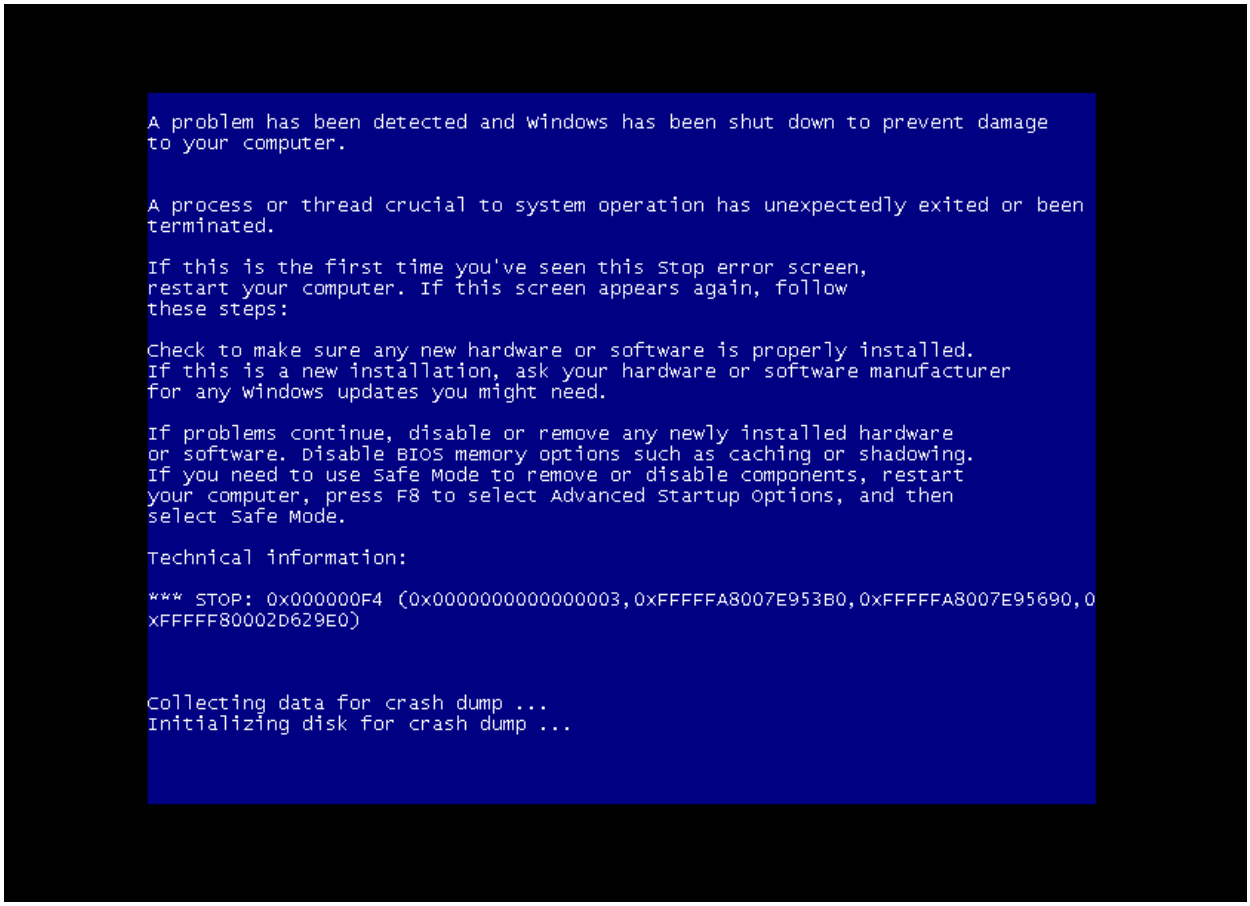

Figure 1. System Fault (post wipe) — Source: Fidelis Security

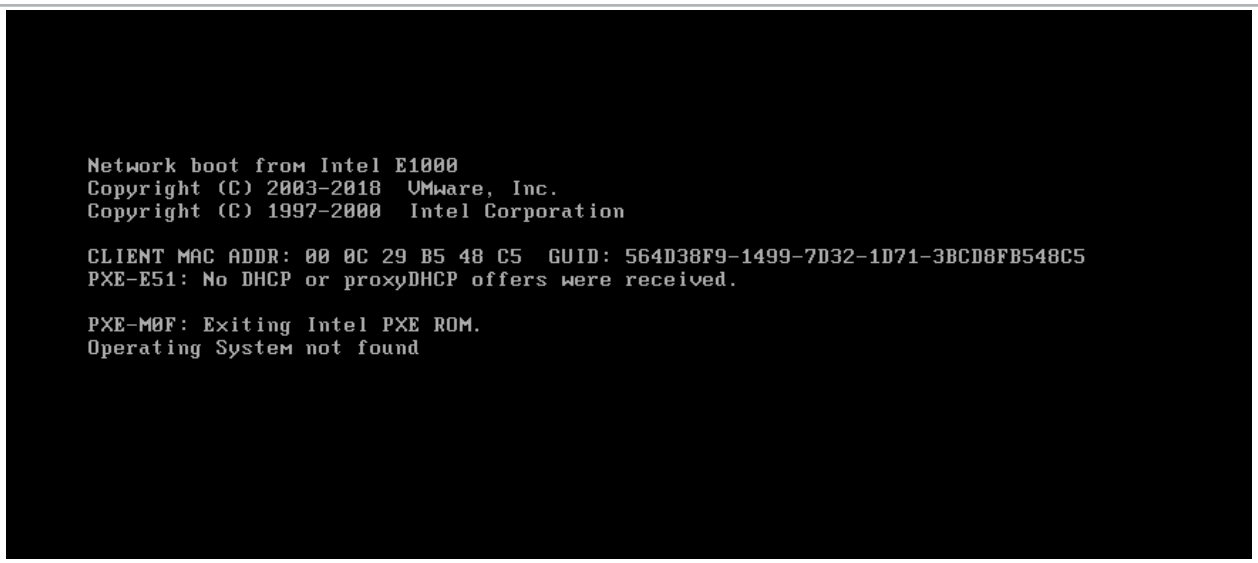

Figure 2. Operating System Not Found (reboot post wipe) — Source: Fidelis Security

CaddyWiper avoids destroying data on domain controllers, leveraging the ***DsRoleGetPrimaryDomainInformation()*** function to determine if a system is registered as a domain controller. This is also the only declared import when analyzed statically – Figure 3 below.

name (1)	group (1)	MITRE-Technique (0)	type (1)	anonymous (0)	blacklist (1)	anti-debug (0)
DsRoleGetPrimaryDomainInfor...	network	-	implicit	-	x	-

Figure 3. Static Analysis of CaddyWiper; declared imports (PEStudio) — Source: Fidelis Security

This specific attribute of the malware most likely exists because it was deployed using Group Policy (GPO) from the victims own domain controller. The GPO distribution technique was also observed with **HermeticWiper** and **IssacWiper** campaigns, it's also a popular technique of high-profile criminal ransomware gangs, though CaddyWiper itself is very distinct from previous wiper malware observed.

Malware analysts frequently encounter malware with a small handful of imports, which is often a solid indication that the malware is packed/crypted for obfuscation. Generally, when we encounter an application claiming a single import, it almost certainly signals dubious intent. As we can see from a static analysis of section entropy, CaddyWiper is not packed/crypted. This signals to us that the obfuscation characteristics of CaddyWiper are germane to the wiper itself, readily providing specific detection or mitigation opportunities.

property	value	value	value
name	.text	.rdata	.reloc
md5	F0D4C11521EC3891965534E...	D4B14CF770A6E660BA6A6E...	0F1286F7C8817E0974DDC3C...
entropy	5.644	0.088	0.082
file-ratio (88.89%)	77.78 %	5.56 %	5.56 %
raw-address	0x00000400	0x00002000	0x00002200
raw-size (8192 bytes)	0x00001C00 (7168 bytes)	0x00000200 (512 bytes)	0x00000200 (512 bytes)
virtual-address	0x00401000	0x00403000	0x00404000
virtual-size (7116 bytes)	0x00001B4A (6986 bytes)	0x0000006A (106 bytes)	0x00000018 (24 bytes)
entry-point	0x00001000	-	-
writable	-	-	-
executable	x	-	-
shareable	-	-	-
discardable	-	-	x
initialized-data	-	x	x
uninitialized-data	-	-	-
readable	x	x	x
self-modifying	-	-	-
blacklisted	-	-	-
virtualized	-	-	-

Figure 4. Static Analysis of CaddyWiper; sections (PEStudio) — Source: Fidelis Security

CaddyWiper is fairly crude in design and doesn't leverage much obfuscation outside of dynamically resolving its other necessary imports (e.g., netapi32.dll) as they are needed, with very basic stack-based string assembly functions – refer to Figure 5 below. This obfuscation technique, most likely designed for evasion and anti-analysis, provides an adequate detection opportunity not just against CaddyWiper but against malware threats using similar techniques.

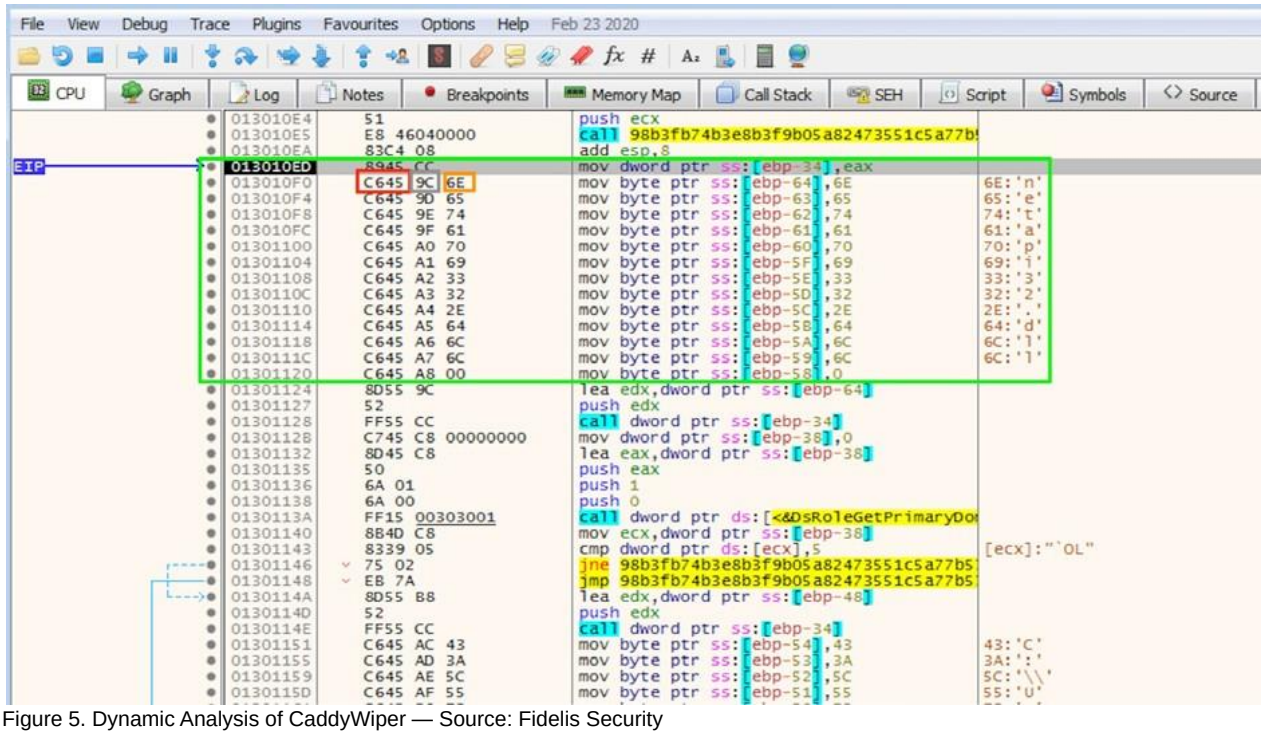

Figure 5. Dynamic Analysis of CaddyWiper — Source: Fidelis Security

Figure 5 above depicts dynamic analysis of CaddyWiper using x32dbg – a popular and effective open-source Debugger. The green box highlights the meat of one of the many dynamic import resolution functions we observed. Fidelis Network® and Fidelis Endpoint® products leverage custom YARA implementations, to effectively alert and classify threats for our customers. We'll use a few examples to demonstrate how Fidelis Security continuously protects clients against dangerous notable threats making the headlines.

Let's break down the function noted above into its respective parts:

- **C645** is the x86 opcode for **mov byte ptr**
- **9C** is the relative stack offset from **ebp** (base pointer) – this is expected to change due to stack management implementations across different Windows versions (e.g., ASLR, DEP).
- **6E** represents a single byte value (ascii **n**), added incrementally to the array referenced by **ebp** – this is expected to remain a constant byte value for malware using this function, calling this specific import, as it is used to dynamically assemble the name of the import.

This function and its import references are hard coded as a **contiguous stream** of bytes, as the binary exists statically. Thus, we can (and we do) leverage the YARA engine to pivot on these distinct code blocks.

An example YARA condition in this case would be:

```
$stk_string1 = {c6 45 ?? 6e c6 45 ?? 65 c6 45 ?? 74 c6 45 ?? 61 c6 45 ?? 70 c6 45 ?? 69 c6 45 ??
33 c6 45 ?? 32 c6 45 ?? 2e c6 45 ?? 64 c6 45 ?? 6c c6 45 ?? 6c} // stack string for netapi32.dll}
```

Additionally, we observed Unicode implementations for stack-string manipulation functions as well (e.g., kernel32.dll) - note **00** as the incremental byte included for the **ebp** offsets in Figure 6 below.

Figure 6. Dynamic Analysis of CaddyWiper — Source: Fidelis Security

Kernel32 is a standard (and quite arguably necessary import) for Windows binaries (occasional exceptions being applications with inlined WinAPI functions). Not seeing Kernel32 referenced as a declared import upon initial static inspection is often a significant indicator of dubious intent. As we can clearly see above, CaddyWiper must resolve the import for necessary functions. In doing so, the malware exposes a weakness that we can quickly capitalize upon, in much the same fashion as we demonstrated with the dynamic ASCII stack-strings.

We also observed contiguous stack-string byte sequences (Figure 7 below) using a combination of ASCII and Unicode. Import resolution methods throughout the binary were not uniform (e.g., netapi32.dll – Figure X above). Almost certainly for the purpose of evasion; more specifically obfuscation of the subsequent Kernel32.FindFirstFileA call, creates for us a unique sequence of bytes which provide a level of distinctness. FindFirstFileA is the WINAPI library leveraged by CaddyWiper to iterate through host files during its static byte overwrite operations.

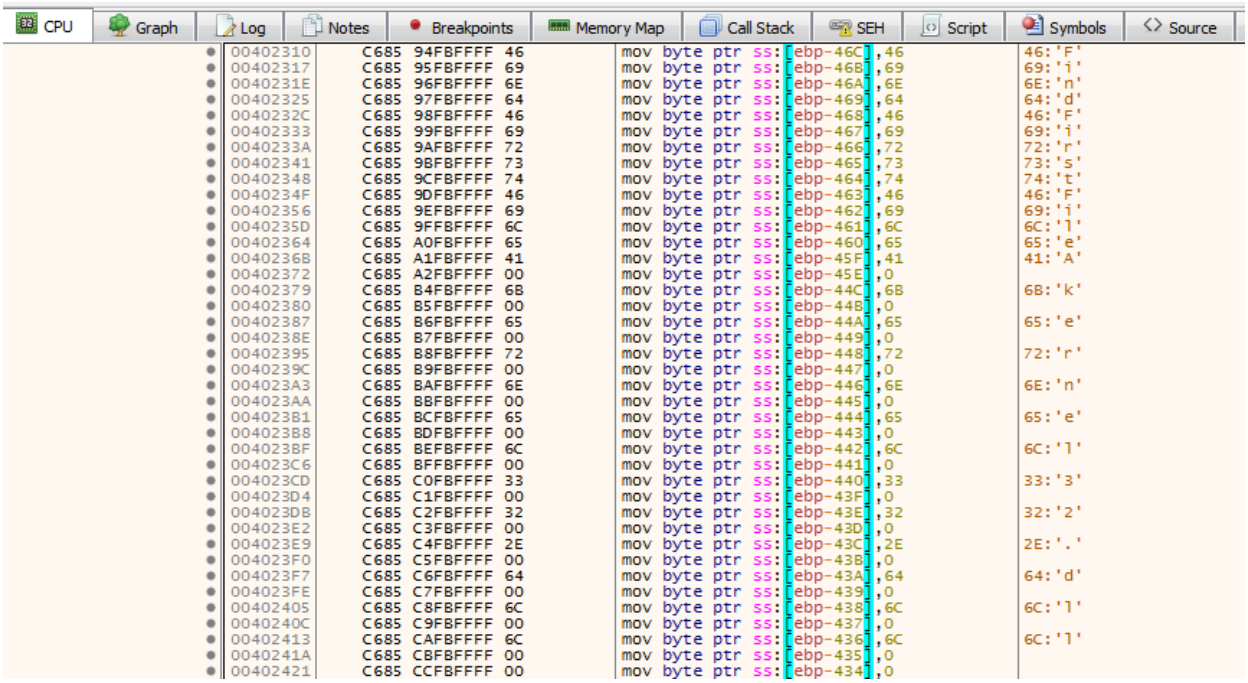

Figure 7. Dynamic Analysis of CaddyWiper — Source: Fidelis Security

An example YARA condition in this case would be:

```
$stk_string2 = {c6 85 ?? 46 c6 85 ?? 69 c6 85 ?? 6e c6 85 ?? 64 c6 85 ?? 46 c6 85 ?? 69 c6 85 ??
72 c6 85 ?? 73 c6 85 ?? 74 c6 85 ?? 46 c6 85 ?? 69 c6 85 ?? 6c c6 85 ?? 65 c6 85 ?? 41 c6 85 ??
00 c6 85 ?? 6b c6 85 ?? 00 c6 85 ?? 65 c6 85 ?? 00 c6 85 ?? 6c c6 85 ?? 00 c6 85 ?? 33 c6 85 ??
00 c6 85 ?? 32 c6 85 ?? 00 c6 85 ?? 2e c6 85 ?? 00 c6 85 ?? 64 c6 85 ?? 00 c6 85 ?? 6c c6 85 ??
00 c6 85 ?? 6c c6 85 ?? 00 // Unicode-ASCII combo - Kernel32.FindFirstFileA}
```

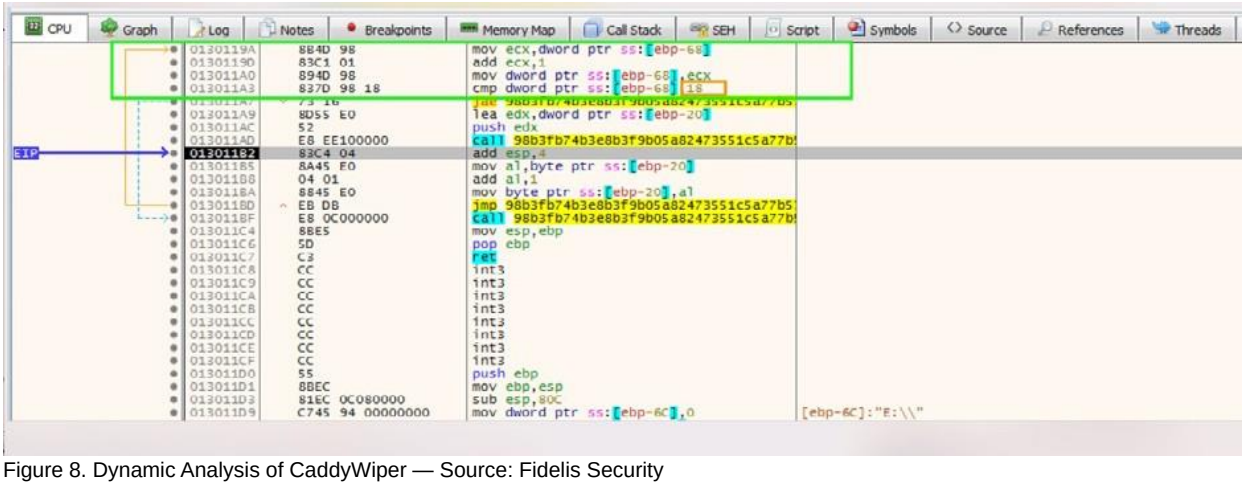

Figure 8. Dynamic Analysis of CaddyWiper — Source: Fidelis Security

Next, we can target the mapped drive enumeration control loop sequence (above) which CaddyWiper uses to enumerate mapped drives of the victim host. Note that hex 18 is decimal 24, thus serving as the control for the **cmp** instruction to signal the loop is complete. 24 is the exact number of Roman-alphabet characters from C to Z, obviously negating characters A and B, which are traditionally assigned to floppy disks.

- ***837D*** is the x86 opcode for ***cmp dword ptr***
- 98 is the relative stack offset from **ebp** (ebp-68) – this as we know is expected to change.
- The **ecx** increment of 1 and the control variable 18 give us solid code-block anchor points from which to build around, because they control this enumeration loop.

An example YARA condition in this case would be:
$drive_enum_function = {8b 4d ?? 83 c1 01 89 4d ?? 83 7d ?? 18} // C-Z Drive enumeration loop}

In closing, we'll say that we actioned many more observations concerning CaddyWiper. Our intent is ***not*** to instruct threat actors on how to write better malware, simply to demonstrate how threat information shared in the intelligence ecosystem is put into an actionable result designed to comprehensively protect our clients.

Continuous DDoS *(Ukraine)*

Ukrainian agencies are reporting that government websites are facing continuous DDoS since the invasion began on 24 February 2022. Despite the ongoing disruption attempts, the State Service of Special Communication and Information Protection (SSSCIP) of Ukraine reports that the websites for many central government resources remain online.

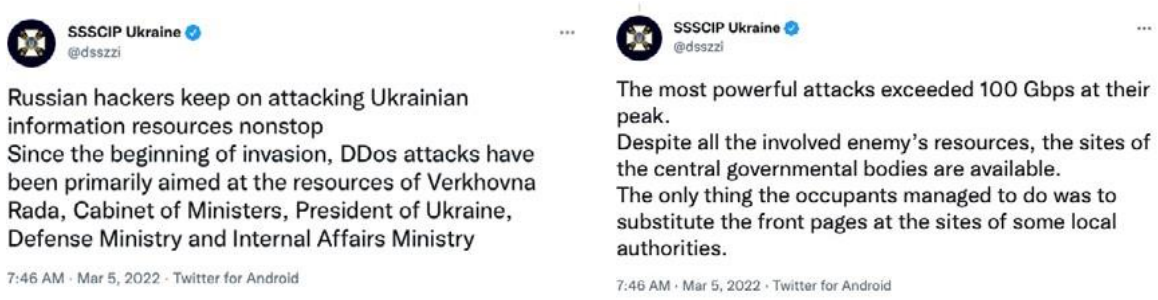

Figure 9. Ukrainian SSSCIP Reports On-going DDoS Attacks — Source: Twitter (@dsszzi)

UNC1151(GhostWriter) Likely Phishing Poland and Ukrainian Government Organizations

Belarusian state-sponsored actors likely conducted credential phishing campaigns in mid-March against Polish and Ukrainian government and military organizations. ***Fidelis has incorporated known network and file-based indicators to provide protection through our network and endpoint product offerings.***

APT28 Likely Phishing Users of Ukrainian Media UkrNet

FancyBear/APT28, a threat actor attributed to Russia GRU, conducted several large credential phishing campaigns in March t argeting ukr.net users; UkrNet is a Ukrainian media company. The phishing emails were sent from a large number of compromised accounts and include links to attacker-controlled domains. ***Fidelis has incorporated known network and file-based indicators to provide protection through our network and endpoint product offerings.***

Russia Names Public and Private Entities Attacking Russian Infrastructure

In early March, the Russian government provided a list of 17,576 IP addresses and 166 domains that it claims are responsible for participating in a series of DDoS attacks targeting Russian domestic infrastructure.

Included were the U.S. Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and websites of several media publications including USA Today, 24News.ge (Georgian News Bureau), megatv.ge (MegaTV – Georgia), and Ukraine's Korrespondent magazine.

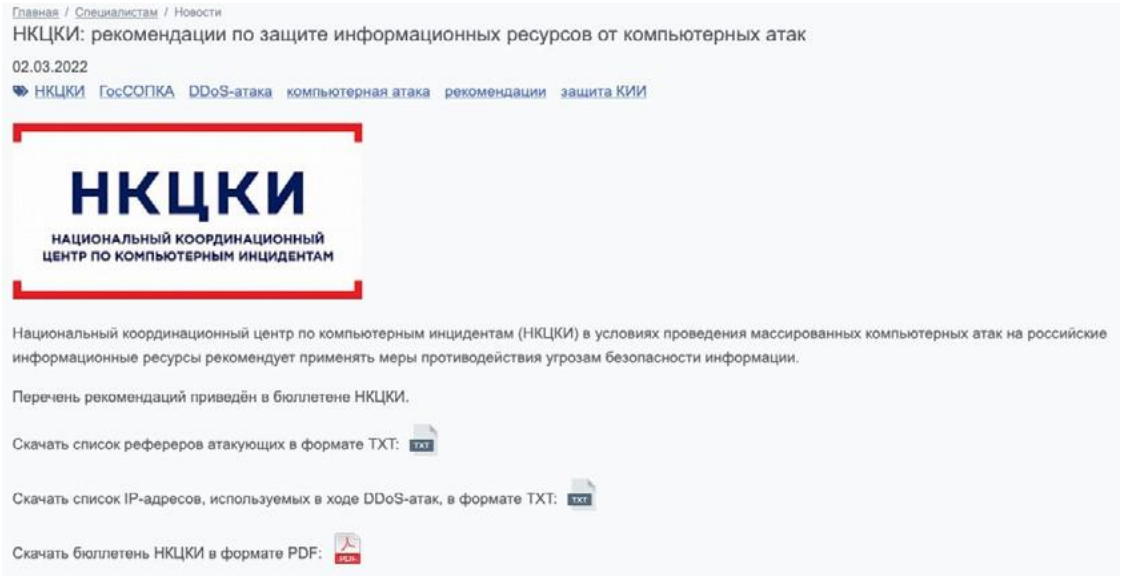

Figure 10. Russian Government Warns Citizens; Names Public and Private Attacking Entities — Source: Safesurf.ru

Attribution is inherently difficult in cyberspace. What's important to highlight is that the confluence of belligerents participating on the cyber-front of the Russo-Ukrainian conflict is unprecedented.

The Anonymous collective declared '**cyber war**' against Russia in late February following the invasion of Ukraine; claiming to have knocked the Russian media organization **Russia Today (RT) off ine**. In their most recent announcement of #OpRussia on 23 March 2022, the Anonymous collective claimed to have hacked the **Central Bank of Russia**, planning to release 3500 sensitive files.

The IT Army of Ukraine, an all-volunteer *multi-national* group **established and backed** by the Ukrainian government is estimated to be about 300,000 strong. This group has implored the international community to attack Russian networks - naming targets, and reporting on the **effects**.

We are all in uncharted territory; especially regarding offensive cyber actions, committed under the banner of a sovereign nation by a largely civilian activist force. The risks for spill-over effects and mis-attribution in this conflict are at an all-time high.

Metrics | March 2022

Malware

Telemetry

Fidelis enabled clients to defend their networks from 186K+ malware threats of high severity (e.g., Ransomware, Trojans, Backdoors, Exploit Kits, Loaders, Droppers) encountered in March 2022. The following are the top malware variants (by volume) Fidelis detected through telemetry:

[1] **H-worm**
- Context; active in the wild since at least 2012.
- Visual Basic Script-based RAT; authored by 'Houdini'
- Alleged connection to njRAT and njW0rm through actor 'njq8'
- Historically observed in regional attacks against the energy sector (MENA – Middle East/North Africa).

[2] **Andromeda**
- A modular Trojan; active 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.

[3] **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 and DocuSign/Invoice Themes).

[4] **Fareit**
- Credential Stealer/Downloader; active in the wild since at least 2012.
- Also identified as Pony; historically associated to threats such as Zeus and Necurs.
- Source for Fareit/Pony 2.0 was leaked nearly a **decade ago**.

[5] **TrickBot**
- Originally a modular Banking Trojan with historical code lineage to Dyre/Dyreza.
- Now functions primarily as a Loader; active in the wild **since at least 2016**.
- Associated with intrusion chains involving Conti ransomware, TA505, UNC18178, Wizard Spider.

Trending In-the-Wild

Comparatively against our telemetry, here is what other open-source intelligence sources are observing and reporting for trending malware submissions and analysis March 2022:

AbuseCH
- Emotet
- Quackbot
- SoulClose
- Shodi
- Urelas

Maldatabase
- Dridex
- AgentTesla
- Emotet
- LokiBot
- TrickBot

Dridex
- Originally designed to be an extensible and modular banking Trojan, Dridex now primarily functions as a loader for other malware leading to intrusions which result in ransomware deployment.
- Referenced in official sanctions against Evil Corp, by Office of Foreign Asset Control (OFAC) – given it's pervasive use by this group.
- Likely shares code-lineage with Bugat/Cridex; active since at least 2013.

Quakbot
- Also identified as Qbot or Qakbot; active since at least 2007.
- A modular Trojan and capable banking Trojan, primarily leveraged now as a loader for other malware leading to intrusions which result in ransomware deployment.

AgentTesla
- Also identified as TeslaAgent or Negasteal; active since at least 2014.
- A .NET based RAT and info-stealer with the ability, among others, to log keystrokes and pilfer victims' clipboard data.
- Once commoditized and readily available to threat actors of various sophistication levels for less than $100 USD in Bitcoin.

TrickBot
- Well-established reputation as versatile banking Trojan; regularly updated and highly modular - primarily functioning as a loader for other malware leading to intrusions which result in ransomware deployment.
- Active since 2016; likely shares code-lineage from Zeus-styled banking Trojan Dyre/Dyreza.
- Trickbot almost certainly supported the rebuild of the Emotet botnet last Fall- distributing Emotet through Trickbots' existing infrastructure.
- The TrickBot development team has likely been absorbed into the Conti ransomware group.

Emotet
- Also identified as Heodo/Geodo; likely shares historical code lineage with Dridex.
- Originally designed as a banking Trojan - primarily functioning as a loader for other malware leading to intrusions which result in ransomware deployment (e.g., Ryuk/Sodinokibi).
- Associated with threat group(s) Gold Cabin, Mummy Spider, Mealybug.
- Infrastructure taken down in January 2021; rebuilt with Trickbot in November 2021.

LokiBot
- Commodity info-stealer malware once broadly sold on cybercriminal forums ($300 USD) by the actor Lokistov (a.k.a. Carter); active in the wild since at least 2015.
- Current iterations are likely 'cracked' versions of the original bot, which have allowed actors of various skill and sophistication to operate the info-stealer without having to purchase it.

SoulClose
- Generic detection for a file prepending worm which has the ability to infect other executables it identifies on the victim host.
- Known to drop other malware for actors of various skill and sophistication.

Shodi
- Generic detection for a file prepending worm which has the ability to infect other executables it identifies on the victim host.
- Known to drop other malware for actors of various skill and sophistication.
- Can be potentially hijacked by other threat actors, as the malware itself presents memory corruption vulnerabilities; **PoC code published**.

Urelas
- Also identified as Glupboot. An info-stealer capable of harvesting credentials, taking screenshots, making system changes, modifying registry and executing additional malware.

Vulnerabilities

Telemetry

Our tailored and community integrated detections helped clients to orient and respond to over 6K+ critical vulnerability exploitation attempts across 16 distinct vulnerabilities targeted in March 2022. Leading the pack for exploitation attempts in March was CVE-2021-26858, a Remote Code Execution (RCE) vulnerability most likely to be leveraged by threat actors in the 'ProxyLogon' exploitation chain against vulnerable on-premises Microsoft Exchange servers.

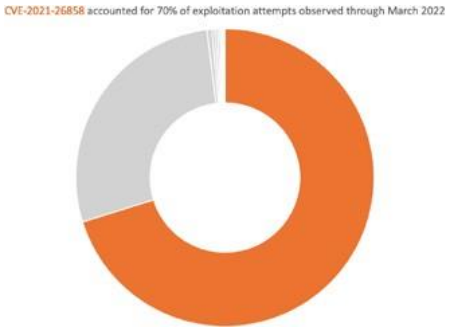

Figure 11. Critical Vulnerability Exploitation Activity for March 2022 — Source: Fidelis Telemetry

Active Exploitation

We continue to observe significant exploitation activity for much older vulnerabilities indicating that threat actors will continue taking advantage of opportunities. Vulnerabilities in user-software such as Microsoft Office provide a unique opportunity for threat actors to gain a foothold when network perimeter posture is hardened. The following vulnerabilities represent 99% of the observed vulnerability exploitation attempts for March 2022:

CVE-2021-26858
(Microsoft Exchange - Remote Code Execution) accounted for approximately **70%** of the observed vulnerability exploitation attempts for March 2022. This vulnerability is most likely to be leveraged by threat actors in the 'ProxyLogon' exploitation chain against vulnerable on-premise Microsoft Exchange servers.

CVE-2017-11882
(Microsoft Office – Remote Code Execution) accounted for approximately **28%** of the observed vulnerability exploitation attempts for March 2022. 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-2018-0802
(Microsoft Office – Remote Code Execution) accounted for less than 1% of the observed vulnerability exploitation attempts for March 2022. A separate memory corruption vulnerability plaguing Equation Editor, following the update patch mitigations for CVE-2017-11882. Most likely to be leveraged by threat actors delivering phishing lures.

CVE-2018-8414
(Windows Shell – Remote Code Execution) accounted for less than **1%** of the observed vulnerability exploitation attempts for March 2022. Vulnerability results from improper path validation and impacts Windows 10/Server. This vulnerability is likely to be leveraged by threat actors in a phishing lure (e.g., enticing a user to open a specially crafted file or click a link where maliciously crafted file is staged).

CVE-2021-44228
Log4j2 – Remote Code Execution) accounted for less than **1%** of the observed vulnerability exploitation attempts for March 2022. Impacts Log4j2 v2.0beta9 - 2.12.1 and 2.13.0 - 2.15.0. Confirmed active exploitation in the wild by actors of various sophistication and motivation. PoC code is **available**.

Emerging

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

[1] CVE-2022-1096

- (Chromium – Remote Code Execution)
- A type confusion vulnerability which leads to RCE. Impacts Google Chrome for Windows, Mac, and Linux prior to version 99.0.1150.55 (latest emergency update issued by Google). Browsers leveraging the Chromium engine (e.g., Edge, Brave, Vivaldi) are also likely impacted.
- Most likely actively exploited in the wild. Likely to be leveraged by threat actors in phishing campaigns, enticing victims to view sites with malicious remote content (e.g., javascript); PoC code has not yet surfaced publicly at the time of writing.

[2] CVE-2022-0847

- (Linux Kernel – Local Privilege Escalation)
- Also identified as the “Dirty Pipe” vulnerability. Present since Linux Kernel 5.8; fixed in Linux Kernel 5.16.11, 5.15.25, 5.10.102. Allows an unprivileged local user to write to pages in the cache backed by read-only files - thereby allowing users to potentially escalate their privileges.
- This vulnerability is most likely to be leveraged by threat actors who have a foothold on the system as a low-privileged user, and are seeking to elevate privileges for persistence and lateral movement.
- PoC code is available.

[3] CVE-2022-0492

- (Linux Kernel - Local Privilege Escalation)
- Vulnerability exists in the cgroups (control groups) library, used to build containerized instances. This LPE vulnerability is most likely to be leveraged by threat actors looking to escape containerized instances (e.g., Kubernetes), potentially allowing the actor to take control of the node running the container.
- Containers running Seccomp, SELinux, or AppArmor are likely protected. Consult your Cloud service or Linux distribution provider for details on mitigation as some patches have been applied irrespective of Kernel versioning.
- PoC code has not yet surfaced publicly at the time of writing, however there is a test script provided by a reputable 3rd party to test if systems are likely vulnerable.

[4] CVE-2022-0778

- (OpenSSL – Denial of Service)
- This vulnerability exists in the BN_mod_sqrt function, allowing an infinite loop condition when calculating non-prime moduli. It is possible for a threat actor to trigger a DoS for a webserver/service supported by a vulnerable instance of OpenSSL, by crafting an illegitimate (most likely to be self-signed) certificate with invalid elliptic curve parameters.
- Affects OpenSSL versions 1.0.2, 1.1.1 and 3.0; fixed in OpenSSL 3.0.2, 1.1.1n, and 1.0.2zd. Most likely to be leveraged by threat actors aiming to create a Denial-of-Service impact against public facing web infrastructure.
- PoC code has not yet surfaced publicly at the time of writing, but is likely in development.

[5] CVE-2022-25636

- (Linux Kernel - Local Privilege Escalation)
- This vulnerability exists in the net/netfilter/nf_dup_net-dev.c library of the Linux kernel, allowing a local user to gain elevated privileges through an out-of-bounds write to heap memory.
- Impacts Linux Kernel 5.4 through 5.6.10
- PoC code is likely in active development.

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.