VEDERE LABS

MONITORING CYBER ACTIVITIES CONNECTED TO THE RUSSIAN-UKRAINIAN CONFLICT

Briefing Notes by Vedere Labs

March 3, 2022

Executive Summary

Forescout's threat intelligence and research team Vedere Labs is continuously monitoring the evolution of cyber activities connected to the Russian-Ukrainian conflict and to Russian state-sponsored actors. This report is meant to share the cybersecurity intelligence we gather regarding active threats, TTPs, indicators of compromise and recommended mitigations.

The Russian invasion of Ukraine on February 24th was preceded and accompanied by cyber-attacks that include Distributed Denial of Service (DDoS) against government agencies and private banks, different data wiper malware families and website clones used to spread malware.

At the same time as the events above unfolded, the UK NCSC and the US CISA released a report about a new malware called Cyclops Blink attributed to the well-known Sandworm threat actor (linked to Russia's GRU). While there is no current link between Cyclops Blink and the ongoing conflict, this sheds light on the evolution of cyber capabilities by Russian state-sponsored actors.

As the conflict developed, other non-state-sponsored actors decided to join either side and launch attacks to inflict damage on their opponents. These are mostly cybercriminal groups, including famous ransomware gangs such as Conti.

The conflict is far from over and so far, there have not been (known) cyber consequences for organizations outside the belligerent countries. However, as time passes and as new groups join the fight, the likelihood of a cyber-attack affecting organizations in third countries increases. CISA continues to issue guidance related to the conflict as part of their Shields Up initiative.

In this report, we present a summary of the threat actors currently involved in the conflict (Section 2), non-malware incidents that took place mostly before the invasion (Section 3), and the results of technical analyses of several malware variants using before and during the invasion (Section 4).

Table of Contents

Active Threat Actors

There are currently two types of threat actors directly involved in the conflict: Russian state-sponsored actors (Section 2.1) and other hacking groups (Section 2.2). After introducing these actors, we present an analysis of threat intelligence gathered by Vedere Labs by relying (among other sources) on data coming from the Forescout Global Cyber Intelligence Dashboard, which leverages 30 billion datapoints collected from millions of deployed IT, IoT, IoMT and OT devices, as well as robust network data stored in our proprietary data lake (Section 2.3).

Russian state-sponsored actors

Several major incidents in recent years have been tracked to Russian state-sponsored actors, including the events targeting the electrical sector in Ukraine in 2015 and 2016, the NotPetya incident in 2017 and the SolarWinds hack in 2020.

There are at least three separate Russian groups that have been linked to these cyber incidents: the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Main Intelligence Directorate (GRU). **Figure 1** provides an overview of these groups and the incidents they have been linked to. This distinction is important because historically, the GRU has been involved in destructive operations, while the SVR and FSB focused on espionage.

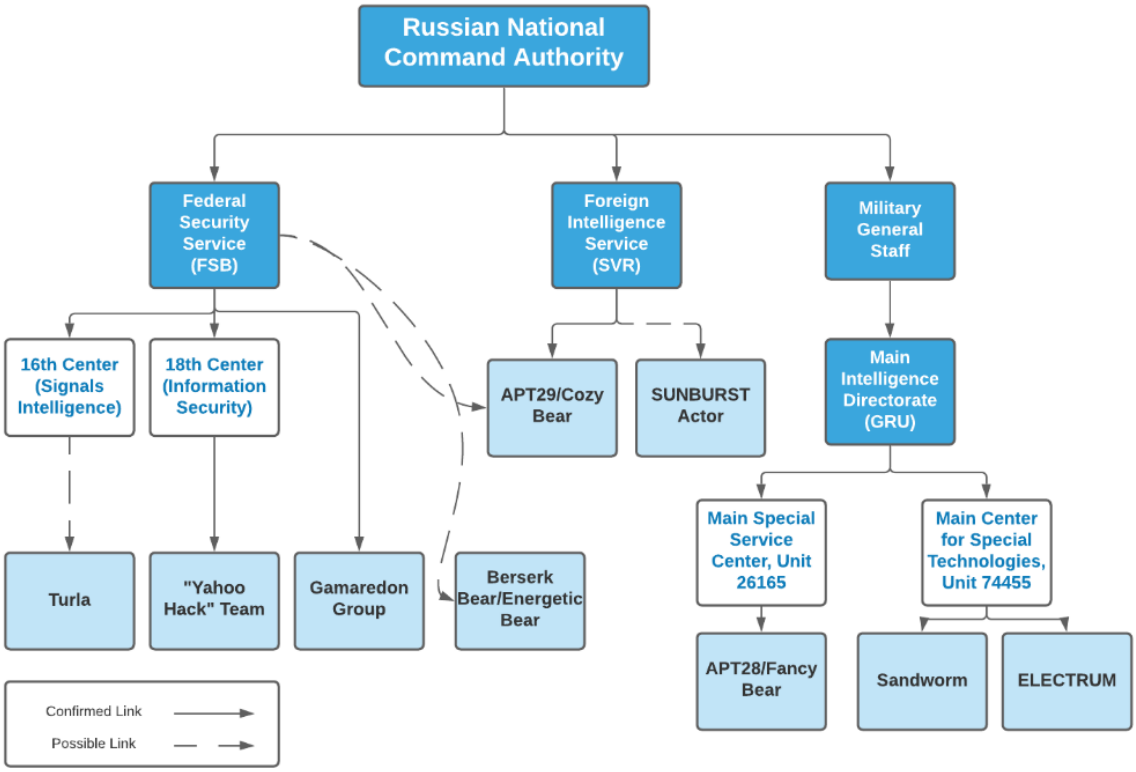

Figure 1 – A summary of Russian state-sponsored actors. [From https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf]

Prior to the invasion, CISA has published several recent alerts about Russian actors targeting US critical infrastructure and government contractors:

- CISA AA22-047A: From January 2020 through February 2022, Russian actors have targeted US defense contractors using common techniques such as spearphishing, credential harvesting, brute force/password spray techniques and known vulnerability exploitation. The goal of the intrusions was to exfiltrate sensitive information related to defense technology.
- CISA AA22-011A: This alert provided an overview of defense against Russian state actors targeting US critical infrastructure. Of particular interest is a list of vulnerabilities commonly used for initial access, which includes the ones in **Table 1**.
- CISA AA21-116A: This alert provided details on Russian threat actors linked to the Russian Intelligence Foreign Service (SVR), which have targeted several US organizations for espionage, including the SolarWinds incident.

CVE ID	Affected Software
CVE-2018-13379	FortiGate VPNs
CVE-2019-1653	Cisco router
CVE-2019-2725	Oracle WebLogic Server
CVE-2019-7609	Kibana
CVE-2019-9670	Zimbra software
CVE-2019-10149	Exim Simple Mail Transfer Protocol
CVE-2019-11510	Pulse Secure
CVE-2019-19781	Citrix
CVE-2020-0688	Microsoft Exchange
CVE-2020-4006	VMWare
CVE-2020-5902	F5 Big-IP
CVE-2020-14882	Oracle WebLogic
CVE-2021-26855	Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Table 1 – Vulnerabilities commonly exploited by Russian state-sponsored actors for initial access

These state actors are believed to be behind several of the capabilities and incidents described in Sections 0 and 0, although this is not yet confirmed.

Hacking groups

Soon after the invasion of Ukraine took place, hacking groups started taking sides on the conflict. On February 25th, the Anonymous hacking collective declared a 'cyber war' against Russia and managed to take the Russian state news website offline.

Over the weekend of February 26th and 27th many other hacking groups joined the fight, either on the Ukrainian or the Russian side. There are currently 24 hacking groups tracked as taking part in the conflict. **Table 2** lists the currently tracked groups. Below are some examples of groups and actions:

- On February 27th, the Cyber Partisan hacking collective compromised railway systems by encrypting data on servers, databases and workstations. As a result, some trains could not run, which the collective hoped would slow Russia's invasion via Belarus.

- Electric vehicle charging stations in Moscow were rendered inoperable by hackers from an unknown group, who displayed messages such as “Glory to Ukraine!” on their screens.
- The famed Conti ransomware sided with Russia. However, one Ukrainian member of the gang hacked their internal communications platform and leaked messages from January 29, 2021 until February 27, 2022. The messages can be seen online (in Russian) and they are currently being analyzed by the security community. Some of the confirmed content shows the relationship between Conti and the TrickBot and Emotet malware groups. On another leak, source code of the Trickbot Command Dispatcher & Trickbot Data Collector malware used by Conti was posted online. Currently, several IoCs are being extracted from that source code.

The escalation of the cyber conflict to include these groups is worrying because their motivations and agendas are not entirely clear and can quickly change. At this point, there is no evidence that these groups are targeting organizations not involved in the conflict. However, Russian groups especially could try to affect businesses in countries that are currently imposing economic sanctions on Russia, such as the US and EU countries.

Group	Supporting	Attack Methods
AgainstTheWest (ATW)	Ukraine	Data Breach & Ransomware
Belarusian Cyber Partisans	Ukraine	Ransomware
Anonymous	Ukraine	DDoS
GhostSec	Ukraine	Hacks
IT Army of Ukraine	Ukraine	DDoS
KelvinSecurity Hacking Team	Ukraine	Hacks
BlackHawk	Ukraine	DDoS
Anonymous Liberland & the PWN-BAR hack team	Ukraine	DDoS
Raidforums admin	Ukraine	Sanction
Netsec	Unknown	Hacks
Free Civilian	Russia	Data Breach
Cooming Project	Russia	Data Breach
Conti Ransomware	Russia	Ransomware
The Red Bandits	Russia	Data Breach
CyberGhost	Russia	Hacks
SandWorm	Russia	Hacks & DDoS
GNG	Ukraine	DDoS
NB65	Ukraine	Hacks
ECO	Unknown	Unknown
Raidforums2	Ukraine	DDoS
ContiLeaks	Ukraine	Data Breach
SHDWSec	Ukraine	Hacks
GhostClan	Ukraine	Hacks & DDoS
Eye of the Storm	Ukraine	Hacks

Table 2 - Currently tracked hacking groups involved in the conflict. [From https://cyberknow.medium.com/2022-russia-ukraine-war-cyber-group-tracker-update-1-ee3834fb03c]

Vedere Labs data analysis

Table 3 lists the top threat actors we have seen active in the last 7 days, mainly identified by malicious domain name requests. Based on an identified domain, we present the associated malware family, several community identifiers for the associated actor, a quick description, and a reference for each actor.

Domain Names	Malware Family	Associated Actor	Description	Reference
baroquetees[.]com	DarkSide	Carbon Spider, Carbanak, GOLD KINGSWOOD, FIN7	Cybercriminal hacking group, believed to be based in Eastern Europe.	https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a
goodtech.cetxlabs[.]com filecabinet.digitalechoes.co[.]uk newsmag.danielolayinkas[.]com	Emotet	Mummy Spider, Emotet, Geodo, GOLD CRESTWOOD, TA542	Malware strain and a cybercrime operation believed to be based in **Ukraine**[1].	https://isc.sans.edu/forums/diary/Emotet+Returns/28044/ https://urlhaus.abuse.ch/url/2024442/ https://isc.sans.edu/diary/Emotet+Returns/28044
zupertech[.]com highdatabase[.]com deftsecurity[.]com	CobaltStrike, SUNBURST	Cozy Bear, APT29, YTTRIUM, CozyCar, CozyDuke, The Dukes, IRON HEMLOCK	**Russian** SVR.	https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack https://otx.alienvault.com/indicator/domain/highdatabase.com https://www.cisa.gov/uscert/ncas/alerts/aa20-352a

Table 3 - Threat actors active in Vedere Labs data analysis

Non-Malware Incidents: Website Defacements, DDoS Attacks and Website Clones

Preceding the invasion, there have been several cybersecurity attacks on Ukrainian institutions that are thought to be linked to Russian state-sponsored actors:

- On January 14th, about 70 Ukrainian government websites were defaced and attackers included text in Ukrainian, Russian and Polish saying “be afraid and wait for the worst.” On the same day, the websites were taken offline and then restored.
- Starting on the afternoon of February 15th, websites of several Ukrainian banks and government agencies, including Privatbank (the largest bank in Ukraine), Oschadbank, the Ukrainian Ministry of Defense, the Ministry of Foreign Affairs, the Ukrainian parliament, and the Security Service of Ukraine were targets of distributed denial of services. There have been two waves of attacks, one on February 15th and another on February 23rd.

[1] https://www.cpomagazine.com/cyber-security/emotet-malware-taken-down-by-global-law-enforcement-effort-cleanup-patch-pushed-to-1-6-million-infected-devices/

- Coinciding with the second wave of DDoS, on February 23rd, Bellingcat reported on a web service hosting cloned copies of several Ukrainian government websites modified to serve malware when visitors click on a specific link. The malware deployed by the websites was linked to previous attacks targeting Ukraine in 2021 and believed to be linked to the GRU.

Malware Incidents and Analysis

There have been three "waves" of malware incidents so far. First, there was the WhisperGate incident that preceded the invasion (Section 4.1). Second, there was a multitude of malware variants used very close to the invasion date (Section 4.2), more of which are being discovered almost daily. Finally, there is the Cyclops Blink malware, which is not connected to the conflict, but developed by a Russian state actor and disclosed to the security community when the conflict was ongoing. Below, we present an analysis of each wave.

Preceding the invasion: WhisperGate

Summary

- On January 15th, Microsoft announced they had uncovered a two-stage destructive malware targeting Ukrainian organizations.
- The threat actor behind the malware is currently unknown (although it is probably Russian) and it was dubbed by Microsoft as DEV-0586, while the malware was dubbed WhisperGate.
- The initial infection vector used to deploy the malware is not yet known. There is no evidence of any 0-days or known vulnerabilities being exploited in any stage of the malware.
- There are no signs of this malware being used to target anything other than Ukrainian organizations.
- After the initial report, researchers uncovered more samples related to this malware, including a stage3, which is much more complicated and is currently being analyzed.
- The first stage overwrites the Master Boot Record (MBR) of affected systems, rendering them unusable. The second stage downloads Stage3. The third stage disables system defenses, wipes files and deletes itself.
- Although the malware displays a ransom note (see Technical Analysis section), there is no recovery mechanism and this is believed to be a decoy. The true goal of the malware seems to be destruction of files and systems rather than financial gain via ransomware.

Technical Analysis

The malware has three known stages so far:

- Stage1 overwrites the Master Boot Record (MBR) on hard disks of affected systems with a ransom note, rendering them unusable. Once a system is rebooted the ransom note below is displayed on the screen. This is not a typical ransomware note since there is no victim-specific ID and no easy means to communicate with the attackers (besides the tox messaging service).

Microsoft has mentioned that Stage1 is executed via Impacket, a tool typically used for lateral movement and malware execution.

- Stage2 sleeps for 20 seconds (using a base64-encoded PowerShell command: powershell -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==)and then downloads Stage3 (disguised as a JPG) via Discord (which is a popular way to distribute malware nowadays). The downloaded file (Stage 3) is reversed and is imported as a Win32 DLL into the process that runs Stage2.
- Stage3 is written in C# and obfuscated with Eazfuscator. This stage contains 3 encoded resources, which are loaded into memory, decoded with XOR, and executed. So far, only one resource (78c855a088924e92a7f60d661c3d1845) is fully understood (our analysis shows that other resources seem to be unused and could have been added as a decoy). This resource is yet another DLL that contains 2 compressed resources:
    - "AdvancedRun.exe" stops the Windows Defender service (C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe"/EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run), deletes the Windows Defender folder (Command:"C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe"/EXEFilename"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run).
    - "Waqybg" (also referenced as Stage4) is a Windows PE executable. It overwrites the first 1MB of each file with 0xCC and overwrites its extension with a random number, then pings an IP address and deletes itself with the following command: cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q \"[Filepath]\". The latter ping technique is commonly used by malware to add execution delay.

IoCs

In the following table, we share the IoCs that can help identifying WhisperGate.

Type	IoC	Source	Notes
File hash	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	VirusTotal	Stage1
File hash	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	VirusTotal	Stage2
File hash	923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6	VirusTotal	Stage3, Tbopbh.jpg

File hash	9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d	VirusTotal	Stage3, *Reversed* Tbopbh.jpg – Frkmlkdkdubkznbkmcf.dll
File hash	35FEEFE6BD2B982CB1A5D4C1D094E8665C51752D0A6F7E3CAE546D770C280F3A	VirusTotal	Decoded Resource "78c855a088924e92a7f60d661c3d1845"
File hash	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B	VirusTotal	AdvancedRun.exe - *this is not a malicious tool in isolation, it has benign uses.*
File hash	DB5A204A34969F60FE4A653F51D64EEE024DBF018EDEA334E8B3DF780EDA846F	VirusTotal	Nmddfrqqrbyjeygggda.vbs
File hash	34CA75A8C190F20B8A7596AFEB255F2228CB2467BD210B2637965B61AC7EA907	VirusTotal	File Wiper
URL	https[:]//cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg	VirusTotal	URL used to download stage3

Mitigation Recommendations

- Update antivirus and EDR tools with the latest signatures.
- Deploy the above-mentioned known IoCs in detection tools.
- Enforce anti-phishing training. *While the initial infection vector is still unknown, it is possible that it was phishing.*
- Use available YARA rules for threat hunting.

References

- https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
- https://www.cadosecurity.com/resources-for-dfir-professionals-responding-to-whispergate-malware/
- https://github.com/cado-security/DFIR_Resources_Whispergate
- https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3
- https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

Accompanying the invasion: HermeticWiper, HermeticRansom, HermeticWizard, IsaacWiper, FoxBlade

Summary

- On February 23rd, the threat intelligence community began observing a new wiper malware sample circulating in Ukrainian organizations. This malware was dubbed *HermeticWiper*.

- The wiper relies on a legitimate partition management driver from EaseUS Partition Master Software (*empntdrv.sys)* to corrupt MBR of the infected Windows machines and delete data. The driver is signed by a digital certificate belonging to a Cyprus-based company Hermetica Digital Ltd. After corrupting the MBR malware reboots the infected machine, resulting in a boot failure.
- According to researchers from ESET, at least in one case, the threat actors had access to a victim's network for deploying the malware.
- Some attacks using HermeticWiper were accompanied by a Go ransomware called HermeticRansom. This was found around the same time as HermeticWiper and probably used as a smokescreen for the wiper, similar to what was seen with WhisperGate.
- In some attacks, HermeticWiper was dropped by a local network worm called HermeticWizard, which leverages WMI and SMB.
- On February 24th yet a new wiper, called IsaacWiper was detected on a Ukrainian governmental network.
- On the same date of February 24th, a new Trojan, named FoxBlade, was detected by Microsoft. Microsoft has not provided details of the Trojan, beyond the fact that it can leverage infected computer for DDoS attacks.
- The initial access vector for these incidents is not known.

Technical Analysis

HermeticWiper uses a certificate from "Hermetica Digital Ltd" to avoid detection once it is delivered to the target Windows machine. It also relies on a legitimate partition management driver from EaseUS Partition Master Software (*empntdrv.sys)* to corrupt the MBR of the infected Windows machines and delete data. This is also likely for avoiding detection, since WhisperGate used Windows API calls for filesystem access and if HermeticWiper used the same technique it could have been detected with already existing malware signatures.

HermeticWiper first sets system privileges required for manipulating files, load drivers and rebooting the infected machine (*SeShutdownPrivilege, SeBackupPrivilege, SeLoadDriverPrivilege*). The malware then checks the OS architecture and drops a corresponding version of the EaseUS driver. It then manipulates Windows Registry keys:

- Sets **HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled** to 0 to avoid writing crash files when the system terminates abnormally.
- Deletes the service registry key **HKLM\SYSTEM\CurrentControlSet\Services.** The malware drops the corresponding version of the EaseUS driver into the "C:\Windows\system32\Drivers" folder and loads it using the *SeLoadDriverPrivilege*. This driver is then run as a service using Windows API.

Next, HermeticWiper obtains a device number (hard drive disk), disables the Volume Shadow Copy Service (VSS), and reads various disk attributes related to MBR. In particular, the malware differentiates between FAT and NTFS partitions since they contain different MBR attributes (different data corruption algorithms are used according to different partition types). Finally, HermeticWiper proceeds with corrupting these attributes, and reboots the infected machine, resulting in a boot failure (i.e., the machine becomes unusable).

Along with the above activities, HermeticWiper enumerates the Windows files, event logs and Windows Restore Points, however at this point it is unclear if anything is being done to these files. It also seems that the malware disables Windows Defender by calling the "mpcmdrun.exe" utility:

C:\ProgramFiles\Windows Defender\mpcmdrun.exe -wdenable

HermeticWizard is a DLL exported as Wizard.dll that contains three encrypted PE files: a sample of HermeticWiper, a DLL that spreads itself on the local network via WMI (exec_32.dll) and a DLL that does the

same via SMB (romance.dll). First, the DLL scans the network for other machines using Windows functions and then tries to connect to the found IP addresses on different ports. When a reachable machine is found, it drops the SMB and WMI spreaders and then HermeticWiper itself.

HermeticRansom was deployed at the same but at a much smaller scale than HermeticWiper. It is written in Golang and doesn't have any anti-analysis techniques. When executed, it creates an ID, identifies hard drives on the system and scans them for files. It then creates a readme file on the Desktop, which contains the victim's ID and the attacker's contact e-mails.

IsaacWiper is either a DLL or EXE that has appeared with several names, such as clean.exe, cl.exe, cl64.dll, cld.dll and cll.dll. IsaacWiper also enumerates hard drives and then wipes the first 0x10000 bytes of each drive with a random number. It then wipes every file found on every disk.

IoCs

Type	IoC	Source	Notes
File hash (SHA256)	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767	JoeSandbox	
File hash (SHA256)	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf	JoeSandbox	
File hash (SHA256)	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	JoeSandbox	
File hash (SHA256)	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	JoeSandbox	
File hash (SHA256)	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767	JoeSandbox	
File hash (SHA1)	912342f1c840a42f6b74132f8a7c4ffe7d40fb77	SentinelOne	Win32 EXE
File hash (SHA1)	61b25d11392172e587d8da3045812a66c3385451	SentinelOne	Win32 EXE
File hash (SHA1)	a952e288a1ead66490b3275a807f52e5	SentinelOne	RCDATA_DRV_X64
File hash (SHA1)	231b3385ac17e41c5bb1b1fcb59599c4	SentinelOne	RCDATA_DRV_X64
File hash (SHA1)	095a1678021b034903c85dd5acb447ad	SentinelOne	RCDATA_DRV_XP_X64
File hash (SHA1)	eb845b7a16ed82bd248e395d9852f467	SentinelOne	RCDATA_DRV_XP_X86
Windows Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnab	SentinelOne	Value changes from 1 to 0
Windows Registry Key	HLKM\SYSTEM\CurrentControlSet\Services	SentinelOne	Deleted
File hash (MD5)	3C54C9A49A8DDCA02189FE15FEA52FE24F41A86F	ESET	HermeticWizard

File hash (MD5)	d5d2c4ac6c724cd63b69ca054713e278	Securelist	HermeticRansom
File hash (MD5)	F32D791EC9E6385A91B45942C230F52AFF1626DF	ESET	HermeticRansom
File hash (MD5)	AD602039C6F0237D4A997D5640E92CE5E2B3BBA3	ESET	IsaacWiper
File hash (MD5)	736A4CFAD1ED83A6A0B75B0474D5E01A3A36F950	ESET	IsaacWiper
File hash (MD5)	E9B96E9B86FAD28D950CA428879168E0894D854F	ESET	IsaacWiper

Mitigation Recommendations

The PowerShell script below can be used to detect executables signed by the same certificate as HermeticWiper. It will scan recursively the C:/ drive and output when an executable matches. It is easy to change it to scan other drives (replace “C:” with the intended drive) and to scan other file types (replace “.exe” with the intended file type).

```
Get-ChildItem -Recurse "C:" -Filter *.exe | Foreach-Object {if ((Get-
AuthenticodeSignature  -LiteralPath
$_.FullName).SignerCertificate.SerialNumber -eq
"0C48732873AC8CCEBAF8F0E1E8329CEC")  {
Write-Output ($_.FullName + " Matched HermiticaWiper certificate")}}
```

References

- https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/
- https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
- https://blog.talosintelligence.com/2022/02/threat-advisory-hermeticwiper.html
- https://twitter.com/fr0gger_/status/1497121876870832128
- https://securelist.com/elections-goransom-and-hermeticwiper-attack/105960/
- https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
- https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

Not in the conflict: Cyclops Blink

Summary

- On February 23rd, CISA and the UK-NCSC released a report about Cyclops Blink, a new malware developed by the Sandworm group to replace VPNFilter.
- Cyclops Blink is a malicious Linux ELF executable that currently targets devices running the 32-bit PowerPC architecture.
- The malware contains a core component and additional modules executed as child processes that can upload/download files, extract device information, and update the malware.
- Command and Control communication uses a custom binary protocol underneath TLS, and messages are individually encrypted.
- The malware has been associated with a large-scale botnet targeting network devices used in small and home offices (mainly WatchGuard Firebox) and active since 2019.

Technical Analysis

A full analysis of two known samples is currently available at *https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf*

The main point still unclear in that analysis is how the WatchGuard vulnerability was exploited by Cyclops Blink. The *WatchGuard FAQ* about the malware mentioned a vulnerability was exploited to install the Cyclops Blink implant but no details on it. A *firmware release* mentions *CVE-2022-23176* (silently fixed in May 2021 but never made public) which is only vaguely described as related to the login process / Web UI. Watchguard claims these issues were *found internally* and *not exploited in the wild*. The latest *firmware release notes* also mentions several other vulnerabilities addressed, which may or may not have been exploited in the wild.

Since the report mentioned the attackers exploited Internet-facing management interfaces, the following are relevant:

Watchguard System Manager : 4105/tcp (unclear, likely SSL)

Watchguard System Manager : 4117/tcp (wgagent XML-RPC - SSL)

Watchguard System Manager : 4118/tcp (wgagent CLI - SSH)

Web UI : 8080/tcp (optionally SSL)

Actively monitoring for increased activity on any of the above ports (in combination with other markers indicating a Watchguard device) can help to detect exploitation.

IoCs

In the following table, we share the IoCs that can help identifying Cyclops Blink.

Type	IoC	Source	Notes
IP addresses	100.43.220[.]234 96.80.68[.]193 188.152.254[.]170	Cyclops-Blink-Malware-Analysis-Report	C&C server addresses

	208.81.37[.]50 70.62.153[.]174 2.230.110[.]137 90.63.245[.]175 212.103.208[.]182 50.255.126[.]65 78.134.89[.]167 81.4.177[.]118 24.199.247[.]222 37.99.163[.]162 37.71.147[.]186 105.159.248[.]137 80.155.38[.]210 217.57.80[.]18 151.0.169[.]250 212.202.147[.]10 212.234.179[.]113 185.82.169[.]99 93.51.177[.]66 80.15.113[.]188 80.153.75[.]103 109.192.30[.]125		
File path	/usr/bin/cpd	Cyclops-Blink-Malware-Analysis-Report	Path location of Cyclops Blink executable
File path	/var/tmp/a.tmp	Cyclops-Blink-Malware-Analysis-Report	Default path location for downloaded files
File hash	50df5734dd0c6c5983c2 1278f119527f9fdf6ef1d7 e808a29754ebc5253e9a86 c082a9117294fa4880d7 5a2625cf80f63c8bb159b 54a7151553969541ac35 862	Cyclops-Blink-Malware-Analysis-Report	Hash corresponding to the executable code segment only
File name	Rootfs_cfg	Cyclops-Blink-Malware-Analysis-Report	File name used to persist C2 server IP addresses on the device filesystem
File path	/var/tmp/a.tmp	Cyclops-Blink-Malware-Analysis-Report	Path to the backed-up legitimate install_upgrade executable

Mitigation Recommendations

- Use available YARA rules for threat hunting.
- Replace any passwords on your devices that may have been compromised.
- Use multi-factor authentication to reduce the impact of password compromises.
- Ensure that the management interface of network devices is not exposed to the internet.
- Follow this guideline to restore your appliance to a clean state.
- Upgrade the appliance to the latest version of Fireware OS.

References

- https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink- replaces-vpnfilter
- https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
- https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

Version	Date	Changes
0.1	February 24th, 2022	Document outline
1.0	February 25th, 2022	Initial shared version
1.1	March 4th, 2022	Initial public version