28 - 30 September, 2022 / Prague, Czech Republic

RUSSIAN WIPERS IN THE CYBERWAR AGAINST UKRAINE

Alexander Adamov

NioGuard Security Lab, Ukraine

Kharkiv National University of Radio Electronics, Ukraine

Blekinge Institute of Technology, Sweden

ada@nioguard.com

ABSTRACT

The paper provides an overview of the tactics and techniques implemented by Russian state hacking groups in their wiper attacks targeting government information systems and critical infrastructure in Ukraine before and during the military invasion in 2022.

INTRODUCTION

The story of Russian wipers launched against Ukraine began in 2015 when the Sandworm group (the Russian GRU) [1] attacked the Ukrainian power grid with the BlackEnergy backdoor and KillDisk wiper, which was used to wipe the traces of the attack by crashing an infected SCADA server in the power distribution centres. The attackers left 230,000 residents of Western Ukraine without electricity for six hours [2].

A year later, on 17 December 2016, the Sandworm APT group launched a new, even more advanced attack, named Industroyer by *ESET* (a.k.a. CRASHOVERRIDE by *Dragos*), once again targeting the Ukrainian power grid [3, 4].

Two years later, in June 2017, the Sandworm group ran a supply-chain attack delivering another wiper, called NotPetya, which was a patched version of the Petya ransomware but without the ability to restore an encrypted Master File Table (MFT) [5].

This year we've seen unprecedented activity of Russian state APT groups (Sandworm, APT28/29, Gamaredon) against the Ukrainian government and critical infrastructure in attacks that have used a variety of different wipers that have nothing in common from a technical perspective, but which share the same motive.

WIPER ATTACKS IN 2022

The year began with the WhisperGate campaign [6, 7, 8], discovered by *Microsoft* on 13 January 2022, against Ukrainian financial and government institutions, in which a rather complex wiper rewrote not only the MBR but also part of the data on all hard disks while in boot mode.

The day before the Russian army invaded Ukraine (23 February 2022), HermeticWiper malware was used in an attack against at least five government organizations in Ukraine. The wiper used legitimate drivers from the *EaseUS Partition Master* software to gain direct access to disk partitions. The wiper was signed with a certificate issued to '*Hermetica Digital Ltd*', generated on 13 April 2021. HermeticRansom was used to cover the wiper's attack [9].

The next day (24 February 2022), researchers from *ESET* detected another wiper, which they called IsaacWiper [10].

Later, on 14 March 2022, *ESET* discovered another basic wiper, CaddyWiper, that simply fills the first 1,920 bytes of the disk with zeros, making a target system unbootable.

The same week, on 17 March 2022, another group sent a spear-phishing email containing a ZIP archive with the file 'Вирус... крайне опасно!!!.zip' (translated from Russian: 'Virus… extremely dangerous!!!.zip'), which contained a .NET wiper called DoubleZero. DoubleZero takes its name from the fact it uses two methods for zeroing files: NtfsControlFile with a control code of FSCTL_SET_ZERO_DATA and the `FileStream.Write()` method [11, 12].

In April, CERT-UA reported a new attack against the Ukrainian power grid with a new version of the Industroyer malware used previously in 2016 by the Russian Sandworm group and an encoded version of CaddyWiper, which was launched and decoded using a patched version of the remote *IDA* debugger server 'win32_remote.exe' known to all reverse engineers. The attackers established a foothold in February 2022 and planned to take down the energy systems on the evening of Friday 8 April 2022 [13].

Date of discovery	Name	Discovered by	Attribution
13 January 2022	WhisperGate	*Microsoft*	DEV-0586 (GRU)
23 February 2022	HermeticWiper (FoxBlade), HermeticWizard, HermeticRansom (SonicVote)	*ESET*	N/A
24 - 25 February 2022	IsaacWiper (Lasainraw)	*ESET*	N/A
Early March 2022	DesertBlade	*Microsoft*	N/A
14 March 2022	CaddyWiper	*ESET*	Sandworm
17 March 2022	DoubleZero (FiberLake)	CERT-UA with *Microsoft* and *ESET*	UAC-0088
February - 8 April 2022	Industroyer2 + CaddyWiper2 (AprilAxe | ARGUEPATCH + CaddyWiper)	CERT-UA with *Microsoft* and *ESET*	Sandworm

Table 1: Discovery of Russian wipers in 2022.

DELIVERY MECHANISM

In the majority of the attacks, Group Policy Object (GPO) was used to deploy wipers with the administrative privilege required to gain direct access to physical disks.

Name	Delivery
WhisperGate	Trojan-Downloader -> Discord -> Trojan-Dropper
HermeticWiper (FoxBlade), HermeticWizard, HermeticRansom (SonicVote)	- GPO - Network worm HermeticWizard using WMI and SMB
IsaacWiper (Lasainraw)	N/A
DesertBlade	GPO
CaddyWiper	GPO
DoubleZero (FiberLake)	Spear-phishing attack with a ZIP archive containing the file 'Вирус... крайне опасно!!!.zip' (translated from Russian: 'Virus… extremely dangerous!!!.zip')
Industroyer2 + CaddyWiper2 (AprilAxe | ARGUEPATCH + CaddyWiper)	GPO

Table 2: The mechanisms used to deliver wipers in 2022.

THREAT ACTORS

Table 3 shows the Russian state-sponsored hacking groups that have been seen active in the Russia-Ukraine cyberwar according to *Microsoft*'s special report on Ukraine [14].

Branch	Unit	APT names	Wipers
GRU (military intelligence service)	Unit 26165	APT28, STRONTIUM	N/A
	Unit 74455	Sandworm, IRIDIUM	CaddyWiper, Industroyer2
	?	DEV-0586	WhisperGate
SVR (diplomatic intelligence service)		NOBELIUM, UNC2452/2652	N/A
FSB (internal intelligence service)		Gamaredon, ACTINIUM	N/A
	Unit 71330	EnergeticBear, BROMINE	N/A
		Turla, KRYPTON	N/A

Table 3: Russian state threat actors.

DISK WIPING TECHNIQUES

Table 4 describes the techniques used by the wipers in 2022.

DEFENCE EVASION

Table 5 describes the defence evasion techniques used by the wipers in 2022, such as the usage of digital certificates, code obfuscation and encoding.

Name	Wiping technique
WhisperGate	- File Corruptor (Tbopbh.jpg) writes 0x100000 (1,048,576 bytes) of the '0xC' byte whilst appending a random 4-byte to its extension to every file. - Writes a small 16-bit wiper code to the MBR. - The 16-bit code in the MBR wipes every 199th sector on a disk, starting from sector 1, with zeros.
HermeticWiper (FoxBlade), HermeticWizard, HermeticRansom (SonicVote)	HermeticWiper - Uses drivers of the *EaseUS Partition Master* software. - The data is overwritten with randomly generated bytes using `CryptGenRandom()`. - Wipes MBR, MFT, system registry, `$Bitmap` and `$LogFile` on all drives, Windows Events Log. HermeticRansom - Encrypts the first 9437184 bytes (9.44 MB) of a file using AES-256-GCM. - AES key is encrypted with RSA-OAEP (the public key is hard coded) and stored in the file's footer.
IsaacWiper (Lasainraw)	- Calls DeviceIoControl with the `IOCTL_STORAGE_GET_DEVICE_NUMBER` to get device numbers for all disks. - Wipes the first 0x10000 bytes of each disk using the Mersenne Twister pseudorandom generator seeded using the `GetTickCount()` value.
DesertBlade	Iteratively overwrites and then deletes overwritten files on all accessible drives. Spares the system if it is a domain controller.
CaddyWiper	To perform disk corruption CaddyWiper obtains access to the disk partitions from '`\.\\\PHYSICALDRIVE9`' to '`\.\\\PHYSICALDRIVE0`' and overwrites the first 1,920 bytes of data with '0' using the `CreateFileW()` and `DeviceIoControl()` functions. This operation can be done only if the malware is executed as administrator. Spares the system if it is a domain controller.
DoubleZero (FiberLake)	- Uses `NtfsControlFile()` with a control code of `FSCTL_SET_ZERO_DATA` (0x980C8) to set the file's content to all zero bytes. - Uses the `FileStream.Write()` method to set the file's content to all zero bytes. - The wiper destroys entries in the System registry
Industroyer2 + CaddyWiper2 (AprilAxe | ARGUEPATCH + CaddyWiper)	Same as for CaddyWiper.

Table 4: The mechanisms used to deliver wipers in 2022.

Name	Defence evasion technique
WhisperGate	Passive: - The second file 'stage2.exe' is a .NET application, which contains a *Microsoft Windows* signature supposedly taken from the Russian version of *Windows Explorer* according to the properties in File Details. - Stage2.exe is obfuscated with Ezfuscator. - File Corruptor (Tbopbh.jpg) is encoded with XOR. - Uses legitimate 'InstallUtil.exe'. Active: - Disables *Windows Defender* by executing the file 'Nmddfrqqrbyjeygggda.vbs' script.
HermeticWiper (FoxBlade), HermeticWizard, HermeticRansom (SonicVote, PartyTicket)	- HermeticWiper and HermeticWizard are signed with a certificate issued to 'Hermetica Digital Ltd', generated on 13 April 2021. - HermeticWiper uses legitimate drivers of the *EaseUS Partition Master* software to perform disk operations.
IsaacWiper (Lasainraw)	N/A
DesertBlade	N/A
CaddyWiper	Obfuscation: all strings are split into single characters.
DoubleZero (FiberLake)	N/A
Industroyer2 + CaddyWiper2 (AprilAxe | ARGUEPATCH + CaddyWiper)	- CaddyWiper payload is executed as a bytecode decoded in the memory using a XOR operation by the patched version of a legitimate component of the *Hex-Rays IDA Pro* software, specifically the remote *IDA* debugger server '`win32_remote.exe`' named as ARGUEPATCH. - Obfuscation: the names of API calls are split into parts and concatenated during runtime linking.

Table 5: The defence evasion techniques of the wipers in 2022.

IMPLEMENTATION ISSUES

During the analysis of the wipers' code, it was discovered that not all of them have operated well, due to implementation issues.

WhisperGate:

- The MBR writer (stage1.exe) doesn't check if it successfully gets a handle to a '\\.\PhysicalDrive0' disk when calling CreateFile(), which may lead to failure when calling WriteFile() with non-admin privileges without throwing and handling an exception.

HermeticRansom:

- The wiper doesn't properly initialize AES key for every new file as the seed is initialized after the key is generated. Therefore, all files are encrypted with the same file key, which made it possible to create a decryptor [15].
- It creates a thread and copy of its file for every enumerated file, which doesn't speed up the encryption process as was intended through multi-threading.

IsaacWiper:

- The file encryption that was implemented in a single thread led to slowing down encryption.
- The first version of the wiper couldn't wipe the disks. A second version was deployed on 25 February 2022 with debug logging enabled.

CaddyWiper2 (ARGUEPATCH, AprilAxe):

- The decoder uses a 16-byte password string to XOR a single byte of the encoded CaddyWiper code, which makes no sense and only wastes the CPU resources.

CONCLUSION

Our analysis showed that the wipers used in the attacks look more like a 'zoo' from an implementation perspective, sharing no common development framework or techniques. The groups used different programming languages (C/C++, C#, Golang) to create wipers. The destructive techniques and targets also vary from wiper to wiper. This may indicate that the wipers were created by different military units. The number of errors in implementation may point to a low level of programming and cryptography skills of the wipers' creators and/or tight deadlines that impacted the quality of the developed malware.

The last attack, with reincarnation of Industroyer and encoded CaddyWiper, planned for 8 April 2022, may indicate that Russian state hacking groups (GRU's Sandworm) are exhausted and have no resources to develop new pieces of sophisticated malware to launch new campaigns and therefore switched to the practice of reuse or 'malware recycling'. The reuse tactic has been already seen: in 2017 the Russian APT28 group used clones of open-source or stolen ransomware such as XData (originally AES-NI ransomware, the source code of which had been stolen), PsCrypt (Globe), WannaCry.NET (similar to WannaCry, the EternalBlue exploit was used in the .NET version of the ransomware) and NotPetya (Petya's binary was patched to irreversibly destroy an MFT) in a supply-chain attack via the compromised *MEDoc* software.

ACKNOWLEDGEMENTS

I'd like to acknowledge the help of Anders Carlsson [16] and Oleksii Baranovskyi [17], my colleagues from Blekinge Institute of Technology, who helped me with the investigation of the attacks.

REFERENCES

[1] Sandworm Team. MITRE. https://attack.mitre.org/groups/G0034/.

[2] Wikipedia. Ukraine power grid hack. https://en.wikipedia.org/wiki/Ukraine_power_grid_hack.

[3] Cherepanov, A., Lipovsky, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. ESET. June 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

[4] CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. Dragos, Inc. June 2017. https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/.

[5] Adamov, A.; Carlsson, A. Battlefield Ukraine: finding patterns behind summer cyber attacks. VB2017. October 2017. https://www.virusbulletin.com/conference/vb2017/abstracts/last-minute-paper-battlefield-ukraine-finding-patterns-behind-summer-cyber-attacks.

[6] Destructive malware targeting Ukrainian organizations. Microsoft. January 2022. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[7] Analysis of WhisperGate. NioGuard Security Lab. January 2022. https://www.nioguard.com/2022/01/analysis-of-whispergate.html.

[8] Analysis of Destructive Malware (WhisperGate) targeting Ukraine. BLKSMTH | S2W TALON. https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3.

[9] HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine. Malwarebytes LABS. March 2022. https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/.

[10] IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. ESET. March 2022. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.

[11] Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243). CERT-UA. March 2022. https://cert.gov.ua/article/38088.

[12] Threat Advisory: DoubleZero. Cisco TALOS. March 2022. https://blog.talosintelligence.com/2022/03/threat-advisory-doublezero.html.

[13] Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435). CERT-UA. April 2022. https://cert.gov.ua/article/39518.

[14] Burt, T. The hybrid war in Ukraine. Microsoft. April 2022. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.

[15] Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities. CrowdStrike. March 2022. https://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine/.

[16] anders.carlsson@bth.se.

[17] oleksii.baranovskyi@bth.se.