Executive summary

- 2022 has experienced an increase in the number of wiper variants targeting Ukrainian entities.
- This blog post looks to explain how wipers work, what makes them so effective and provides a short overview of the most recent samples that appeared in the eastern Europe geopolitical conflict.

How does wiper malware work?

Wiper's main objective is to destroy data from any storage device and make the information unavailable (T1485). There are two ways of removing files, logical and physical.

Logical file removal is the most common way of erasing a file, performed by users daily when a file is sent to (and emptied from) the Recycle bin, or when it is removed with the command line or terminal with the commands del/rm. This action deletes the pointer to the file but not the file data, making it recoverable with forensic tools as long as the Operative System does not write any other file in the same physical location.

However, malware wipers aim to make the data irrecoverable, so they tend to remove the data from the physical level of the disk. The most effective way to remove the data/file is by overwriting the specific physical location with other data (usually a repeated byte like 0xFF). This process usually involves writing to disk several Gigabytes (or Terabytes) of data and can be time consuming. For this reason, in addition to destroying the data, many wipers first destroy two special files in the system:

- The Master Boot Record (MBR), which is used during the boot process to identify where the Operative System is stored in the disk. By replacing the MBR, the boot process crashes, making the files inaccessible unless forensic methodologies are used.
- The Master File Table (MFT) is exclusive to NTFS file systems, contains the physical location of files in the drive as well as logical and physical size and any associated metadata. If big files need to be stored in the drive, and cannot use consecutive blocks, these files will have to be fragmented in the disk. The MFT holds the information of where each fragment is stored. Removing the MFT will require the use of forensic tools to recover small files, and basically prevents recovery of fragmented files since the link between fragments is lost.

The main difference between wipers and ransomware is that it's impossible to retrieve the impacted information after a wiper attack. Attackers using wipers do not usually target financial reward but intend to disrupt the victim's operations as much as possible. Ransomware operators aim to get a payment in exchange for the key to decrypt the user's data.

With both wiper and ransomware attacks, the victim depends on their back up system to recover after an attack. However, even some wiper attacks carry ransom notes requesting a payment to recover the data. It is important that the victim properly identifies the attack they've suffered, or they may pay the ransom without any chance of retrieving the lost data.

In the last month and a half, since the war started in Eastern Europe, several wipers have been used in parallel with DDoS attacks (T1499) to keep financial institutions and government organizations, mainly Ukrainian, inaccessible for extended periods of time. Some of the wipers observed in this timeframe have been: WhisperKill, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero Wiper and AcidRain.

Most recent wiper examples

WhisperKill

On January 14, 2022, the Ukrainian government experienced a coordinated attack on 22 of their government agencies, defacing their websites. Almost all the compromised websites were developed by the same Ukranian IT company, Kitsoft, and all of them were built on OctoberCMS. Therefore, the attack vector was most probably a supply chain attack on the IT provider, or an exploitation of an OctoberCMS vulnerability, combined with exploitations of Log4Shell vulnerability (T1190).

defaced Ukrainian website

Figure 1. Example of defaced Ukrainian government website.

In addition to the website defacement, Microsoft Threat Intelligence Center (MSTIC), identified in a report destructive malware samples targeting Ukrainian organizations with two malware samples. Microsoft named the samples WhisperGate, while other security companies labeled the downloader as WhisperGate and WhisperKill as the actual wiper, which was considered a component of WhisperGate.

The identified files were:

- Stage1 replaces the Master Boot Record (MBR) with a ransom note when the system is powered down, deeming the machine unbootable after that point. When booted up, the system displays Figure 2 on screen. Despite the ransom request, the data will not be recoverable since all efforts made by WhisperKill are looking to destroy data, not encrypt it. In this case, the wallet is most probably an attempt to decoy attribution efforts.

wiper ransom note

Figure 2. Ransom note obtained by MSTIC.

- Stage 2 attempts to download the next stage malware (T1102.003) from the Discord app, if unsuccessful, it sleeps and tries again. The payload downloaded from the messaging app destroys as much data as possible by overwriting certain file types with 0xCC for the first MB of the file. Then it modifies the file extension to a random four-byte extension. By selecting the file types to be wiped and only writing over the first MB of data, the attackers are optimizing the wiping process. This is due to not wasting time on system files and only spending the necessary time to wipe each file, rapidly switching to the next file as soon as the current one is unrecoverable. Finally, the malware executes a command to delete itself from the system (T1070.004).

HermeticWiper

A month after, on February 23rd 2022, ESET Research reported a new Wiper being used against hundreds of Ukrainian systems. The wiper receives its name from the stolen certificate (T1588.003) it was using to bypass security controls “Hermetica Digital Ltd” (T1588.003). According to a Reuters article, the certificate could have also been obtained by impersonating the company and requesting a certificate from scratch.

hermetica certificate

Figure 3. Hermetica Digital Ltd certificate.

The attackers have been seen using several methods to distribute the wiper through the domain, like: domain Group Policy Object (GPO) (T1484.001), Impacket or SMB (T1021.002) and WMI (T1047) with an additional worm component named HermeticWizard.

The wiper component first installs the payload as a service (T1569.002) under C:\Windows\system32\Drivers\. Afterwards, the service corrupts the first 512 bytes of the MBR of all the Physical Drives, and then enumerates their partitions. Before attempting to overwrite as much data as the wiper can it will delete key files in the partition, like MFT, $Bitmap, $LogFile, the NTUSER registry hive (T1112) and the event logs (T1070.001).

On top of deleting key file system structures, it also performs a drive fragmentation (breaking up files and segregating them in the drive to optimize the system’s performance). The combination of the file fragmentation and the deletion of the MFT makes file recovery difficult, since files will be scattered through the drive in small parts - without any guidance as to where each part is located.

Finally, the malware writes randomized contents into all occupied sectors in the partition in an attempt to remove all potential hope of recovering any data with forensic tools or procedures.

IsaacWiper

A day after the initial destructive attack with HermeticWiper, on February 24th, 2022, a new wiper was used against the Ukrainian government, as reported by ESET, without any significant similarities to the HermaticWiper used the day before.

IsaacWiper identifies all the physical drives not containing the Operative System and locks their logical partitions by only allowing a single thread to access each of them. Then it starts to write random data into the drives in chunks of 64 KB. There is a unique thread per volume, making the wiping process very long.

Once the rest of the physical drives and the logical partitions sharing physical drive with the Operative System’s volume have been wiped, this last volume is wiped by:

- Erasing the MBR.
- Overwriting all files with 64 KB chunks of random data with one thread.
- Creating a new file under the C drive which will be filled with random data until it takes the maximum space it can from the partition, overwriting the already overwritten existing files. This process is performed with a different thread, but it would still take a long time to write the full partition since both concurrent threads are actually attempting to write random data on the full disk.

Isaacwiper strings

Figure 4. IsaacWiper strings.

When comparing IsaacWiper to WhisperKill, the attackers' priorities become clear. WhisperKill creators prioritized speed and number of affected files over ensuring the full drive is overwritten, since only 1 MB of each file was overwritten. On the other hand, IsaacWiper creators gave total priority to deliver the most effective wiper, no matter how long it takes to overwrite the full physical disk.

AcidRain

On the same day IsaacWiper was deployed, another wiper attacked Viasat KA-SAT modems in Ukraine, this time with a different wiper, named AcidRain by SentinelLABS. This wiper was particularly aimed at modems, probably to disrupt Internet access from Ukraine. This new wiper showed similarities to previously seen botnets targeting modems using VPNFilter. It was used in 2018, targeting vulnerabilities in several common router brands: Linksys, MikroTik, NETGEAR, and TP-Link. Exploiting vulnerabilities allowed the attackers to obtain Initial Access inside all types of networks, where the bot would search for Modbus traffic to identify infected systems with Industrial Control Systems (ICS).

The wiper used was the ELF MIPS wiper targeting Viasat KA-SAT modems, which aimed to firstly overwrite any file outside of the any common *nix installation: bin, boot, dev, lib, proc, sbin, sys, sur, etc. to then delete data from /dev/.

CaddyWiper

The first version of CaddyWiper was discovered by ESET researchers on 2022-03-14 when it was used against a Ukrainian bank. This new wiper variant does not have any significant code similarities to previous wipers. This sample specifically sets an exclusion to avoid infecting Domain Controllers in the infected system. Afterwards, it targets C:/Users and any additional attached drive all the way to letter Z:/ and zeroes all the files present in such folders/drives. Finally, the extended information of the physical drives is destroyed, including the MBR and partition entries.

A variant of CaddyWiper was used again on 2022-04-08 14:58 against high-voltage electrical substations in Ukraine. This latest version of the wiper was delivered together with Industroyer2, an evolution of Industroyer, which has the main functionn being to communicate with industrial equipment. In this case, the wiper was used with the purpose of slowing down the recovery process from the Industroyer2 attack and gaining back control of the ICS consoles, as well as covering the tracks of the attack. According to Welivesecurity, who have been cooperating with CERT-UA in this investigation, the Sandworm Team is behind this latest attack.

In this same attack against the energy station in Ukraine, other wiper samples for Linux and Solaris were observed by WeliveSecurity. These wipers leverage the shred command if present, otherwise they use the basic dd or rm commands to wipe the system.

DoubleZero wiper

On March 22, 2022 CERT-UA reported a new wiper used against their infrastructure and enterprises. Named DoubleZero, the wiper was distributed as a ZIP file containing an obfuscated .NET program. The wiper's routine sets a hardcoded list of system directories, which are skipped during an initial wiping targeting user files. Afterwards, the skipped system directories are targeted and finally the registry hives: HKEY_LOCAL_MACHINE (containing the hives Sam, Security, Software and System), HKEY_CURRENT_USER and HKEY_USERS.

There are two wiping methods, both of which zero out the selected file.

doublezero wiper

Figure 5. DoubleZero first wiping function.

Conclusion

As we have seen in the examples above, the main objective of the attackers behind wipers is to destroy all possible data and render systems unbootable (if possible), potentially requiring a full system restore if backups aren't available. These malware attacks can be as disruptive as ransomware attacks, but wipers are arguably worse since there is no potential escape door of a payment to recover the data.

There are plenty of ways to wipe systems. We've looked at 6 different wiper samples observed targeting Ukranian entities. These samples approach the attack in very different ways, and most of them occur faster than the time required to respond. For that reason, it is not effective to employ detection of wiper malware, as once they are in the system as it is already too late. The best approach against wipers is to prevent attacks by keeping systems up to date and by increasing cybersecurity awareness. In addition, consequences can be ameliorated by having periodic backup copies of key infrastructure available.

Associated indicators (IOCs)

The following technical indicators are associated with the reported intelligence. A list of indicators is also available in the following OTX Pulses:

- WhisperKill
- HermeticWiper and IsaacWiper
- AcidRain
- CaddyWiper
- DoubleZero

Please note, the pulses may include other activities related but out of the scope of the report.

TYPE	INDICATOR	DESCRIPTION
SHA256	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	WhisperKill (stage1.exe)
SHA256	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	WhisperKill (stage2.exe)
SHA256	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	HermeticWiper
SHA256	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	HermeticWiper
SHA256	13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033	IsaacWiper
SHA256	9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a	AcidRain
SHA256	47f521bd6be19f823bfd3a72d851d6f3440a6c4cc3d940190bdc9b6dd53a83d6	AcidRain
SHA256	Fc0e6f2effbfa287217b8930ab55b7a77bb86dbd923c0e8150551627138c9caa	CaddyWiper
SHA256	7062403bccacc7c0b84d27987b204777f6078319c3f4caa361581825c1a94e87	Industroyer2
SHA256	3b2e708eaa4744c76a633391cf2c983f4a098b46436525619e5ea44e105355fe	DoubleZero
SHA256	30b3cbe8817ed75d8221059e4be35d5624bd6b5dc921d4991a7adc4c3eb5de4a	DoubleZero

Mapped to MITRE ATT&CK

The findings of this report are mapped to the following MITRE ATT&CK Matrix techniques:

- TA0001: Initial Access
  - T1190: Exploit Public-Facing Application
- TA0002: Execution
  - T1047: Windows Management Instrumentation
  - T1569: System Services
    - T1569.002: Service Execution
- TA0008: Lateral Movement
  - T1021: Remote Services
    - T1021.002: SMB/Windows Admin Shares

- TA0005: Defense Evasion
    - T1070: Indicator Removal on Host
        - T1070.004: File Deletion
        - T1070.001: Clear Windows Event Logs
    - T1112: Modify Registry
    - T1484: Domain Policy Modification
        - T1484.001: Group Policy Modification
- TA0011: Command and Control
    - T1102: Web Service
        - T1102.003: One-Way Communication
- TA0040: Impact
    - T1485: Data Destruction
    - T1499: Endpoint Denial of Service
- TA0042: Resource Development
    - T1588: Obtain Capabilities
        - T1588.003: Code Signing Certificates