IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine

ESET researchers uncover a new wiper that attacks Ukrainian organizations and a worm component that spreads HermeticWiper in local networks

As the recent hostilities started between Russia and Ukraine, ESET researchers discovered several malware families targeting Ukrainian organizations.

- On February 23rd, 2022, a destructive campaign using HermeticWiper targeted multiple Ukrainian organizations.
- This cyberattack preceded, by a few hours, the start of the invasion of Ukraine by Russian Federation forces
- Initial access vectors varied from one organization to another. We confirmed one case of the wiper being dropped by GPO, and uncovered a worm used to spread the wiper in another compromised network.
- Malware artifacts suggest that the attacks had been planned for several months.
- On February 24th, 2022, a second destructive attack against a Ukrainian governmental network started, using a wiper we have named IsaacWiper.
- ESET Research has not yet been able to attribute these attacks to a known threat actor.

Destructive attacks in Ukraine

As stated in this ESETResearch *tweet* and *WLS blogpost*, we uncovered a destructive attack against computers in Ukraine that started around 14:52 on February 23rd, 2022 UTC. This followed distributed denial-of-service (DDoS) *attacks against major Ukrainian websites* and preceded the Russian military invasion by a few hours.

These destructive attacks leveraged at least three components:

- **HermeticWiper**: makes a system inoperable by corrupting its data
- **HermeticWizard**: spreads HermeticWiper across a local network via WMI and SMB
- **HermeticRansom**: ransomware written in Go

HermeticWiper was observed on hundreds of systems in at least five Ukrainian organizations.

On February 24th, 2022, we detected yet another new wiper in a Ukrainian governmental network. We named it IsaacWiper and we are currently assessing its links, if any, with HermeticWiper. It is important to note that it was seen in an organization that was *not* affected by HermeticWiper.

Attribution

At this point, we have not found any tangible connection with a known threat actor. HermeticWiper, HermeticWizard, and HermeticRansom do not share any significant code similarity with other samples in the ESET malware collection. IsaacWiper is still unattributed as well.

Timeline

HermeticWiper and HermeticWizard are signed by a code-signing certificate (shown in Figure 1) assigned to `Hermetica Digital Ltd` issued on April 13th, 2021. We requested the issuing CA (DigiCert) to revoke the certificate, which it did on February 24th, 2022.

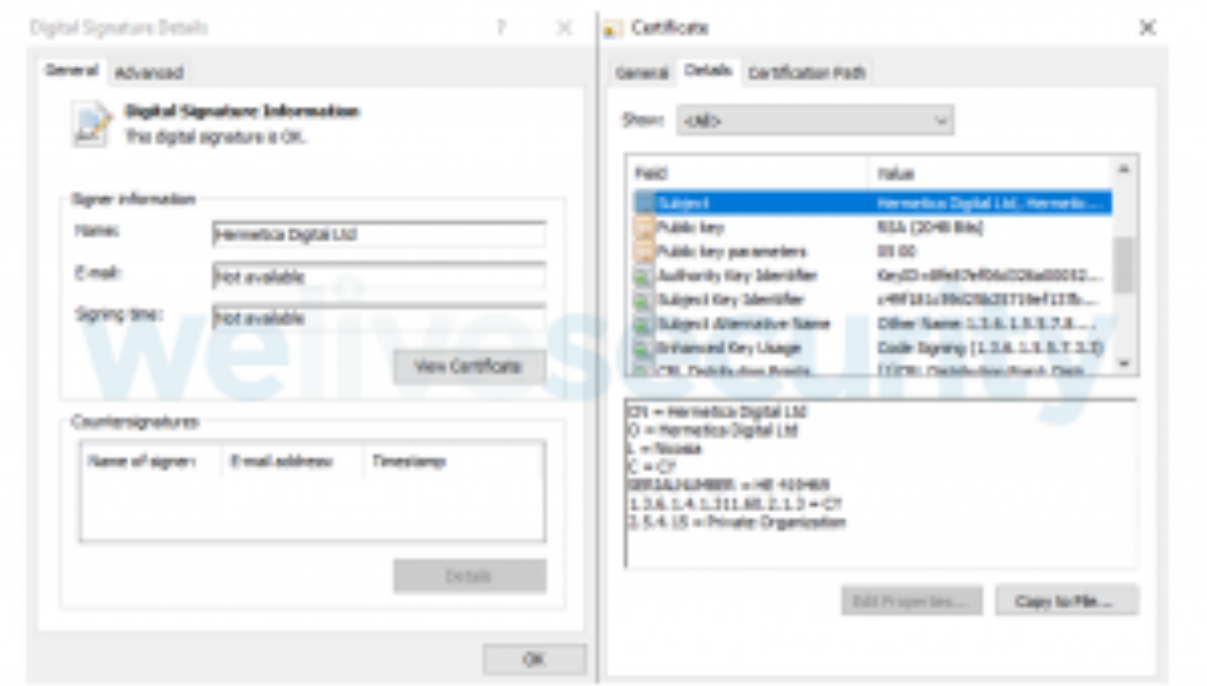


Figure 1. Code-signing certificate assigned to Hermetic Digital Ltd

According to a *report by Reuters*, it seems that this certificate was not stolen from Hermetica Digital. It is likely that instead the attackers impersonated the Cypriot company in order to get this certificate from DigiCert.

ESET researchers assess with high confidence that the affected organizations were compromised well in advance of the wiper's deployment. This is based on several facts:

- HermeticWiper PE compilation timestamps, the oldest being December 28th, 2021
- The code-signing certificate issue date of April 13th, 2021
- Deployment of HermeticWiper through GPO in at least one instance suggests the attackers had prior access to one of that victim's Active Directory servers

The events are summarized in the timeline in Figure 2.

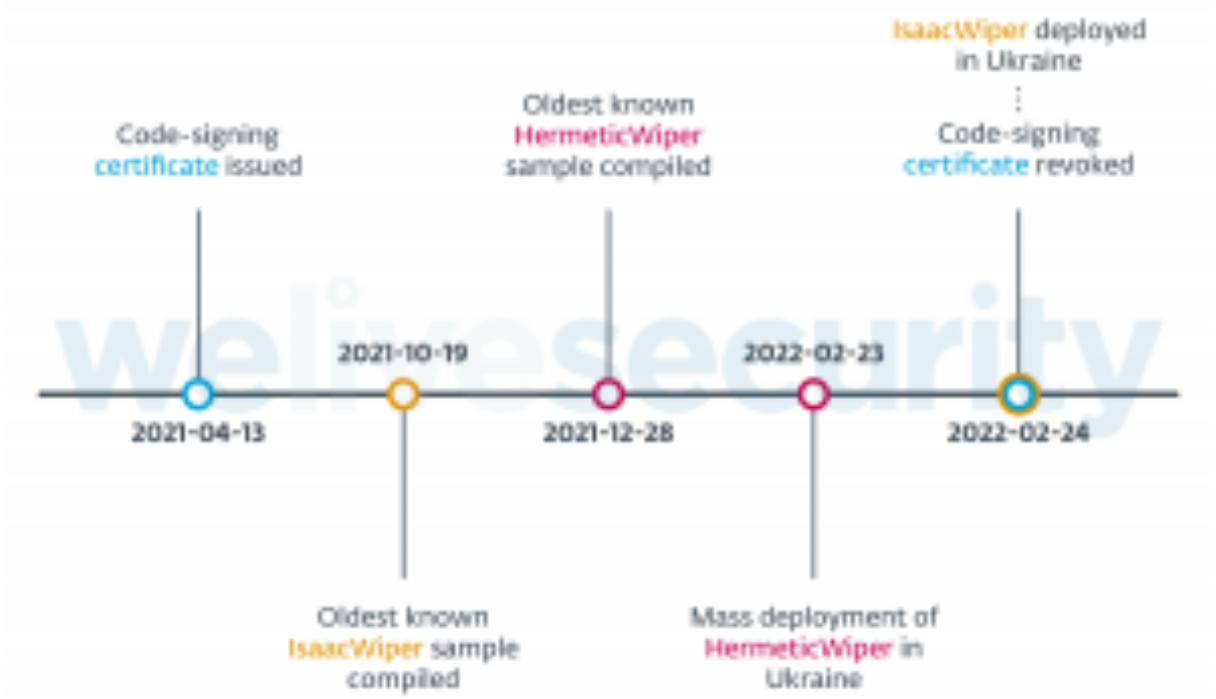


Figure 2. Timeline of important events

Initial access

HermeticWiper

The initial access vector is currently unknown but we have observed artifacts of lateral movement inside the targeted organizations. In one entity, the wiper was deployed through the default domain policy (GPO), as shown by its path on the system:

```
C:\Windows\system32\GroupPolicy\DataStore\0\sysvol\<redacted>\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\cc.exe
```

This indicates that attackers likely took control of the Active Directory server.

In other instances, it is possible that *Impacket* was used to deploy HermeticWiper. A Symantec *blogpost* states that the wiper was deployed using the following command line:

```
cmd.exe /Q /c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1
CSIDL_WINDOWS\policydefinitions\postgresql.exe 1>
\\127.0.0.1\ADMIN$\__1636727589.6007507 2>&1
```

The last part is the same as the default behavior in Impacket's `wmiexec.py`, found on *GitHub*.

Finally, a custom worm that we have named HermeticWizard was used to spread HermeticWiper across the compromised networks via SMB and WMI.

IsaacWiper

The initial access vector is also currently unknown. It is likely that attackers used tools such as Impacket to move laterally. On a few machines, we have also observed *RemCom*, a remote access tool, being deployed at the same time as IsaacWiper.

Technical analysis

HermeticWiper

HermeticWiper is a Windows executable with four drivers embedded in its resources. They are legitimate drivers from the EaseUS Partition Master software signed by `CHENGDU YIWO Tech Development Co.`, and they implement low-level disk operations. The following files were observed:

- `0E84AFF18D42FC691CB1104018F44403C325AD21`: x64 driver
- `379FF9236F0F72963920232F4A0782911A6BD7F7`: x86 driver
- `87BD9404A68035F8D70804A5159A37D1EB0A3568`: x64 XP driver
- `B33DD3EE12F9E6C150C964EA21147BF6B7F7AFA9`: x86 XP driver

Depending on the operating system version, one of those four drivers is chosen and dropped in `C:\Windows\System32\drivers\<4 random letters>.sys`. It is then loaded by creating a service.

HermeticWiper then proceeds by disabling the Volume Shadow Copy Service (VSS) and wipes itself from disk by overwriting its own file with random bytes. This anti-forensic measure is likely intended to prevent the analysis of the wiper in a post-incident analysis.

It is interesting to note that most of the file operations are performed at a low level using `DeviceIoControl` calls.

The following locations are overwritten with random bytes generated by the Windows API function `CryptGenRandom`:

- The master boot record (MBR)
- The master file table (MFT)
- `$Bitmap` and `$LogFile` on all drives
- The files containing the registry keys (`NTUSER*`)
- `C:\Windows\System32\winevt\Logs`

In addition, it also recursively wipes folders and files in `Windows`, `Program Files`, `Program Files (x86)`, `PerfLogs`, `Boot`, `System Volume Information`, and `AppData` folders, using a `FSCTL_MOVE_FILE` operation. This technique appears to be quite unusual and very similar to what is implemented in the *Windows Wipe project on GitHub* (see the `wipe_extent_by_defrag` function). It also wipes symbolic links and big files in `My Documents` and `Desktop` folders by overwriting them with random bytes.

Finally, the machine is restarted. However, it will fail to boot, because the MBR, the MFT, and most files were wiped. We believe it is not possible to recover the impacted machines.

HermeticWizard

Looking for other samples signed by the same code-signing certificate (`Hermetica Digital Ltd`), we found a new malware family that we named HermeticWizard.

It is a worm that was deployed on a system in Ukraine at 14:52:49 on February 23rd, 2022 UTC. It is a DLL file developed in C++ that exports the functions `DllInstall`, `DllRegisterServer`, and `DllUnregisterServer`. Its export DLL name is `Wizard.dll`. It contains three resources, which are encrypted PE files:

- A sample of HermeticWiper (`912342F1C840A42F6B74132F8A7C4FFE7D40FB77`)
- `exec_32.dll`, responsible for spreading to other local computers via WMI (`6B5958BFABFE7C731193ADB96880B225C8505B73`)
- `romance.dll`, responsible for spreading to other local computers via SMB (`AC5B6F16FC5115F0E2327A589246BA00B41439C2`)

The resources are encrypted with a reverse XOR loop. Each block of four bytes is XORed with the previous block. Finally, the first block is XORed with a hardcoded value, `0x4A29B1A3`.

HermeticWizard is started using the command line `regsvr32.exe /s /i <path>`.

First, HermeticWizard tries to find other machines on the local network. It gathers known local IP addresses using the following Windows functions:

- `DNSGetCacheDataTable`
- `GetIpNetTable`
- `WNetOpenEnumW(RESOURCE_GLOBALNET, RESOURCETYPE_ANY)`
- `NetServerEnum`
- `GetTcpTable`
- `GetAdaptersAddresses`

It then tries to connect to those IP addresses (and only if they are local IP addresses) to see if they are still reachable. In case the `-s` argument was provided when HermeticWizard was started (`regsvr32.exe /s /i:-s <path>`), it also scans the full /24 range. So, if `192.168.1.5` was found in, for example, the DNS cache, it incrementally scans from `192.168.1.1` to `192.168.1.254`. For each IP address, it tries to open a TCP connection on the following ports:

- `20: ftp`
- `21: ftp`
- `22: ssh`
- `80: http`
- `135: rpc`

- `137: netbios`
- `139: smb`
- `443: https`
- `445: smb`

The ports are scanned in a random order so it's not possible to fingerprint HermeticWizard traffic that way.

When it has found a reachable machine, it drops the WMI spreader (detailed below) on disk and creates a new process with the command line `rundll32 <current folder>\<6 random letters>.ocx #1 -s <path to HermeticWizard> - i <target IP>`.

It does the same with the SMB spreader (detailed below) that is also dropped in `<current folder>\<6 random letters>.ocx`, but with different random letters.

Finally, it drops HermeticWiper in `<current folder>\<6 random letters>.ocx` and executes it.

WMI spreader

The WMI spreader, named by its developers `exec_32.dll`, takes two arguments:

- `-i`: The target IP address
- `-s`: The file to copy and execute on the target machine

First, it creates a connection to the remote `ADMIN$` share of the target using `WNetAddConnection2W`. The file provided in the `-s` argument is then copied using `CopyFileW`. The remote file has a random name generated with `CoCreateGUID` (e.g., `cB9F06408D8D2.dll`) and the string format `c%02X%02X%02X%02X%02X%02X`.

Second, it tries to execute the copied file, HermeticWizard, on the remote machine using DCOM. It
calls `CoCreateInstance` with `CLSID_WbemLocator` as argument. It then uses WMI `Win32_Process` to create a new process on the remote machine, with the command line `C:\windows\system32\cmd.exe /c start C:\windows\system32\\regsvr32.exe /s /i C:\windows\<filename>.dll`.

Note that the `-s` argument is not passed to HermeticWizard, meaning that it won't scan the local network again from this newly compromised machine.

If the WMI technique fails, it tries to create a service using `OpenRemoteServiceManager` with the same command as above.

If it succeeds in executing the remote DLL in any way, it sleeps until it can delete the remote file.

SMB spreader

The SMB spreader, named by its developers `romance.dll`, takes the same two arguments as the WMI spreader. Its internal name is likely a reference to the EternalRomance exploit, even if it does not use any exploit.

First it attempts to connect to the following pipes on the remote SMB share (on port 445):

- `samr`
- `browser`
- `netlogon`
- `lsarpc`
- `ntsvcs`
- `svcctl`

These are pipes known to be used in lateral movement. The spreader has a list of hardcoded credentials that are used in attempts to authenticate via NTLMSSP to the SMB shares:

```
— usernames —
guest
test
admin
user
root
administrator
manager
operator


— passwords —
123
Qaz123
Qwerty123
```

This list of credentials is surprisingly short and is unlikely to work in even the most poorly protected networks.

If the connection is successful, it attempts to drop, to the target `ADMIN$` share, the file referenced by the `-s` argument. As for the

WMI spreader, the remote filename is generated by a call to `CoCreateInstance`.

It then executes, via SMB, the command line `cmd /c start regsvr32 /s /i ..\\<filename> & start cmd /c \"ping localhost -n 7 & wevtutil cl System\"`.

HermeticRansom

ESET researchers also observed HermeticRansom – ransomware written in Go – being used in Ukraine at the same time as the HermeticWiper campaign. HermeticRansom was first reported in the early hours of February 24th, 2022 UTC, in a *tweet* from AVAST. Our telemetry shows a much smaller deployment compared to HermeticWiper. This ransomware was deployed at the same time as HermeticWiper, potentially in order to hide the wiper's actions. On one machine, the following timeline was observed:

- 2022-02-23 17:49:55 UTC: HermeticWiper in `C:\Windows\Temp\cc.exe` deployed
- 2022-02-23 18:06:57 UTC: HermeticRansom in `C:\Windows\Temp\cc2.exe` deployed by the `netsvcs` service
- 2022-02-23 18:26:07 UTC: Second HermeticWiper in `C:\Users\com.exe` deployed

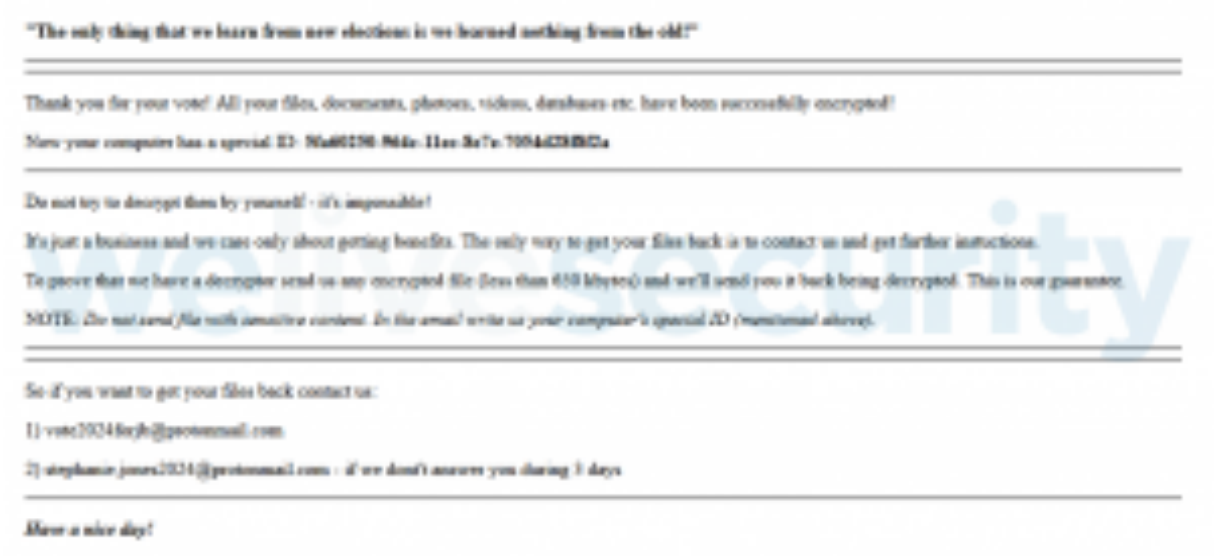
On one occasion, we observed HermeticRansom being deployed through GPO, just like HermeticWiper:

```
C:\WINDOWS\system32\GroupPolicy\DataStore\0\sysvol\<redacted>\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\cpin.exe
```

A few strings were left in the binary by the attackers; they reference US President Biden and the White House:

- `_/C_/projects/403forBiden/wHiteHousE.baggageGatherings`
- `_/C_/projects/403forBiden/wHiteHousE.lookUp`
- `_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess`
- `_/C_/projects/403forBiden/wHiteHousE.GoodOffice1`

Once files are encrypted, the message in Figure 3 is displayed to the victim.


"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID:

Do not try to decrypt them by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instructions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024hrjh@protonmail.com

2) stephanie.jones2024@protonmail.com - if we don't answers you during 3 days

Have a nice day!

Figure 3. HermeticRansom's ransom note

IsaacWiper

IsaacWiper is found in either a Windows DLL or EXE with no Authenticode signature; it appeared in our telemetry on February 24th, 2022. As mentioned earlier, the oldest PE compilation timestamp we have found is October 19th, 2021, meaning that if its PE compilation timestamp was not tampered with, IsaacWiper might have been used in previous operations months earlier.

For DLL samples, the name in the PE export directory is `Cleaner.dll` and it has a single export `_Start@4`.

We have observed IsaacWiper in `%programdata%` and `C:\Windows\System32` under the following filenames:

- `clean.exe`

- `cl.exe`
- `cl64.dll`
- `cld.dll`
- `cll.dll`

It has no code similarity with HermeticWiper and is way less sophisticated. Given the timeline, it is possible that both are related but we haven't found any strong connection yet.

IsaacWiper starts by enumerating the physical drives and calls `DeviceIoControl` with the IOCTL `IOCTL_STORAGE_GET_DEVICE_NUMBER` to get their device numbers. It then wipes the first 0x10000 bytes of each disk using the *ISAAC* pseudorandom generator. The generator is seeded using the `GetTickCount` value.

It then enumerates the logical drives and recursively wipes every file of each disk with random bytes also generated by the ISAAC PRNG. It is interesting to note that it recursively wipes the files in a single thread, meaning that it would take a long time to wipe a large disk.

On February 25th, 2022, attackers dropped a new version of IsaacWiper with debug logs. This may indicate that the attackers were unable to wipe some of the targeted machines and added log messages to understand what was

happening. The logs are stored in `C:\ProgramData\log.txt` and some of the log messages are:

- `getting drives…`
- `start erasing physical drives…`
- `-- start erasing logical drive`
- `start erasing system physical drive…`
- `system physical drive -- FAILED`
- `start erasing system logical drive`

Conclusion

This report details a destructive cyberattack that impacted Ukrainian organizations on February 23rd, 2022, and a second attack that affected a different Ukrainian organization from February 24th through 26th, 2022. At this point, we have no indication that other countries were targeted.

However, due to the current crisis in Ukraine, there is still a risk that the same threat actors will launch further campaigns against countries that back the Ukrainian government or that sanction Russian entities.

A list of IoCs can also be found in our GitHub repository.

IoCs

SHA-1	Filename	ESET detection name	Description
912342F1 C840A42F 6B74132F 8A7C4FFE 7D40FB77	com.exe	Win32/KillDisk.NCV	HermeticWiper
61B25D11 392172E5 87D8DA30 45812A66 C3385451	conhosts.exe	Win32/KillDisk.NCV	HermeticWiper
3C54C9A4 9A8DDCA0 2189FE15 FEA52FE2 4F41A86F	c9EEAF78C9A12.dat	Win32/GenCBL.BSP	HermeticWizard
F32D791E C9E6385A 91B45942 C230F52A FF1626DF	cc2.exe	WinGo/Filecoder.BK	HermeticRansom
AD602039 C6F0237D 4A997D56 40E92CE5 E2B3BBA3	cl64.dll	Win32/KillMBR.NHP	IsaacWiper

SHA-1	Filename	ESET detection name	Description
736A4CFAD1ED83A6A0B75B0474D5E01A3A36F950	cld.dll	Win32/KillMBR.NHQ	IsaacWiper
E9B96E9B86FAD28D950CA428879168E0894D854F	clean.exe	Win32/KillMBR.NHP	IsaacWiper
23873BF2670CF64C2440058130548D4E4DA412DD	XqoYMlBX.exe	Win32/RiskWare.RemoteAdmin.RemoteExec.AC	Legitimate RemCom remote access tool

MITRE ATT&CK techniques

This table was built using *version 10* of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1588.002	Obtain Capabilities: Tool	Attackers used RemCom and potentially Impacket as part of their campaign.

Tactic	ID	Name	Description
	T1588.003	Obtain Capabilities: Code Signing Certificates	Attackers acquired a code-signing certificate for their campaigns.
Initial Access	T1078.002	Valid Accounts: Domain Accounts	Attackers were able to deploy wiper malware through GPO.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Attackers used the command line during their attack (e.g., possible Impacket usage).
	T1106	Native API	Attackers used native APIs in their malware.
	T1569.002	System Services: Service Execution	HermeticWiper uses a driver, loaded as a service, to corrupt data.
	T1047	Windows Management Instrumentation	HermeticWizard attempts to spread to local computers using WMI.
Discovery	T1018	Remote System Discovery	HermeticWizard scans local IP ranges to find local machines.
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	HermeticWizard attempts to spread to local computers using SMB.

Tactic	ID	Name	Description
	T1021.003	Remote Services: Distributed Component Object Model	HermeticWizard attempts to spread to local computers using `WbemLocator` to remotely start a new process via WMI.
Impact	T1561.002	Disk Wipe: Disk Structure Wipe	HermeticWiper corrupts data in the system's MBR and MFT.
	T1561.001	Disk Wipe: Disk Content Wipe	HermeticWiper corrupts files in `Windows`, `Program Files`, `Program Files(x86)`, `PerfLogs`, `Boot`, `System Volume Information`, and `AppData`.
	T1485	Data Destruction	HermeticWiper corrupts user data found on the system.
	T1499.002	Endpoint Denial of Service: Service Exhaustion Flood	By using DDoS attacks, the attackers made a number of government websites unvailable.