# Threat Advisory: HermeticWiper

By Cisco Talos

Published: 2022-02-24 · Archived: 2026-04-05 18:04:07 UTC

Thursday, February 24, 2022 15:00

**This post is also available in:**

日本語 (Japanese)

Українська (Ukrainian)

### Update: March 1, 2022

Cisco Talos is aware of reporting related to additional components discovered to be associated with ongoing HermeticWiper attacks. These additional components include:

- HermeticWizard, which allows HermeticWiper to be propagated to and deployed on additional systems within affected environments. It performs network scanning activities to take an inventory of the environment and propagates the HermeticWiper malware to additional systems via SMB or WMI.
- IsaacWiper, an additional wiper responsible for the destruction of systems and data.
- HermeticRansom, a ransomware family that has been observed being deployed at the same time as HermeticWiper, possibly as a diversionary tactic.

Analysis is currently ongoing to confirm the details included in these reports.

### Update: Feb. 26, 2022

Additional details added to the embedded resources section, specifically around driver usage.

### Update: Feb. 25, 2022

During the additional investigation, Cisco Talos has found that, in some cases, along with HermeticWiper, the adversaries also dropped a legitimate copy of the sysinternals tool sdelete. We are still investigating its potential usage as a failsafe or some other unused mechanism in the attack. We will update as further information becomes available. This hash has been added to the IOC section for reference, along with several others associated with HermeticWiper.

---

Cisco Talos is aware of a second wave of wiper attacks ongoing inside Ukraine, leveraging a new wiper that has been dubbed "HermeticWiper." Deployment of the destructive malware began on Feb. 23, 2022. HermeticWiper features behavioral characteristics similar to what was observed during the WhisperGate attacks that occurred in

January. The malware has two components designed for destruction: one that targets the Master Boot Record (MBR) and another targeting partitions.

## Wiper analysis

The wiper is a relatively small executable — approximately 115KB in size — with a majority of it consisting of embedded resources. This executable is signed with a digital signature issued to "Hermetica Digital Ltd" valid from April 2021 to April 2022.

```
Signers:
   Hermetica Digital Ltd
        Cert Status:    Valid
        Valid Usage:    Code Signing
        Cert Issuer:    DigiCert EV Code Signing CA (SHA2)
        Serial Number:  0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC
        Thumbprint:     1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
        Algorithm:      sha256RSA
        Valid from:     7:00 PM 4/12/2021
        Valid to:       6:59 PM 4/14/2022
   DigiCert EV Code Signing CA (SHA2)
        Cert Status:    Valid
        Valid Usage:    Code Signing
        Cert Issuer:    DigiCert High Assurance EV Root CA
        Serial Number:  03 F1 B4 E1 5F 3A 82 F1 14 96 78 B3 D7 D8 47 5C
        Thumbprint:     60EE3FC53D4BDFD1697AE5BEAE1CAB1C0F3AD4E3
        Algorithm:      sha256RSA
        Valid from:     7:00 AM 4/18/2012
        Valid to:       7:00 AM 4/18/2027
   DigiCert High Assurance EV Root CA
        Cert Status:    Valid
        Valid Usage:    All
        Cert Issuer:    DigiCert High Assurance EV Root CA
        Serial Number:  02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77
        Thumbprint:     5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25
        Algorithm:      sha1RSA
        Valid from:     7:00 PM 11/9/2006
        Valid to:       7:00 PM 11/9/2031
```

Digital certificate on the wiper executables.

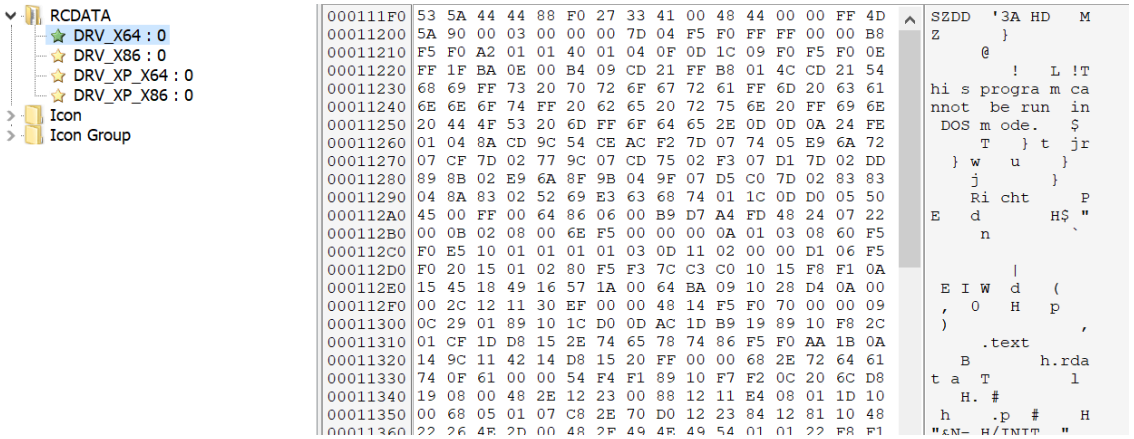
One of the wiper executables was compiled on Feb. 23, 2022 and saw deployment the very same day. While another copy of the wiper was compiled as early as Dec. 28, 2021, indicating that the attackers have been working on developing the wiper for several months.

| | | |
|---|---|---|
| Machine | 14c | Intel 386 |
| Sections Count | 5 | 5 |
| Time Date Stamp | 61caccbc | Tuesday, 28.12.2021 08:37:16 UTC |
| Ptr to Symbol T... | 0 | 0 |
| Num. of Symbols | 0 | 0 |
| Size of Optional... | e0 | 224 |

Compilation timestamp of one of the earliest known HermeticWiper samples.

## Embedded Resources

Hermetic wiper consists of four embedded resources. These resources are compressed copies of drivers used by the wiper.

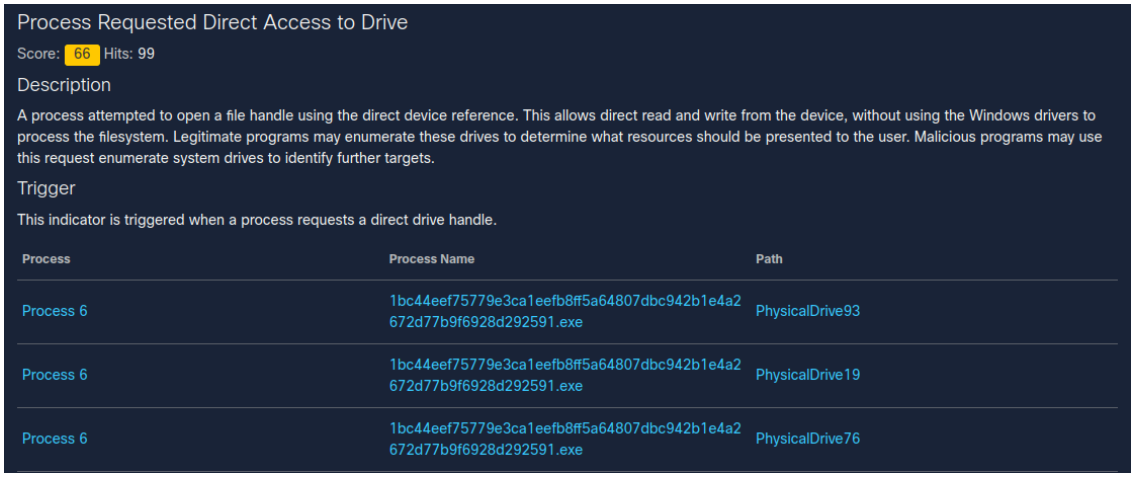



These resources are drivers associated with the legitimate program, [EaseUS Partition Master], which the malware leverages to interact with storage devices present on infected systems. The use of legitimate drivers to facilitate direct interaction with storage devices is consistent with wiper malware previously observed over the past several years.

One of the advantages of using a driver as opposed to traditional mechanisms is the ability to leverage input/output controls or IOCTLs. The use of IOCTLs allows for deeper, direct access to underlying operating system and file system components and attributes, and is typically reserved for device drivers. Detection is commonly built on the usage of Windows native APIs and in this particular instance allows for the wiper to conduct its destructive actions leveraging the IOCTLs provided by the EaseUS Partition Master driver, potentially evading detection and prevention of the destructive actions. For instance these techniques could defeat detections looking for disk writes to certain sectors, including partition tables.

The IOCTLs leveraged by the wiper are:

- IOCTL_STORAGE_GET_DEVICE_NUMBER
- IOCTL_DISK_GET_DRIVE_GEOMETRY_EX
- IOCTL_DISK_GET_DRIVE_LAYOUT_EX
- IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS
- FSCTL_GET_RETRIEVAL_POINTERS
- FSCTL_GET_VOLUME_BITMAP
- FSCTL_LOCK_VOLUME
- FSCTL_DISMOUNT_VOLUME
- FSCTL_MOVE_FILE
- FSCTL_GET_NTFS_FILE_RECORD
- FSCTL_GET_NTFS_VOLUME_DATA




### Wiper process

The wiper process begins by assigning itself two privileges:

- SeShutDownPrivilege: To shut down the endpoint once it's been wiped.
- SeBackupPrivilege: This privilege allows for file content retrieval for files whose security descriptor does not grant such access.

Depending on the version of the Windows operating system running on the infected system, the wiper will then begin extracting the applicable embedded driver. The driver is loaded into the wiper's process memory space, decompressed and written to disk at "C:\Windows\System32\drivers\<4_random_characters>.sys".

Before beginning the wipe process, the wiper will also disable generation of crash dumps via HKLM\SYSTEM\CurrentControlSet\Control\CrashControl | CrashDumpEnabled = 0x0

```
lea     eax, [ebp+phkResult]
mov     [ebp+phkResult], 0
push    eax             ; phkResult
push    offset SubKey   ; "SYSTEM\\CurrentControlSet\\Control\\Cra"...
push    HKEY_LOCAL_MACHINE ; hKey
call    ds:RegOpenKeyW
test    eax, eax
jnz     short loc_3E2BB4
push    4               ; cbData
mov     dword ptr [ebp+Data], eax
lea     eax, [ebp+Data]
push    eax             ; lpData
push    4               ; dwType
push    0               ; Reserved
push    offset ValueName ; "CrashDumpEnabled"
push    [ebp+phkResult] ; hKey
call    ds:RegSetValueExW ; disable crash dump collection = 0x0
push    [ebp+phkResult] ; hKey
call    ds:RegCloseKey
```

Disabling crash dump generation.

For each physical device on the system ranging 0 to 100, the wiper starts the process of enumerating the physical drives on the system. After identifying the physical drives, it corrupts the first 512 bytes to destroy the MBR.

```
push    ecx
push    offset pszFmt   ; "\\\\.\\PhysicalDrive%u"
xorps   xmm0, xmm0
mov     [ebp+var_1C], edx
lea     eax, [ebp+pszDest]
mov     [ebp+var_10], 0
push    104h            ; cchDest
xor     esi, esi
movq    [ebp+var_24], xmm0
xor     edi, edi
mov     [ebp+BytesReturned], esi
push    eax             ; pszDest
movups  [ebp+var_44], xmm0
mov     [ebp+var_18], edi
movups  xmmword ptr [ebp+dwBytes], xmm0
call    ds:wnsprintfW
add     esp, 10h
lea     eax, [ebp+var_50]
lea     edx, [ebp+var_44]
lea     ecx, [ebp+pszDest] ; lpFileName
push    eax             ; int
call    get_device_number
mov     ebx, eax
cmp     ebx, 0FFFFFFFFh
jz      loc_A91F73
test    ebx, ebx
jz      loc_A91FA8
mov     edi, 24C0h
push    edi             ; dwBytes
push    8               ; dwFlags
call    ds:GetProcessHeap
push    eax             ; hHeap
call    ds:HeapAlloc
push    0               ; lpOverlapped
mov     esi, eax
lea     eax, [ebp+BytesReturned]
push    eax             ; lpBytesReturned
push    edi             ; nOutBufferSize
push    esi             ; lpOutBuffer
push    0               ; nInBufferSize
push    0               ; lpInBuffer
push    70050h          ; dwIoControlCode
push    ebx             ; hDevice
call    ds:DeviceIoControl
```

Physical drive enumeration.

At this point, it turns its attention to partitions and begins enumerating the individual partitions. First, the wiper disables the Volume Shadow Copy Service (VSS). The wiper then uses different destructive mechanisms on the partitions depending on the type: FAT or NTFS. In both cases, the partitions are corrupted, causing additional damage. This ensures that systems with both MBR and GPT drives are affected, similar to how WhisperKill operated.

The wiper will also attempt to corrupt housekeeping files such as $LOGFILE and $BITMAP for NTFS along with streams such as $INDEX_ALLOCATION, $DATA etc.

The final stage of the wiper consists of waiting for all sleeping threads to complete and initiating a reboot, ensuring the wiping activity is complete.

## Coverage

Ways our customers can detect and block this threat are listed below.

| Product | Protection |
| --- | --- |
| Cisco Secure Endpoint (AMP for Endpoints) | ✓ |
| Cloudlock | N/A |
| Cisco Secure Email | ✓ |
| Cisco Secure Firewall/Secure IPS (Network Security) | ✓ |
| Cisco Secure Malware Analytics (Threat Grid) | ✓ |
| Umbrella | ✓ |
| Cisco Secure Web Appliance (Web Security Appliance) | N/A |

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here. For an in-depth look at Cisco Secure Endpoint and HermeticWiper see here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Malware Analytics (formerly Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Firepower Threat Defense (FTD), Firepower Device Manager (FDM), Threat Defense Virtual, Adaptive Security Appliance can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

For guidance on using Cisco Secure Analytics to respond to this threat, please click here.

Meraki MX appliances can detect malicious activity associated with this threat.

Umbrella, Secure Internet Gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

**Orbital Queries**

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here and here.

Snort SIDs: **59099-59100**

The following ClamAV signatures available for protection against this threat:

- Win.RedTrixx.Wiper.tii.Hunt

Umbrella SIG customers will be protected from this threat if configured to leverage IPS or Malware Analytics capabilities.

## IOCs

### Wiper EXEs

0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767

### Sysinternals SDelete

49E0BA14923DA608ABCAE04A9A56B0689FE6F5AC6BDF0439A46CE35990AC53EE

### EaseUS Partition Master drivers

b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d

---