Disruptive HermeticWiper Attacks Targeting Ukrainian Organizations

secureworks.com/blog/disruptive-hermeticwiper-attacks-targeting-ukrainian-organizations

Counter Threat Unit Research Team

Prior to the Russian military invasion, Ukrainian government and financial organizations were impacted by distributed denial of service and wiper attacks. Friday, February 25, 2022 *By: Counter Threat Unit Research Team*

Secureworks® Counter Threat Unit™ (CTU) researchers are investigating reports of disruptive activity that began targeting organizations in Ukraine on February 23, 2022. This activity mirrors attacks that occurred on January 13 and 14, 2022. Distributed denial of service (DDoS) attacks on February 23 reportedly caused intermittent loss of access to government websites belonging to the Ukrainian Ministry of Foreign Affairs, Ministry of Defense, Security Service, Ministry of Internal Affairs, and Cabinet of Ministers. PrivatBank and Oschadbank, which were targeted in DDoS attacks on February 15, were again subjected to DDoS activity on February 23.

At approximately the same time as the DDoS attacks, threat actors deployed a novel wiper to a small number of government and financial organizations in Ukraine. An antivirus vendor observed the first samples in its telemetry at 14:52 UTC (16:52 local time in Ukraine). These disruptive events preceded the February 24 Russian military invasion of Ukraine. The wiper's primary function is data destruction.

The wiper has been dubbed HermeticWiper based on the "Hermetica Digital Ltd" company name used in the malware's signing certificate (see Figure 1). It is unclear how the threat actors obtained this certificate.

```
Hermetica Digital Ltd
Name    Hermetica Digital Ltd
Status  Valid
Issuer  DigiCert EV Code Signing CA (SHA2)
Valid From  12:00 AM 04/13/2021
Valid To    11:59 PM 04/14/2022
Valid Usage Code Signing
Algorithm   sha256RSA
Thumbprint  1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
Serial Number   0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC
```

Figure 1. HermeticWiper signed with valid 'Hermetic Digital Ltd' code-signing certificate. (Source: Secureworks)

HermeticWiper abuses a legitimate EaseUS partition management driver. This approach is similar to the Iranian Shamoon and North Korean DarkSeoul wipers, which abused the EIDos Raw Disk driver to obtain access to low-level disk functions.

Before starting the EaseUS driver, HermeticWiper modifies several registry keys. One modification disables crash dumps by setting HKLM\SYSTEM\ControlSet001\Control\CrashControl\CrashDumpEnabled to 0. This change is likely to reduce forensic artifacts if the malware causes the system to stop unexpectedly.

HermeticWiper deploys a signed driver with the internal filename empntdrv.sys to the infected system. This benign driver is signed by a certificate issued to CHENG DU YIWO Tech Development Co., Ltd. (see Figure 2). This Chinese company develops the EaseUS Partition Master software and specializes in data backup and security.

```
Name    CHENGDU YIWO Tech Development Co., Ltd.
Status  This certificate or one of the certificates in the certificate chain is not time valid.
Issuer  VeriSign Class 3 Code Signing 2010 CA
Valid From  12:00 AM 04/23/2012
Valid To    11:59 PM 09/11/2014
Valid Usage Code Signing
Algorithm   sha1RSA
Thumbprint  9AC3C64696772A86BCE7EB308025358F4DD08A24
Serial Number   33 C3 4C CA 6E 68 16 B6 2B 67 7D 44 B0 68 35 E5
```

Figure 2. Legitimate signed driver deployed by HermeticWiper. (Source: Secureworks)

The malware contains driver copies for multiple operating system versions and architecture as ms-compressed resources. Most of the 114KB HermeticWiper binary is consumed by these resource files. The malware deploys the appropriate driver depending on the system being infected.

HermeticWiper installs the EaseUS driver using a four-character filename. This filename is generated using the current process ID, which results in a pseudorandom string (e.g., C:\Windows\sysnative\drivers\njdr.sys). The malware disables the volume shadow copy service to hinder recovery attempts. This tactic is commonly used by ransomware developers.

HermeticWiper corrupts the master boot record (MBR), overwrites files in specific system locations, and modifies partition information. To corrupt the MBR, it enumerates each of the physical disks, iterating through \??\PhysicalDrive0 to \??\PhysicalDrive100, and then overwrites the first 512 bytes. These bytes contain the MBR.

The malware uses the EaseUS driver to perform destructive operations, opening a handle to the physical disk before overwriting it with randomly generated data. The handle is obtained via \\EPMNTDRV\%u, where %u is replaced with the physical disk number. SetFilePointerEx is then used to locate the data to be overwritten, and WriteFile is used to overwrite the content with randomly generated data (see Figure 3).

```
wnsprintfW(pszDest, 260, L"\\\\.\\EPMNTDRV\\%u", drive_number_1);
device_number = ioctl_device_number(pszDest, (int)v14, 0);
v4 = (void *)device_number;
if ( !device_number || device_number == -1 )
  goto LABEL_15;
random_data = lpThreadParameter->random_data;
LODWORD(nNumberOfBytesToWrite) = lpThreadParameter->data_size;
do
{
  v5 = v2[2];
  v6 = v2[3];
  v7 = __PAIR64__(v6, v5) + *((_QWORD *)v2 + 2);
  HIDWORD(nNumberOfBytesToWrite) = v6;
  if ( __SPAIR64__(v6, v5) < v7 )
  {
    do
    {
      NumberOfBytesWritten = 0;
      if ( !SetFilePointerEx(v4, (LARGE_INTEGER)__PAIR64__(v6, v5), 0, 0) )
        GetLastError();
      if ( !WriteFile(v4, random_data, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0) )
        GetLastError();
      v6 = (nNumberOfBytesToWrite + (unsigned __int64)(unsigned int)v5) >> 32;
      v5 += nNumberOfBytesToWrite;
      v8 = *((_QWORD *)v2 + 1) + *((_QWORD *)v2 + 2);
      HIDWORD(nNumberOfBytesToWrite) = v6;
    }
```

Figure 3. HermeticWiper routine overwrites data. (Source: Secureworks)

The malware also overwrites files under the following paths:

- C:\Documents and Settings\
- C:\System Volume Information\
- C:\Windows\SYSVOL\
- C:\Windows\System32\winevt\Logs

Finally, it determines if the partition's file system is File Allocation Table (FAT) or New Technology File System (NTFS) and attempts to corrupt the partition using a method appropriate for that type. Once execution is complete, the system is forced to shut down.

HermeticWiper generates random data to overwrite files and partition tables (e.g., the MBR) but does not appear to encrypt files. Unlike WhisperGate, HermeticWiper does not attempt to masquerade as ransomware and does not display a fake ransom note when the system is booted. CTU™ analysis did not reveal a network-based command and control (C2) or propagation mechanism within the binary.

While the DDoS and wiper attacks were being conducted, additional disruptive cyber activity was occurring in Ukraine. On February 23, CTU researchers observed website defacements affecting at least 13 Ukrainian government entities, most of them under Ukraine's Ministry of Social Policy. The defacement image is nearly identical to the ransomware-like image used during the January 14 attacks impacting a range of Ukrainian government sites. Both images include anti-Ukrainian icons, warn readers of data destruction, and describe leaks of

personal data (see Figure 4). Unlike the January defacement image, the February image file does not contain geolocation or timestamp metadata that CTU researchers believe were false flags intended to confuse attribution.

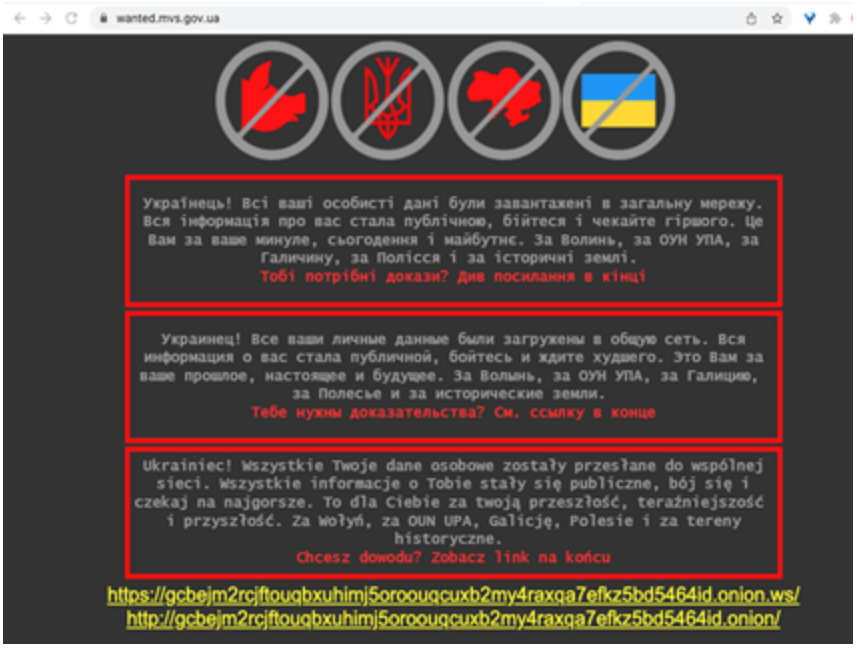

Figure 4. February 23 defacement closely resembles January 14 image. (Source: Secureworks)

The February 23 image includes links to a Tor site operated by "Free Civilian," a group offering to sell sets of stolen personal data belonging to Ukrainian citizens (see Figure 5). CTU researchers are unable to confirm if this group possesses citizens' data or if any sales have occurred. The "*NEW* New leaks" section of the Free Civilian site lists fifty Ukrainian government websites from which confidential data has purportedly been taken and will be published. On February 23, thirteen of the sites in the list displayed the latest defacement image. As of February 24, only one website was still defaced.

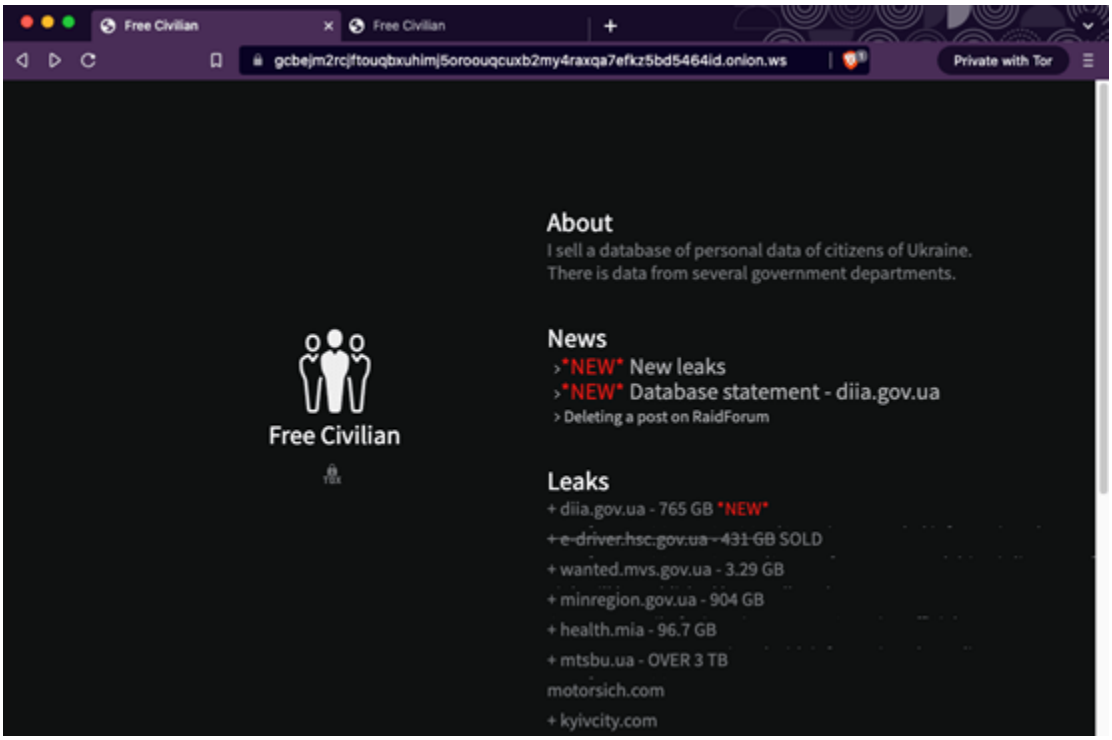

Figure 5. 'Free Civilian' Tor site claiming leaks of Ukrainian citizens' personal data. (Source: Secureworks)

A "FreeCivilian" account created on the RaidForums underground forum in late January claimed to have a database of sensitive personal information for over two million Ukrainian citizens. This list was purportedly obtained from the Ministry of Digital Transformation of Ukraine (DIIA), a government portal that handles passports, driver's licenses, and military cards. The Tox messaging ID in that post and on the "Free Civilian" website are identical. Ukrainian officials dismissed FreeCivilian's claim as a scam designed to undermine trust in the Ukrainian government. The "FreeCivilian" RaidForums account has since been banned.

On February 18, the Computer Emergency Response Team of Ukraine (CERT-UA) warned of possible cyberattacks on February 22 based on threats posted to RaidForums by another persona named "Carzita." As of this publication, it is unclear if the Carzita and FreeCivilian RaidForums accounts are associated. However, it is likely that the February website defacements and threats of data leaks were intended to cause panic and coincide with the DDoS and wiper attacks.

CTU researchers do not expect widespread repeated use of HermeticWiper outside of Ukraine. However, due to the invasion of Ukraine by Russian forces on February 24, cyberattacks will likely continue to play a significant supporting role to conventional military attacks.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1.

Indicator	Type	Context

Indicator	Type	Context
84ba0197920fd3e2b7dfa719fee09d2f	MD5 hash	HermeticWiper malware
912342f1c840a42f6b74132f8a7c4ffe7d40fb77	SHA1 hash	HermeticWiper malware
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	SHA256 hash	HermeticWiper malware
3f4a16b29f2f0532b7ce3e7656799125	MD5 hash	HermeticWiper malware
61b25d11392172e587d8da3045812a66c3385451	SHA1 hash	HermeticWiper malware
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	SHA256 hash	HermeticWiper malware

Table 1. Indicators for this threat.