Threat Thursday: HermeticWiper Targets Defense Sectors in Ukraine

blogs.blackberry.com/en/2022/03/threat-thursday-hermeticwiper

The BlackBerry Research & Intelligence Team

New Disk Wiper Malware Hits Hundreds of Ukrainian Computers

In addition to suffering a full-scale military invasion in recent weeks, Ukraine is also being subjected to numerous cyberattacks aimed at crippling its organizations and digital infrastructure. One of the latest of these is HermeticWiper, a new data wiper malware that targets infrastructure and defense sectors in Ukraine, with additional reports of compromised systems coming from Lithuania and Latvia.

HermeticWiper shares some similarities with the recently discovered WhisperGate malware, in that it appears to function solely as a tool for destruction. After wiping the victim's disk, it then targets the Master Boot Record (MBR) before forcing a reboot, resulting in a total boot failure and rendering the system inoperable.

First reported in a tweet by ESET Research on February 23rd, 2022, the threat intelligence community subsequently named the new malware HermeticWiper, a reference to two of its main activities. The wiper first hijacks a valid code-signing certificate from Hermetica Digital

Ltd. to gain the victim's trust. It then uses a legitimate disk recovery program from EaseUS Data Recovery Wizard, packed by the threat authors as a driver, to overwrite data in the victim's Master Boot Record (MBR) and thus corrupt the file system.

A decoy ransomware component has also been reported on some systems affected by HermeticWiper, to distract the victim while the main functionality occurs.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	High
Risk	Low

Technical Analysis

Wiper Overview

In this blog, BlackBerry researchers will analyze a sample hash of HermeticWiper, to see what lies under the hood.

Sample hash:
0385EEAB00E946A302B24A91DEA4187C1210597B8E17CD9E2230450F5ECE21DA

The file presents itself as "conhost.exe," borrowing the filename of the Console Windows Host for Microsoft® Windows®. The executable file uses a standard Visual Studio Project icon, as seen in Figure 1, and displays the Hermetica certificate shown in Figure 2. This inclusion of a valid certificate helps the wiper to evade detection on the system by appearing to come from a legitimate and trusted source.

Figure 1 – Program icon

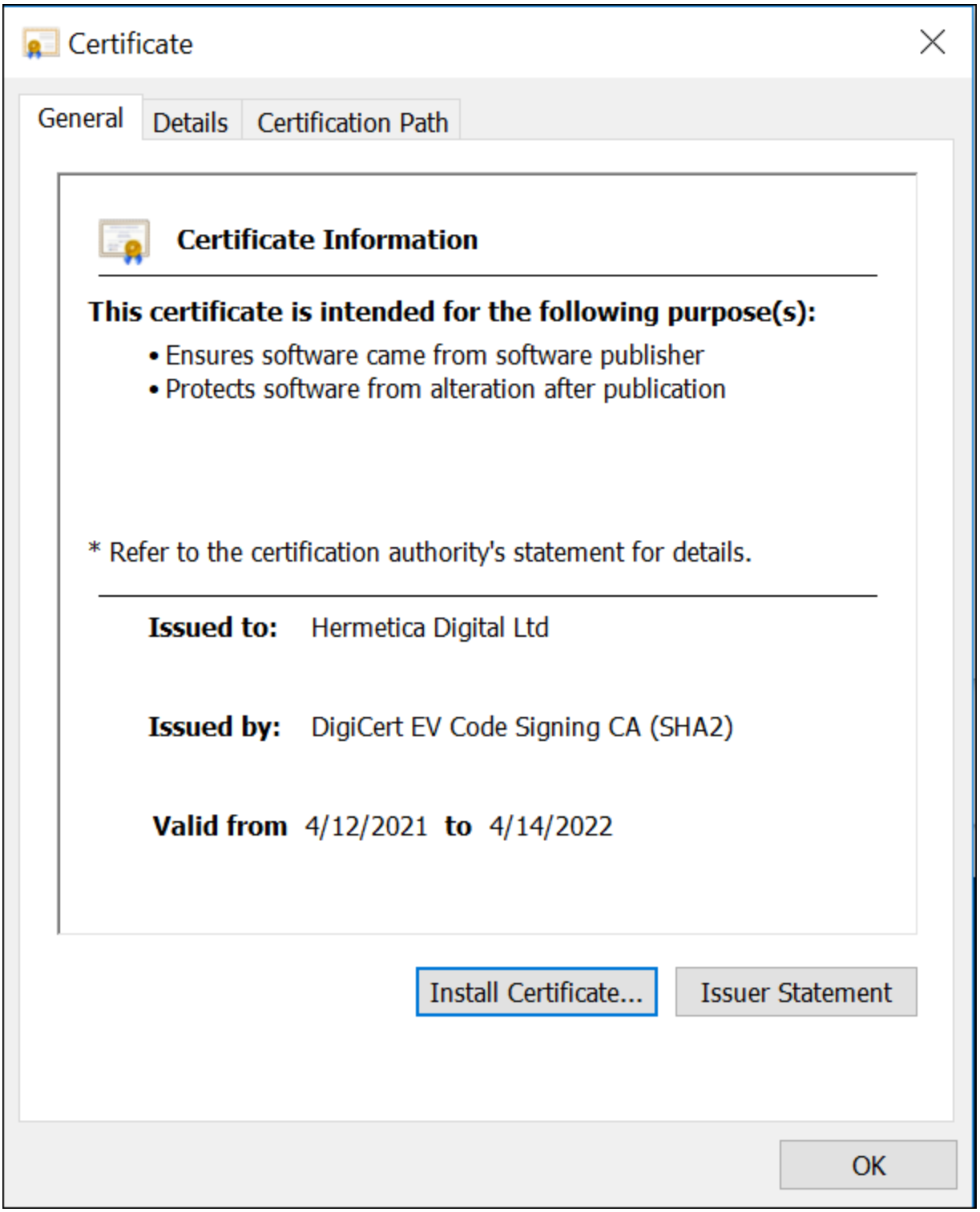

Figure 2 – Hermetica certificate

A brief look into the file shows there are four drivers packaged inside. These drivers are named DRV_X64, DRV_X86, DRV_XP_X64, and DRV_XP_X86, with each having “SZDD” as the first few bytes of the file, as seen in Figure 3. This indicates that the drivers are compressed with the built-in MS-DOS “compress.exe.”

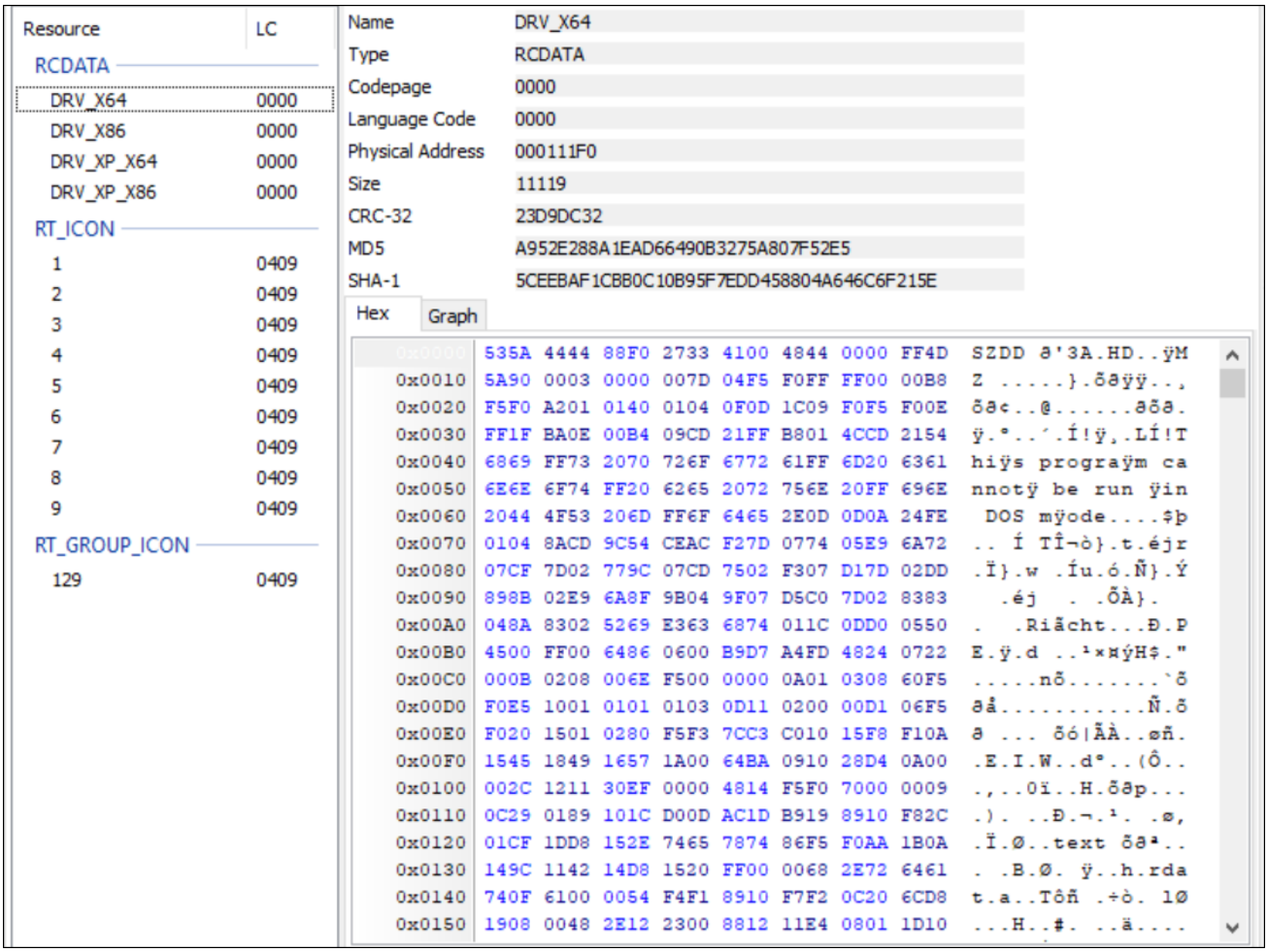

Figure 3 – Compressed drivers

Once each driver has been extracted and saved as their own file on the victim's system, an unzipping program such as 7-Zip can be used to decompress the files and reveal what they really are. An expired certificate shown in Figure 4 for CHENGDU YIWO Tech Development Co. Ltd. can be found in each driver. A quick Internet search links this certificate to a disk recovery software program called EaseUS Data Recovery Wizard.

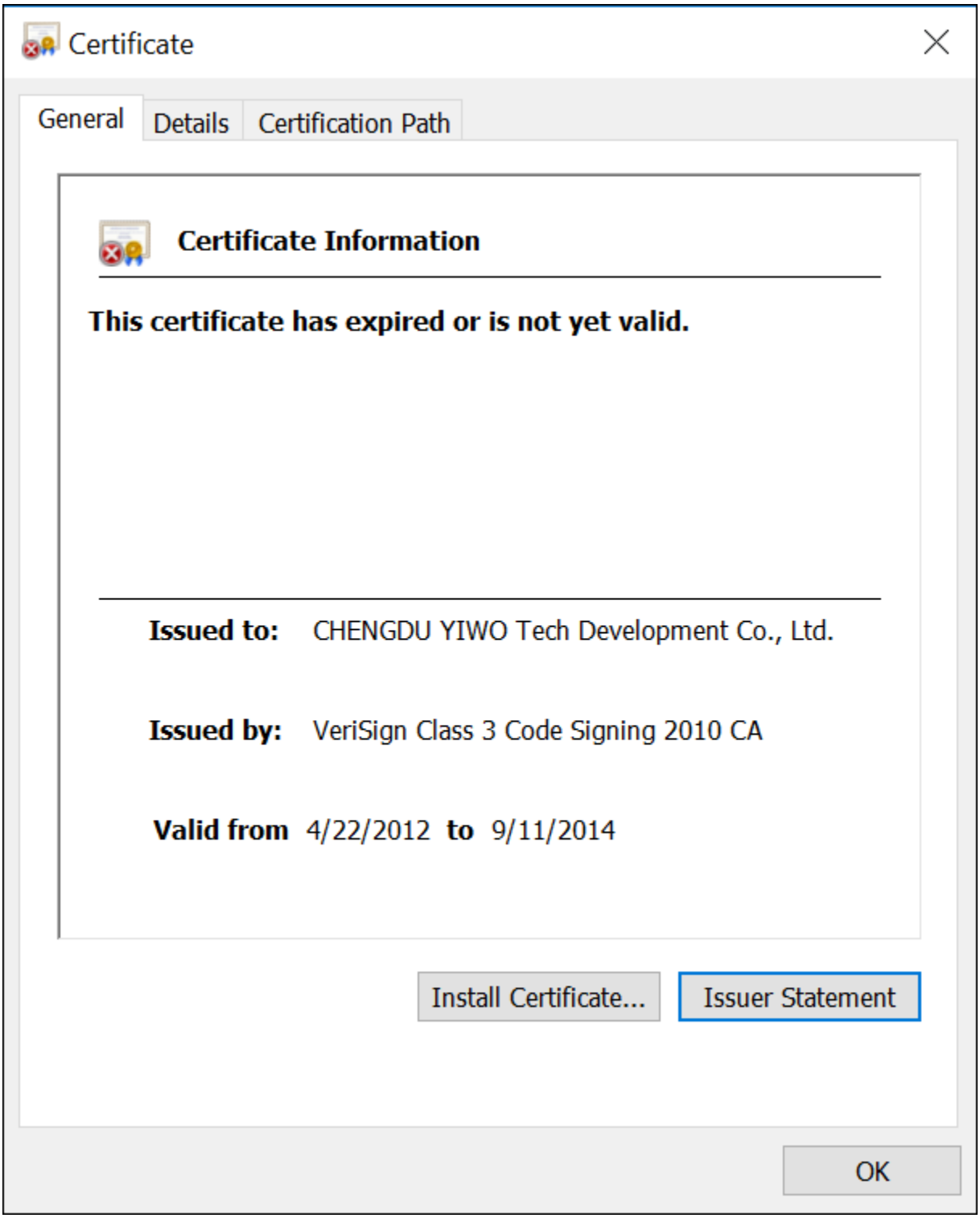

Figure 4 – CHENGDU YIWO Tech Development certificate

Wiper Behavior

The files must be launched as Administrator for the wiper to execute. And for the system reboot to be triggered, the first character of the file name must be C.

Immediately after launch, a new service with a four-character randomized name starts to run, as seen in Figure 5.

Figure 5 – Service starts with random four-character name

By using a hex editor like HxD before and after launching, you can reveal the damage that HermeticWiper is causing to the C:\ disk. Before execution, you can see the standard 52 90 4E 54 46 53 20 bytes (shown in Figure 6) that represent the start of an NTFS formatted drive. After HermeticWiper begins to run, the threat corrupts those bytes, as you can see in Figure 7. The malicious wiper will continue to change these values as it completes its execution.

```
000000000  EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 00 00 00 00 00 F8 00 00  ëR.NTFS    .........ø..
000000018  3F 00 FF 00 00 30 11 00 00 00 00 00 80 00 80 00 FF C7 6E 07 00 00 00 00  ?.ÿ..0......€.€.ÿÇn.....
000000030  00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00 F6 00 00 00 01 00 00 00  ................ö.......
000000048  79 89 A3 1E B6 A3 1E 1A 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  y‰£.¶£......ú3ÀŽÐ¼.|ûhÀ.
000000060  1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E 54 46 53 75 15 B4 41 BB  ..hf.Ëˆ...f.>..NTFSu.´A»
000000078  AA 55 CD 13 72 0C 81 FB 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  ªUÍ.r..ûUªu.÷Á..u.éÝ..ƒì
000000090  18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13 9F 83 C4 18 9E 58 1F 72  .h..´HŠ...‹ô..Í.Ÿƒ Ä.žX.r
0000000A8  E1 3B 06 0B 00 75 DB A3 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  á;...uÛ£..Á.....Z3Û¹. +È
0000000C0  66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 4B 00 2B C8 77 EF B8 00  fÿ.......ŽÂÿ...èK.+Èwï¸.
0000000D8  BB CD 1A 66 23 C0 75 2D 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  »Í.f#Àu-f.ûTCPAu$.ù..r..
0000000F0  68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66 55 16 16 16 68 B8 01 66  h.».hR..h..fSfSfU...h¸.f
000000108  61 0E 07 CD 1A 33 C0 BF 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E  a..Í.3À¿..¹ö.üóªéþ...f`.
000000120  06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00 00 66 50 06 53 68 01 00  .f¡..f.....fh....fP.Sh..
000000138  68 10 00 B4 42 8A 16 0E 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F  h..´BŠ.....‹ôÍ.fY[ZfYfY.
000000150  0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF 0E 16 00 75 BC 07 1F 66  .‚..fÿ.......ŽÂÿ...u¼..f
000000168  61 C3 A1 F6 01 E8 09 00 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09  aÃ¡ö.è..¡ú.è..ôëý‹ð¬<.t.
000000180  B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64 20  ´.»..Í.ëòÃ..A disk read
000000198  65 72 72 6F 72 20 6F 63 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52  error occurred...BOOTMGR
0000001B0  20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73 20 43   is compressed...Press C
0000001C8  74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A  trl+Alt+Del to restart..
0000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8A 01  ......................Š.
0000001F8  A7 01 BF 01 00 00 55 AA 07 00 42 00 4F 00 4F 00 54 00 4D 00 47 00 52 00  §.¿...Uª..B.O.O.T.M.G.R.
000000210  04 00 24 00 49 00 33 00 30 00 00 D4 00 00 00 24 00 00 00 00 00 00 00 00  ..$.I.3.0..Ô...$........
000000228  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000000240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E9 C0  ......................éÀ
000000258  00 90 05 00 4E 00 54 00 4C 00 44 00 52 00 07 00 42 00 4F 00 4F 00 54 00  ....N.T.L.D.R...B.O.O.T.
000000270  54 00 47 00 54 00 07 00 42 00 4F 00 4F 00 54 00 4E 00 58 00 54 00 00 00  T.G.T...B.O.O.T.N.X.T...
000000288  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 41 6E 20 6F  ..................An o
0000002A0  70 65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 20 77 61 73 6E 27 74 20 66  perating system wasn't f
```

Figure 6 – C:\ drive before HermeticWiper runs

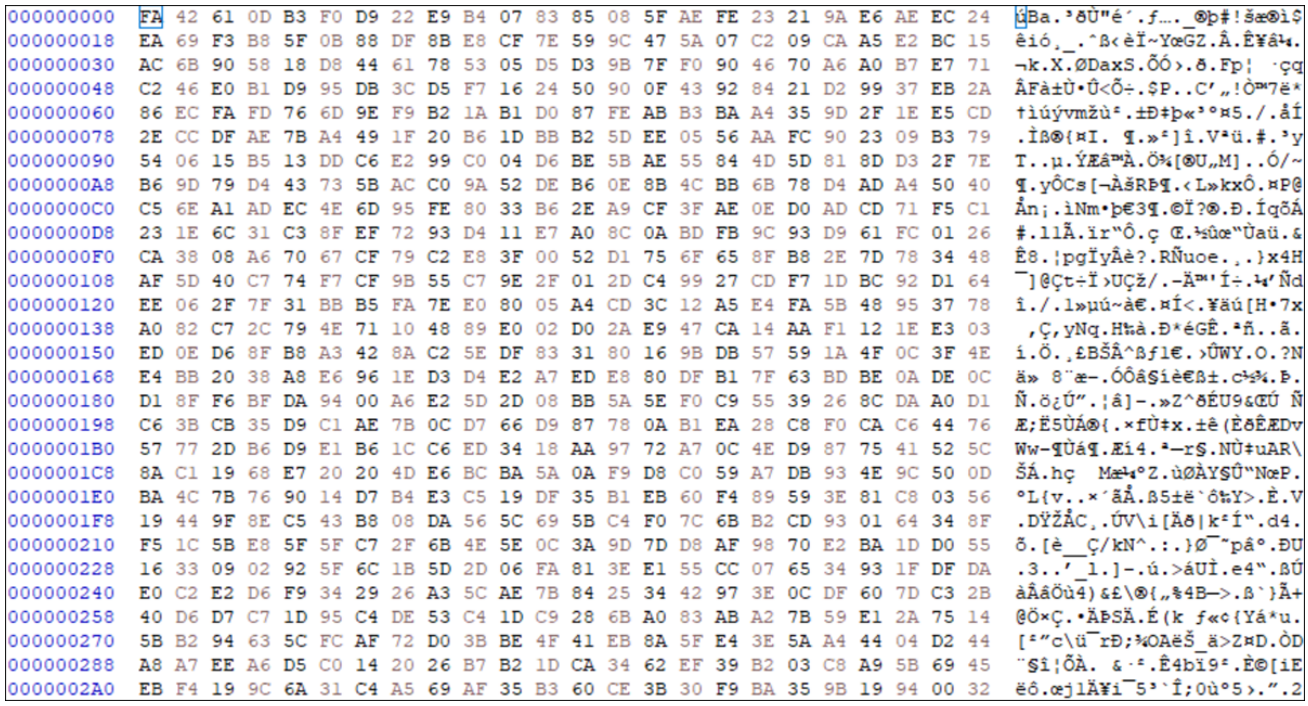

Figure 7 – C:\ drive after HermeticWiper runs

When HermeticWiper has finished corrupting the C:\ drive, the malware restarts the affected system, which results in the dreaded Blue Screen of Death (BSOD). After attempting to restart again, the victim will be greeted with a new message indicating that their operating system is missing, as shown in Figure 8. The C:\ drive is now wiped, and the system is inoperable.

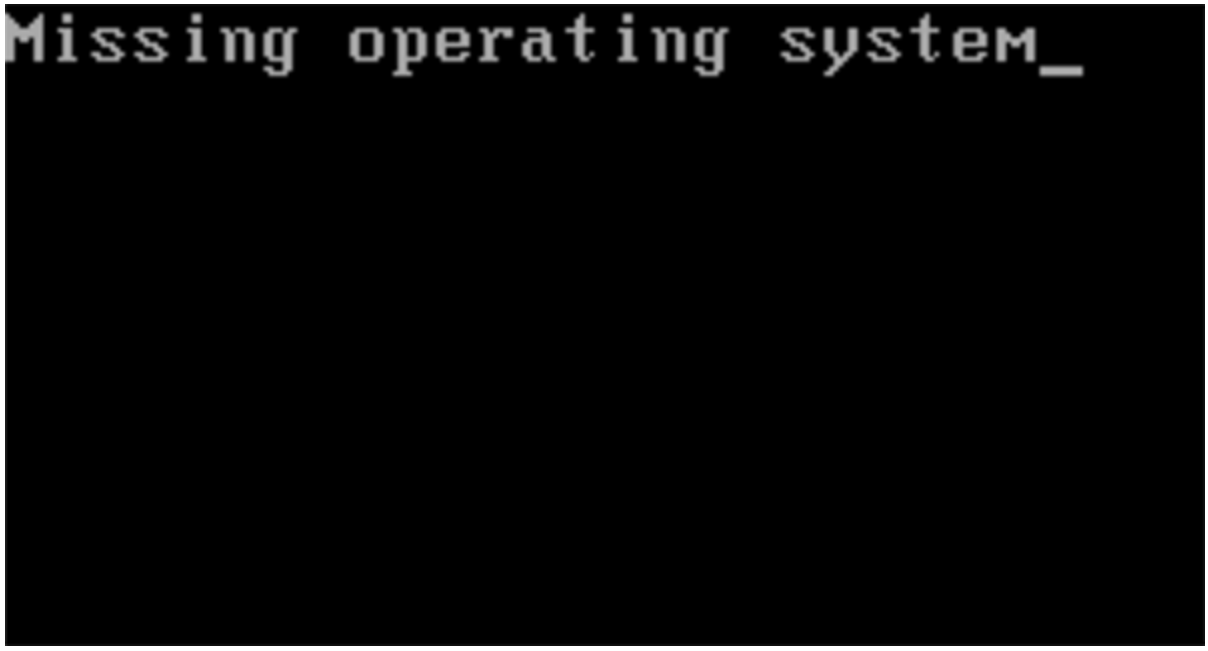

Figure 8 – The last thing any user wants to see upon reboot

Load Driver and Wipe Disk

Taking a step back, let's take a look at the EaseUS Data Recovery Wizard. This is loaded by the malware as a compressed driver. The wiper contains four copies of this driver, with each corresponding to different OS versions (Windows XP or Windows 7+) and architectures (32-bit or 64-bit). As shown in Figure 9, system information first needs to be loaded by the wiper so it can then choose to start the correct driver version.

Figure 9 – Driver selection by HermeticWiper

Once the OS is identified by the malware, the corresponding compressed driver is loaded.

- DRV_X64 – Windows 7+ 64-bit
- DRV_X86 – Windows 7+ 32-bit
- DRV_XP_X64 – Windows XP 64-bit

- DRV_XP_X86 – Windows XP 32-bit

HermeticWiper then decompresses the drivers with the LZMA algorithm. It uses “DeviceIoControl” for file operations such as finding the PhysicalDriveID to get information on the victim’s disk partitions, as shown in Figure 10.

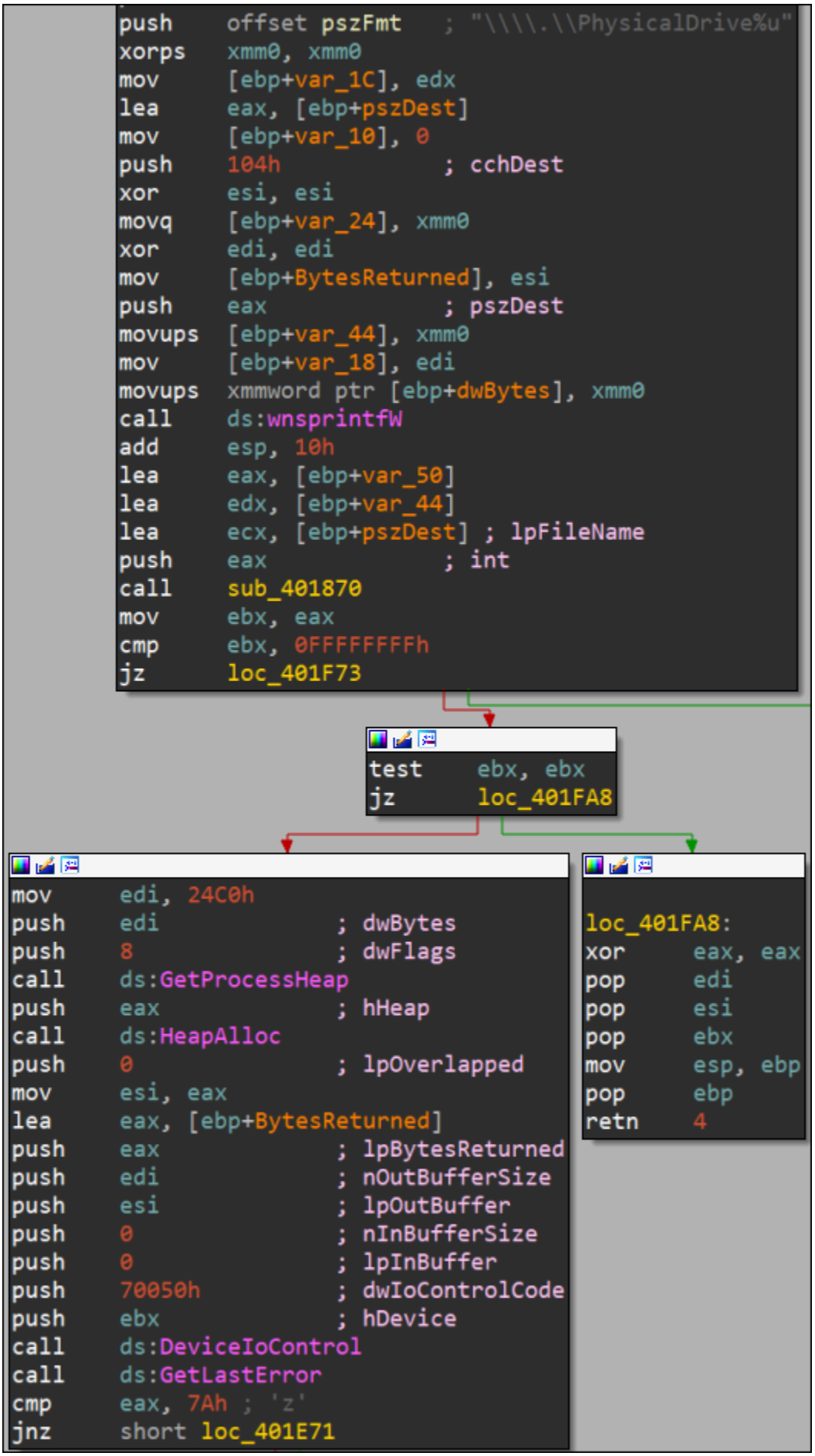
push offset pszFmt ; "\\\\.\\PhysicalDrive%u"
xorps xmm0, xmm0
mov [ebp+var_1C], edx
lea eax, [ebp+pszDest]
mov [ebp+var_10], 0
push 104h ; cchDest
xor esi, esi
movq [ebp+var_24], xmm0
xor edi, edi
mov [ebp+BytesReturned], esi
push eax ; pszDest
movups [ebp+var_44], xmm0
mov [ebp+var_18], edi
movups 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 sub_401870
mov ebx, eax
cmp ebx, 0FFFFFFFFh
jz loc_401F73
test ebx, ebx
jz loc_401FA8
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
call ds:GetLastError
cmp eax, 7Ah ; 'z'
jnz short loc_401E71
loc_401FA8:
xor eax, eax
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
retn 4

Figure 10 – Find PhysicalDriveID

With the drive information loaded, the CryptGenRandom function then begins to overwrite data in the Master File Table fields, $Bitmap and $LogFile files, recursively in the AppData, MyDocuments, Desktop, and Documents and Settings folders, and then the MBR. Once the malware has finished overwriting this data with random bytes, the system will automatically restart. This time, however, it will not boot because almost all the data on disk has been wiped. The victim's device is now unrecoverable.

Ransomware Component

Decoys and false flags are deployed in many scenarios where the goal is to confuse and misdirect victims, to buy the adversary time to conduct its real mission of destroying and disabling their opponent's systems and infrastructure.

Let's take a closer look at HermeticWiper's decoy.

Sample hash:
4DC13BB83A16D4FF9865A51B3E4D24112327C526C1392E14D56F20D6F4EAF382

There is a ransomware component that, according to AVAST, sometimes comes along with the wiper as a tool of misdirection. Upon launch, the ransomware (written in the programming language "Go") displays behavior typical of ransomware. The victim device's CPU utilization jumps to 100% as their files are encrypted. Once files are encrypted, they are renamed with an ".encryptedJB" extension.

There is some good news, however. The encryption used by HermeticWiper is not strong, and a free decryptor has already been made available for any files that victims are able to salvage from their machines.

Conclusion

HermeticWiper differentiates itself from other wipers by its creator's efforts to help it evade detection. This malware was created specifically to destroy the machines of victims. HermeticWiper was initially observed targeting Ukraine, but we are now hearing that it has also spread to organizations in other countries. This sort of spillover was also observed with the NotPetya attack, which affected numerous organizations in countries outside Ukraine.

While we're used to seeing financially motivated malware such as ransomware, wipers that exist solely for the purpose of data destruction have become a convenient tool for nefarious actors when their goal is to cripple individual organizations or even entire industries within a target area.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
rule HermeticWiper{

    meta:
        description = "Detects HermeticWiper"
        author = "BlackBerry Threat Research Team"
        date = "2022-03-09"
        license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or
organization, as long as you use it under this license and ensure originator credit
in any derivative to The BlackBerry Research & Intelligence Team"

    strings:
        $s1 = "\\\\.\\EPMNTDRV\\%u" wide
        $s2 = "\\\\.\\PhysicalDrive%u" wide
        $s3 = "SYSTEM\\CurrentControlSet\\Control\\CrashControl" wide

        $sd1 = "DRV_X64" wide
        $sd2 = "DRV_X86" wide
        $sd3 = "DRV_XP_X64" wide
        $sd4 = "DRV_XP_X86" wide

        $c = { 0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC }

        $x = { 53 5A 44 44 88 F0 27 33 41 00 48 ?? 00 00 FF 4D
            5A 90 00 03 00 00 00 7D 04 F5 F0 FF FF 00 00 B8
            F5 F0 ?? 01 01 40 01 04 0F 0D 1C 09 ?? ?? ?? ?? }

    condition:
        uint16(0) == 0x5a4d and filesize < 150KB and all of them

}
```

Indicators of Compromise (IoCs)

HermeticWiper

06086C1DA4590DCC7F1E10A6BE3431E1166286A9E7761F2DE9DE79D7FDA9C397

3C557727953A8F6B4788984464FB77741B821991ACBF5E746AEBDD02615B1767

2C10B2EC0B995B88C27D141D6F7B14D6B8177C52818687E4FF8E6ECF53ADF5BF

0385EEAB00E946A302B24A91DEA4187C1210597B8E17CD9E2230450F5ECE21DA

1BC44EEF75779E3CA1EEFB8FF5A64807DBC942B1E4A2672D77B9F6928D292591

4AA186B5FDCC8248A9672BF21241F77DD395872EC4876C90AF5D27AE565E4CB7

Resource.zip – contains the wiper

92B9198B4AED95932DB029236CB8879A01C73494B545BCACB1ED40596D56990C

DRV_X64 - Windows 7+ 64-bit
E5F3EF69A534260E899A36CEC459440DC572388DEFD8F1D98760D31C700F42D5

Decompressed Hash

96B77284744F8761C4F2558388E0AEE2140618B484FF53FA8B222B340D2A9C84

DRV_X86 - Windows 7+ 32-bit
B01E0C6AC0B8BCDE145AB7B68CF246DEEA9402FA7EA3AEDE7105F7051FE240C1

Decompressed Hash

8C614CF476F871274AA06153224E8F7354BF5E23E6853358591BF35A381FB75B

DRV_XP_X64 - Windows XP 64-bit
B6F2E008967C5527337448D768F2332D14B92DE22A1279FD4D91000BB3D4A0FD

Decompressed Hash

23EF301DDBA39BB00F0819D2061C9C14D17DC30F780A945920A51BC3BA0198A4

DRV_XP_X86 - Windows XP 32-bit
FD7EACC2F87ACEAC865B0AA97A50503D44B799F27737E009F91F3C281233C17D

Decompressed Hash

2C7732DA3DCFC82F60F063F2EC9FA09F9D38D5CFBE80C850DED44DE43BDB666D

Ransom Component

4DC13BB83A16D4FF9865A51B3E4D24112327C526C1392E14D56F20D6F4EAF382

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back