

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

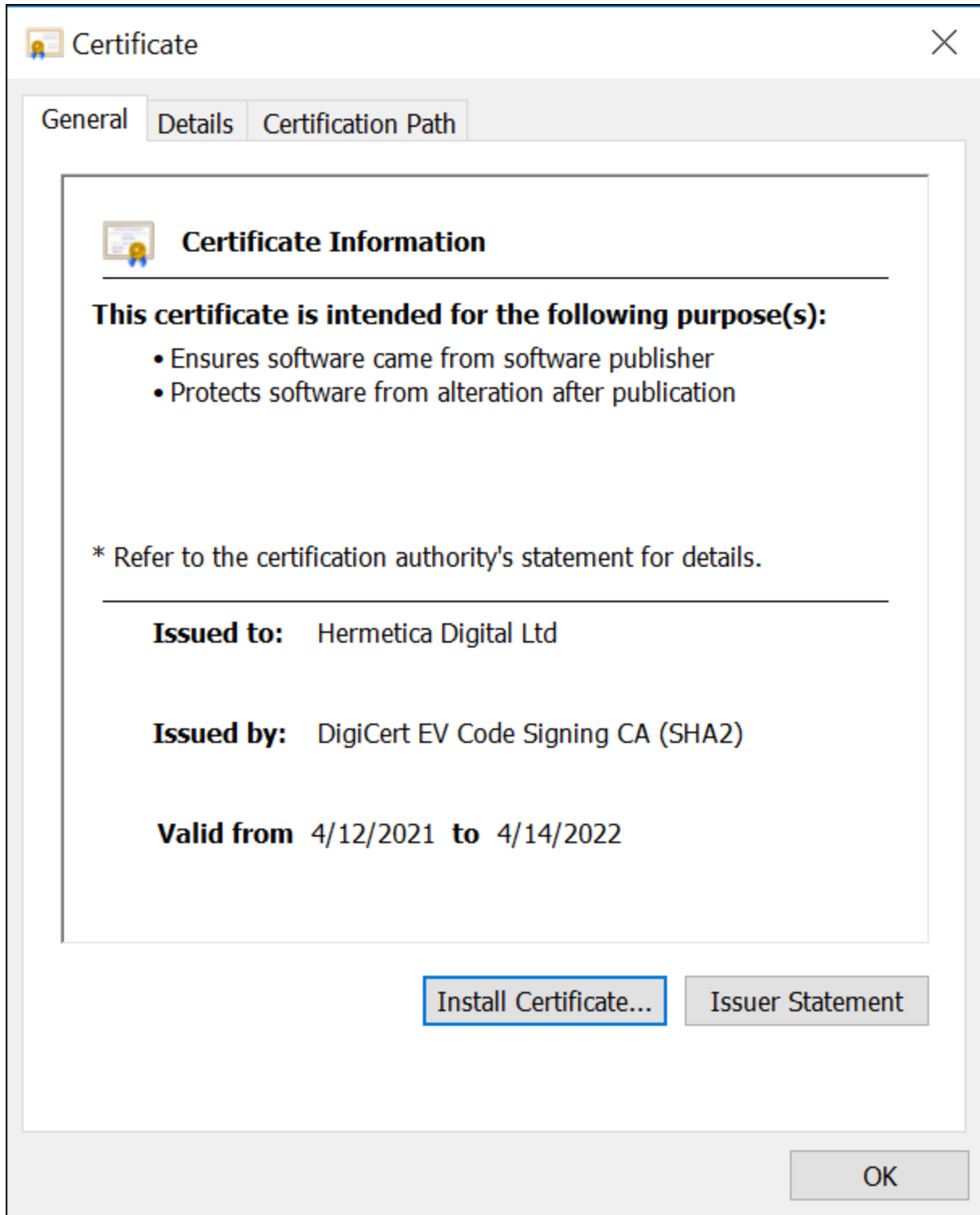


Figure 2 – Hermetica certificate

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.”

Resource	LC	Name	DRV_X64
RCDATA		Type	RCDATA
DRV_X64	0000	Codepage	0000
DRV_X86	0000	Language Code	0000
DRV_XP_X64	0000	Physical Address	000111F0
DRV_XP_X86	0000	Size	11119
RT_ICON		CRC-32	23D9DC32
1	0409	MD5	A952E288A1EAD66490B3275A807F52E5
2	0409	SHA-1	5CCEBAF1CB80C10B95F7EDD458804A646C6F215E
3	0409	Hex	Graph
4	0409	0x0000	535A 4444 88F0 2733 4100 4844 0000 FF4D SZDD 8'3A.HD..ým
5	0409	0x0010	5A90 0003 0000 007D 04F5 F0FF FF00 00B8 Z}ššÿÿ..
6	0409	0x0020	F5F0 A201 0140 0104 0F0D 1C09 F0F5 F00E šše...@.....ššš.
7	0409	0x0030	FF1F BA0E 00B4 09CD 21FF B801 4CCD 2154 Ÿ.*...'.í!ÿ,..LÍ!T
8	0409	0x0040	6869 FF73 2070 726F 6772 61FF 6D20 6361 hiÿs prograym ca
9	0409	0x0050	6E6E 6F74 FF20 6265 2072 756E 20FF 696E nnotÿ be run ÿin
RT_GROUP_ICON		0x0060	2044 4F53 206D FF6F 6465 2E0D 0D0A 24FE DOS mÿode....šp
129	0409	0x0070	0104 8ACD 9C54 CEAC F27D 0774 05E9 6A72 .. í Tí-ò}.t.éjr
		0x0080	07CF 7D02 779C 07CD 7502 F307 D17D 02DD .Ï}.w .Íu.ó.Ñ}.ÿ
		0x0090	898B 02E9 6A8F 9B04 9F07 D5C0 7D02 8383 .éj . .ÖÀ}.
		0x00A0	048A 8302 5269 E363 6874 011C 0DD0 0550 . .Riächt...Đ.P
		0x00B0	4500 FF00 6486 0600 B9D7 A4FD 4824 0722 E.ÿ.d ..'xMÿHš."
		0x00C0	000B 0208 006E F500 0000 0A01 0308 60F5nš.....'š
		0x00D0	FOE5 1001 0101 0103 0D11 0200 00D1 06F5 šš.....Ñ.š
		0x00E0	F020 1501 0280 F5F3 7CC3 C010 15F8 F10A š ... šó ÄÄ..šñ.
		0x00F0	1545 1849 1657 1A00 64BA 0910 28D4 0A00 .E.I.W..d*..(Ö..
		0x0100	002C 1211 30EF 0000 4814 F5F0 7000 0009 .,..0i...H.ššp...
		0x0110	0C29 0189 101C D00D AC1D B919 8910 F82C .). ...Đ..'. .e,
		0x0120	01CF 1DD8 152E 7465 7874 86F5 FOAA 1B0A .Ï.š...text šš^..
		0x0130	149C 1142 14D8 1520 FF00 0068 2E72 6461 . .B.š. Ÿ..h.rda
		0x0140	740F 6100 0054 F4F1 8910 F7F2 0C20 6CD8 t.a..Tšñ .+š. 1š
		0x0150	1908 0048 2E12 2300 8812 11E4 0801 1D10 ...H..#. ...ä....

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.

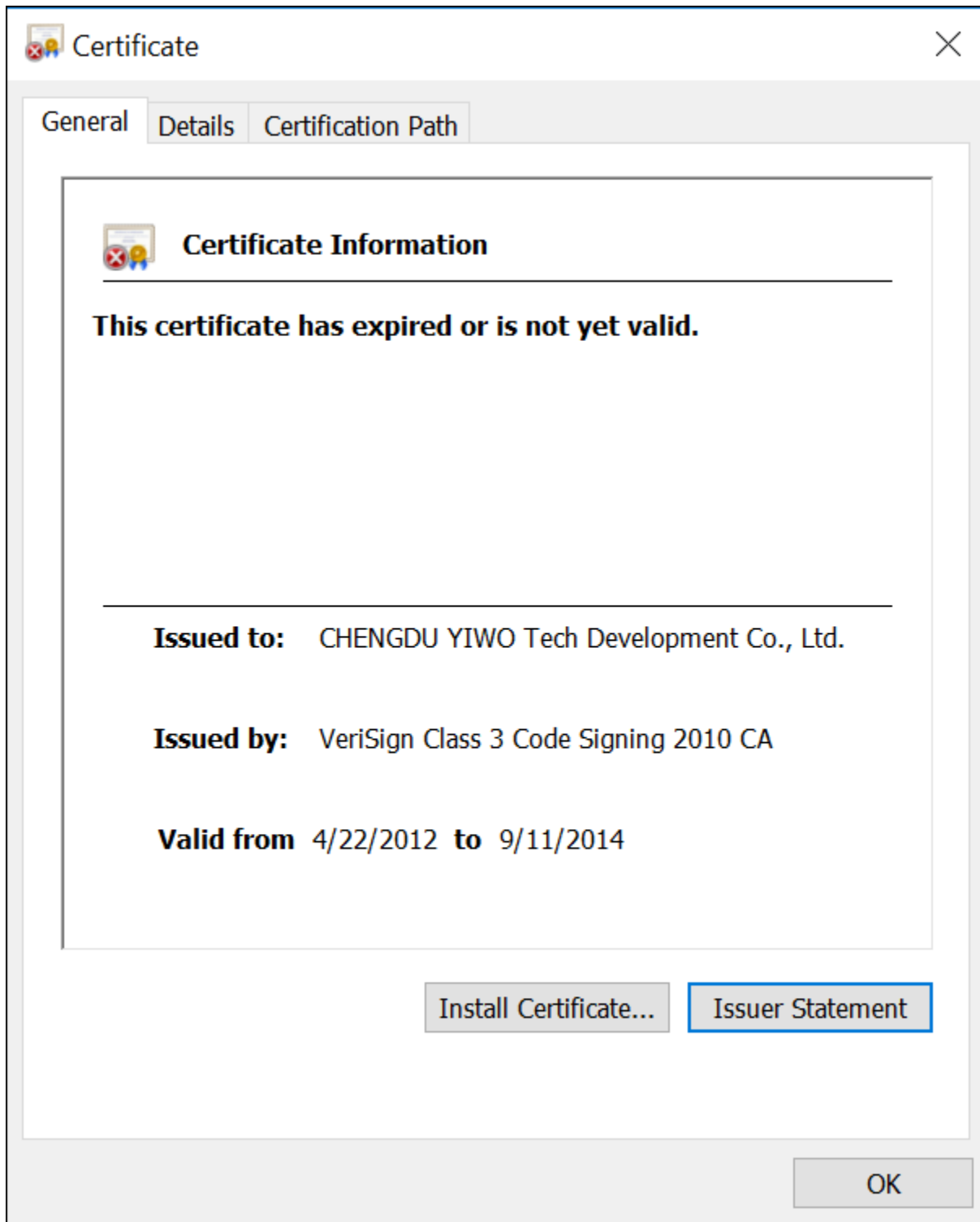


Figure 4 – CHENGDU YIWO Tech Development certificate

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 00 00 00 F8 00 00	eR.NTFS
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 00	?..ÿ..0.....€..€.ÿçñ.....
000000030	00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00 F6 00 00 00 01 00 00 00ö.....
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	ÿ*£.¥£.....ú3ÅŽĐ*. ùhÀ.
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.È^...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	*Uí.r..ûU*u.-Á..u.éÝ...fi
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...<ö..í.ÝfÄ.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.....Z3Û². +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	fý.....ŽÄÿ...èK.+Èwi,..
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.3Å¿...²ö.úó*ép...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.....<óí.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	...fý.....ŽÄÿ...u*.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	aÄ;ö.è..jù.è..öëý<ö-<.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.èöÄ..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 8A 01Š.
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	\$.¿...U²..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..Ö...\$......
000000228	00 00
000000240	00 E9 C0éÀ
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 6FAn 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

```
000000000 FA 42 61 0D B3 F0 D9 22 E9 B4 07 83 85 08 5F AE FE 23 21 9A E6 AE EC 24 kBa.'sU"e'.f...._@p#!sæ@iç
000000018 EA 69 F3 B8 5F 0B 88 DF 8B E8 CF 7E 59 9C 47 5A 07 C2 09 CA A5 E2 BC 15 èiô,_.^B<èI~YeGZ.À.È¥ã4.
000000030 AC 6B 90 58 18 D8 44 61 78 53 05 D5 D3 9B 7F F0 90 46 70 A6 A0 B7 E7 71 ~k.X.ØDaxS.ØÓ>.8.Fp! çcq
000000048 C2 46 E0 B1 D9 95 DB 3C D5 F7 16 24 50 90 0F 43 92 84 21 D2 99 37 EB 2A ÅFã±Ü•Ü<Ô~.çP.„!Ô™7è*
000000060 86 EC FA FD 76 6D 9E F9 B2 1A B1 D0 87 FE AB B3 BA A4 35 9D 2F 1E E5 CD tíúývmžú².±ð#p<³º#5./ .ãí
000000078 2E CC DF AE 7B A4 49 1F 20 B6 1D BB B2 5D EE 05 56 AA FC 90 23 09 B3 79 .Ìã@{#I. ç.»²}i.V²ú.#.³y
000000090 54 06 15 B5 13 DD C6 E2 99 C0 04 D6 BE 5B AE 55 84 4D 5D 81 8D D3 2F 7E T.µ.ÝEã™À.Ø¼{ØU„M]..Ó/~
0000000A8 B6 9D 79 D4 43 73 5B AC C0 9A 52 DE B6 0E 8B 4C BB 6B 78 D4 AD A4 50 40 ç.yÔç[-ÀšRßç{<L>KxÔ. #P@
0000000C0 C5 6E A1 AD EC 4E 6D 95 FE 80 33 B6 2E A9 CF 3F AE 0E D0 AD CD 71 F5 C1 Åñ; .ìNm•pè3ç.ØÍ?@.ÍçðÅ
0000000D8 23 1E 6C 31 C3 8F EF 72 93 D4 11 E7 A0 8C 0A BD FB 9C 93 D9 61 FC 01 26 #.llÅ.ir"Ô.ç E.³súe"Üã. &
0000000F0 CA 38 08 A6 70 67 CF 79 C2 E8 3F 00 52 D1 75 6F 65 8F B8 2E 7D 78 34 48 È8. !pgÏyÅè?.RÑuoe. .)x4H
000000108 AF 5D 40 C7 74 F7 CF 9B 55 C7 9E 2F 01 2D C4 99 27 CD F7 1D BC 92 D1 64 ]@çt-Ï>UçZ/.-Å™.Í- .¼'Nd
000000120 EE 06 2F 7F 31 BB B5 FA 7E E0 80 05 A4 CD 3C 12 A5 E4 FA 5B 48 95 37 78 i. / .l»ú~ã€.#Í<çãú[H•7x
000000138 A0 82 C7 2C 79 4E 71 10 48 89 E0 02 D0 2A E9 47 CA 14 AA F1 12 1E E3 03 ,ç,yNq.Huã.ð*éGÊ.*ñ. .ã.
000000150 ED 0E D6 8F B8 A3 42 8A C2 5E DF 83 31 80 16 9B DB 57 59 1A 4F 0C 3F 4E í.Ô.„èBšÅ^ãflè. >ÜWY.O.?N
000000168 E4 BB 20 38 A8 E6 96 1E D3 D4 E2 A7 ED E8 80 DF B1 7F 63 BD BE 0A DE 0C à» 8"æ-.ÓÓãšieèš±.ç³4.ß.
000000180 D1 8F F6 BF DA 94 00 A6 E2 5D 2D 08 BB 5A 5E F0 C9 55 39 26 8C DA A0 D1 Ñ.ø¿Ü".;ã]-.»Z^ðÈUçæçU Ñ
000000198 C6 3B CB 35 D9 C1 AE 7B 0C D7 66 D9 87 78 0A B1 EA 28 C8 F0 CA C6 44 76 E;ÈSÜÅ@{.*fÜ+x.±è(ÈðÈEðv
0000001B0 57 77 2D B6 D9 E1 B6 1C C6 ED 34 18 AA 97 72 A7 0C 4E D9 87 75 41 52 5C Ww-çÜãç.Èi4.*-rç.NÜ+uAR\
0000001C8 8A C1 19 68 E7 20 20 4D E6 BC BA 5A 0A F9 D8 C0 59 A7 DB 93 4E 9C 50 0D ŠÅ.hç Mæ+ºZ.ùòÀÝçU"ÑøP.
0000001E0 BA 4C 7B 76 90 14 D7 B4 E3 C5 19 DF 35 B1 EB 60 F4 89 59 3E 81 C8 03 56 °L{v. .x'ãÅ.ß5±è'òtY>.È.V
0000001F8 19 44 9F 8E C5 43 B8 08 DA 56 5C 69 5B C4 F0 7C 6B B2 CD 93 01 64 34 8F .DÝžÅç.„ÚV\i[Åð|k²Í".d4.
000000210 F5 1C 5B E8 5F 5F C7 2F 6B 4E 5E 0C 3A 9D 7D D8 AF 98 70 E2 BA 1D D0 55 ô.[è__ç/kN^.:.)ø"pá°.ðU
000000228 16 33 09 02 92 5F 6C 1B 5D 2D 06 FA 81 3E E1 55 CC 07 65 34 93 1F DF DA .3..' _l.]-.ú.>ãUÍ.e4".BÜ
000000240 E0 C2 E2 D6 F9 34 29 26 A3 5C AE 7B 84 25 34 42 97 3E 0C DF 60 7D C3 2B àããòù4)æè\@{„*4B->.ß`}ã+
000000258 40 D6 D7 C7 1D 95 C4 DE 53 C4 1D C9 28 6B A0 83 AB A2 7B 59 E1 2A 75 14 @Ô×ç. .ãßšÅ.É(k f«c{Yã*u.
000000270 5B B2 94 63 5C FC AF 72 D0 3B BE 4F 41 EB 8A 5F E4 3E 5A A4 44 04 D2 44 [²"ç\ü_rð;¼OAEš_ã>ZMD.ØD
000000288 A8 A7 EE A6 D5 C0 14 20 26 B7 B2 1D CA 34 62 EF 39 B2 03 C8 A9 5B 69 45 "šì;ÖÅ. & .².È4b19².È@{IE
0000002A0 EB F4 19 9C 6A 31 C4 A5 69 AF 35 B3 60 CE 3B 30 F9 BA 35 9B 19 94 00 32 èð.æj1ãÏi'5³.Í;0ù°5>."2
```

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.

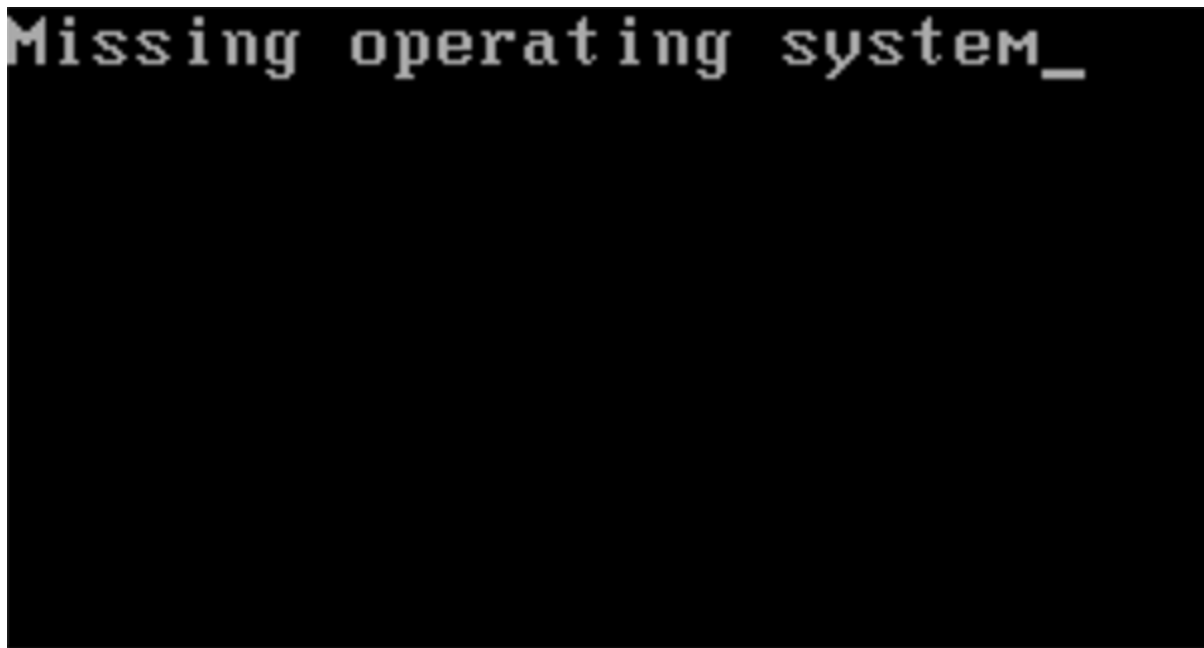


Figure 8 – The last thing any user wants to see upon reboot

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\%" wide
    $s2 = "\\.\.\PhysicalDrive%" 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>

The advertisement banner features the BlackBerry logo and tagline "Intelligent Security. Everywhere." on the left. The central text reads "THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER." followed by the URL "BlackBerry.com/beacon". On the right, there is a book cover for "FINDING BEACONS" by Mattia Carlini. The background is blue with faint white icons of various devices.

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](#)