

SIGNER

```
***** X *****  
[0032FD08]-> (null)  
[0032FD1C]-> DigiCert EU Code Signing CA (SHA2)  
[0032FD20]-> Hermetica Digital Ltd  
[0032FD0C]-> (null)  
[0032FD10]-> (null)  
[00372180]-> 0c 48 73 28 73 ac 8c ce ba f8 f0 e1 e8 32 9c ec
```

DRIVER WITHIN THE 1st STAGE PE

```
.rsrc -SIZE-> 015a80  
FILE SIZE: 17480 BYTES
```

WriteFile (HANDLE hFile, LPCVOID lpBuffer ...)

```
0000 c4 00 5a 00 e0 c6 5b 00 5b 10 00 ff 00 78 70 78 78 ..Z...[...pxxxx  
0011 70 70 00 29 07 57 50 29 50 08 57 50 08 72 10 68 11 pp.)WP)P.WP.r.h  
0022 fe d4 02 49 6e 76 61 6c 69 64 ff 20 70 61 72 61 6d ...Invalid param  
0033 65 74 fb 65 72 87 10 73 73 65 64 20 ff 74 6f 20 43 et.er.ssed.to.cti  
0044 20 72 75 6e ff 74 69 6d 65 20 66 75 6e bf 63 74 69 runtime.fun.cti  
0055 6f 6e 2e 6b 31 00 ff 52 53 44 53 8e 3e 68 aa ff d9 on.kl.RSDS.>h...  
0066 74 46 4c 83 38 31 dc ef 5f 69 c0 2c 1a 20 00 68 3a tFL.81...i...:h:  
0077 ff 5c 65 70 6d 32 2e 30 5c ff 30 31 5f 70 72 6f 6a .\epm2.0\01_proj  
0088 65 ff 63 74 61 72 65 61 5c 30 ff 30 5f 73 6f 75 72 e.ctarea\0.0_sour  
0099 63 65 fe ce 12 5c 6d 6f 64 2e 77 69 ff 6e 64 69 73 ce...mod.wi.ndis
```

SYSFILE (EASUS recovery & disk management)



SIGNER

```
[0032F8B0]-> (null)  
[0032F8C4]-> VeriSign Class 3 Code Signing 2010 CA  
[0032F8C8]-> CHENGDU YIWO Tech Development Co., Ltd.  
[0032F8B4]-> (null)  
[0032F8B8]-> (null)  
[00C72180]-> 33 c3 4c ca 6e 68 16 b6 2b 67 7d 44 b0 68 35 e5
```

```
OpenSCManagerW ( NULL, "ServicesActive", SC_MANAGER_CONNECT | SC_MANAGER_CREATE_SERVICE )  
OpenSCManagerW ( NULL, "ServicesActive", SC_MANAGER_ALL_ACCESS )
```

DRIVER TYPE

```
TYPE : 1 KERNEL_DRIVER  
STATE : 4 RUNNING  
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)  
WIN32_EXIT_CODE : 0 (0x0)  
SERVICE_EXIT_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT_HINT : 0x0
```

```
\\Device\Harddisk%u\Partition0  
\\. \EPMNIDRV\0  
wsprintfW(&var_210, 0x4051fc, 0x4051f0, arg1) {"\\.\\"} {"%s%.2s"}  
CreateFileW(lpFileName: arg1, dwDesiredAccess ...)
```

DeviceIoControl(HANDLE hDevice ...)

IoCreateSymbolicLink
IoDeleteDevice

SECTOR 0 BEFORE

```
00000000 EB 52 90 4E 54 46 53 20 20 20 02 08 00 00 00  
00000001 00 00 00 00 80 00 00 00 3F 0F FF 03 00 00 00 00  
00000002 00 00 00 00 80 00 80 00 FF 0F 03 00 00 00 00  
00000003 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00  
00000004 F6 00 00 00 01 00 00 00 07 39 64 E8 68 E6 66  
00000005 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  
00000006 1F 1E 68 66 0C 8B 16 0E 00 66 81 3E 03 00 4E  
00000007 54 56 53 75 1B 84 41 BB AA 55 CD 13 72 C0 81 F7  
00000008 5A AA 75 0E F7 C1 01 00 75 03 E9 D0 00 1E 83 EC  
00000009 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13  
0000000A 9F 03 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3  
0000000B 06 0F C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  
0000000C 66 FF 06 11 00 00 16 0F 00 0E C2 FF 06 16 00 E8  
0000000D 4B 00 2B C8 77 EF B8 00 BB CD 1A 6E 23 C0 75 2D  
0000000E 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  
0000000F 68 07 BB 16 68 70 0E 16 68 09 00 66 53 66 53 66  
00000010 25 16 16 16 68 88 01 66 61 0E 07 CD 1A 33 C0 BF  
00000011 28 10 B9 D8 0F FC F3 AA E9 5F 01 90 90 66 60 1E  
00000012 06 6A A1 11 00 66 03 06 C 00 1E 66 68 00 00 00  
00000013 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E  
00000014 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F  
00000015 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF  
00000016 0E 16 00 75 BC 07 1F 66 61 C3 A0 F8 01 E8 09 00  
00000017 A0 FB 01 E8 03 0F F4 EB FD B4 01 B8 F0 AC 3C 00  
00000018 74 09 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20  
00000019 64 69 73 6B 20 72 65 61 64 20 65 72 6F 72 6F 72  
0000001A 6F 63 63 72 72 65 64 00 D9 0A 42 4F 5F 44 5A  
0000001B 47 52 20 69 73 20 6D 69 73 73 6D 6E 67 00 0D 0A  
0000001C 42 4F 54 4D 47 52 20 69 73 20 63 6F 6D 70 7A  
0000001D 65 73 73 65 64 00 0A 50 72 65 73 73 20 43 74  
0000001E 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F 20 72 65  
0000001F 73 74 61 72 74 0D 0A 00 8C A9 BE D6 00 00 55 AA
```

SECTOR 0 AFTER

```
00000000 04 00 4E 00 50 B7 4F 00 05 60 B4 54 61 60 C3 A1  
00000001 94 05 60 70 C4 A0 9E C4 A0 1A 04 61 A4 C4 A0 B3  
00000002 1B 16 60 05 61 91 60 69 A2 91 60 70 A1 C0 91 60  
00000003 AA 1C B6 20 4A 05 60 D4 A9 60 1B 59 10 C1 61 24  
00000004 59 70 55 76 59 70 80 05 60 7C 59 70 FE 59 70 A6  
00000005 7C 61 04 1E 47 10 B5 20 AB 05 60 4A B5 20 A3  
00000006 B5 20 0C 05 60 B4 21 C9 B5 20 5A 04 61 F0 B5 20  
00000007 7C 61 04 1E 47 10 B5 20 AB 05 60 4A B5 20 A3  
00000008 F4 32 6E 63 3C FD 60 E9 8D FD 60 1C 61 F0 FD 60  
00000009 F3 20 0D 03 00 50 F9 50 1B 7D 3B 7D 3B 7D 3B  
0000000A 3A 27 6E 63 3C FD 60 E9 8D FD 60 1C 61 F0 FD 60  
0000000B 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000000C 5B 7D 0E 03 00 50 F9 50 1B 7D 3B 7D 3B 7D 3B  
0000000D 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000000E 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000000F 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000010 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000011 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000012 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000013 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000014 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000015 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000016 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000017 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000018 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
00000019 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000001A 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000001B 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000001C 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000001D 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000001E 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D  
0000001F 7D 7D 7B 7B 7B 7B 7B 7D 7B 7D 7B 7D 7B 7D
```

REBOOT



```
Status: 0xc000000f  
Info: A required device isn't connected or can't be accessed.
```