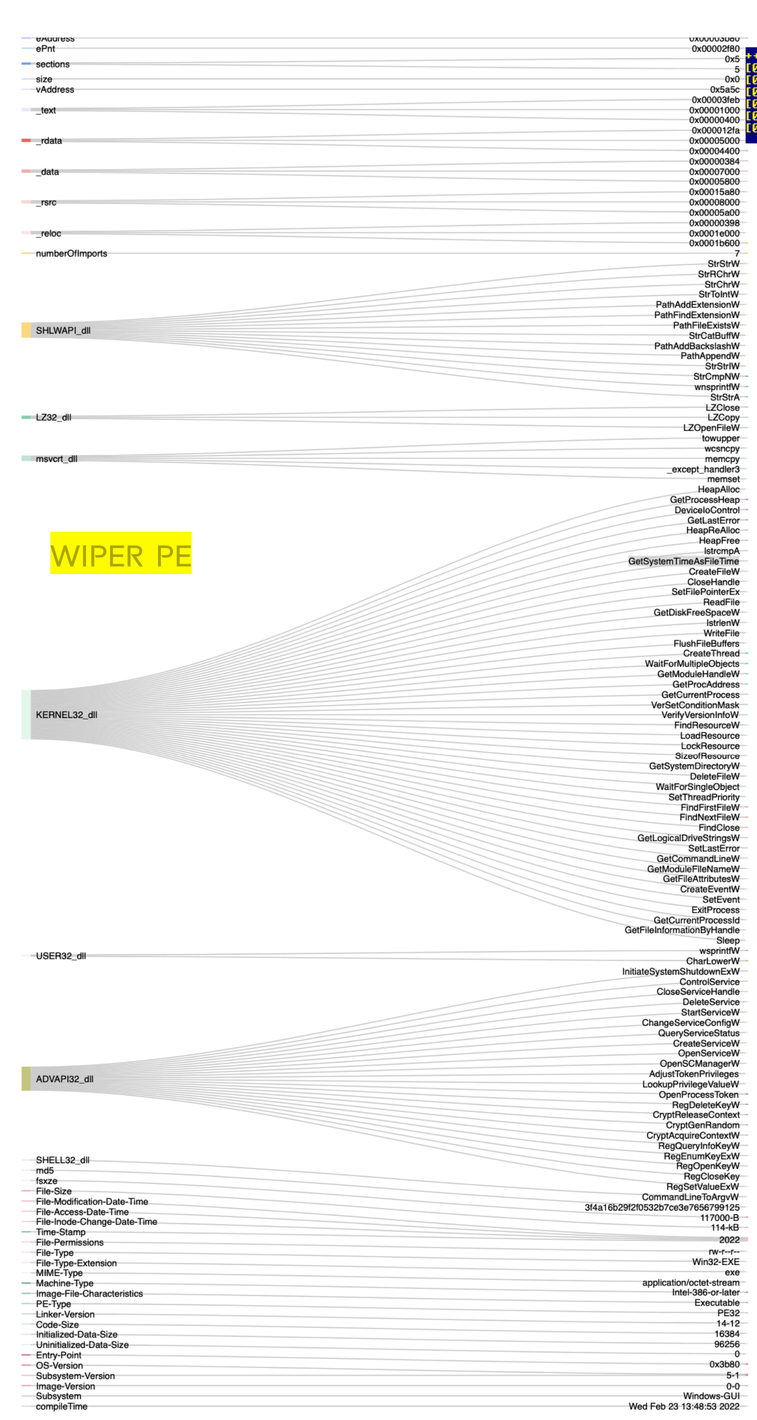


WIPER PE

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
```

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)

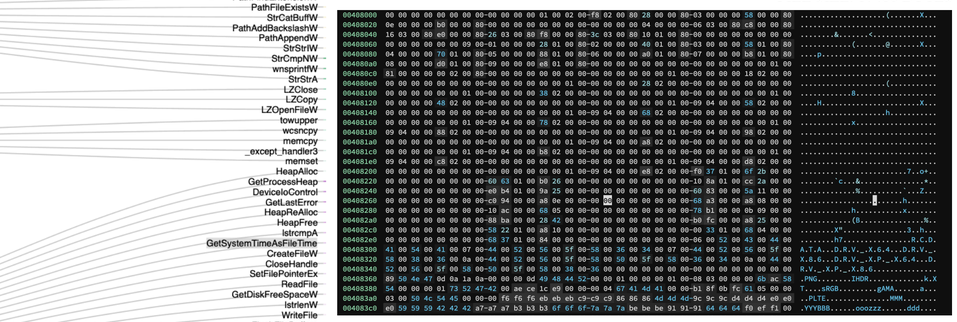
DRIVER

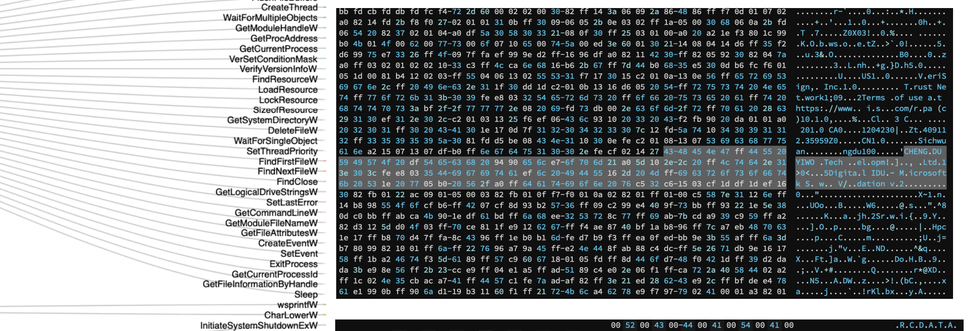
TYPE : 1 KERNEL_DRIVER
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

DRIVER WITHIN THE 1st STAGE PE

.rsrc —SIZE—> ***015a80***

FILE SIZE: 17480 BYTES





\Device\Harddisk%u\Partition0

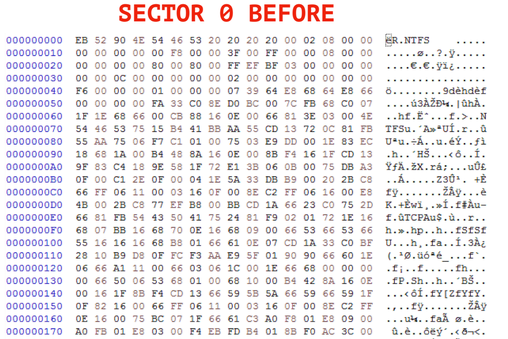
\\.\EPMNTDRV\0

wsprintfW(&var_210, 0x4051fc, 0x4051f0, arg1) {"\\.\"} {"%s%.2s"}
CreateFileW(lpFileName: arg1, dwDesiredAccess …)

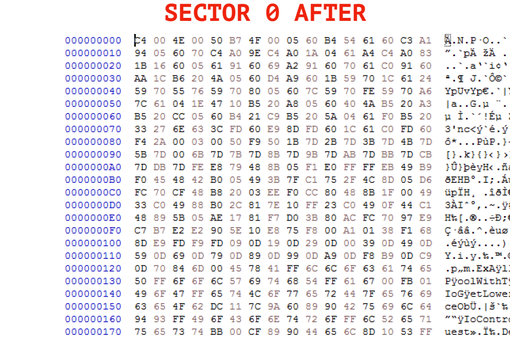
DeviceIoControl(HANDLE hDevice …)

IoCreateSymbolicLink
IoDeleteDevice

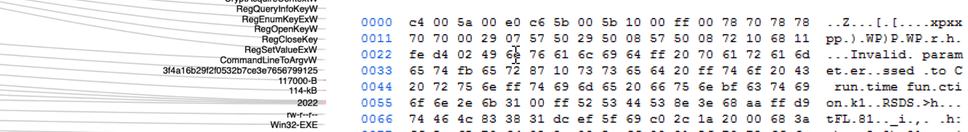
SECTOR 0 BEFORE



SECTOR 0 AFTER



WriteFile (HANDLE hFile, LPCVOID lpBuffer …)



REBOOT

```
Status: 0xc000000f

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