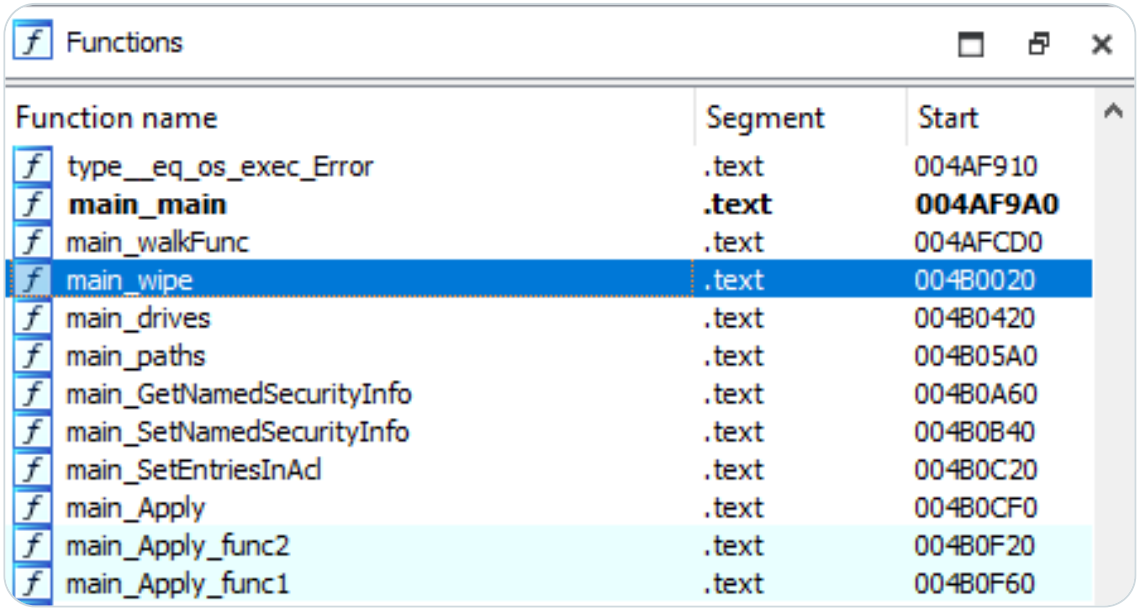
Thread

ESET Research
@ESETresearch

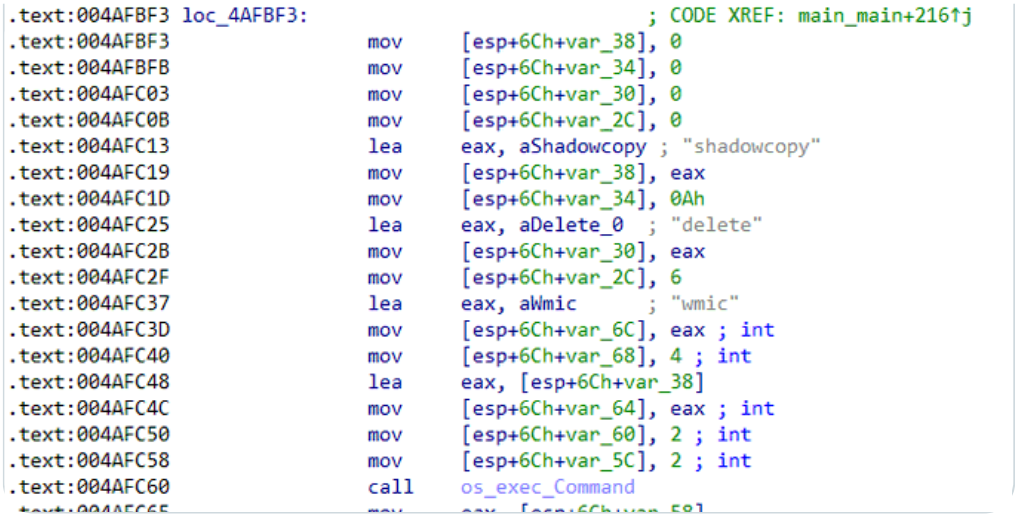
#BREAKING On January 25th #ESETResearch discovered a new cyberattack in 🇺🇦 Ukraine. Attackers deployed a new wiper we named #SwiftSlicer using Active Directory Group Policy. The #SwiftSlicer wiper is written in Go programing language. We attribute this attack to #Sandworm. 1/3



2:12 PM · Jan 27, 2023 · **116K** Views

240 Retweets **13** Quote Tweets **441** Likes

ESET Research @ESETresearch · Jan 27
Replying to @ESETresearch
Once executed it deletes shadow copies, recursively overwrites files located in %CSIDL_SYSTEM%\drivers, %CSIDL_SYSTEM_DRIVE%\Windows\NTDS and other non-system drives and then reboots computer. For overwriting it uses 4096 bytes length block filled with randomly generated byte 2/3



```
.text:004AFBF3 loc_4AFBF3:                             ; CODE XREF: main_main+216↑j
.text:004AFBF3                 mov     [esp+6Ch+var_38], 0
.text:004AFBFB                 mov     [esp+6Ch+var_34], 0
.text:004AFC03                 mov     [esp+6Ch+var_30], 0
.text:004AFC0B                 mov     [esp+6Ch+var_2C], 0
.text:004AFC13                 lea     eax, aShadowcopy ; "shadowcopy"
.text:004AFC19                 mov     [esp+6Ch+var_38], eax
.text:004AFC1D                 mov     [esp+6Ch+var_34], 0Ah
.text:004AFC25                 lea     eax, aDelete_0  ; "delete"
.text:004AFC2B                 mov     [esp+6Ch+var_30], eax
.text:004AFC2F                 mov     [esp+6Ch+var_2C], 6
.text:004AFC37                 lea     eax, aWmic      ; "wmic"
.text:004AFC3D                 mov     [esp+6Ch+var_6C], eax ; int
.text:004AFC40                 mov     [esp+6Ch+var_68], 4 ; int
.text:004AFC48                 lea     eax, [esp+6Ch+var_38]
.text:004AFC4C                 mov     [esp+6Ch+var_64], eax ; int
.text:004AFC50                 mov     [esp+6Ch+var_60], 2 ; int
.text:004AFC58                 mov     [esp+6Ch+var_5C], 2 ; int
.text:004AFC60                 call    os_exec_Command
```

1 13 44 6,700

ESET Research @ESETresearch · Jan 27

IoCs:

📄7346E2E29FADDD63AE5C610C07ACAB46B2B1B176

ESET Detection names:

🚨 WinGo/KillFiles.C trojan 3/3

1 11 41 5,657