Analysis of CaddyWiper

nioguard.com/2022/03/analysis-of-caddywiper.html

Summary

- Name: CaddyWiper
- Discovered in March 2022
- Was used in a targeted attack in Ukraine
- Deployed via Microsoft Active Directory GPO
- Corrupts files and disk partitions
- PE32 sample written in C++
- Compiled on the same day when it was deployed on targeted systems in Ukraine

by Denis Popov

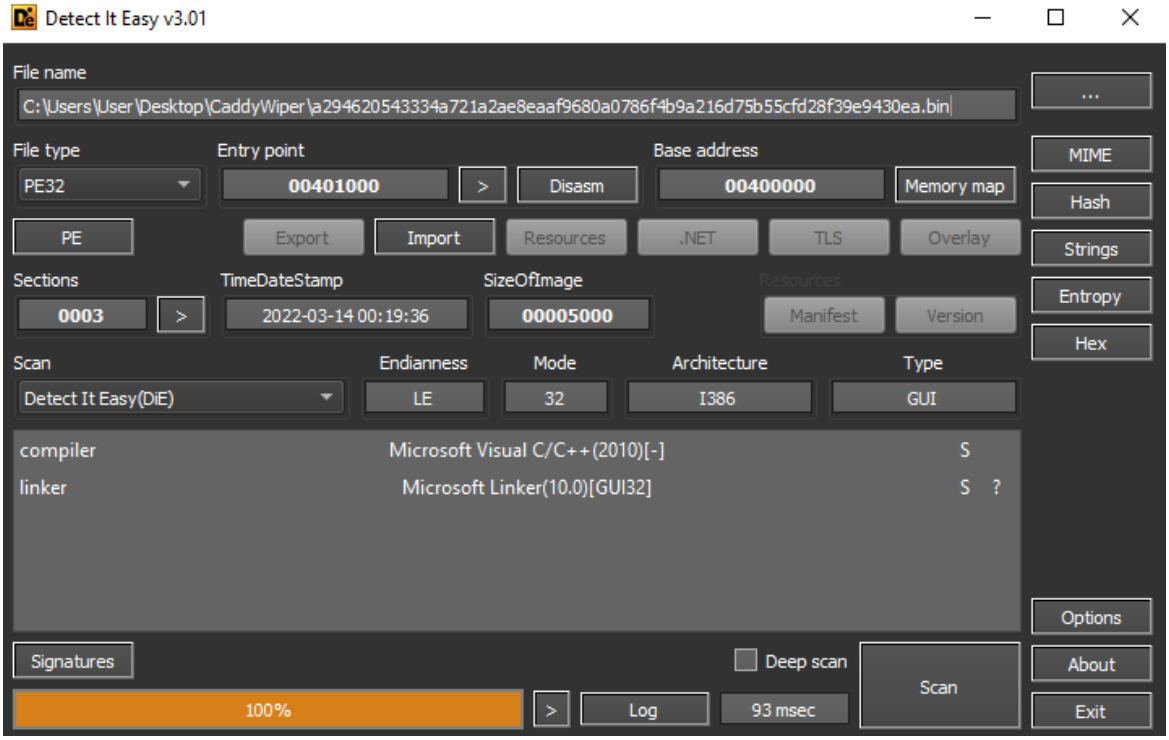
Introduction

On March 14 2022 ESET research found a new disruptive malware deployed in Ukraine. It was called CandyWiper and it is already the third wiper that was found in the Ukrainian systems. The previous ones were WhisperGate and HermeticWiper. As well as the HermeticWiper, CaddyWiper was also deployed via Microsoft Active Directory GPO.

Technical Details

Overview

The CaddyWiper sample was written in C++ and had compilation timestamp 14-03-2022, which matches with the day when it was deployed in the victim's system. This sample has only 10 functions.



Execution

All code in the sample is obfuscated in an interesting way. All strings are separated by one character. Even function calls are obfuscated in the same way, so malware has only one imported function and library, but others will be imported during execution.

```
.text:00651071 mov     [ebp+var_3], 0
.text:00651075 mov     [ebp+var_48], 61h ; 'a'
.text:00651079 mov     [ebp+var_47], 64h ; 'd'
.text:0065107D mov     [ebp+var_46], 76h ; 'v'
.text:00651081 mov     [ebp+var_45], 61h ; 'a'
.text:00651085 mov     [ebp+var_44], 70h ; 'p'
.text:00651089 mov     [ebp+var_43], 69h ; 'i'
.text:0065108D mov     [ebp+var_42], 33h ; '3'
.text:00651091 mov     [ebp+var_41], 32h ; '2'
.text:00651095 mov     [ebp+var_40], 2Eh ; '.'
.text:00651099 mov     [ebp+var_3F], 64h ; 'd'
.text:0065109D mov     [ebp+var_3E], 6Ch ; 'l'
.text:006510A1 mov     [ebp+var_3D], 6Ch ; 'l'
.text:006510A5 mov     [ebp+var_3C], 0
.text:006510A9 mov     [ebp+var_30], 4Ch ; 'L'
.text:006510AD mov     [ebp+var_2F], 6Fh ; 'o'
.text:006510B1 mov     [ebp+var_2E], 61h ; 'a'
.text:006510B5 mov     [ebp+var_2D], 64h ; 'd'
.text:006510B9 mov     [ebp+var_2C], 4Ch ; 'L'
.text:006510BD mov     [ebp+var_2B], 69h ; 'i'
.text:006510C1 mov     [ebp+var_2A], 62h ; 'b'
.text:006510C5 mov     [ebp+var_29], 72h ; 'r'
.text:006510C9 mov     [ebp+var_28], 61h ; 'a'
.text:006510CD mov     [ebp+var_27], 72h ; 'r'
.text:006510D1 mov     [ebp+var_26], 79h ; 'y'
.text:006510D5 mov     [ebp+var_25], 41h ; 'A'
```

CaddyWiper retrieves the machine role in the system using the ‘DsRoleGetPrimaryDomainInformation’ function. If the obtained value is ‘DsRole_RolePrimaryDomainController’, the wiper terminates its execution, if other, then it proceeds.

```
.text:006510EA add     esp, 8
.text:006510ED mov     [ebp+var_34], eax
.text:006510F0 mov     [ebp+var_64], 6Eh ; 'n'
.text:006510F4 mov     [ebp+var_63], 65h ; 'e'
.text:006510F8 mov     [ebp+var_62], 74h ; 't'
.text:006510FC mov     [ebp+var_61], 61h ; 'a'
.text:00651100 mov     [ebp+var_60], 70h ; 'p'
.text:00651104 mov     [ebp+var_5F], 69h ; 'i'
.text:00651108 mov     [ebp+var_5E], 33h ; '3'
.text:0065110C mov     [ebp+var_5D], 32h ; '2'
.text:00651110 mov     [ebp+var_5C], 2Eh ; '.'
.text:00651114 mov     [ebp+var_5B], 64h ; 'd'
.text:00651118 mov     [ebp+var_5A], 6Ch ; 'l'
.text:0065111C mov     [ebp+var_59], 6Ch ; 'l'
.text:00651120 mov     [ebp+var_58], 0
.text:00651124 lea     edx, [ebp+var_64]
.text:00651127 push    edx
.text:00651128 call    [ebp+var_34]
.text:0065112B mov     [ebp+Buffer], 0
.text:00651132 lea     eax, [ebp+Buffer]
.text:00651135 push    eax                             ; Buffer
.text:00651136 push    1                               ; InfoLevel
.text:00651138 push    0                               ; lpServer
.text:0065113A call    ds:DsRoleGetPrimaryDomainInformation
```

The first folder where CaddyWiper starts its operation is the “C:\Users”. File corruption routine is the ‘*sub_6522A0()*’ function.

```
.text:0039114A lea     edx, [ebp+var_48]
.text:0039114D push    edx
.text:0039114E call    [ebp+var_34]
.text:00391151 mov     [ebp+var_54], 43h ; 'C'
.text:00391155 mov     [ebp+var_53], 3Ah ; ':'
.text:00391159 mov     [ebp+var_52], 5Ch ; '\'
.text:0039115D mov     [ebp+var_51], 55h ; 'U'
.text:00391161 mov     [ebp+var_50], 73h ; 's'
.text:00391165 mov     [ebp+var_4F], 65h ; 'e'
.text:00391169 mov     [ebp+var_4E], 72h ; 'r'
.text:0039116D mov     [ebp+var_4D], 73h ; 's'
.text:00391171 mov     [ebp+var_4C], 0
.text:00391175 lea     eax, [ebp+var_54]
.text:00391178 push    eax
.text:00391179 call    sub_3922A0
.text:0039117E add     esp, 4
.text:00391181 mov     [ebp+var_20], 44h ; 'D'
.text:00391185 mov     [ebp+var_1F], 3Ah ; ':'
.text:00391189 mov     [ebp+var_1E], 5Ch ; '\'
.text:0039118D mov     [ebp+var_1D], 0
.text:00391191 mov     [ebp+var_68], 0
.text:00391198 jmp     short loc_3911A3
```

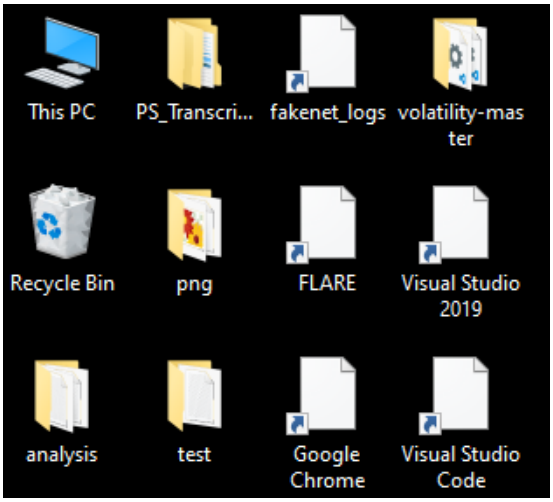
During '*sub_6522A0()*' execution wiper loads and uses next functions:

- FindFirstFileA
- FindNextFileA
- CreateFileA
- LocalAlloc
- SetFilePointer
- WriteFile
- LocalFree
- CloseHandle
- FindClose
- SetEntriesInAclA
- AllocateAndInitializeSid
- SetNamedSecurityInfoA
- GetCurrentProcess
- OpenProcessToken

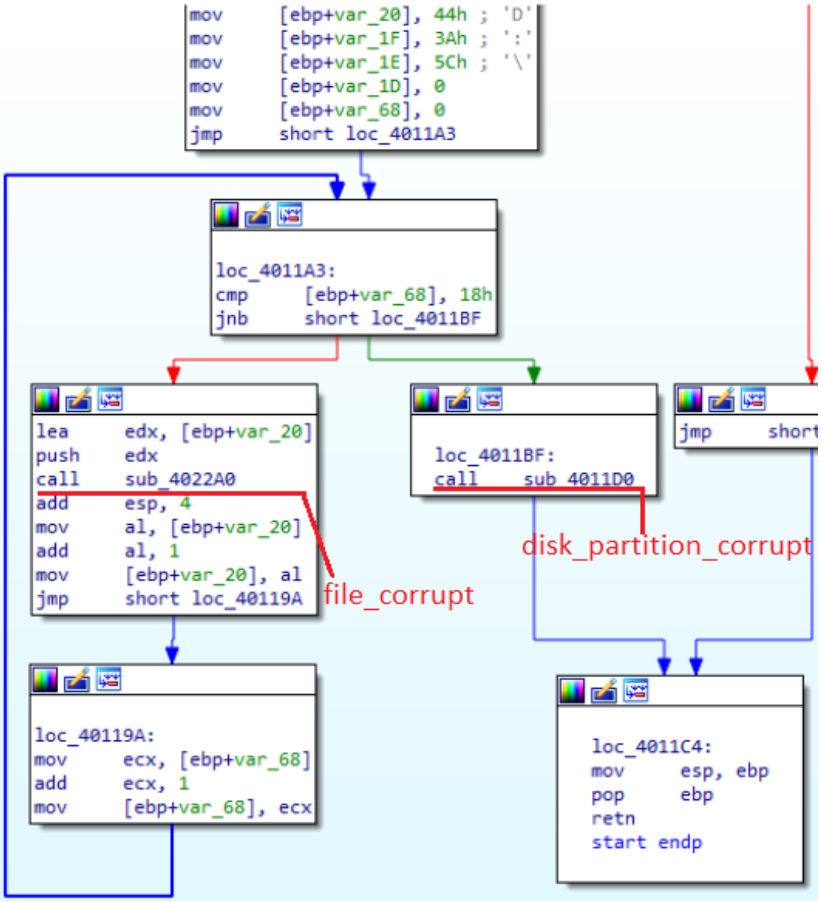
- FreeSid

If the current file is used by another process, CaddyWiper obtains access to it using “SeTakeOwnershipPrivilege”. The first file in the system which CaddyWiper overwrites is ‘*C:\Users\desktop.ini*’. After overwriting this file the desktop background will be deleted and all shortcuts will be unusable.

a29462054333...	8848	QueryRemotePr...	C:\Users\desktop.ini	INVALID PARAME...		648
a29462054333...	8848	QuerySecurityFile	C:\Users\desktop.ini	SUCCESS	Information: Owner...	648
a29462054333...	8848	SetSecurityFile	C:\Users\desktop.ini	SUCCESS	Information: DACL	648
a29462054333...	8848	ReadFile	C:\$Secure:$SDS:$DATA	SUCCESS	Offset: 2,420,736, ...	648
a29462054333...	8848	ReadFile	C:\$Secure:$SDS:$DATA	SUCCESS	Offset: 2,158,592, ...	648
a29462054333...	8848	CloseFile	C:\Users\desktop.ini	SUCCESS		648
a29462054333...	8848	CreateFile	C:\Users\desktop.ini	SUCCESS	Desired Access: G...	648
a29462054333...	8848	QueryStandardI...	C:\Users\desktop.ini	SUCCESS	AllocationSize: 176...	648
a29462054333...	8848	WriteFile	C:\Users\desktop.ini	SUCCESS	Offset: 0, Length: 1...	648
a29462054333...	8848	CloseFile	C:\Users\desktop.ini	SUCCESS		648



After corrupting the ‘*C:\Users*’ folder, malware proceeds and goes to the ‘*D:*\’ logical drive. If it’s present, malware will corrupt its files in the same way as the previous one. This operation will be repeated for all logical drives from ‘*D:*\’ to ‘*Z:*\’. If these drives are missing or file corruption is done, it calls the ‘*sub_4011D0()*’ function, which will corrupt the disk partition.



To perform disk corruption CaddyWiper obtains access to the disk partitions from '\.*PHYSICALDRIVE9*' to '\.*PHYSICALDRIVE0*' and performs overwriting the first 1920 bytes of data with '0' using 'CreateFileW' and 'DeviceIoControl' functions. This operation can be done only if the malware was executed as administrator.

```
.text:00391454 push    0
.text:00391456 lea     eax, [ebp+var_808]
.text:0039145C push    eax
.text:0039145D push    0
.text:0039145F push    0
.text:00391461 push    780h
.text:00391466 lea     ecx, [ebp+var_7F0]
.text:0039146C push    ecx
.text:0039146D push    7C054h
.text:00391472 mov     edx, [ebp+var_4]
.text:00391475 push    edx
.text:00391476 call    [ebp+var_6C]
.text:00391479 mov     eax, [ebp+var_4]
.text:0039147C push    eax
.text:0039147D call    [ebp+var_8]
```

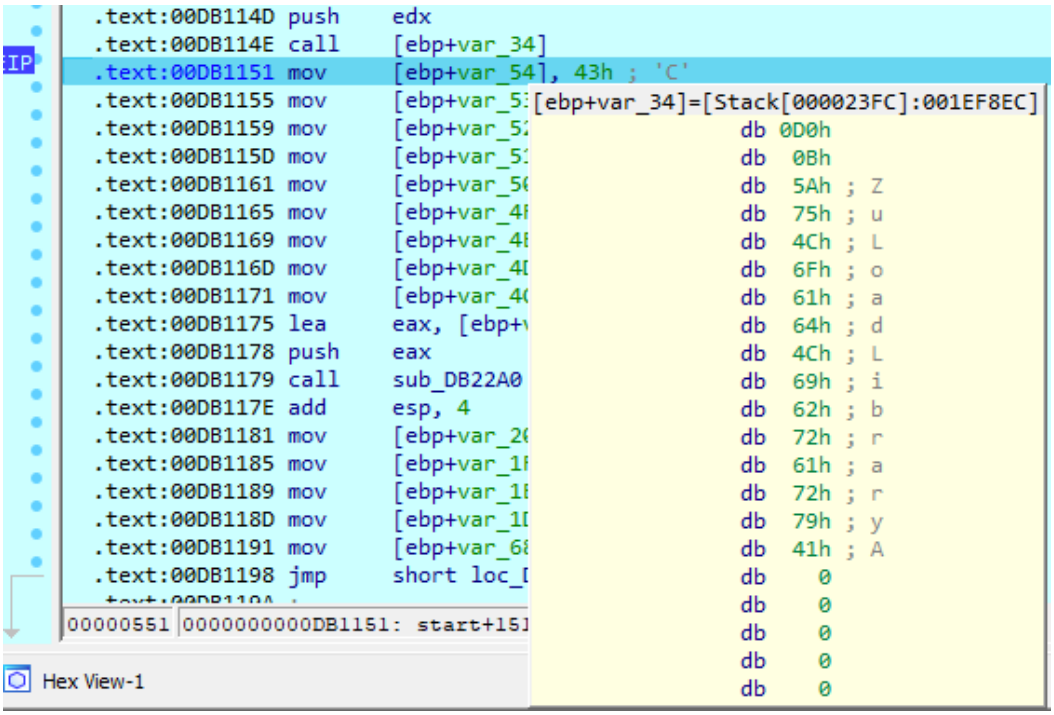
Overwriting first 780h(1920 in decimal) bytes

```
Stack[00001124]:00D3FA32 db  5Ch ; \  Stack[00001124]:00D3FA54 db  44h ; D
Stack[00001124]:00D3FA33 db    0      Stack[00001124]:00D3FA55 db  65h ; e
Stack[00001124]:00D3FA34 db  50h ; P  Stack[00001124]:00D3FA56 db  76h ; v
Stack[00001124]:00D3FA35 db    0      Stack[00001124]:00D3FA57 db  69h ; i
Stack[00001124]:00D3FA36 db  48h ; H  Stack[00001124]:00D3FA58 db  63h ; c
Stack[00001124]:00D3FA37 db    0      Stack[00001124]:00D3FA59 db  65h ; e
Stack[00001124]:00D3FA38 db  59h ; Y  Stack[00001124]:00D3FA5A db  49h ; I
Stack[00001124]:00D3FA39 db    0      Stack[00001124]:00D3FA5B db  6Fh ; o
Stack[00001124]:00D3FA3A db  53h ; S  Stack[00001124]:00D3FA5C db  43h ; C
Stack[00001124]:00D3FA3B db    0      Stack[00001124]:00D3FA5D db  6Fh ; o
Stack[00001124]:00D3FA3C db  49h ; I  Stack[00001124]:00D3FA5E db  6Eh ; n
Stack[00001124]:00D3FA3D db    0      Stack[00001124]:00D3FA5F db  74h ; t
Stack[00001124]:00D3FA3E db  43h ; C  Stack[00001124]:00D3FA60 db  72h ; r
Stack[00001124]:00D3FA3F db    0      Stack[00001124]:00D3FA61 db  6Fh ; o
Stack[00001124]:00D3FA40 db  41h ; A  Stack[00001124]:00D3FA62 db  6Ch ; l
Stack[00001124]:00D3FA41 db    0      Stack[00001124]:00D3FA63 db    0
Stack[00001124]:00D3FA42 db  4Ch ; L  Stack[00001124]:00D3FA64 db  43h ; C
Stack[00001124]:00D3FA43 db    0      Stack[00001124]:00D3FA65 db  72h ; r
Stack[00001124]:00D3FA44 db  44h ; D  Stack[00001124]:00D3FA66 db  65h ; e
Stack[00001124]:00D3FA45 db    0      Stack[00001124]:00D3FA67 db  61h ; a
Stack[00001124]:00D3FA46 db  52h ; R  Stack[00001124]:00D3FA68 db  74h ; t
Stack[00001124]:00D3FA47 db    0      Stack[00001124]:00D3FA69 db  65h ; e
Stack[00001124]:00D3FA48 db  49h ; I  Stack[00001124]:00D3FA6A db  46h ; F
Stack[00001124]:00D3FA49 db    0      Stack[00001124]:00D3FA6B db  69h ; i
Stack[00001124]:00D3FA4A db  56h ; V  Stack[00001124]:00D3FA6C db  6Ch ; l
Stack[00001124]:00D3FA4B db    0      Stack[00001124]:00D3FA6D db  65h ; e
Stack[00001124]:00D3FA4C db  45h ; E  Stack[00001124]:00D3FA6E db  57h ; W
```

After disk partitions are corrupted the machine will be rebooted, but the system won't be started, instead the "*FATAL: INT18: BOOT FAILURE*" message will be shown on the screen.

Obfuscation

All function calls and library names are separated in the PE file. Also, malware employs WinAPI calls obfuscation.



Conclusion

CaddyWiper continues the trend of data wipers in Ukraine. It is the third one found. The previous ones were WhisperGate and HermeticWiper. CaddyWiper doesn't have any similarities with them, but as well as HermeticWiper, was deployed via Microsoft Active Directory GPO. The analyzed sample has obfuscated strings and API calls. It has two main disruptive functions, one of them corrupts files in the '*C:\Users*' folder and logical drives from '*D:*\' to '*Z:*\', the second one overwrites disk partitions from '\.\\\PHYSICALDRIVE9' to '\.\\\PHYSICALDRIVE0'. After the corruption process is done the system will be rebooted, but won't be started.

IoCs

Files

File name	SHA256
caddy1.exe	a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea

MITRE attack techniques

Tactic	Technique
Defense evasion	T1140 – Deobfuscate/Decode Files or Information T1027 – Obfuscated Files or Information
Discovery	T1083 – File and Directory Discovery T1082 - System Information Discovery
Impact	T1485 – Data Destruction T1529 – System Shutdown/Reboot

References

1. https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/
2. https://www.virustotal.com/gui/file/a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea/details
3. https://app.any.run/tasks/399165f5-4f4d-417f-93dd-077718d81512/