

# eSentire Threat Intelligence Malware Analysis: CaddyWiper

[esentire.com/blog/esentire-threat-intelligence-malware-analysis-caddywiper](https://esentire.com/blog/esentire-threat-intelligence-malware-analysis-caddywiper)



First discovered by ESET researchers in March 2022, CaddyWiper malware is a new type of wiper malware used by Russian threat actors to target Ukrainian organizations, and the fourth wiper identified since the invasion of the Ukraine. Unlike ransomware, the only objective of using wiper malware is to damage files, data, hard drives, or entire programs and cause as much destruction as possible in the targeted organization's endpoints and network.

eSentire's Threat Intelligence (TI) team assesses with high confidence that as the hybrid war between Russia and Ukraine continues, threat actors will continue developing more destructive malware with the goal to disrupt the operations in Ukrainian infrastructure since the wiping malware does not need to be sophisticated to perform the basic wiping capabilities.

## Key Takeaways

- eSentire TI assesses that CaddyWiper has a low level of sophistication compared to the other wipers observed targeting Ukrainian organizations (HermeticWiper).

- CaddyWiper specifically doesn't target Domain Controllers to keep the foothold on the victim's network to be able to obtain credentials, move laterally and infect more machines.
- eSentire TI assesses that it's probable that this is done to keep the foothold on the Domain Controller and gain access to other machines on the network.
- eSentire's Threat Response Unit (TRU) is currently implementing the detections developed to identify CaddyWiper malware activities across MDR for Endpoint, performing global threat hunts against the IOCs associated with the CaddyWiper malware, and actively monitoring for any signs of compromise.

## Case Study

The destructive malware named CaddyWiper was first reported by [ESET](#) Researchers on March 14, 2022. The malware was first detected at 11:38 a.m. local time (5:38 a.m. EST) targeting organizations in Ukraine. According to ESET, the infection mechanism is similar to the HermeticWiper malware in that it operates via Default Domain Policy.

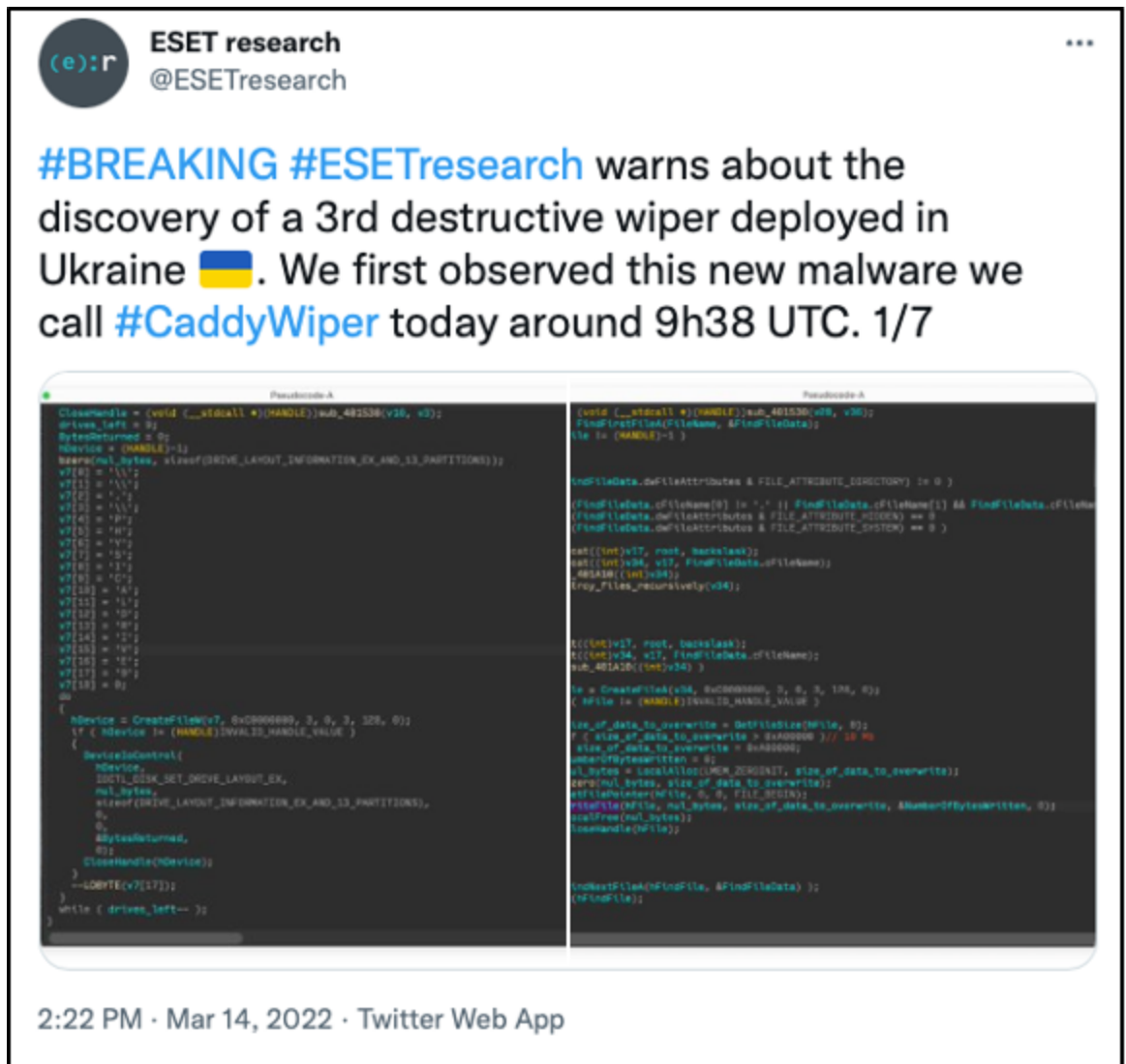


Exhibit 1:

First CaddyWiper detection by ESET

## Technical Analysis on CaddyWiper

---

eSentire TI has observed 4 CaddyWiper samples targeting Ukrainian organizations in the wild including a UPX packed version. CaddyWiper is the fourth wiper observed targeting Ukrainian organizations since January 2022.

CaddyWiper is a PE32 (32-bit) executable written in C++ programming language with a file size of 9.00 KB (9,216 bytes). The compilation timestamp for all the wiper samples dates to March 14, 2022 (on the same day when the first attacks were observed).

The malware samples do not appear to be digitally signed except for one sample (SHA-256: 1e87e9b5ee7597bdce796490f3ee09211df48ba1d11f6e2f5b255f05cc0ba176). The file is signed by TrustAsia (Exhibit 2).

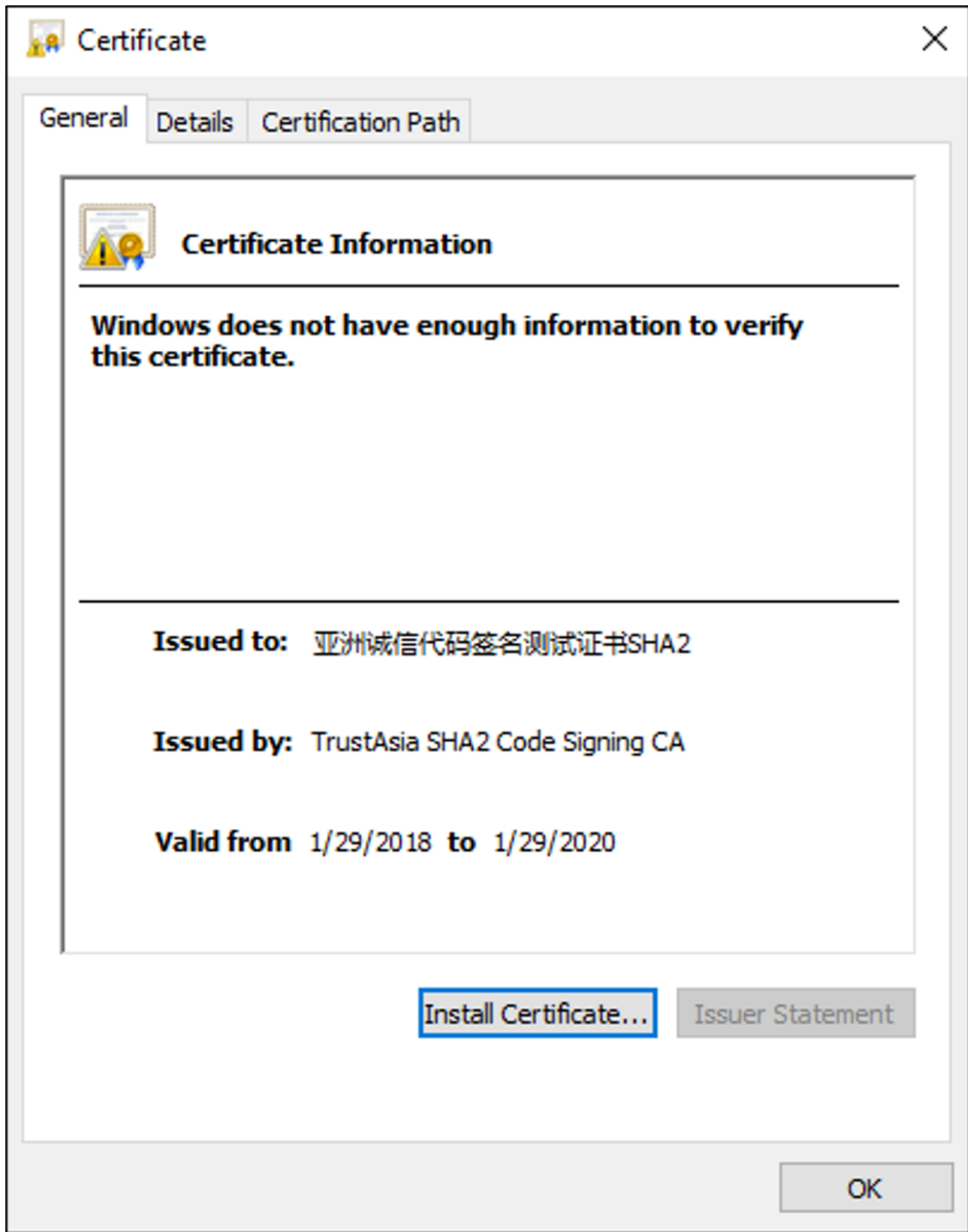
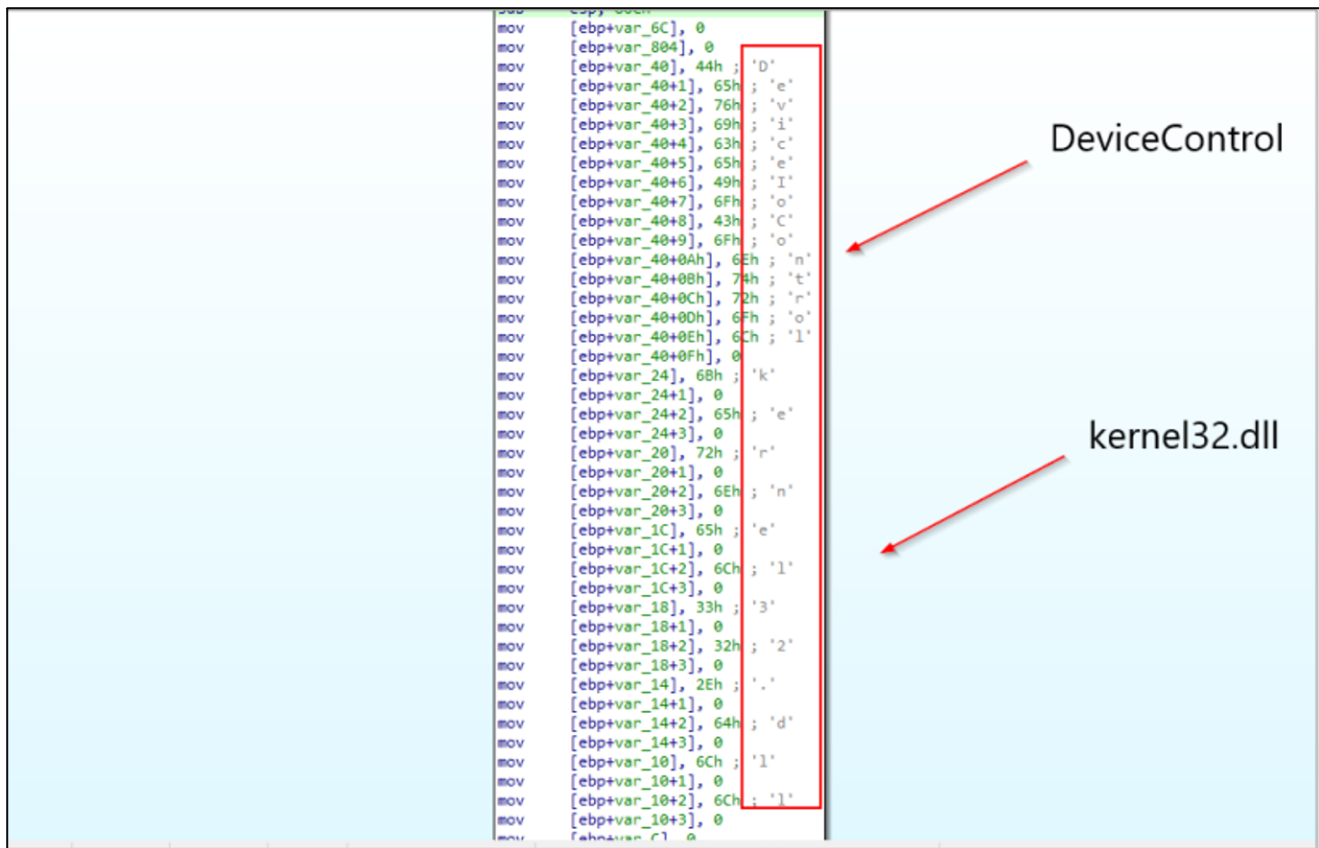


Exhibit 2: Digital Signature details

The wiper uses stackstrings, which is the technique used by malware developers to “conceal” the strings from an analyst (Exhibit 3).



The image shows a snippet of assembly code with stackstrings. A red box highlights the string 'DeviceControl' stored in memory. Two red arrows point from the labels 'DeviceControl' and 'kernel32.dll' to their respective locations in the code.

```
mov [ebp+var_6C], 0
mov [ebp+var_804], 0
mov [ebp+var_40], 44h ; 'D'
mov [ebp+var_40+1], 65h ; 'e'
mov [ebp+var_40+2], 76h ; 'v'
mov [ebp+var_40+3], 69h ; 'i'
mov [ebp+var_40+4], 63h ; 'c'
mov [ebp+var_40+5], 65h ; 'e'
mov [ebp+var_40+6], 49h ; 'I'
mov [ebp+var_40+7], 6Fh ; 'o'
mov [ebp+var_40+8], 43h ; 'C'
mov [ebp+var_40+9], 6Fh ; 'o'
mov [ebp+var_40+0Ah], 6Eh ; 'n'
mov [ebp+var_40+0Bh], 74h ; 't'
mov [ebp+var_40+0Ch], 72h ; 'n'
mov [ebp+var_40+0Dh], 6Fh ; 'o'
mov [ebp+var_40+0Eh], 6Ch ; 'l'
mov [ebp+var_40+0Fh], 0
mov [ebp+var_24], 68h ; 'k'
mov [ebp+var_24+1], 0
mov [ebp+var_24+2], 65h ; 'e'
mov [ebp+var_24+3], 0
mov [ebp+var_20], 72h ; 'r'
mov [ebp+var_20+1], 0
mov [ebp+var_20+2], 6Eh ; 'n'
mov [ebp+var_20+3], 0
mov [ebp+var_1C], 65h ; 'e'
mov [ebp+var_1C+1], 0
mov [ebp+var_1C+2], 6Ch ; 'l'
mov [ebp+var_1C+3], 0
mov [ebp+var_18], 33h ; '3'
mov [ebp+var_18+1], 0
mov [ebp+var_18+2], 32h ; '2'
mov [ebp+var_18+3], 0
mov [ebp+var_14], 2Eh ; '.'
mov [ebp+var_14+1], 0
mov [ebp+var_14+2], 64h ; 'd'
mov [ebp+var_14+3], 0
mov [ebp+var_10], 6Ch ; 'l'
mov [ebp+var_10+1], 0
mov [ebp+var_10+2], 6Ch ; 'l'
mov [ebp+var_10+3], 0
mov [ebp+var_0C], 0
```

Exhibit 3: Stackstrings used in CaddyWiper

The wiper checks if the infected machine is a Domain Controller via the **DsRoleGetPrimaryDomainInformation** API. The API gets state data for the computer, which includes the state of the directory service installation and domain data. If the infected machine is not a Domain Controller, the malware recursively wipes the files in *C:\Users* and *D:\* directories. Additionally, CaddyWiper attempts to wipe the files in the driver letters alphabetically starting from *D:\* drive until it reaches *Z:\* drive (Exhibit 4).

While running the sample on the sandbox machine, the malware did not wipe all the files completely in the mentioned folders, except for shortcut files. The sample also skips wiping the files under *C:\* drive.

```

strcpy((char *)v9, "k");
strcpy((char *)&v9[1], "e");
strcpy(v10, "r");
strcpy(&v10[2], "n");
strcpy(v11, "e");
strcpy(&v11[2], "l");
strcpy(v12, "3");
strcpy(&v12[2], "2");
strcpy(v13, ".");
strcpy(&v13[2], "d");
strcpy(v14, "l");
strcpy(&v14[2], "l");
v14[4] = 0;
v14[5] = 0;
strcpy(v4, "advapi32.dll");
strcpy(v7, "LoadLibraryA");
v6 = PEB_ldr(v9, v7);
strcpy(v2, "netapi32.dll");
((void (__stdcall *)(char *))v6)(v2);
Buffer = 0;
result = DsRoleGetPrimaryDomainInformation(0, DsRolePrimaryDomainInfoBasic, &Buffer);
if ( *(_DWORD *)Buffer != 5 )
{
    ((void (__stdcall *)(char *))v6)(v4);
    strcpy(v3, "C:\\Users");
    wiping_files((int)v3);
    strcpy(v8, "D:\\");
    for ( i = 0; i < 24; ++i )
    {
        wiping_files((int)v8);
        ++v8[0];
    }
    return wiping_physical_drive();
}
return result;
}

```

*Exhibit 4: CaddyWiper wipes the drives from D to Z letters*

If the infected machine is the Domain Controller, the wiper will exit (Exhibit 5).

00DA113A	FF15 0030DA00	call dword ptr ds:[&&DsRoleGetPrimaryDomainInformation]	
00DA1140	8B4D C8	mov ecx,dword ptr ss:[ebp-38]	
00DA1143	8339 05	cmp dword ptr ds:[ecx],5	
EIP	00DA1146	jne caddywiper.DA114A	
00DA1148	EB 7A	jmp caddywiper.DA11C4	
00DA114A	8D55 B8	lea edx,dword ptr ss:[ebp-48]	
00DA114D	52	push edx	
00DA114E	FF55 CC	call dword ptr ss:[ebp-34]	
00DA1151	C645 AC 43	mov byte ptr ss:[ebp-54],43	43:'C'
00DA1155	C645 AD 3A	mov byte ptr ss:[ebp-53],3A	3A:':'
00DA1159	C645 AE 5C	mov byte ptr ss:[ebp-52],5C	5C:'\'
00DA115D	C645 AF 55	mov byte ptr ss:[ebp-51],55	55:'U'
00DA1161	C645 B0 73	mov byte ptr ss:[ebp-50],73	73:'s'
00DA1165	C645 B1 65	mov byte ptr ss:[ebp-4F],65	65:'e'
00DA1169	C645 B2 72	mov byte ptr ss:[ebp-4E],72	72:'r'
00DA116D	C645 B3 73	mov byte ptr ss:[ebp-4D],73	73:'s'
00DA1171	C645 B4 00	mov byte ptr ss:[ebp-4C],0	
00DA1175	8D45 AC	lea eax,dword ptr ss:[ebp-54]	
00DA1178	50	push eax	
00DA1179	E8 22110000	call <caddywiper.sub_DA22A0>	
00DA117E	83C4 04	add esp,4	
00DA1181	C645 E0 44	mov byte ptr ss:[ebp-20],44	44:'D'
00DA1185	C645 E1 3A	mov byte ptr ss:[ebp-1F],3A	3A:':'
00DA1189	C645 E2 5C	mov byte ptr ss:[ebp-1E],5C	5C:'\'
00DA118D	C645 E3 00	mov byte ptr ss:[ebp-1D],0	
00DA1191	C745 98 00000000	mov dword ptr ss:[ebp-68],0	
00DA1198	EB 09	jmp caddywiper.DA11A3	
00DA119A	8B4D 98	mov ecx,dword ptr ss:[ebp-68]	
00DA119D	83C1 01	add ecx,1	
00DA11A0	894D 98	mov dword ptr ss:[ebp-68],ecx	
00DA11A3	837D 98 18	cmp dword ptr ss:[ebp-68],18	
00DA11A7	73 16	jae caddywiper.DA11BF	
00DA11A9	8D55 E0	lea edx,dword ptr ss:[ebp-20]	
00DA11AC	52	push edx	
<			

Jump is not taken  
caddywiper.00DA114A

.text:00DA1146 caddywiper:51146 #546

Exhibit 5: The malware doesn't proceed with executing the wiping instructions on a Domain Controller

The jump to the function responsible for wiping the files is not taken. Instead, it will exit via the **RtlExitUserThread** command (Exhibit 6).

EIP	752662C4	50	push eax	
	752662C5	FF15 A4182D75	call dword ptr ds:[&RtlExitUserThread]	
	752662CB	FF15 E8192D75	call dword ptr ds:[&RtlGetSuiteMask]	
	752662D4	5C	pop eax	

The jump to the function responsible for wiping the files is not taken. Instead, it will exit via the **RtlExitUserThread** command (Exhibit 6).

The wiper enumerates through the files, takes ownership of the files overrides File Permissions with **SeTakeOwnershipPrivilege** and **AdjustTokenPrivileges** APIs and overwrites 10485760 bytes of data with zeroes (Exhibit 7).

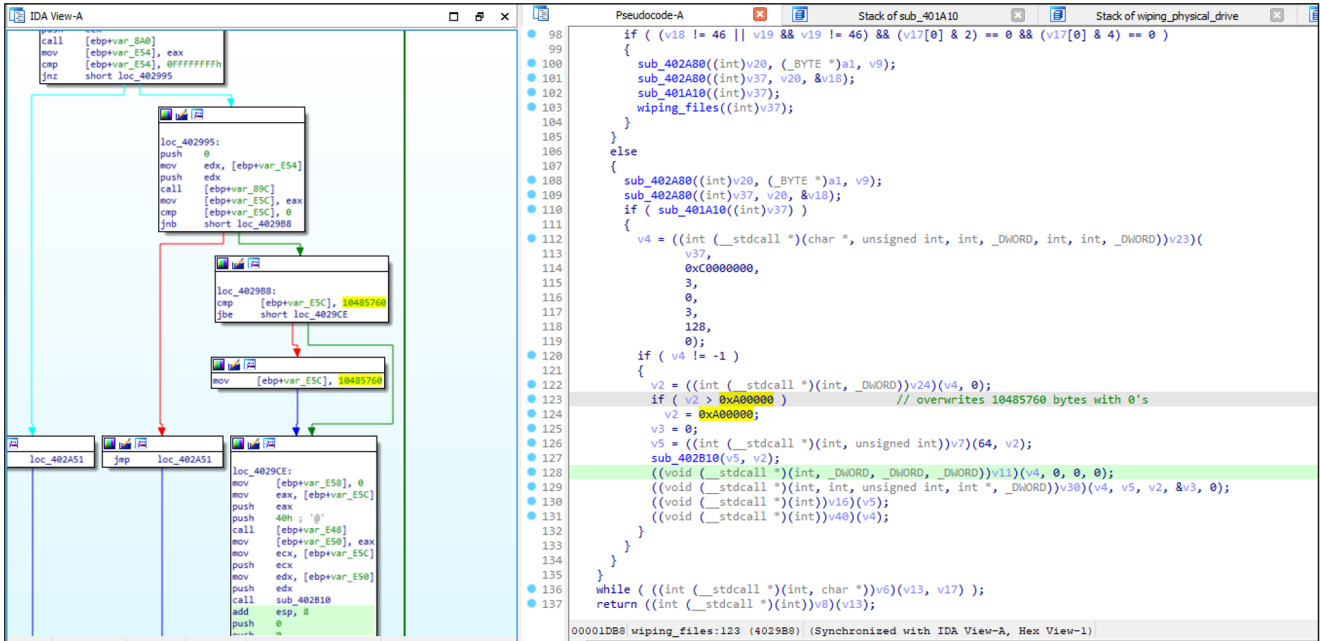


Exhibit 7: The wiper is overwriting 10485760 bytes of data with 0's

After the malware finishes overwriting the files, it uses the **DeviceIoControl** API with the control code **IOCTL\_DISK\_SET\_DRIVE\_LAYOUT\_EX** to access the extended information about the drive's partitions (decrements from Physical Drive 9 to Physical Drive 0). Specifically, it accesses the data on the Master Boot Record (MBR) and GUID Partition Table (GPT) partitions of the hard drives to proceed with the wiping process.

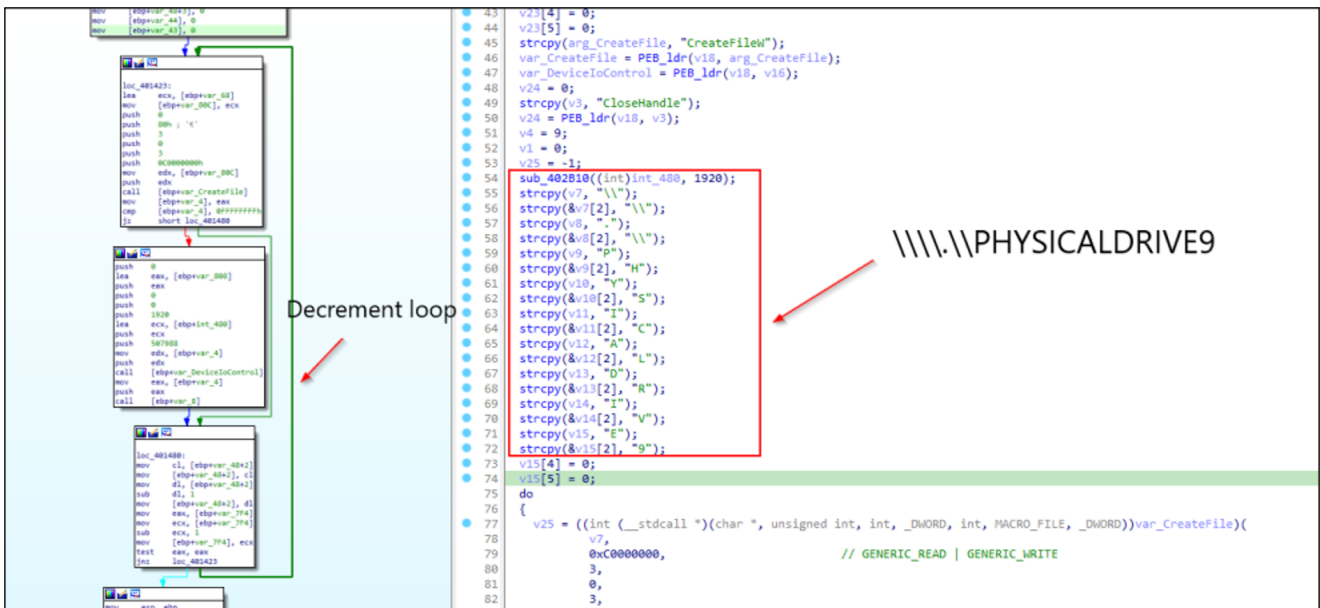


Exhibit 8: Decrementing loop (the wiper decrements the drives from 9 to 0)

We assess that the wiper sample does not have any similarities with the previous wipers (WhisperGate, HermeticWiper, IsaacWiper) that were used to target Ukrainian organizations. The only distinctive characteristic of CaddyWiper is that it does not target Domain



Controllers. We believe it's probable that this is done to keep the foothold on the Domain Controller to gain access to other machines on the network and that CaddyWiper was developed within one month or less.

## What eSentire is doing about it

---

Our Threat Response Unit (TRU) combines threat intelligence gleaned from research, security incidents, and the external threat landscape to create actionable outcomes for our customers. We are taking a holistic response approach to combat all malware by deploying countermeasures, such as:

- Implementing the detections to identify CaddyWiper malware activities across eSentire MDR for Endpoint solutions.
- Performing global threat hunts against the IOCs associated with the CaddyWiper malware
- Actively monitoring for any signs of compromise.

Our detection content is backed by investigation runbooks, ensuring our SOC cyber analysts respond rapidly to any intrusion attempts. In addition, our Threat Response Unit closely monitors the threat landscape and addresses capability gaps and conducts retroactive threat hunts to assess customer impact.

## Recommendations from eSentire's Threat Response Unit (TRU)

---

We recommend implementing the following controls to help secure your organization against the CaddyWiper malware:

- Address security issues in Active Directory: thoroughly reviewing and securing SYSVOL permissions, patching any known vulnerabilities, implementing Least-Privilege Administrative Models.
- If working with organizations based in Ukraine, perform access control review on the traffic.
- Confirm that all the devices are protected with Endpoint Detection and Response (EDR) solutions.

While the Tactics, Techniques, and Procedures (TTPs) used by adversaries grow in sophistication, they lead to a limited set of choke points at which critical business decisions must be made. Intercepting the various attack paths utilized by the modern threat actor requires actively monitoring the threat landscape, developing, and deploying endpoint detection, and the ability to investigate logs & network data during active intrusions.

eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced

threats.

If you're not currently engaged with an MDR provider, eSentire MDR can help you reclaim the advantage and put your business ahead of disruption.

Learn what it means to have an elite team of Threat Hunters and Researchers that works for you. [Connect](#) with an eSentire Security Specialist.

## Appendix

---

### Sources

---

#### Indicators of Compromise

---

Name	File Hash (SHA-256)
CaddyWiper	ea6a416b320f32261da8dafcf2faf088924f99a3a84f7b43b964637ea87aef72
CaddyWiper	a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
CaddyWiper	1e87e9b5ee7597bdce796490f3ee09211df48ba1d11f6e2f5b255f05cc0ba176
CaddyWiper (UPX packed)	f1e8844dbfc812d39f369e7670545a29efef6764d673038b1c3edd11561d6902

#### Yara Rules

---

```
import "pe"
import "hash"
import "math"
rule CaddyWiper_1: detection
CaddyWiper_a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
{
condition:
    for any i in (0..pe.number_of_sections - 1): (
        hash.md5(pe.sections[i].raw_data_offset,
            pe.sections[i].raw_data_size) ==
            "f0d4c11521fc3891965534e6c52e128b" and
            pe.sections[i].name == ".text") and
    for any i in (0..pe.number_of_sections - 1): (
        math.entropy(pe.sections[i].raw_data_offset, pe.sections[i].raw_data_size) >=
5 and
        pe.sections[i].name == ".text") and
        pe.imports("netapi32.dll", "DsRoleGetPrimaryDomainInformation") and
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
        filesize < 11KB
}
```

```
rule CaddyWiper: detection CaddyWiper_2
{
meta:
    hash = "f1e8844dbfc812d39f369e7670545a29efef6764d673038b1c3edd11561d6902"
strings:
    $packer = "UPX0" ascii nocase
    $packer1 = "UPX1" ascii nocase
    $packer2 = "UPX2" ascii nocase
    $function = "DsRoleGetPrimaryDomainInformation" ascii nocase
condition:
    uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550
    and (3 of ($packer*) and $function)
    and filesize < 26KB
}
```

## Skip To:

---

- Key Takeaways
- Case Study
- Technical Analysis on CaddyWiper
- What eSentire is doing about it
- Recommendations from eSentire's Threat Response Unit (TRU)
- Appendix