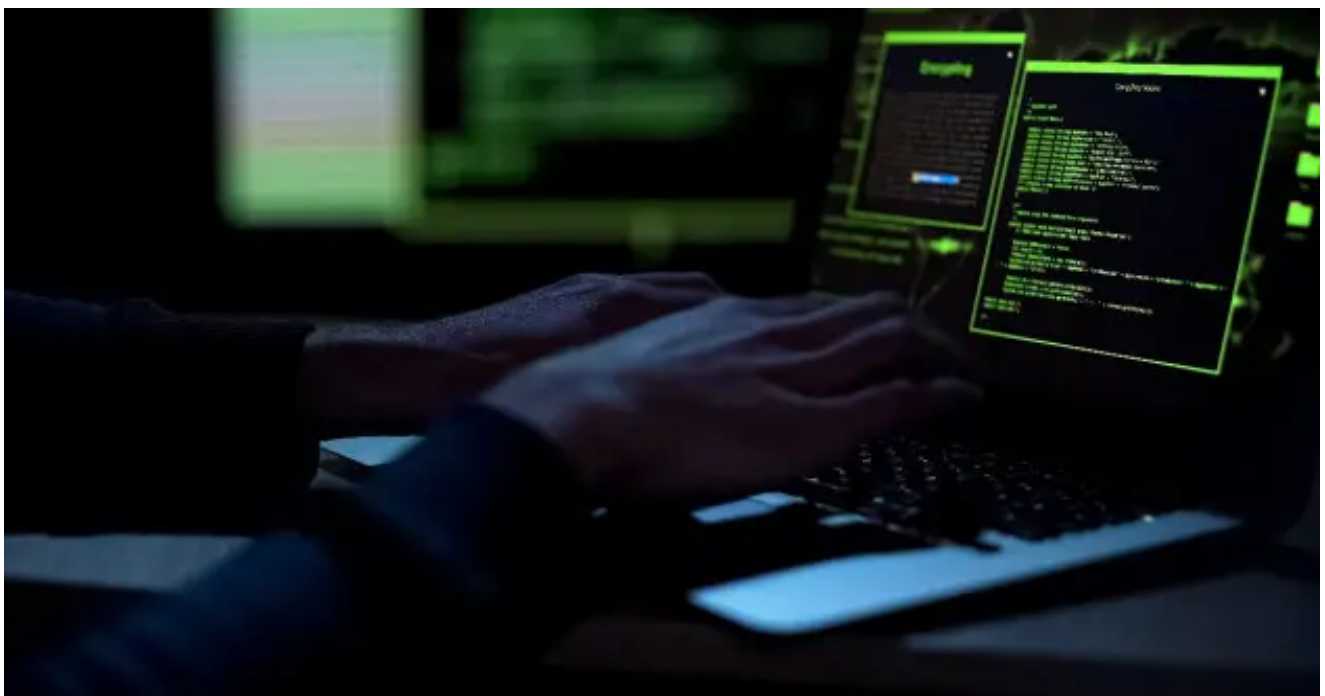
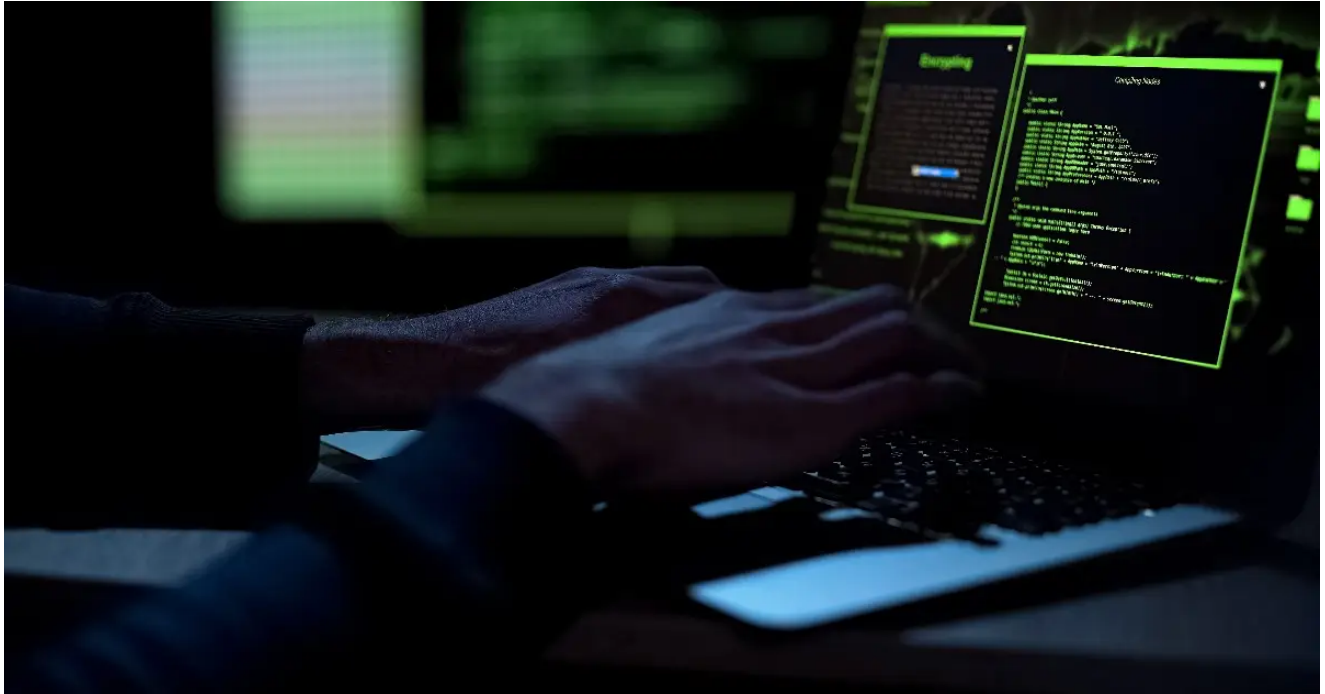


New Destructive Malware Used In Cyber Attacks on Ukraine

 securityintelligence.com/posts/new-destructive-malware-cyber-attacks-ukraine/



Malware February 24, 2022

By Christopher Del Fierro co-authored by John Dwyer 8 min read

This post was written with contributions from IBM Security X-Force's Anne Jobmann, Claire Zaboeva and Richard Emerson.

February 25, 2022 Update

On February 24 2022, Symantec Enterprise [reported](#) a ransomware dubbed as PartyTicket was deployed alongside the HermeticWiper malware. IBM Security X-Force obtained a sample of the PartyTicket ransomware and has provided technical analysis, indicators of compromise, and detections within the PartyTicket section of this blog.

On February 23, 2022, open-source intelligence sources began [reporting](#) detections of a wiper malware — a destructive family of malware designed to permanently destroy data from the target — executing on systems belonging to [Ukrainian organizations](#). IBM Security X-Force obtained a [sample](#) of the wiper named HermeticWiper. It uses a benign partition manager driver (a copy of *empntdrv.sys*) to perform its wiping capabilities corrupting all available physical drives' Master Boot Record (MBR), partition, and file system (FAT or NTFS).

This is not the first wiper malware targeting Ukrainian organizations X-Force has analyzed. In January 2022, X-Force analyzed the [WhisperGate malware](#) and did not identify any code overlaps between WhisperGate and HermeticWiper.

This blog post will detail IBM Security X-Force's insights into the HermeticWiper malware, technical analysis of the sample, and indicators of compromise (IoC) to help organizations protect themselves from this malware.

Why This Is Important

In January 2022, X-Force analyzed the [WhisperGate malware](#). HermeticWiper is the second newly seen destructive malware family observed in the past two months targeting organizations in Ukraine, and reportedly other countries in Eastern Europe. No code overlaps were identified between WhisperGate and HermeticWiper.

The pace at which these new, destructive malware families are being deployed and discovered is unprecedented, and further highlights the need for organizations to have an active and informed defense strategy that expands beyond signature-based defenses.

As the conflict in the region continues to evolve and given the destructive capabilities of both WhisperGate and HermeticWiper, IBM Security X-Force recommends critical infrastructure organizations within the targeted region fortify defenses. Those organizations should focus on preparation for potential attacks that can destroy or encrypt data or otherwise significantly impact operations.

It is of X-Force's opinion that destructive cyber attacks will likely continue to be leveraged against civilian targets in support of hybrid operations. In addition, X-Force believes it is likely cyber attacks will continue to escalate and expand in parallel with the scope of the ongoing

conflict. It should be noted the increasing number of destructive capabilities focused against private industry and entities associated with the Ukraine and its perceived allies, will likely alter the cyber security environment by creating an elevated threat to regional commerce.

Analysis Details

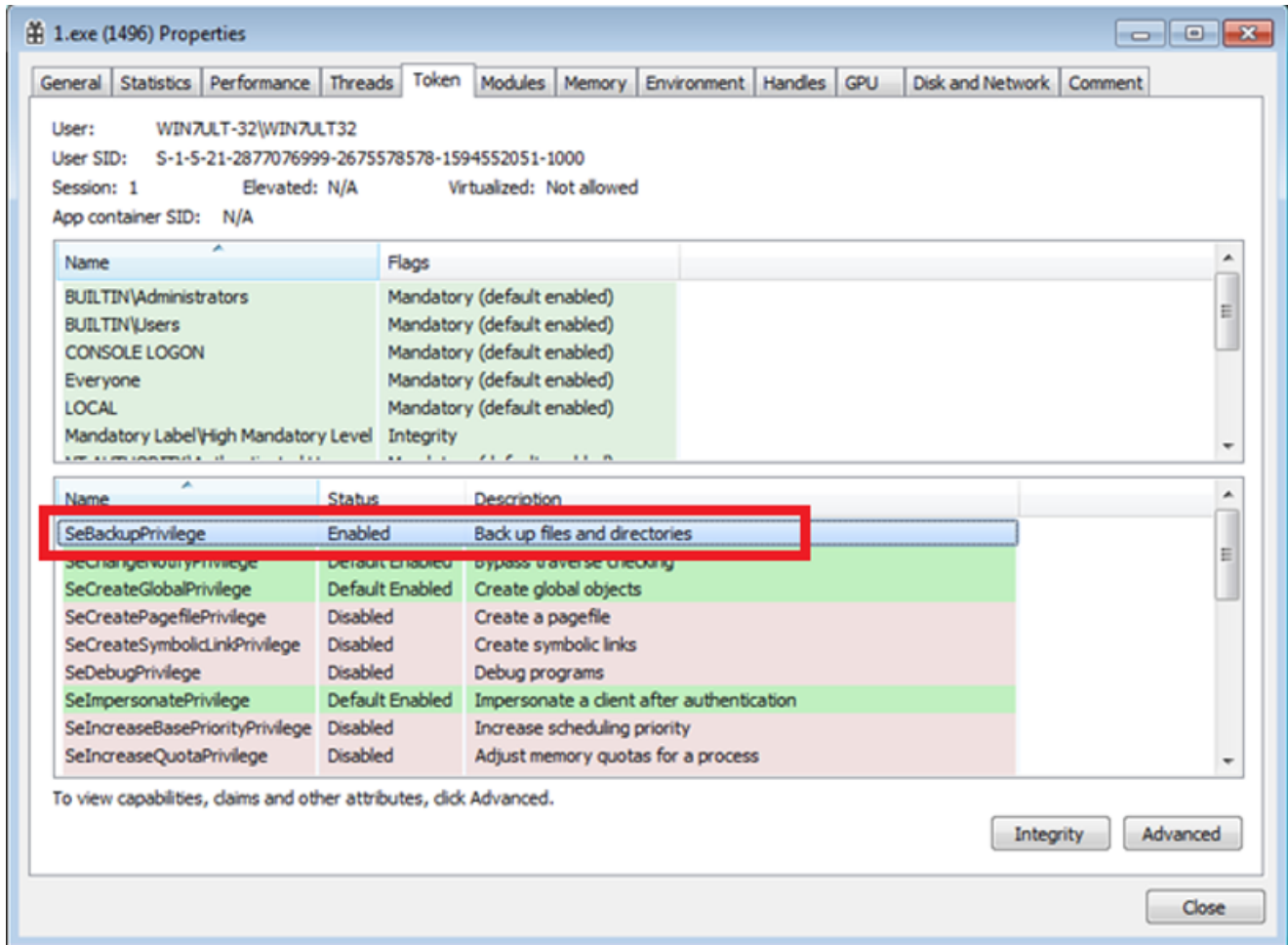
This section contains the results of the analysis performed for the submitted samples. Typical analysis includes both behavioral and static analysis.

Behavioral analysis describes the malware behavior observed on a system during execution. Behavioral analysis typically includes actions performed on the system such as files dropped, persistence, details surrounding process execution and any C2 communications. It should be noted that behavioral analysis may not capture all notable malware behavior as certain functions may only be performed by the malware under specific conditions.

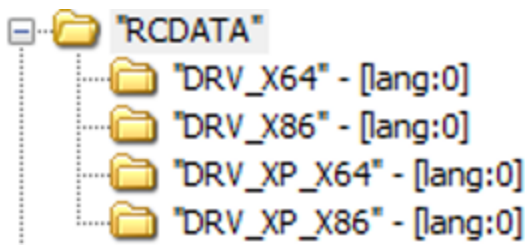
Static analysis is a deeper dive into the technical analysis of the malware. Static analysis typically includes further details about the functionality, obfuscation or packing in the sample, encryption used by the malware, configuration information or other notable technical detail.

Behavioral Analysis

Upon execution, HermeticWiper immediately adjusts its process token privileges and enables *SeBackupPrivilege*. This gives the malware read access control to any file, regardless of whatever is specified in access control list (ACL).



It then checks for the system's OS version to know which version copy of a benign partition management driver (EaseUS Partition Manager: *epmntdrv.sys*) it will use. The driver is initially Microsoft compressed (SZDD compression) and embedded in its resource named RCDATA.



For Windows XP:

- x86 – it uses DRV_XP_X86
- x64 – it uses DRV_XPX64

For Windows 7 and up:

- x86 – it uses DRV_X86
- x64 – it uses DRV_X64

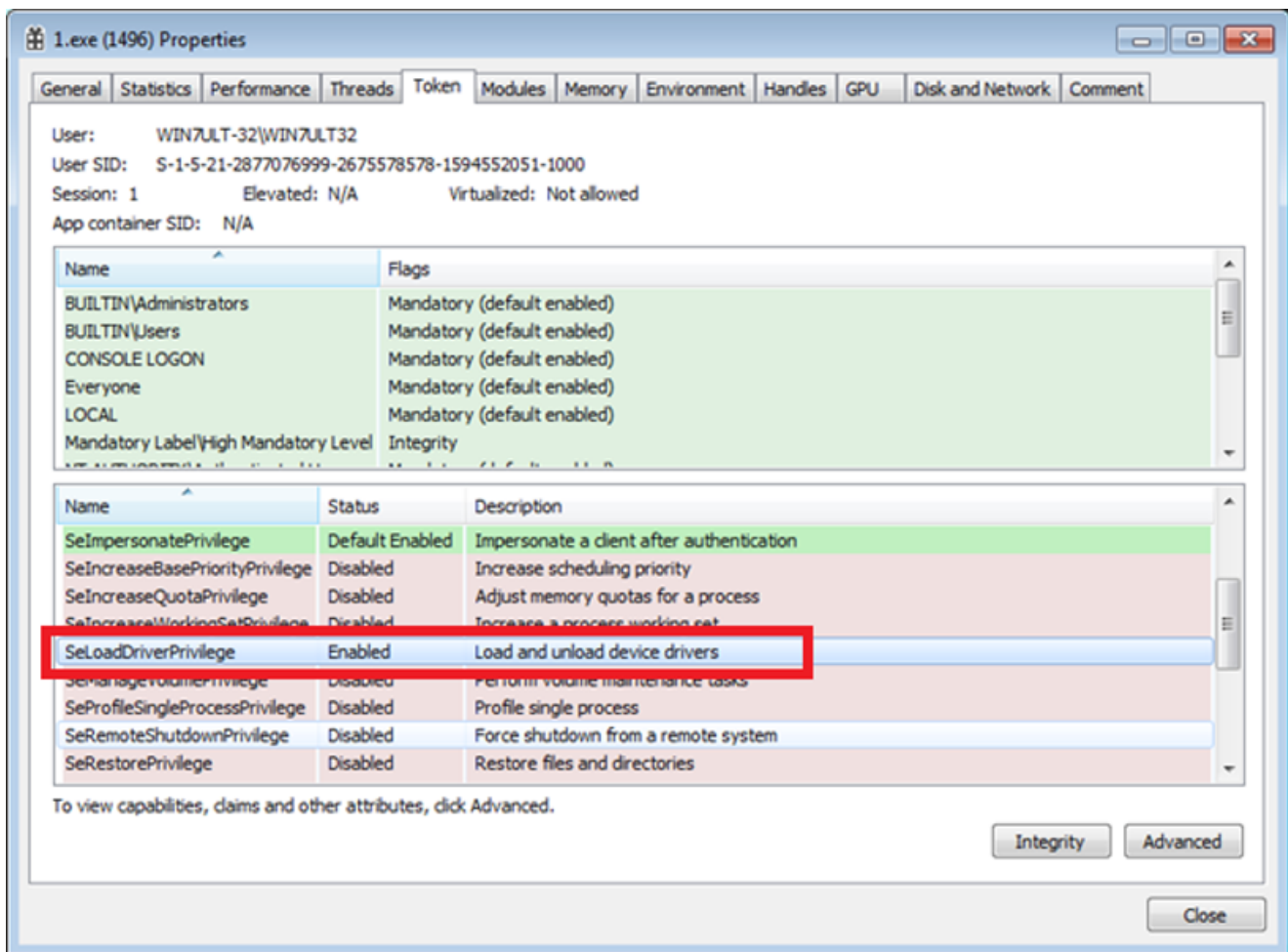
After verifying what version it will use, the SZDD compressed benign partition management driver is then dropped in the following directory as:

`%WINDIR%\system32\driver\
Example: C:\Windows\system32\Drivers\vfdr`

It then proceeds to decompress it and adds “.sys” as file extension.

Example: `C:\Windows\system32\Drivers\vfdr.sys`

It then proceeds to adjust its process token privileges again to enable *SeLoadDriverPrivilege*. This token enables the process of HermeticWiper have the ability to load and unload device drivers.



Next, it disables crash dumps by modifying the following registry key:

`HKLM\SYSTEM\CurrentControlSet\Control\CrashControl`
`CrashDumpEnabled = 0`

Note that crash dumps are memory dumps that contains information why the system stops unexpectedly. With this option disabled, the system will be prevented to create any dumps, thus successfully covering its tracks.

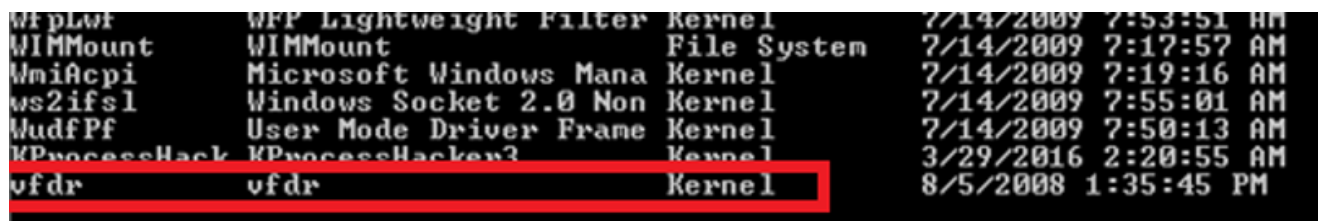
It also disables Volume Shadow Service (vss) if enabled, and disables *ShowCompColor* and *ShowInfoTip* in all HKEY_USERS registry:

```
HKEY_USERS\<<ID>\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
ShowCompColor = 0
ShowInfoTip = 0
```

ShowCompColor option displays compressed and encrypted NTFS files in color while *ShowInfoTip* shows pop-up descriptions for folder and desktop items.

HermeticWiper then proceeds to add and load the created driver as a service using Windows APIs such as *OpenSCManagerW()*, *OpenServiceW()*, *CreateServiceW()* and *StartServiceW()*.

Example:



vfpLof	vfp Lightweight Filter	Kernel	7/14/2009	7:53:51 AM
WIMMount	WIMMount	File System	7/14/2009	7:17:57 AM
WmiAcpi	Microsoft Windows Mana	Kernel	7/14/2009	7:19:16 AM
ws2ifsl	Windows Socket 2.0 Non	Kernel	7/14/2009	7:55:01 AM
MudfPf	User Mode Driver Frame	Kernel	7/14/2009	7:50:13 AM
KProcessHack	KProcessHacker3	Kernel	3/29/2016	2:20:55 AM
vfd	vfd	Kernel	8/5/2008	1:35:45 PM

This creates a service entry in the registry:

```
HKLM\SYSTEM\CurrentControlSet\services\<<random_2chars>dr
```

Once the benign driver service is started and loaded in the system, it then proceeds to cover its tracks once again by deleting the created driver in %WINDIR%\system32\drivers and deleting the created service in the registry.

HermeticWiper enumerates a range of up to 100 Physical Drives by looping 0-100. It uses the benign partition manager, now loaded in the system, to corrupt all Master Boot Record (MBR) for every Physical Drive present in the system.

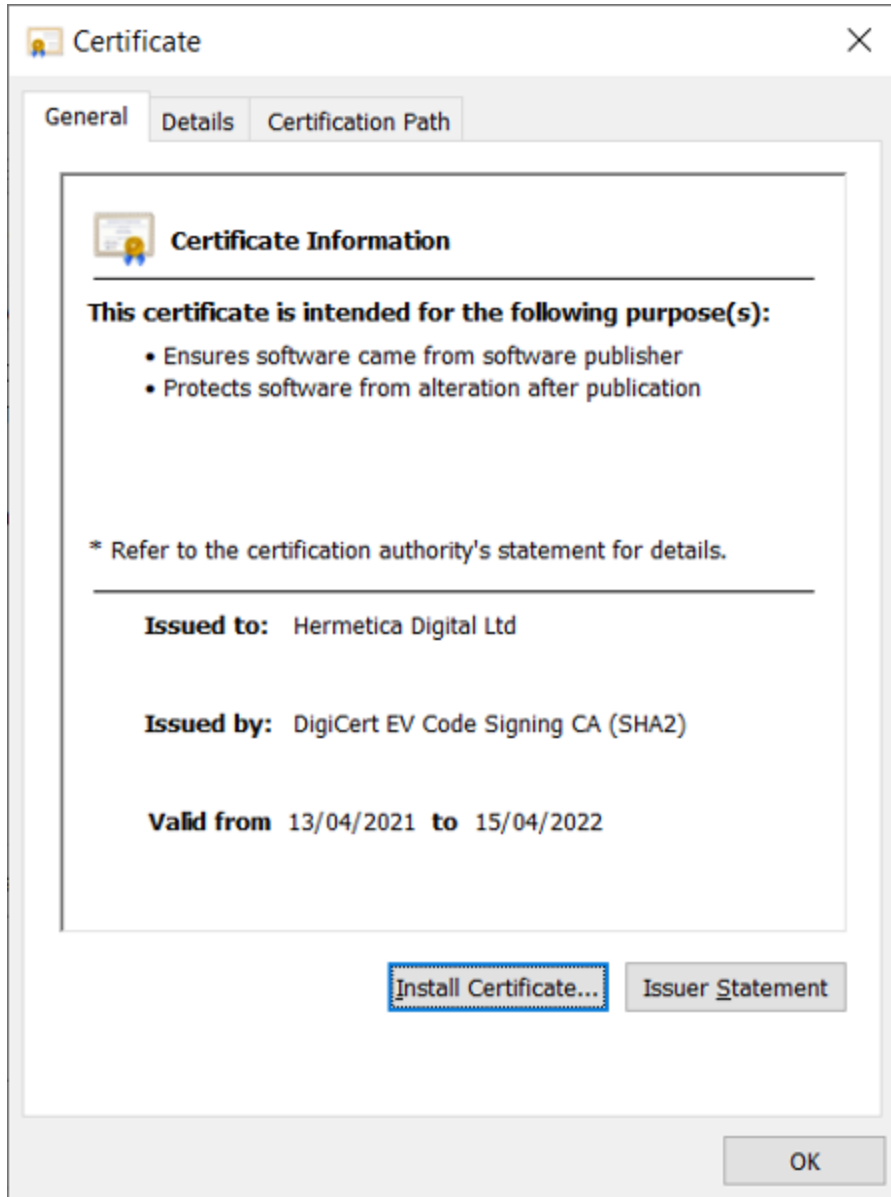
But it doesn't stop there, it also corrupts all the available partition even supporting both FAT and NTFS file system. For NTFS, it also corrupts the Master File Table (MFT) which holds all information about a file to ensure that data will be unrecoverable.

Once all disks are corrupted, the system should result to a crash, but just in case, HermeticWiper also created a fail-safe sleeping thread that triggers a system shutdown to force restart the target system.

Static Analysis

Analysis of the wiper sample revealed it was signed with a digital certificate issued to an organization named 'Hermetica Digital Ltd' and was created April 15, 2021. A digital certificate is a file or cryptographic signature that proves the authenticity of an item such as a file, server, or user.

HermeticWiper contains the following digital certificate:



Indicators of Compromise (IOCs)

Hermeticwiper

FILE SYSTEM:

`%WINDIR%\system32\driver\`

REGISTRY:

```
HKLM\SYSTEM\CurrentControlSet\Control\CrashControl
CrashDumpEnabled = 0
HKEY_USERS\<ID>\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
ShowCompColor = 0
ShowInfoTip = 0
HKLM\SYSTEM\CurrentControlSet\services\<random_2chars>dr
```

SERVICE:

```
service name: <random_2chars>dr
```

Hermetic Malware Samples

- <https://www.virustotal.com/gui/file/0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da/detection>
- <https://www.virustotal.com/gui/file/1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591>

Detection

IBM Security X-Force has developed the following Yara signature to detect additional instances of the HermeticWiper.

```
import "pe"
rule XFTI_HermeticWiper : HermeticWiper
{
meta:
author = "IBM X-Force Threat Intelligence Malware Team"
description = "Detects the wiper targeting Ukraine."
threat_type = "Malware"
rule_category = "Malware Family"
usage = "Hunting and Identification"
ticket = "IRIS-12790"
hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591"
yara_version = "4.0.2"
date_created = "24 Feb 22"
date_updated = ""
reference = ""
xfti_reference = ""
strings:
$s1 = "\\.\EPMNTDRV\%u" wide fullword
$s2 = "C:\Windows\SYSTEM32" wide fullword
$s3 = "DRV_X64" wide fullword
$s4 = "DRV_X86" wide fullword
$s5 = "DRV_XP_X64" wide fullword
$s6 = "DRV_XP_X86" wide fullword
condition:
```



```
uint16(0) == 0x5A4D and 4 of them and
pe.imports("lz32.dll", "LZOpenFileW") and
pe.imports("kernel32.dll", "FindResourceW") and
pe.imports("advapi32.dll", "CryptAcquireContextW")
}
```

PartyTicket Analysis

The ransomware sample dubbed as PartyTicket is a Golang compiled ransomware which is believed to be distributed alongside the HermeticWiper malware that targets Ukraine organizations.

PartyTicket ransomware doesn't include any escalation of privileges and will execute within the context of the current user. This means that if it was executed with a non-privileged account, folders and files requiring higher privileges will not be encrypted.

PartyTicket adds “**[].encryptedJB**” as file extension to all files it encrypts. It uses both RSA and AES to encrypt targeted files.

Initial static analysis of the ransomware reveals “Biden” and “Whitehouse” referenced within the code.

```
if ( os_Args.len == 1 )
{
    str = os_Args.array->str;
    _C__projects_403forBiden_wHiteHouseE_FileName.len = os_Args.array->len;
    if ( *( _DWORD * ) &runtime_writeBarrier.enabled )
        runtime_gcWriteBarrier();
    else
        _C__projects_403forBiden_wHiteHouseE_FileName.str = str;
    typb = ( unsigned __int128 ) _C__projects_403forBiden_wHiteHouseE_GoodOffice1();
    partyTicket_len = *( ( _QWORD * ) &typb + 1 );
    partyTicket_ptr = ( string * ) typb;
    main_voteFor403();
    for ( j = 0LL; j < partyTicket_len; j = i + 1 )
    {
        i = j;
        sync_ptr_WaitGroup_Add( _waitGroup, 1LL );
        runtime_newproc( 24, ( runtime_funcval * ) &stru_553D28 );
    }
    sync_ptr_WaitGroup_Wait( _waitGroup );
}
```

Upon execution, PartyTicket ransomware builds a list of files to encrypt by checking for all available drives from A: to Z: and traversing all directories except for those containing “Windows” and “Program Files”.

While traversing the directory structure, the ransomware enumerates a target list of files containing the following extensions:

```
.acl, .avi, .bat, .bmp, .cab, .cfg, .chm, .cmd, .com, .crt, .css, .dat,
.dip, .dll, .doc, .dot, .exe, .gif, .htm, .ico, .iso, .jpg, .mp3, .msi,
.odt, .one, .ova, .pdf, .png, .ppt, .pub, .rar, .rtf, .sfx, .sql, .txt,
.url, .vdi, .vsd, .wma, .wmv, .wtv, .xls, .xml, .xps, .zip, .docx, .epub,
.html, .jpeg, .pptx, .xlsx, .pgsql, .contact, inc
```

Note that **.exe** is included in the target file to encrypt, indicating that the ransomware will encrypt itself afterwards.

Once the target list is created, the ransomware will create a copy of itself with a universally unique identifier (UUID) name for every file within the target list. The copies are executed with a thirty-second timeout as children of the original PartyTicket process, each responsible for encrypting a file within the target file list.

Example PartyTicket child process execution lifecycle:

```
C:\Windows\system32\cmd.exe cmd /c copy <PartyTicket.exe> b6771851-a968-11eb-9f9f-000c29fc4fde.exe
b6771851-a968-11eb-9f9f-000c29fc4fde.exe.exe <target_file_to_encrypt>
timeout /t 30 && C:\Windows\system32\cmd.exe /C del <UUID>.exe
```

PartyTicket Indicators of Compromise (IOCs)

FILE SYSTEM:

```
%DESKTOP%\read_me.html
<encrypted_files>.[[email protected]].encryptedJB
```

PartyTicket Detection

IBM Security X-Force has developed the following Yara signature to help identify instances of the PartyTicket ransomware.

```
rule XFTI_PartyTicket : PartyTicket
{
meta:
author = "IBM Security X-Force "
description = "Detects the PartyTicket ransomware deployed alongside the HermeticWiper malware. The rule includes notable strings and function names."
threat_type = "Malware"
rule_category = "Malware Family"
usage = "Hunting and Identification"
hash = "4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382"
yara_version = "4.0.2"
date_created = "25 Feb 22"
strings:
```

```
$main_func1 = "pr1me"  
$main_func2 = "dtFie"  
$main_func3 = "getBoo"  
$main_func4 = "selfElect"  
$main_func5 = "highWay60"  
$main_func6 = "voteFore403"  
$main_func7 = "subscribeNewPartyMember"  
$proj_path = "/403forBiden/"  
$file_ext = ".encryptedJB"  
condition:  
uint16(0) == 0x5A4D and 7 of them  
}
```

Response

At this time, X-Force recommends organizations implement detections for the file system, registry, and Windows service indicators listed in this report as well as leveraging the provided Yara rule to scan files. Additionally, global businesses should seek to establish sound insight into their respective networks, supply chains, third parties, and partnerships that are based in, or serve in-region institutions. It is also advised that organizations open lines of communications between relevant information-sharing entities to ensure the receipt and exchange of actionable indicators.

In addition to response measures associated with the indicators of compromise, X-Force recommends organizations consider the following proactive measures:

- Block high-risk protocols on all B2B VPNs
- Implement netflow monitoring at all egress points
- Have contingency plans in place to disconnect B2B VPNs, particularly those that are high-risk
- Prevent loading of unknown driver files

If you have questions and want a deeper discussion about the malware and prevention techniques, you can [schedule a briefing here](#). Get the latest updates as more information develops on the IBM Security [X-Force Exchange](#) and the [IBM PSIRT blog](#).

If you are experiencing cybersecurity issues or an incident, contact X-Force to help.

US hotline 1-888-241-9812

Global hotline (+001) 312-212-8034

Christopher Del Fierro

X-Force IRIS Malware Reverse Engineer

Chris is a seasoned malware and threat researcher, certified system security engineer, MCP, and ethical hacker (CEHv5). Before joining IBM, Christopher was a...

think 2022



IBM Think Broadcast
Let's think together.

Watch on demand →

