eSentire Threat Intelligence Malware Analysis: HermeticWiper & PartyTicket

esentire.com/blog/esentire-threat-intelligence-malware-analysis-hermeticwiper-partyticket

Recently, there have been multiple reports of new wiper malware observed targeting Ukrainian organizations as part of cyber warfare stemming from the ongoing Russia-Ukraine conflict. This new wiper malware, also known as HermeticWiper, was first detected in February 2022, and was deployed after a wave of multiple Distributed Denial of Service (DDoS) attacks launched by Russian threat actors against Ukrainian law enforcement and government agencies.

eSentire's Threat Intelligence team has performed a technical malware analysis on HermeticWiper and PartyTicket. This technical analysis provides a detailed breakdown of how HermeticWiper fulfills its objective of accessing the Physical Drives and encrypting the targeted filetypes in the host device and network.

With the ongoing Russia-Ukraine conflict, it's probable that threat actors from Russia and Ukraine will leverage new malware in the ongoing hybrid war and improve their malware development capabilities to evade detections.

Key Takeaways:

- HermeticWiper malware is more sophisticated than WhisperGate in terms of implementing third-party drivers to facilitate access to the Physical Drives as well as modifying its access token to enable interaction with the kernel.
- HermeticWiper is abusing legitimate EaseUS partition management drivers to retrieve partition information and destroy data. This shows development maturity compared to WhisperGate.
- The main purpose of the decoy ransomware (PartyTicket, also known as HermeticRansom) is to limit the victim's interactions with the infected system.
- Due to the poor implementation of the encryption algorithm or the coding error, PartyTicket cannot be considered as a sophisticated decoy ransomware, but it certainly made more improvements compared to WhisperGate.
- The threat actor(s) behind HermeticWiper prevented the possibility of recovery by deleting shadow copies. It's probable that this was done to clear logs to avoid detection and attribution.
- As a result of this research, we have created an additional 5 detections to reduce the risk of this threat and are performing global threat hunts for indicators associated with HermeticWiper & Party Ticket malware.

Case Study

The destructive malware dubbed as 'HermeticWiper' by SentinelLabs was first detected by researchers at ESET on February 23rd, 2022, at 10am EST. Five hours later, the Cyber Police of Ukraine reported DDoS attacks on several Ukrainian government agencies, including Cabinet of Ministers of Ukraine, Verkhovna Rada (unicameral parliament of Ukraine), Security Service of Ukraine, Ministry of Foreign Affairs, and other Ukrainian government organizations.

The reports stated that the DDoS attacks had been ongoing since February 15th and linked the attacks, including numerous phishing attempts, to Russian threat actors. As part of these attacks, HermeticWiper was installed on hundreds of machines in Ukraine, but evidence of HermeticWiper was also found in Lithuania and Latvia.

On February 27th Ukrainian border control was reported to be infected with HermeticWiper, which prevented refugees from being able to cross into Romania. Symantec also reported that the ransomware named PartyTicket was dropped on the compromised machines.

Initial Compromise

On February 24-25th researchers at Symantec reported three potential initial vectors of compromise:

1. Ukraine, December 23, 2021 – The abuse of SMB on Microsoft Exchange Servers followed by credential stealing and web shell.
2. Lithuania, November 12, 2021 – Tomcat exploitation followed by the creation of scheduled tasks to gain persistence on the compromised system.
3. Ukraine, November 11, 2021 – An exploit abusing Microsoft SQL Elevation of Privilege Vulnerability (CVE-2021-1636).

Technical Analysis on HermeticWiper

SHA-256: 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

HermeticWiper is a 32-bit executable written in C++ and at 114 KB, it's over four times bigger than its predecessor, WhisperGate (27 KB). WhisperGate was also used as a decoy ransomware and destructive malware in January 2022 to target Ukrainian organizations. The compiler timestamp dates to December 28, 2021. However, it should be noted that the timestamp can be easily modified by the threat actors. The malware sample was signed by Hermetica Digital Ltd, a Cyprus-based company, and is valid from April 12, 2021 until April 14, 2022 (Exhibit 1). Based on this discovery, eSentire's Threat Intelligence team has determined it's probable that the malware was developed in April 2021.

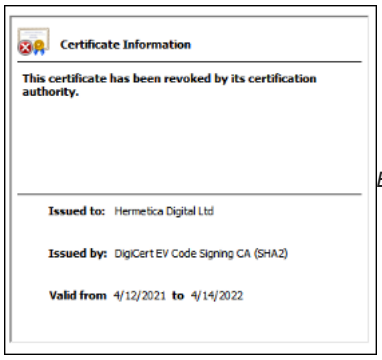

Exhibit 1: HermeticWiper digital signature

The RCDATA resource (the raw data resource of an application) contains 4 drivers: **DRV_X64, DRV_X86, DRV_XP_X64, DRV_XP_X86**. The drivers are compressed with SZDD (Haruhiko Okumura's LZSS), a compression algorithm known to be used by Microsoft installation programs (Exhibit 2).

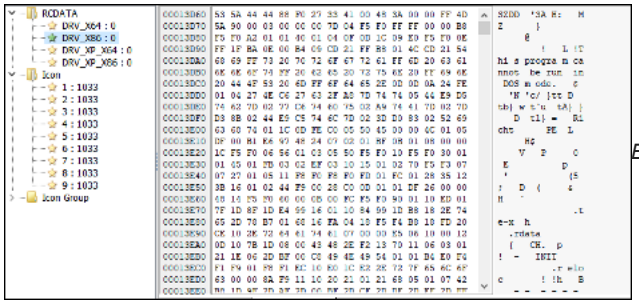

Exhibit 2: HermeticWiper Resources

The decompressed drivers are signed by Chengdu YIWO Tech Development Co Ltd, the developer of EaseUS (Exhibit 3).

Exhibit 3: Digital Certificate of the extracted drivers

The implementation of EaseUS partition management driver in the wiper to access the file systems shows an improvement compared to WhisperGate. The drivers contain the program database (PDB) path, which contains debugging information, to: *d:\epm_epm_main\mod.windiskaccessdriver\windiskaccessdriver\objfre_wlh_x86\i386\epmntdrv.pdb*

This indicates that the attackers abused the legitimate driver *epmntdrv.sys* developed by EaseUS to facilitate access to the physical drives of the victim's machine.

The wiper will choose which driver to plant on the victim's machine based on the Windows version, which uses major and minor conventions for its Operating Systems (OS). If the major and minor versions of the OS is greater or equal to 6 and 0 respectively, it will assign the **DRV_X64, DRV_X86** drivers to it. Otherwise, it will assign **DRV_XP_X64, DRV_XP_X86** drivers (Exhibit 4).

Please refer to the chart compiled by Microsoft that contains operating system version information for more information.

```
memset(&VersionInformation, 0, sizeof(VersionInformation));
VersionInformation.dwOSVersionInfoSize = 284;
VersionInformation.dwMajorVersion = 6;
VersionInformation.dwMinorVersion = 0;
v5 = VerSetConditionMask(0i64, 2u, 3u);
v6 = VerSetConditionMask(v5, 1u, 3u);
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");
}
```

Exhibit 4: Assigning drivers to the appropriate OS

The wiper then assigns itself the following privileges:

- **SeLoadDriverPrivilege –** enables the user to unload and load device drivers in kernel mode. In our case, this will allow the threat actor to load the EaseUS drivers used to corrupt and destroy data.
- **SeBackupPrivilege –** provides an attacker with the ability to create system backups and full read permissions without further escalating the privileges.

A service named after the dropped system driver will be created by the wiper via the **CreateServiceW** API, which will point to *C:\Windows\System32\drivers\rhdr.sys* (Note that the driver's name will be randomly created with 4 characters). After the service has successfully started, it will sleep for 1000 milliseconds (about 1 second) and then be marked for deletion, at which point the user cannot manually delete or stop it.

EPMNTDRV will be pointed to the path of the dropped system driver (Exhibit 5), and will also be used to retrieve the Physical Drive number via DeviceIoControl API (used to get information about the drive).

```
wnsprintfW(Destination, 260, L"\\\\.\\EPMNTDRV\\%u", 0);
ptr_driver_num = (void *)get_driver_num(Destination, 0, 0);
if ( !ptr_driver_num || ptr_driver_num == (void *)-1 )
{
  *(_DWORD *)Data = &pszDest[v38];
  if ( GetSystemDirectoryW(*(LPWSTR *)Data, 0x104u) )
  {
    PathAppendW(pszDest, L"Drivers");
    PathAddBackslashW(pszDest);
    v38 = 26;
    v12 = &pszDest[wcslen(pszDest)];
```

Exhibit 5: EPMTDRV pointing to the dropped driver

HermeticWiper initiates a loop that enumerates the Physical Drives to 100, in contrast to WhisperGate's loop which is repeated up to 199 times (Exhibit 6). For every enumerated Physical Drive, the wiper will overwrite the first section of the master boot record (MBR) with 512 bytes, making the machine unbootable upon manual restart.

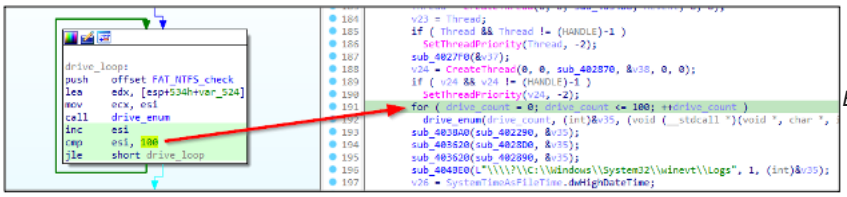

Exhibit 6: Drive Enumeration

In addition to the drive enumeration, the wiper also looks for the following folders:

- Desktop
- My Documents
- AppData
- C:\Documents and Settings
- C:\Windows\System32\winevt\Logs
- Windows
- Program Files
- Program Files(x86)
- PerfLogs
- Boot
- System Volume Information
- AppData

Boot and System Volume Information are two important folders that are responsible for Windows operability. Boot folder stores the Boot Configuration Data (BCD) which contains information about the OS and boot parameters. Without the BCD file, Windows will not be able to boot. The System Volume Information folder is utilized by the System Restore tool to store the restore points.

The purpose of enumerating the above folders is unclear. It is notable that the threat actors crafted the malware to make sure all the folders and logs are wiped, and that the victim's machine remains inoperable if the MBR wiping goes wrong. We believe it's probable that this was done to clear logs to avoid detection and attribution.

Next, the crash dump logging is disabled by setting the registry value CrashDumpEnabled to 0 (Exhibit 7).

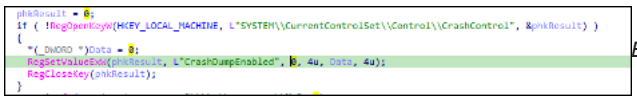

Exhibit 7: Disabling crash dump by setting the registry key to 0

The Volume Shadow Copy Service (VSS) is also disabled via ChangeServiceConfigW API (the API allows to change the service configurations) through the **SERVICE_DISABLED** parameter (Exhibit 8).

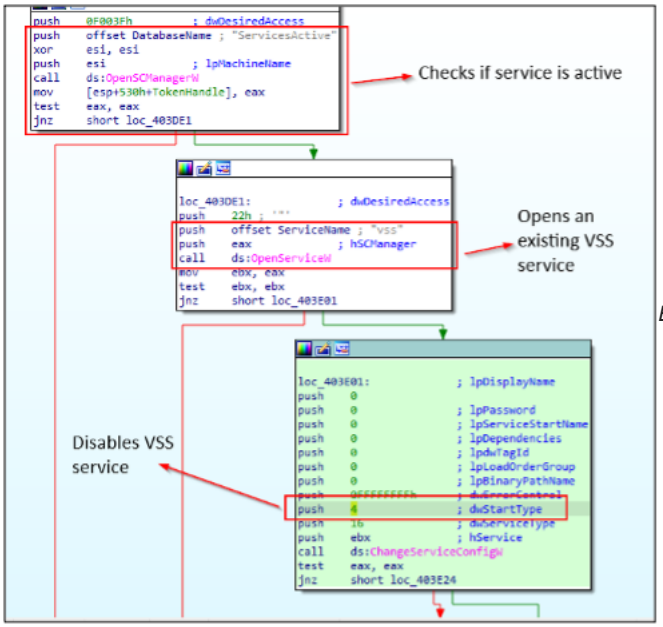

Exhibit 8: Disabling Volume Shadow Copy Service (VSS)

The sample also queries for NTFS attribute types and metadata:

- $DATA
- $I30
- $INDEX_ALLOCATION
- $Bitmap (Keeps track of cluster allocation on NTFS volume)
- $Logfile (Logs all changes to the file system)

Other attributes such as $REPARSE_POINT and $LOGGED_UTILITY_STREAM were also found in the .rdata section but were never referenced by anything. The partition corruption is dependent on whether the system has NTFS or FAT partitions (Exhibit 9).

```
v19 = 0;
*(_DWORD *)String1 = *(_DWORD *)(a2 + 3);
v18 = *(_DWORD *)(a2 + 7);
if ( lstrcmpA(String1, "NTFS    ") )
{
  *(_DWORD *)String1 = *(_DWORD *)(a2 + 54);
  v18 = *(_DWORD *)(a2 + 58);
  v19 = 0;
  if ( StrStrA(String1, "FAT")
    || (v9 = *(_DWORD *)(a2 + 82),
        v18 = *(_DWORD *)(a2 + 86),
        *(_DWORD *)String1 = v9,
        (result = (int)StrStrA(String1, "FAT")) != 0) )
  {
    v11 = *(unsigned __int16 *)(a2 + 22);
    if ( !(_WORD)v11 )
      v11 = *(_DWORD *)(a2 + 36);
    v10 = *(unsigned __int16 *)(a2 + 11);
```

Exhibit 9: Different partition corruption capabilities based on NTFS and FAT

Technical Analysis of PartyTicket

SHA-256: 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382

The ransomware sample is a 64-bit binary written in Golang with a size of 3.14 MB and an empty compilation timestamp. The following sections in the sample are responsible for determining the filetypes to encrypt, which directories to skip, drive letters to enumerate (Exhibit 10).

```
_C_projects_403forBiden_wHiteHousE_GoodOffice1                .text
_C_projects_403forBiden_wHiteHousE_baggageGatherings          .text
_C_projects_403forBiden_wHiteHousE_init                       .text
_C_projects_403forBiden_wHiteHousE_lookUp                     .text
_C_projects_403forBiden_wHiteHousE_primaryElectionProcess     .text
```

Exhibit 10: Sections mentioning “Biden”

As mentioned previously, the function at **_C__projects_403forBiden_wHiteHousE_baggageGatherings** is enumerating through the drive letters from A to Z (Exhibit 11).

```
while ( v0 < 27 )
{
  *((_QWORD *)&baggage_len + 1) = v1;
  v28 = v2;
  *(_QWORD *)&baggage_len = v3;
  r = (unsigned __int8)aAbcdefghijklmn_1[v0];
  if ( (unsigned int)r >= 0x80 )
  {
    drive_letter.str = (uint8 *)"ABCDEFGHIJKLMNOPQRSTUVWXYZ ";
    drive_letter.len = 27LL;
    a_8 = runtime_decoderune(drive_letter, v0);
    r = a_8.r;
    pos = a_8.pos;
  }
  else
  {
    pos = v0 + 1;
  }
  v26 = pos;
  v25 = r;
  v[0] = runtime_intstring((uint8 (*)[4])v22, r);
  v[1].str = (uint8 *)":\\";
  v[1].len = 2LL;
  buf = runtime_concatstring2(0LL, *(string (*)[2])&v[0].str);
  aa = os_Open(buf);
```

Exhibit 11: Drive letter enumeration

The function at **__C__projects_403forBiden_wHiteHousE_init** checks if the OS supports AVX (Advanced Vector Extensions that are supposed by Windows 7 SP1 and later) and is also responsible for folder and file manipulations as well as getting the time zone data.

The function at **_C__projects_403forBiden_wHiteHousE_FileName** gets up 55 file extensions and converts them to lower strings (Exhibit 12).

```
  while ( 1 )
  {
    if ( v2 >= 55 )
      return v3;
    path.str = input.str;
    path.len = len;
    path_filepath_Ext(path);
    v8 = strings_ToLower(s);
    v4 = v8.len;
    if ( s.len != v9[2 * v8.len] )
      goto LABEL_7;
    s.str = (uint8 *)s.len;
    runtime_memequal();
    if ( !LOBYTE(s.len) )
      break;
    v4 = v8.len;
    str_high = 1;
LABEL_6:
    len = input.len;
    v3 = str_high;
    v2 = v4 + 1;
  }
```

Exhibit 12: Retrieving file extensions

Approximately 54 file extensions get retrieved from memory for further encryption, not including the encrypted file extension, ".Encryptedjb" (Exhibit 13).

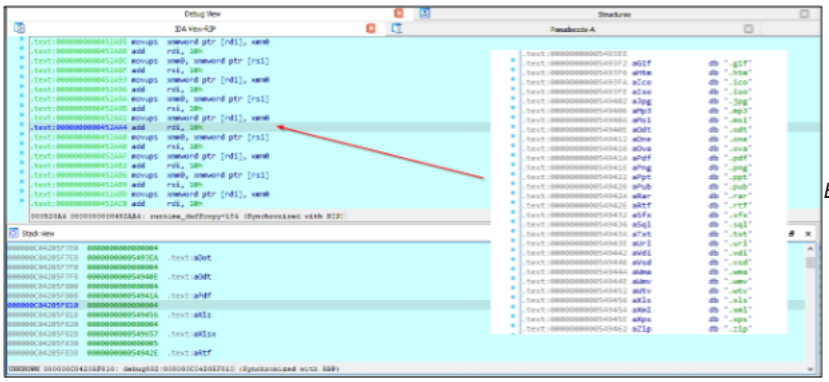

Exhibit 13: Populating the extensions from memory

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

During the encryption process, the sample writes a ransomware note called "read_me.html" to the victim's Desktop containing the contact information (Exhibit 14-15).

```
v20 = v0;
v21 = main_ContactInfo;                     // vote2024forjb@protonmail.com
v22 = main_ContactInfo2;                    // stephanie.jones2024@protonmail.com
u_8.array = (string *)&a;
u_8.len = 7LL;
u_8.cap = 7LL;
*(_QWORD *)&ua[48] = runtime_concatstrings(0LL, u_8).str;
sdf_len = perm_16.len;
sdf_ptr = perm_16.str;
*(_QWORD *)ua = "USERPROFILE";
*(_QWORD *)&ua[8] = 11LL;
*(string *)&ua[32] = os_Getenv(*(string *)ua);
*(_QWORD *)&ua[8] = *(_QWORD *)&ua[16];
*(_QWORD *)&ua[16] = *(_QWORD *)&ua[24];
*(_QWORD *)&ua[24] = "\\Desktop\\";
*(_QWORD *)&ua[32] = 9LL;
runtime_concatstring2((uint8 (*)[32])buf, *(string (*)[2])&ua[8]);
*(_QWORD *)&ua[8] = *(_QWORD *)&ua[40];
*(_QWORD *)&ua[16] = *(_QWORD *)&ua[48];
*(_QWORD *)&ua[24] = "read_me.html";
*(_QWORD *)&ua[32] = 12LL;
```

Exhibit 14: Creating read_me.html ransomware note

"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

Exhibit 15: Ransomware note (read_me.html)

The ransomware implements AES-GCM encryption for the files (Exhibit 16). An RSA public key is also used to encrypt the AES key, which is base64-encoded and embedded in the encrypted file. Here is the decoded RSA-OAEP public key with exponent 65537:

{“N”:257177505385644458758837704503150101577005970875073349074035004439130737027209399318246082709800202065660175387515

```
while ( (unsigned __int64)&nnc_len <= *(_QWORD *)(*(_QWORD *)NtCurrentTeb() + NtTib.ArbitraryUserPointer + 16LL) )
  runtime_morestack_noctxt();
cipher = crypto_aes_NewCipher(param0);
if ( cipher._r2.tab )
{
  _r2._r2.array = 0LL;
  *(_QWORD *)&_r2._r2.len = 0LL;
  _r2._r3 = cipher._r2;
}
else
{
  key_16 = crypto_cipher_NewGCM(cipher._r1);
  if ( key_16._r2.tab )
  {
    _r2._r2.array = 0LL;
    *(_QWORD *)&_r2._r2.len = 0LL;
    _r2._r3 = key_16._r2;
  }
  else
  {
```

Exhibit 16: AES-GCM encryption

The AES key is created with math/rand, which produces a pseudorandom (inevitably, deterministic) sequence of values. That means that the key can be easily obtained to decrypt the files. During the analysis, we observed the same AES 16-bit key being used to encrypt the file, *“6FBBD7P95OE8UT5QRTTEBIWAR88S74DO”*, because the same seed value is being used in the code (Exhibit 17).

All encrypted file names will have the following extension: *“.[].encryptedJB”* and each encrypted file will contain the marker *“ZVL2KH87ORH3OB1J1PO2SBHWJSNFSB4A”* at the end.

```
  if ( AES_key >> 63 << 63 )
  {
    v29 = ((2 * AES_key) >> 31) + 0xDD7B17F80LL;
    v28 &= 0x3FFFFFFFu;
  }
  v30 = 0LL;
  v25 = v28;
  v26 = v29;
  v27 = 0LL;
  if ( v28 >> 63 << 63 )
  {
    v5 = v28;
    v6 = ((2 * v28) >> 31) + 0xDD7B17F80LL;
  }
  else
  {
    v6 = v26;
    v5 = v28;
  }
  math_rand_Seed((v5 & 0x3FFFFFFF) + 1000000000 * v6 - 0x5E4DFC14C2E60000LL);
  if ( os_Args.len <= 1uLL )
    runtime_panicindex();
  encryption_JB(os_Args.array[1]);
}
```

Exhibit 17: AES key creation using math/rand

During the encryption process, the main executable creates duplicates of itself in the working directory. Each duplicate is named with a GUID in the format *“xxxxxxxx-11ec-xxx-000c29xxxxxx.exe”* (Exhibit 18) *and* will copy itself using the same pattern with a command *“cmd /c copy C:\workdir\xxxxxxxx-xxxx-11ec-xxxx-000c29xxxxxx.exe xxxxxxxx-xxxx-11ec-xxxx-000c29xxxxxx.exe* (Exhibit 19).

The duplicated binaries are responsible for encrypting each file on the system, which significantly slows down the infected system. After the encryption, the binaries are removed from the directory, leaving only 200-300 copies. The encryption process can be easily stopped by terminating the process tree.

PartyTicket.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8553557-98e9-11ec-ba98-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8543287-98e9-11ec-ba98-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8535583-98e9-11ec-ba98-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8535583-98e9-11ec-ba97-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8534277-98e9-11ec-ba97-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8516339-98e9-11ec-ba95-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8516339-98e9-11ec-ba94-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8516339-98e9-11ec-ba93-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8495715-98e9-11ec-ba6b-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8495715-98e9-11ec-ba6a-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8481557-98e9-11ec-ba62-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8481557-98e9-11ec-ba61-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8476297-98e9-11ec-ba5b-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8476297-98e9-11ec-ba5a-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8468895-98e9-11ec-ba55-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8468895-98e9-11ec-ba54-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8468895-98e9-11ec-ba53-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB
d8461220-98e9-11ec-ba53-000c29c21f00.exe	2/27/2022 5:41 PM	Application	3,218 KB

Exhibit 18: Duplicated binaries in the working directory

PartyTicket.exe	2944		Medium	8.96	182.88 MB
conhost.exe	5424	ASLR	Medium	0.97	5.8 MB
cmd.exe	4840	ASLR	Medium		4.83 MB
cmd.exe	5788	ASLR	Medium		1.41 MB
cmd.exe	8520	ASLR	Medium		1.44 MB
cmd.exe	8216	ASLR	Medium		4.27 MB
cmd.exe	8164	ASLR	Medium		2.76 MB
cmd.exe	8316	ASLR	Medium		2.5 MB
cmd.exe	8572	ASLR	Medium		4.71 MB
cmd.exe	9068	ASLR	Medium		4.7 MB
cmd.exe	8476	ASLR	Medium		1.44 MB

Exhibit 19: Duplication process

Comparing HermeticWiper, and PartyTicket to WhisperGate

From the technical analysis, we have derived that HermeticWiper is more sophisticated than WhisperGate in terms of implementing third-party drivers to facilitate access to the Physical Drives and modify its access token to enable interaction with the kernel. Moreover, the threat actor(s) behind HermeticWiper prevented the possibility of recovery by deleting shadow copies. Although the purpose of enumerating the critical parts of the OS is still not clear, we believe it's probable that this was done to clear logs to avoid detection and attribution.

As mentioned previously, PartyTicket has been observed on machines infected with HermeticWiper. The technical analysis of PartyTicket indicates that the threat actor(s) implemented AES-GCM encryption along with RSA public key for the targeted file extensions, making the attack look almost like an actual ransomware attempt, whereas WhisperGate decoy ransomware only overwrote the targeted files with 0xCC bytes and corrupted MBR by overwriting it with a fake ransom note.

PartyTicket, the decoy ransomware, contains political messages based on the strings found mentioning "Biden" and a ransom note saying, "The only thing that we learned from new elections is we learned nothing from the old!"

HermeticWiper samples have different hashes but the same functionality. WhisperGate has only one known reported hash for the wiper sample, which likely means that HermeticWiper was able to spread across more machines than WhisperGate.

With the ongoing Russia-Ukraine conflict, it's probable that threat actors from Russia and Ukraine will leverage new malware and that threat actors will likely improve their malware development capabilities to evade detection.

How eSentire is Responding

Our Threat Response Unit (TRU) combines 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 modern ransomware by deploying countermeasures, such as:

- Developing threat detections to identify the initial and post-compromise activities of HermeticWiper and PartyTicket (HermeticRansom) and ensure these detections are in place across both eSentire MDR for Endpoint and MDR for Log.
- Performing global threat hunts for indicators associated with HermeticWiper and Party Ticket malware.

Our detection content is backed by investigation runbooks, ensuring our SOC cyber analysts respond rapidly to any intrusion attempt tied to known ransomware tactics, techniques, and procedures. In addition, our Threat Response Unit closely monitors the ransomware 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 HermeticWiper, and PartyTicket malware:

- Ensure that Microsoft Exchange and Apache Tomcat servers are patched and up to date. Specifically ensuring your organization has patched:
  - CVE-2020-0688 – Microsoft Exchange
  - CVE-2021-26855 – Microsoft Exchange
  - CVE-2021-26857 – Microsoft Exchange
  - CVE-2021-26858 – Microsoft Exchange
  - CVE-2021-27065 – Microsoft Exchange
- Patch any external-facing applications and devices on an ongoing basis. Conduct regular vulnerability scans to ensure your team is staying on top of identifying, and patching, all known vulnerabilities.
- Consider implementing a comprehensive vulnerability management program that includes continuous awareness of the threat landscape, vulnerability scanning to understand which systems are inadvertently exposed, and disciplined patch management.
- Ensure your team is enforcing strong password policies for all employees as part of strengthening your organization's overall cyber hygiene.

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

Indicators of Compromise

Name	File Hash (SHA-256)
HermeticWiper	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
HermeticWiper	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
HermeticWiper	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
HermeticWiper	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
HermeticWiper	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
PartyTicket	4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382
RCDATA_DRV_X64	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
RCDATA_DRV_X86	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
RCDATA_DRV_XP_X64	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
RCDATA_DRV_XP_X86	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Yara Rules

```
rule  HermeticWiper {

    meta:
        author = "eSentire TI"
        filetype = "Win32 EXE"
        date = "03/02/2022"
        version = "1.0"
        hash = "0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da"

    strings:
        $drv1 = "\\\\.\\PhysicalDrive%u" wide fullword
        $drv2 = "\\\\.\\EPMNTDRV\\%u" wide fullword
        $NTFS1 = "$Bitmap" wide fullword nocase
        $NTFS2 = "$Logfile" wide fullword nocase
        $NTFS3 = "$I30" wide fullword nocase
        $rcdata1 = "DRV_X64" wide fullword nocase
        $rcdata2 = "DRV_X86" wide fullword nocase
        $rcdata3 = "DRV_XP_X86" wide fullword nocase
        $rcdata4 = "DRV_XP_X64" wide fullword nocase
        $storage1 = "GetLogicalDriveStrings" ascii nocase
        $storage2 = "GetDiskFreeSpace" ascii nocase

    condition:
        (uint16(0) == 0x5A4D or uint32(0) == 0x4464c457f)
        and filesize > 113KB
        and (2 of ($drv*) and 3 of ($NTFS*) and 2 of ($rcdata*) and 2 of ($storage*))

}
rule  PartyTicket {

    meta:
        author = "eSentire TI"
        filetype = "Win64 EXE"
        date = "03/02/2022"
        version = "1.0"
        hash = "4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382"

    strings:
        $project = "C:/projects/403forBiden/wHiteHousE/wHiteHousE.go" ascii nocase
        $string1 = "vote_result.cap" ascii nocase
        $string2 = "main.subscribeNewPartyMember" ascii nocase
        $string3 = "main.voteFor403" ascii nocase
        $string4 = "main.highWay60" ascii nocase
        $string5 = "main.BulletinNumber" ascii nocase

    condition:
        (uint16(0) == 0x5A4D or uint32(0) == 0x4464c457f)
        and filesize > 3100KB
        and $project and 3 of ($string*)

}
```

Sources

Skip To: