

Search ...



SIGN UP

Get notified when we post new content.

Business Email

>

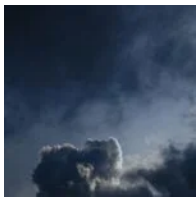
By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne [Privacy Notice](#). SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the [Google Privacy Policy](#) and [Terms of Service](#) apply.

This post was updated Feb 28th 2022 to include new IOCs and the PartyTicket ‘decoy ransomware’.

Executive Summary

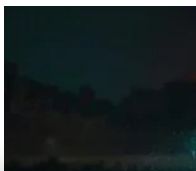
- On February 23rd, the threat intelligence community began observing a new wiper malware sample circulating in Ukrainian organizations.
- Our analysis shows a signed driver is being used to deploy a wiper that targets Windows devices, manipulating the MBR resulting in subsequent boot failure.
- This blog includes the technical details of the wiper, dubbed HermeticWiper, and includes IOCs to allow organizations to stay protected from this attack.

RECENT POSTS



Cloud Malware | A Threat Hunter’s Guide to Analysis, Techniques and Delivery

📅 OCTOBER 24, 2024



China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

[Cookies Settings](#)

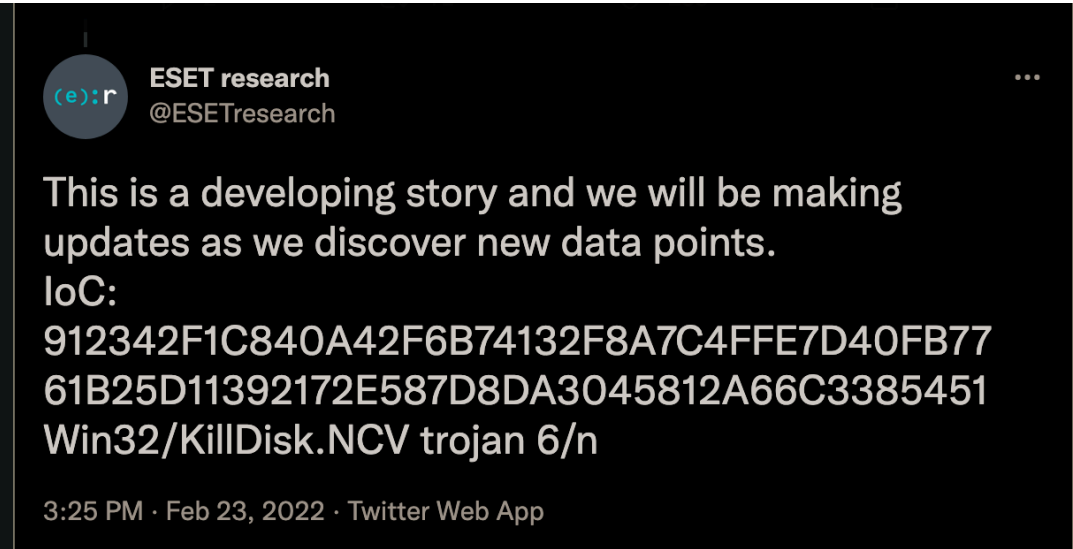
Accept All Cookies



action is needed.

Background

On February 23rd, our friends at Symantec and ESET research tweeted hashes associated with a wiper attack in Ukraine, including one which is not publicly available as of this writing.



We started analyzing this new wiper malware, calling it ‘HermeticWiper’ in reference to the digital certificate used to sign the sample. The digital certificate is issued under the company name ‘Hermetica Digital Ltd’ and valid as of April 2021. At this time, we haven’t seen any legitimate files signed with this certificate. It’s possible that the attackers used a shell company or appropriated a defunct company to issue this digital certificate.

Signature Verification

✔

Signed file, valid signature

File Version Information

Signers

— Hermetica Digital Ltd

Name	Hermetica Digital Ltd
Status	Valid
Issuer	DigiCert EV Code Signing CA (SHA2)
Valid From	12:00 AM 04/13/2021
Valid To	11:59 PM 04/14/2022
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
Serial Number	0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC

2024

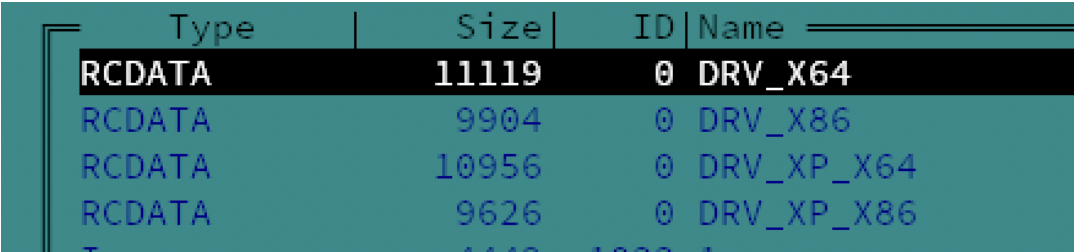
LABS CATEGORIES

- Crimeware
- Security Research
- Advanced Persistent Threat
- Adversary
- LABScon
- Security & Intelligence

our small part to the collective analysis effort.

Technical Analysis

At first glance, HermeticWiper appears to be a custom-written application with very few standard functions. The malware sample is 114KBs in size and roughly 70% of that is composed of resources. The developers are using a tried and tested technique of wiper malware, abusing a benign partition management driver, in order to carry out the more damaging components of their attacks. Both the Lazarus Group ([Destover](#)) and APT33 ([Shamoon](#)) took advantage of Eldos Rawdisk in order to get direct userland access to the filesystem without calling Windows APIs. HermeticWiper uses a similar technique by abusing a different driver, `empntdrv.sys`.



Type	Size	ID	Name
RCDATA	11119	0	DRV_X64
RCDATA	9904	0	DRV_X86
RCDATA	10956	0	DRV_XP_X64
RCDATA	9626	0	DRV_XP_X86

HermeticWiper resources containing EaseUS Partition Manager drivers

The copies of the driver are ms-compressed resources. The malware deploys one of these depending on the OS version, bitness, and SysWow64 redirection.

EaseUS driver resource selection

The benign EaseUS driver is abused to do a fair share of the heavy-lifting when it comes to accessing Physical Drives directly as well as getting partition information. This adds to the difficulty of analyzing HermeticWiper, as a lot of functionality is deferred to `DeviceIoControl` calls with specific IOCTLs.

MBR and Partition Corruption

should be enough for the device not to boot again, HermeticWiper proceeds to enumerate the partitions for all possible drives.

They then differentiate between FAT and NTFS partitions. In the case of a FAT partition, the malware calls the same ‘bit fiddler’ to corrupt the partition. For NTFS, the HermeticWiper parses the Master File Table before calling this same bit fiddling function again.

MFT parsing and bit fiddling calls

We euphemistically refer to the bit fiddling function in the interest of brevity. Looking through it, we see calls to Windows APIs to acquire a cryptographic context provider and generate random bytes. It’s likely this is being used for an inlined crypto implementation and byte overwriting, but the mechanism isn’t entirely clear at this time.

Further functionality refers to interesting MFT fields (`$bitmap` , `$logfile`) and NTFS streams (`$DATA` , `$I30` , `$INDEX_ALLOCATION`). The malware also enumerates common folders (‘My Documents’, ‘Desktop’, ‘AppData’), makes references to the registry (‘ntuser’), and Windows Event Logs (`"\\?\\C:\\Windows\\System32\\winevt\\Logs"`). Our analysis is ongoing to determine how this functionality is being used, but it is clear that having already corrupted the MBR and partitions for all drives, the victim system should be inoperable by this point of the execution.

Along the way, HermeticWiper’s more mundane operations provide us with further IOCs to monitor for. These include the momentary creation of the abused driver as well as a system service. It also modifies several registry keys, including setting the `SYSTEM\\CurrentControlSet\\Control\\CrashControl\\CrashDumpEnabled` key to `0`, effectively disabling crash dumps before the abused driver’s execution starts.

A Decoy Ransomware – PartyTicket

On February 24th, 2022, Symantec researchers pointed to a new Go ransomware being used as a decoy alongside the deployment of HermeticWiper. During our analysis we decided to name it PartyTicket based on some of the strings used by the malware developers:

The idea of using a ransomware as a decoy for a wiper is counterintuitive. In particular, a ransomware as poorly coded as PartyTicket is more likely to tie up resources during the execution of an otherwise efficient wiper.

As often happens to amateur Go developers, the malware has poor control over its concurrent threads and the commands it attempts to run. This leads to hundreds of threads and events spawned in our consoles. That is to say, it’s a very loud and ineffective ransomware that should fire alerts left and right.

The folder organization and function naming conventions within the binary show the developer’s intent for taunting the U.S. Government and the Biden administration.

Project folders and function names referring to the Biden Administration

Similar taunting can be found in the ransom note after execution:

In trying to understand the execution flow of PartyTicket, we see the `403forBiden.wHiteHousE.primaryElectionProcess()` function recursively enumerating folders:

PartyTicket looping over non-system folders

The resulting number of folders will be used as an upperbound

makes a copy with a `<UUID>.exe` name and deletes the original file. Then we expect a second loop to relieve that queue of files and run each through a standard Go AES crypto implementation. However, execution is unlikely to get this far with the current design of PartyTicket.

(Thanks to Joakim Kennedy (Intezer) for pointing out this indirect call)

Crypto routine for files queued in the ‘salary’ channel

Overall our analysis of PartyTicket indicates it to be a rather simple, poorly coded, and loud malware. Its possible role as a decoy ransomware deployed alongside HermeticWiper is more likely to be effective for its accidental hogging of the victim organization’s system resources rather than the encryption of files itself. IOCs and Yara rules have been added below.

Conclusion

After a week of defacements and increasing DDoS attacks, the proliferation of sabotage operations through wiper malware is an expected and regrettable escalation. At this time, we have a very small sliver of aperture into the attacks in Ukraine and subsequent spillover into neighboring countries and allies. If there’s a silver lining to such a difficult situation, it’s seeing the open collaboration between threat intel research teams, independent researchers, and journalists looking to get the story straight. Our thanks to the researchers at Symantec, ESET, Stairwell, and RedCanary among others who’ve contributed samples, time, and expertise.

SentinelOne Customers Protected

Indicators of Compromise

(Updated February 28th, 2022)

ms-compressed resources	SHA1
RCDATA_DRV_X64	5ceebaf1cbb0c10b95f7edd458804a646c6f215e
RCDATA_DRV_X86	0231721ef4e4519ec776ff7d1f25c937545ce9f4
RCDATA_DRV_XP_X64	9c2e465e8dfdfc1c0c472e0a34a7614d796294af
RCDATA_DRV_XP_X86	ee764632adedf6bb4cf4075a20b4f6a79b8f94c0

HermeticWiper	SHA1
Win32 EXE	0d8cc992f279ec45e8b8dfd05a700ff1f0437f29
Win32 EXE	61b25d11392172e587d8da3045812a66c3385451
Win32 EXE	912342f1c840a42f6b74132f8a7c4ffe7d40fb77
Win32 EXE	9518e4ae0862ae871cf9fb634

230f52aff1626df

YARA Rules

(https://github.com/SentineLabs/Yara/blob/main/APT_RU_SunFlowerSeed.yar)

```
import "pe"

rule MAL_HERMETIC_WIPER {
  meta:
    desc = "Hermetic Wiper - broad hunting rule"
    author = "Hegel @ SentinelLabs"
    version = "1.0"
    last_modified = "02.23.2022"
    hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2"
    reference = "https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/"
  strings:
    $string1 = "DRV_XP_X64" wide ascii nocase
    $string2 = "EPMNTDRV\\%u" wide ascii nocase
    $string3 = "PhysicalDrive%u" wide ascii nocase
    $cert1 = "Hermetica Digital Ltd" wide ascii nocase
  condition:
    uint16(0) == 0x5A4D and
    all of them
}

rule MAL_PARTY_TICKET {
  meta:
    desc = "PartyTicket / HermeticRansom Golang Ransomware"
    author = "Hegel @ SentinelLabs"
    version = "1.0"
    last_modified = "02.24.2022"
    hash = "4dc13bb83a16d4ff9865a51b3e4d24112327c526c13"
    reference = "https://twitter.com/juanandres_gs/status/149"
  strings:
    $string1 = "/403forBiden/" wide ascii nocase
    $string2 = "/wHiteHousE/" wide ascii
    $string3 = "vote_result." wide ascii
    $string4 = "partyTicket." wide ascii
    $buildid1 = "Go build ID: \"qb0H7AdWAYDzfMA1J80B/nJ9"
    $project1 = "C:/projects/403forBiden/wHiteHousE/" wide
  condition:
    uint16(0) == 0x5A4D and
```



```

    last_modified = "03.01.2022"
    hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2"
    reference = "https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/"
    condition:
      uint16(0) == 0x5a4d and
      for any i in (0 .. pe.number_of_signatures) : (
        pe.signatures[i].issuer contains "DigiCert EV Code Signing" and
        pe.signatures[i].serial == "0c:48:73:28:73:ac:8c:ce:ba:f8:3d:00:00:00:00:00:00:00:00:00:00"
      )
  }

rule MAL_ISSAC_WIPER {
  meta:
    desc = "Issac Wiper - broad hunting rule"
    author = "Hegel @ SentinelLabs"
    version = "1.0"
    last_modified = "03.01.2022"
    hash = "13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83"
    reference = "https://www.welivesecurity.com/2022/03/01/issac-wiper-ukraine/"
  strings:
    $name1 = "Cleaner.dll" wide ascii
    $name2 = "cl.exe" wide ascii nocase
    $name3 = "cl64.dll" wide ascii nocase
    $name4 = "cld.dll" wide ascii nocase
    $name5 = "cld.dll" wide ascii nocase
    $name6 = "Cleaner.exe" wide ascii
    $export = "_Start@4" wide ascii
  condition:
    uint16(0) == 0x5A4D and
    (any of ($name*) and $export)
  }

rule MAL_HERMETIC_WIZARD {
  meta:
    desc = "HermeticWizard hunting rule"
    author = "Hegel @ SentinelLabs"
    version = "1.0"
    last_modified = "03.01.2022"
    reference = "https://www.welivesecurity.com/2022/03/01/hermetic-wizard-ukraine/"
  strings:
    $name1 = "Wizard.dll" wide ascii
    $name2 = "romance.dll" wide ascii
    $name3 = "exec_32.dll" wide ascii
    $function1 = "DNSGetCacheDataTable" wide ascii
    $function2 = "GetIpNetTable" wide ascii
    $function3 = "WNetOpenEnumW" wide ascii
    $function4 = "NetServerEnum" wide ascii
    $function5 = "NetServerEnum" wide ascii
  condition:
    (any of ($name*) and ($function1 or $function2 or $function3 or $function4 or $function5))
  }
```

SentinelOne STAR Rules

```
EventType = "Process Creation" AND TgtProcPublisher = "HEF"
( SrcProcSignedStatus = "signed" AND IndicatorPersistenceCo
```

UKRAINE

WIPER

SHARE













JUAN ANDRÉS GUERRERO-SAADE

Juan Andrés is AVP of Research for SentinelLabs and Distinguished Resident Fellow for Threat Intelligence at the Johns Hopkins SAIS Alperovitch Institute. Before joining SentinelOne, JAGS led multiple threat intelligence teams at Google, Chronicle, was a Principal Security Researcher at GReAT focusing on targeted attacks, and worked as Senior Cybersecurity and National Security Advisor to the Government of Ecuador. In 2023, JAGS was presented with a Presidential Volunteer Service Award for furthering U.S. cyber preparedness. His research work is the subject of two permanent exhibits at the International Spy Museum in Washington, DC.



PREV



Sanctions Be Damned | From Dridex to Macaw, The Evolution of Evil Corp

NEXT



Zen and the Art of SMM Bug Hunting | Finding, Mitigating and Detecting UEFI Vulnerabilities

ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware

JUNE 26 2024

Unmasking I-Soon | The Leak That Revealed China’s Cyber Operations

FEBRUARY 21 2024

ScarCruft | Attackers Gather Strategic Intelligence and Target Cybersecurity Professionals

JANUARY 22 2024

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

RECENT POSTS



Cloud Malware | A Threat Hunter’s Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024



China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

OCTOBER 16, 2024



Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

SEPTEMBER 23, 2024



protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.



Twitter



LinkedIn

©2024 SentinelOne, All Rights Reserved.

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.