Ukrainian Targets Hit by HermeticWiper, New Datawiper Malware

Oblog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware

Mayuresh Dani

March 1, 2022

General	Details Compatibility	Previous Versions Digital Signatures
Signer inform Name: E-mail: Signing time:	Hermetica Digital L Not available	td
Currhavian		View Certificate
Countersigna		Timestamp
		Details

The Ukrainian Government has been targeted by HermeticWiper, a new ransomware-like data wiper. Its aim is not simply to encrypt the victim's data, but rather to render a system essentially unusable. In this blog, our Research Team details our analysis of how this aggressive new malware works.

The origin of HermeticWiper seems to be closely connected to the start of the Russia/Ukraine conflict. HermeticWiper is a new ransomware-like data wiper that was deployed beginning February 23, 2022. Based on multiple intelligence reports, the wiper-

ware is preceded by exploits that aid in malware deployment or multiple distributed denial-ofservice attacks to shut down protective services. Attacks have been observed against hundreds of Ukrainian websites related to the local government. Discovered mere hours before Russian troops rolled into Ukraine, the cyberattack is widely seen as the opening salvo of Moscow's invasion. As of this writing, HermeticWiper activity has since been found in Latvia and Lithuania.

The primary objective of the HermeticWiper is to destroy the master boot record (MBR) of a system, shredding data and rendering the system unusable.

Portable Executable Details of HermeticWiper

The file that we analyzed has a timestamp of "2021-12-28". This wiper-ware got its name because the attackers used a code-signing certificate issued to "Hermetica Digital Ltd." This traces back to a small videogame design business based in Cyprus with no links to Russia that claims it never applied for a digital certificate, pointing to possible identity theft. Operating systems use code-signing as an initial check on software, so it may have been designed to help the rogue program dodge anti-virus protections.

The sample we analyzed presented the following details:

	curity	84464fb77741b82199 Details	91acbf5e746aebdd0 × Previous Versions Digital Signatures	
Gen	eiai c	ompationity	Engital orginataree	
Digi	tal Signature Deta	iils	?	×
Ger		gnature Informatio signature is not valid.		
	Signer information			
	Name:	Hermetica Digital L	td	
	E-mail:	Not available		
	Signing time:	Not available		
			View Certificate	
	Countersignatures	1		
	Name of signer:	E-mail address:	Timestamp	
	L		Details	
			0	K

Another quirk that we noticed from most of the HermeticWiper samples was the use of the "gift" icon.



Whether this was a sick joke on the part of the attackers, or merely use of a commonly observed Visual Studio icon – we will never know.

Technical Details of HermeticWiper

HermeticWiper itself is just 115kbs and comes packed with drivers, which are extracted depending on the operating system. These drivers are compressed in "<u>SZDD</u>" format as can be seen here:

✓ ····· 🕕 RCDATA	000111F0	53	5A	44	44	88	FO	27	33	41	00	48	44	00	00	FF	4D	^	SZDD	'3A	HD	М
☆ DRV_X64:0	00011200	5A	90	00	03	00	00	00	7D	04	F5	F0	FF	FF	00	00	B8		Z	}		
DRV X86:0	00011210	F5	F0	A 2	01	01	40	01	04	0F	0D	1C	09	F0	F5	FO	0E			6		
_	00011220	FF	1F	BA	0E	00	Β4	09	CD	21	FF	B8	01	4C	CD	21	54			1	L	!T
DRV_XP_X64:0	00011230	68	69	FF	73	20	70	72	6F	67	72	61	FF	6D	20	63	61		hi s	progr	a m	ca
→ DRV_XP_X86:0	00011240	6E	6E	6F	74	FF	20	62	65	20	72	75	6E	20	FF	69	6E		nnot	be r	un	in
> 🧧 Icon	00011250	20	44	4F	53	20	6D	FF	6F	64	65	2E	0D	0D	0A	24	FE		DOS	m ode		\$
							-														-	

As the names suggest, drivers are dropped after meeting the operating system criteria:

- 1. DRV_X64: Windows 7+ 64-bits
- 2. DRV_X86: Windows 7+ 32-bits
- 3. DRV_XP_X64: Windows XP 64-bits
- 4. DRV_XP_X32: Windows XP 32-bits

Interestingly, the sample that we analyzed made use of an expired certificate from the "CHENGDU YIWO Tech Development Co. Ltd." A basic Google search reveals that this is a professional data recovery and data security company based in Sichuan, China. This certificate appears to be legitimate.

DRV_	X64.sys Properties			×	
General	Digital Signatures	Security Details	Previous Versions		
Dig	gital Signature Detai	ils		?	×
G	eneral Advanced				
	A required	ainst the current s	tion thin its validity period ystem clock or the ti		
	Name:		Tech Development (Co., Ltd.	
	E-mail: Signing time:	Not available Not available			,
		,	View Ce	ertificate	
	Countersignatures				
	Name of signer:	E-mail address:	: Timestamp		
			De	tails	
				OK	

Other researchers have found similar drivers from EaseUS Partition Manager. A search for that company name comes up with more details on the Chengdu YIWO Tech and EaseUS relationship:

Contact EaseUS - Professional D ×	https://www.easeus.com/contact.htr × +
\leftarrow \rightarrow C \textcircled{a}	view-source:https://www.easeus.com/contact.htm
<pre>5 <meta black"="" content="telephon
6 <meta content=" m<br=""/>7 <meta content="yee" nam<br=""/>8 <meta con<br="" http-equiv="conte
9 <title>Content Earcols =
10 <meta name='description
11 <meta name='robots"/>12 <meta content="contact. company, EaseUS" name='robots" con</pre></th><td><pre>scale=1.0,user-scalable=no,maximum-scale=1,width=device-width" name="viewport" /> e=no" name="format-detection" /> ame="apple-mobile-web-app-status-bar-style" /> ="apple-mobile-web-app-capable" /> int-Type" content="text/html; charset=UTF-8" /> Professional Data Backup & Recovery Company: CHENGDU Yiwo Tech Development Co., Ltd.</title> '/> ent="index.follow,all" /> ent="index.follow,all" /> ent=scale='contact: _/> ent=scale='contact: _/> ent=scale=' mode: _/> ent=scale='', _/></pre>	

This driver does the heavy lifting of causing harm to your system. This is a known technique and has been used a couple of times by well-known Advanced Persistent Threat groups.

DETECTION TIP #1

Watch out for processes executing drivers or dynamic link libraries with expired certificates.

Post execution, HermeticWiper gains the following privileges:

- 1. SeBackupPrivilege
- 2. SeDebugPrivilege
- 3. SeLoadDriverPrivilege

00673D64	FFD6	CALL ESI	esi:EntryPoint
00673D66	8D43 10	LEA EAX, DWORD PTR DS: [EBX+10]	
00673D69	50	PUSH EAX	10
00673D6A	68 A8556700	PUSH 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b	6755A8:L"SeBackupPrivilege"
00673D6F	6A 00	PUSH 0	
00673D71	FFD6	CALL ESI	esi:EntryPoint
00673D73	6A 00	PUSH 0	
00673D75	6A 00	PUSH 0	
00673D77	6A 00	PUSH 0	
00673D79	53	PUSH EBX	
00673D7A	C703 02000000	MOV DWORD PTR DS:[EBX],2	
00673D80	6A 00	PUSH 0	
00673D82	C743 0C 02000000	MOV DWORD PTR DS:[EBX+C],2	
00673D89	C743 18 02000000	MOV DWORD PTR DS: [EBX+18],2	
00673D90	FF7424 24	PUSH DWORD PTR SS [ESP+24]	
00673D94	FF15 28506700	CALL DWORD PTR DS: [<&AdjustTokenPrivileges>]	
00673D9A	FFD7	CALL EDI	edi:EntryPoint

Later in the execution chain, the SeLoadDriverPrivilege is used to load the extracted driver. Then one of the four drivers is dropped, after which the Volume Shadow Copy (VSS) service – which allows backups to be performed – is stopped.

DETECTION TIP #2

- 1. Watch out for processes gaining unnecessary and sensitive privileges like the ones mentioned above.
- 2. Watch out for important Windows service stoppages.

00673DE1	6A 22	PUSH 22	
00673DE3	68 <u>8C586700</u>	PUSH 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615	b 67588C:L"vss"
00673DE8	50	PUSH EAX	10 M
00673DE9	FF15 20506700	CALL DWORD PTR DS: [<&OpenServiceW>]	
00673DEF	8BD 8	MOV EBX, EAX	
00673DF1	85DB	TEST EBX,EBX	
00673DF3	75 0C	JNE 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615t	
00673DF5	FFD7	CALL EDI	edi:EntryPoint
00673DF7	8B3D 08506700	MOV EDI, DWORD PTR DS: [<&CloseServiceHandle>]	edi:EntryPoint

HermeticWiper then changes the CrashDumpEnabled registry key value to 0, under the System\CurrentControlSet\Control\CrashControl registry setting, so that memory dumps are disabled.

00E22B7B	50	push eax
00E22B7C	68 B856E200	push 3c557727953a8f6b4788984464fb77741b[E256B8:L"SYSTEM\\CurrentControlSet\\Control\\CrashControl"
00E22B81	68 02000080	push 80000002
00E22B86	FF15 4C50E200	call dword ptr ds:[<&RegOpenKevW>]
00E22B8C	85C0	test eax.eax
00E22B8E	75 24	ine 3c557727953a8f6b4788984464fb77741b8
00E22B90	6A 04	push 4
00E22B92	8945 F4	mov dword ptr ss:[ebp-C],eax
00E22B95	8D45 F4	lea eax,dword ptr ss:[ebp-C]
00E22B98	50	push eax
00E22B99	6A 04	push 4
00E22B9B	6A 00	push 0
00E22B9D	68 1457E200	push 3c557727953a8f6b4788984464fb77741b E25714:L"CrashDumpEnabled"
00E22BA2	FF75 FC	push dword ptr ss: [ebp-4]
00E22BA5	FF15 5450E200	call dword ptr ds:[<&RegSetValueExw>]
00E22BAB	FF75 FC	push dword ptr ss: [ebp-4]
00E22BAE	FF15 5050E200	call dword ptr ds:[<&RegCloseKey>]
ooroop 4	C1 00	

DETECTION TIP #3

Watch out for unauthorized processes making registry changes.

After this registry change, <u>ShowCompColor</u> and <u>ShowInfoTip</u> keys are also modified to disable the display of compressed and encrypted NTFS files in color. This setting allows you to see compressed files in a blue color. For example:



<u>Qualys Multi-Vector EDR</u> customers are presented with the following details capturing the behavior.

Qualys. Cloud Platform				0
\leftarrow Event Details:HKU\S-	-1-5-21-645655768-1046706414-3109199117-1002\SOFTWARE\Microsoft\Windows\Curre			Previous Next
VIEW MODE	Process Tree			^
Summary Event History Parent Process	HKU\S-1-5-21-645655768-1046706414-3109199117-1002\SOFTWARE\Microsoft\Windows\CurrentV Registry Value: ShowCompColor	/ersion\Explor	rer\Advanced	
Process Tree	+	⊾ ⁷ F	REGISTRY DI	ETAILS
			₽	HKU\S-1-5-21-645655768-1046706414-3109_
		E	Event	
			ID	RTR_797708e6-0a50-355a-a048-d3aa353b33ba_26-2- 2022
	Mutex 1 0		Event Collecte	Feb 26, 2022 10:23 PM
	O HermeticWip		Object Type	REGISTRY
	O Registry 1 ● 1903/051-021-4446557861.	F	Registry	
			Action	WRITE
			Key	HKU/S-1-5-21-645655768-1046706414-3109199117- 1002/SOFTWARE/Microsoft/Windows/CurrentVersion \Explorer\Advanced
			Value	ShowCompColor 👻

Then, hard drives on a system are enumerated and for each drive, the \\.\EPMNTDRV\ device is called. Then the driver that was extracted is loaded by creating a new service using the CreateServiceW which rewrites the first 512 bytes of the Master Boot Record (MBR).

000221000		push cur puncturizer occas
00E21D6C	51	push ecx
00E21D6D	68 <u>A851E200</u>	push 3c557727953a8f6b4788984464fb77741b821991acbf E251A8:L"\\\.\\PhysicalDrive%u"
00E21D72	0F57C0	xorps xmm0,xmm0
00E21D75	8955 E4	mov dword ptr ss: ebp-1C edx
00E21D78	8D85 A4FDFFFF	lea eax,dword ptr_ss:[ebp-25C]

The code further suggests that HermeticWiper enumerates the following files and folders...

AppData

- Desktop
- ProgramFiles
- ProgramFiles(x86)
- Perflogs
- C:\Documents and Settings
- C:\Windows\System32\winevt\logs
- System Volume Information

...the following Master File Table metafiles...

- \$LogFile: Journal to record metadata transactions.
- \$Bitmap: Records allocation status of each cluster in the file system.
- \$Attribute_List:

...and the following NTFS streams:

- \$DATA Contains file data.
- \$I30 NTFS index attribute
- \$INDEX_ALLOCATION: Stream type of a directory.

DETECTION TIP #4

Watch out for processes enumerating multiple locations and data streams.

Post successful execution, HermeticWiper makes use of the InitiateSystemShutdownEx API to shut down the system. Once rebooted, since the MBR has been rewritten, we see a blank screen with the words "Missing operating system."

76E55280	8BFF	mov edi,edi	InitiateSystemShutdownExW
76E55282		push ebp	
76E55283	8BEC	mov ebp,esp	
76E55285	83E4 F8	and esp,FFFFFF8	
70000000	0000 40	Levels see a dec	

HermeticWiper Detection with Qualys Multi-Vector EDR

Out of the box, Qualys Multi-Vector EDR provides detection and prevention capabilities that can help enterprise security teams to find Indicators of Compromise.

Event Details.90	b77284744f8761c4f2558388e0aee21406	10040411331000222034002030	JUN CAC	1	
MODE	Summary			Asset Det	ails
hary	-				
tistory Process s Tree	96b77284744f8761c4f255 Path: C:\Users\Mayuresh\Down	58388e0aee2140618b484ff53fa8b222 loads	b340d2a9c84.exe		Mayuresh-W10-CA oS:Windows
s moe				Identificat	tion
	Threat Details			DNS Hostni	ame Mayuresh-W10-CA
	Family	Category	Score	FQDN	MAYURESH-W10-CA.WORKGROU
	HermeticWiper	Trojan	8	IPv4	10.113.107.114
				IPv6	fe80:0:0:0:a181:3a43:b219:68f5
				Asset ID	489709912
	File			A attivity	
	File Action RENAME	File Type PE File	File Extension exe	Activity	
				Last User L	ogin Mayuresh
	File Name 96b77284744f8761c4f2558388e0aee	File Size 2 17.07 KB	Version -	Last System	Bo Feb 25, 2022 07:06 PM
	140618b484ff53fa8b222b340d2a9c8 exe	4.		Created On	Feb 25, 2022 07:35 PM
				Last Check	ed In Feb 25, 2022 08:09 PM
	Created On Feb 25, 2022 07:47 PM	Modified On Feb 23, 2022 01:02 PM	Accessed On Feb 25, 2022 07:47 PM	Location	
	Product	Company	Copyright		

HermeticWiper MITRE ATT&CK TID Map

Tactic	TID	Technique	Procedure
Privilege Escalation	T1134	Access Token Manipulation	HermeticWiper modifies its security token to grants itself debugging privileges by adding SeDebugPrivilege, creating backups by adding SeBackupPrivilege and load drivers by adding SeLoadDriverPrivilege.
Discovery	T1082	System Information Discovery	HermeticWiper enumerates the operating system and its bit-size according to which embedded drivers are dropped
Defense Evasion	T1112	Modify Registry	HermeticWiper modifies multiple keys
Execution	T1106	Native API	HermeticWiper uses the AdjustTokenPrivileges to give itself the following privileges: SeShutdownPrivilege, SeBackupPrivilege and SeLoadDriverPrivilege.
Persistence	T1543.003	Create or Modify System Process: Windows Service	HermeticWiper loads the extracted driver, by creating a new service using the CreateServiceW API.
Impact	T1561.002	Disk Wipe: Disk Structure Wipe	HermeticWiper damages the Master Boot Record (MBR) of the infected computer.
Impact	T1490	Inhibit System Recovery	HermeticWiper stops the Volume Shadow Copy service.

Tactic	TID	Technique	Procedure
Impact	T1489	Service Stop	HermeticWiper stops the Volume Shadow Copy service.
Discovery	T1083	File and Directory Discovery	HermeticWiper enumerates multiple files and folders such as AppData, Desktop, etc.
Impact	T1529	System Shutdown/Reboot	HermeticWiper initiates a system shutdown via the InitiateSystemShutdownEx API.

HermeticWiper IOCs

SHA256

0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da 06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397 095c7fa99dbc1ed7a3422a52cc61044ae4a25f7f5e998cc53de623f49da5da43 0db5e5b68dc4b8089197de9c1e345056f45c006b7b487f7d8d57b49ae385bad0 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf 34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382 7e154d5be14560b8b2c16969effdb8417559758711b05615513d1c84e56be076 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1 b60c0c04badc8c5defab653c581d57505b3455817b57ee70af74311fa0b65e22 b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd c2d06ad0211c24f36978fe34d25b0018ffc0f22b0c74fd1f915c608bf2cfad15

d4e97a18be820a1a3af639c9bca21c5f85a3f49a37275b37fd012faeffcb7c4a

dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78

e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

f50ee030224bf617ba71d88422c25d7e489571bc1aba9e65dc122a45122c9321

fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d