Trellix Global Defenders: Cyberattacks Targeting Ukraine and HermeticWiper Protections

trellix.com/en-us/about/newsroom/stories/threat-labs/defenders-blog-on-cyberattacks-targeting-ukraine.html

Cyberattacks Targeting Ukraine and HermeticWiper Protections

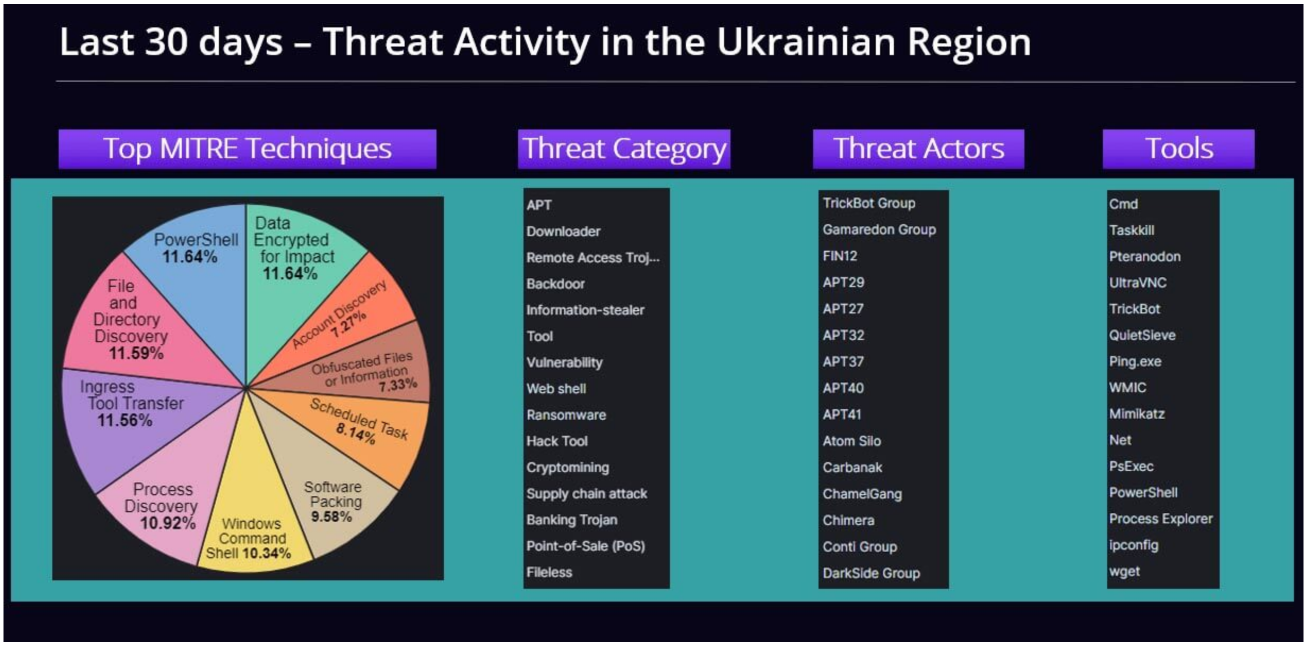
Stories

The latest cybersecurity trends, best practices,
security vulnerabilities, and more

By Taylor Mullins · February 28, 2022

Trellix is monitoring the ongoing cyberattacks targeting the Ukraine and any threat activity targeting entities outside of the Ukraine. Trellix is continuing to add protections to our products via the Global Threat Intelligence (GTI) feed and content updates as new malware variants and behavior indicators are discovered. The Trellix Advanced Programs Group (APG) is also monitoring the threat actors currently targeting the Ukraine and the threat tools being observed in those attacks, monitoring for usage of these tools in your environment can be a proactive step in detecting compromise of your infrastructure.

Analysis from the Trellix Advanced Threat Research (ATR) team into the activity of wipers being deployed within the Ukraine leads them to believe that there is a likely a connection between Whispergate, and the newly identified HermeticWiper.



Threat Category	Threat Actors	Tools
APT	TrickBot Group	Cmd
Downloader	Gamaredon Group	Taskkill
Remote Access Troj...	FIN12	Pteranodon
Backdoor	APT29	UltraVNC
Information-stealer	APT27	TrickBot
Tool	APT32	QuietSieve
Vulnerability	APT37	Ping.exe
Web shell	APT40	WMIC
Ransomware	APT41	Mimikatz
Hack Tool	Atom Silo	Net
Cryptomining	Carbanak	PsExec
Supply chain attack	ChamelGang	PowerShell
Banking Trojan	Chimera	Process Explorer
Point-of-Sale (PoS)	Conti Group	ipconfig
Fileless	DarkSide Group	wget

Figure 1. Breakdown of Activity in the Ukrainian Region in the past 30 Days. Source: Trellix APG Team

Recommended Steps to Prevent Initial Access

Organizations should look to review the Initial Access Tactics, techniques, and procedures (TTPs) associated with Russian nation state activity to proactively protect their environment from infiltration.

- Phishing/Spearphishing attacks utilizing shortened URLs of malicious domains.
- Monitor for brute force activity to identify valid account credentials and Microsoft 365 Accounts.
- Enable multifactor authentication (MFA) for all users, without exception.
- Exploiting Public Facing Systems – CISA maintains a full list of CVEs that are known to be exploited: CISA: KNOWN EXPLOITED VULNERABILITIES CATALOG
- Disabling all ports and protocols that are not essential, especially anything related to remote services.
- unt and block open-source tools not related to business activities that have been seen in prior attacks – UltraVNC, AdvancedRun, wget, and Impacket

Trellix Protections for the HermeticWiper Malware

Trellix is currently monitoring the latest wiper malware dubbed "HermeticWiper" that has been observed in attacks against the Ukraine. Trellix Global Threat Intelligence (GTI) is currently protecting against all known indicators associated with "HermeticWiper" and MVISION Insights will note detections in your environment as well.

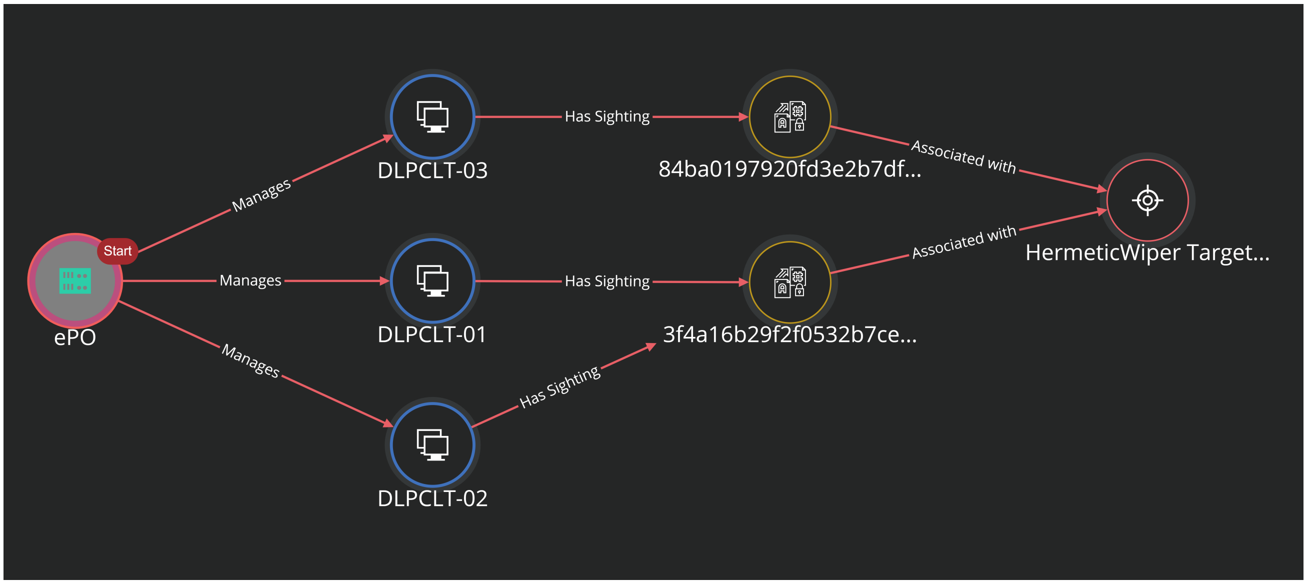
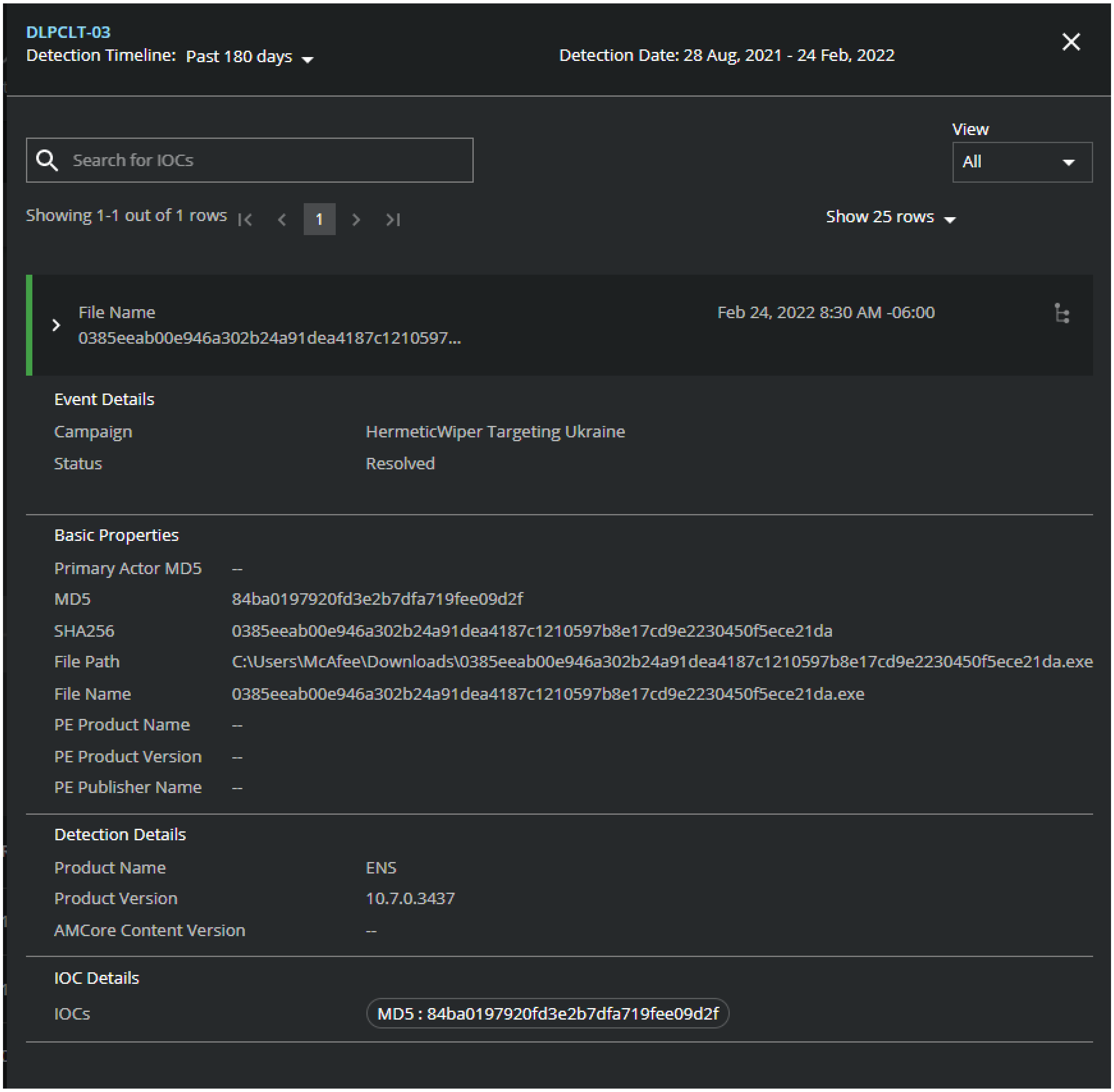


Figure 2. Test system detections of HermeticWiper IOCS. Source: MVISION Insights



DLPCLT-03

Detection Timeline: Past 180 days

Detection Date: 28 Aug, 2021 - 24 Feb, 2022

File Name
0385eeab00e946a302b24a91dea4187c1210597...

Feb 24, 2022 8:30 AM -06:00

Event Details

Campaign	HermeticWiper Targeting Ukraine
Status	Resolved

Basic Properties

Primary Actor MD5	--
MD5	84ba0197920fd3e2b7dfa719fee09d2f
SHA256	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
File Path	C:\Users\McAfee\Downloads\0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da.exe
File Name	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da.exe
PE Product Name	--
PE Product Version	--
PE Publisher Name	--

Detection Details

Product Name	ENS
Product Version	10.7.0.3437
AMCore Content Version	--

IOC Details

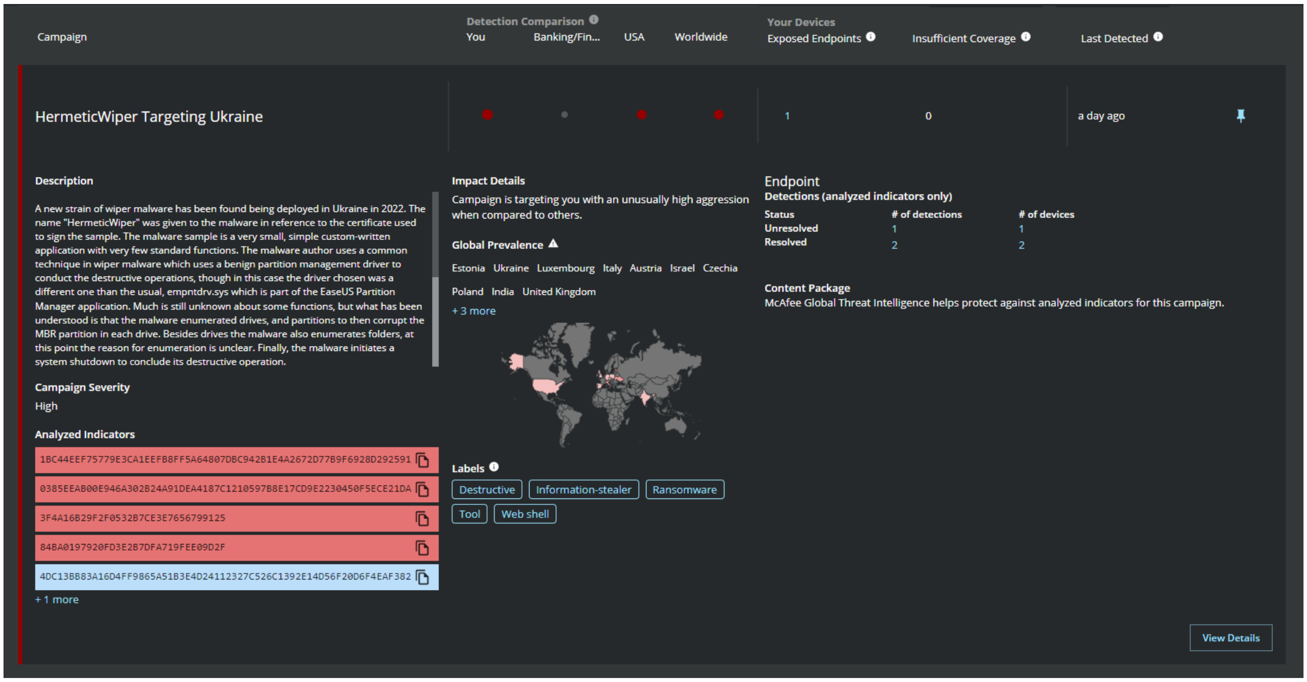
IOCs	MD5 : 84ba0197920fd3e2b7dfa719fee09d2f

Figure 3. Event details of successful containment of HermeticWiper by ENS.

HermeticWiper Threat Intelligence from MVISION Insights

MVISION Insights will provide the current threat intelligence and known indicators for HermeticWiper. MVISION Insights will alert to detections and process traces that have been observed and systems that require additional attention to prevent widespread infection. MVISION Insights will also include Hunting Rules for threat hunting and further intelligence gathering of the threat activity and adversary behind the campaign.

MVISION Insights Campaign Names: HermeticWiper Targeting Ukraine



HermeticWiper Targeting Ukraine

Exposed Endpoints	Insufficient Coverage	Last Detected
1	0	a day ago

Description

A new strain of wiper malware has been found being deployed in Ukraine in 2022. The name "HermeticWiper" was given to the malware in reference to the certificate used to sign the sample. The malware sample is a very small, simple custom-written application with very few standard functions. The malware author uses a common technique in wiper malware which uses a benign partition management driver to conduct the destructive operations, though in this case the driver chosen was a different one than the usual, empntdrv.sys which is part of the EaseUS Partition Manager application. Much is still unknown about some functions, but what has been understood is that the malware enumerated drives, and partitions to then corrupt the MBR partition in each drive. Besides drives the malware also enumerates folders, at this point the reason for enumeration is unclear. Finally, the malware initiates a system shutdown to conclude its destructive operation.

Campaign Severity

High

Analyzed Indicators

```
1BC44EEF75779E3CA1EEFB8FF5A64807DBC942B1E4A2672D77B9F6928D292591
0385EEAB00E946A302B24A91DEA4187C1210597B8E17CD9E2230450F5ECE21DA
3F4A16B29F2F0532B7CE3E7656799125
84BA0197920FD3E2B7DFA719FEE09D2F
4DC13BB83A16D4FF9865A51B3E4D24112327C526C1392E14D56F20D6F4EAF382
```

+ 1 more

Impact Details

Campaign is targeting you with an unusually high aggression when compared to others.

Global Prevalence ⚠

Estonia Ukraine Luxembourg Italy Austria Israel Czechia Poland India United Kingdom

+ 3 more

Labels

Endpoint

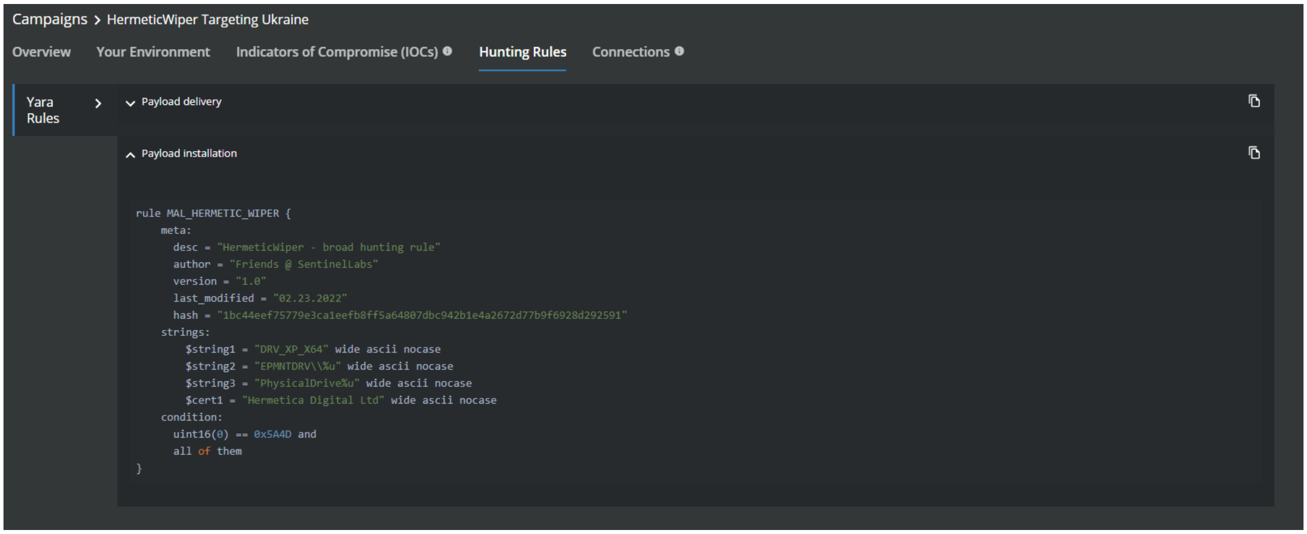
Detections (analyzed indicators only)

Status	# of detections	# of devices
Unresolved	1	1
Resolved	2	2

Content Package

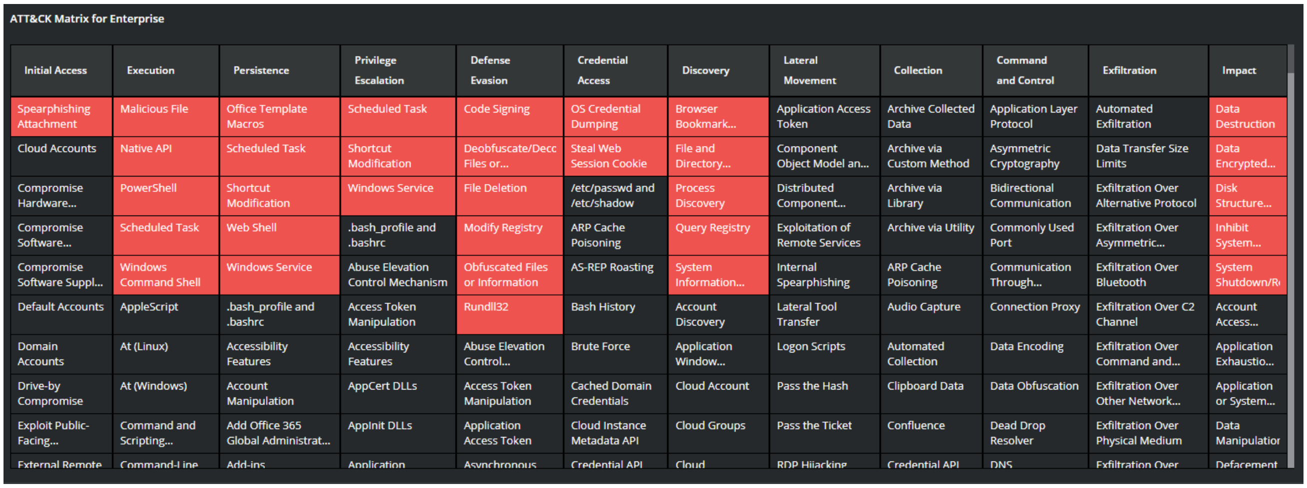
McAfee Global Threat Intelligence helps protect against analyzed indicators for this campaign.

Figure 4. HermeticWiper campaign description and detections



```
rule MAL_HERMETIC_WIPER {
    meta:
      desc = "HermeticWiper - broad hunting rule"
      author = "Friends @ SentinelLabs"
      version = "1.0"
      last_modified = "02.23.2022"
      hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591"
    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
}
```

Figure 5. Hunting Rules for HermeticWiper Malware



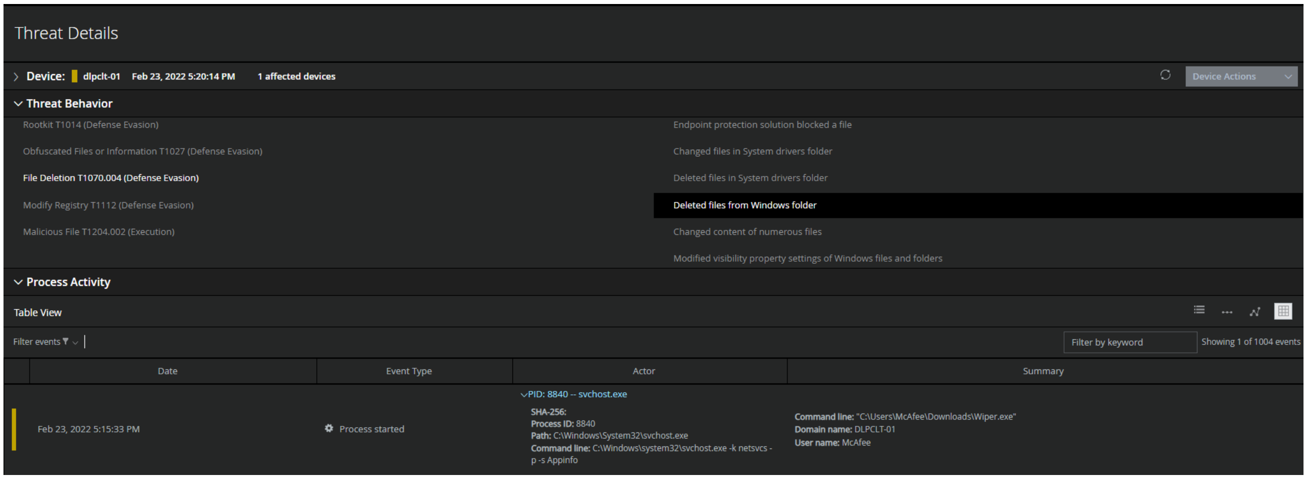
ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Spearphishing Attachment	Malicious File	Office Template Macros	Scheduled Task	Code Signing	OS Credential Dumping	Browser Bookmark...	Application Access Token	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Data Destruction
Cloud Accounts	Native API	Scheduled Task	Shortcut Modification	Deobfuscate/Decc Files or...	Steal Web Session Cookie	File and Directory...	Component Object Model an...	Archive via Custom Method	Asymmetric Cryptography	Data Transfer Size Limits	Data Encrypted...
Compromise Hardware...	PowerShell	Shortcut Modification	Windows Service	File Deletion	/etc/passwd and /etc/shadow	Process Discovery	Distributed Component...	Archive via Library	Bidirectional Communication	Exfiltration Over Alternative Protocol	Disk Structure...
Compromise Software...	Scheduled Task	Web Shell	.bash_profile and .bashrc	Modify Registry	ARP Cache Poisoning	Query Registry	Exploitation of Remote Services	Archive via Utility	Commonly Used Port	Exfiltration Over Asymmetric...	Inhibit System...
Compromise Software Suppl...	Windows Command Shell	Windows Service	Abuse Elevation Control Mechanism	Obfuscated Files or Information	AS-REP Roasting	System Information...	Internal Spearphishing	ARP Cache Poisoning	Communication Through...	Exfiltration Over Bluetooth	System Shutdown/R
Default Accounts	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Rundll32	Bash History	Account Discovery	Lateral Tool Transfer	Audio Capture	Connection Proxy	Exfiltration Over C2 Channel	Account Access...
Domain Accounts	At (Linux)	Accessibility Features	Accessibility Features	Abuse Elevation Control...	Brute Force	Application Window...	Logon Scripts	Automated Collection	Data Encoding	Exfiltration Over Command and...	Application Exhaustio...
Drive-by Compromise	At (Windows)	Account Manipulation	AppCert DLLs	Access Token Manipulation	Cached Domain Credentials	Cloud Account	Pass the Hash	Clipboard Data	Data Obfuscation	Exfiltration Over Other Network...	Application or System...
Exploit Public-Facing...	Command and Scripting...	Add Office 365 Global Administrat...	AppInit DLLs	Application Access Token	Cloud Instance Metadata API	Cloud Groups	Pass the Ticket	Confluence	Dead Drop Resolver	Exfiltration Over Physical Medium	Data Manipulatior
External Remote	Command-Line	Add-ins	Application	Asynchronous	Credential API	Cloud	RDP Hijacking	Credential API	DNS	Exfiltration Over	Defacement

Figure 6. MITRE ATT&CK Framework for HermeticWiper Malware

Detecting Malicious Activity with MVISION EDR

MVISION EDR is currently monitoring for the activity associated with HermeticWiper and will note the MITRE techniques and any suspicious indicators related to the adversarial activity. Detecting and preventing HermeticWiper from spreading throughout your environment is critical due to the destructive nature of the malware, once the HermeticWiper has infected a system it will remove the System Drivers and Windows files leaving the system inoperable.



Threat Details

Device: dlpclt-01 Feb 23, 2022 5:20:14 PM 1 affected devices

Threat Behavior

Rootkit T1014 (Defense Evasion)	Endpoint protection solution blocked a file
Obfuscated Files or Information T1027 (Defense Evasion)	Changed files in System drivers folder
File Deletion T1070.004 (Defense Evasion)	Deleted files in System drivers folder
Modify Registry T1112 (Defense Evasion)	Deleted files from Windows folder
Malicious File T1204.002 (Execution)	Changed content of numerous files
	Modified visibility property settings of Windows files and folders

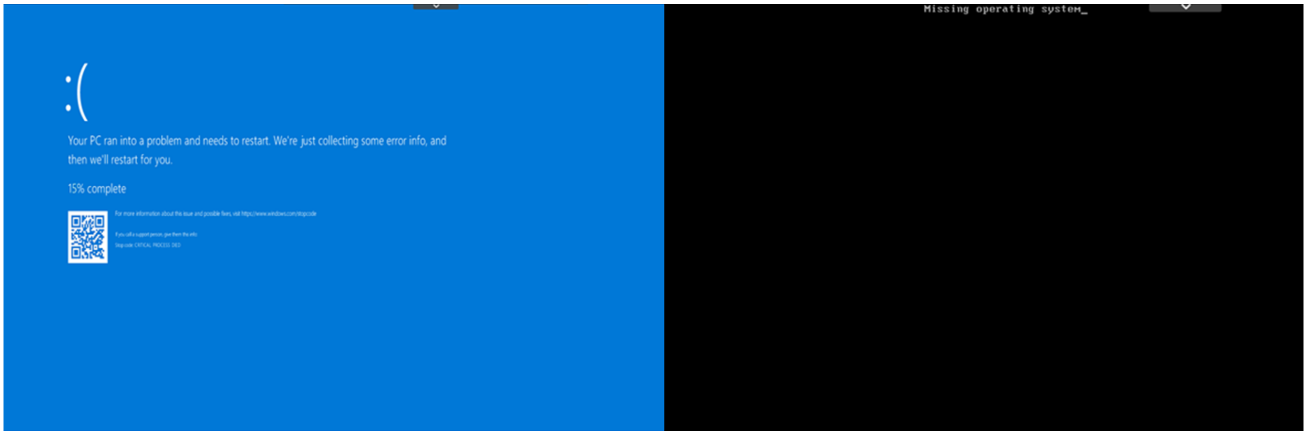
Process Activity

Table View

Showing 1 of 1004 events

Date	Event Type	Actor	Summary
Feb 23, 2022 5:15:33 PM	Process started	PID: 8840 -- svchost.exe SHA-256: Process ID: 8840 Path: C:\Windows\System32\svchost.exe Command line: C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo	Command line: "C:\Users\McAfee\Downloads\Wiper.exe" Domain name: DLPCLT-01 User name: McAfee

Figure 7. MITRE Techniques and Threat Behavior noting deletion of System Drivers and Windows files



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

15% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: CRITICAL PROCESS DIED

```
Missing operating system_
```

Figure 8. Once the deletion of data is complete, a reboot executes, and the system is no longer operable

Featured Content

PERSPECTIVES

Our CEO On Living Security

By Bryan Palma · January 19, 2022

Trellix CEO, Bryan Palma, explains the critical need for security that's always learning.

Read More

XDR

Time to Drive Change by Challenging the Challengers

By Michelle Salvado · January 19, 2022

Dynamic threats call for dynamic security – the path to resiliency lies in XDR.

Read More

THREAT LABS

2022 Threat Predictions

By Trellix · January 19, 2022

What cyber security threats should enterprises look out for in 2022?

Read More

Get the latest

We're no strangers to cybersecurity. But we are a new company.
Stay up to date as we evolve.

Please enter a valid email address.

Zero spam. Unsubscribe at any time.