CrowdStrike Protects from Wiper Malware Used in Ukraine Attacks

crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/

February 25, 2022

CrowdStrike Falcon Protects from New Wiper Malware Used in Ukraine Cyberattacks

February 25, 2022

William Thomas - Adrian Liviu Arsene - Farid Hendi Endpoint & Cloud Security

- On Feb. 23, 2022, a new wiper malware was reported targeting Ukraine systems
- The wiper destroys files on infected Windows devices by corrupting specific elements of connected hard drives
- CrowdStrike Intelligence refers to this destructive malware as DriveSlayer
- DriveSlayer is the second recent destructive malware targeting Ukraine, following WhisperGate
- The CrowdStrike Falcon® platform provides continuous protection from DriveSlayer and wiper-style threats by offering real-time visibility across workloads

On Feb. 23, 2022, a new wiper malware was reported publicly as affecting Ukrainian-based systems. Following a series of denial-of-service attacks and website defacements, the new destructive malware corrupts the master boot record (MBR), partition and file system of all available

physical drives on Windows machines.

CrowdStrike Intelligence refers to this new destructive malware as DriveSlayer, and it's the second wiper to affect Ukraine following the recent WhisperGate. DriveSlayer is digitally signed using a valid certificate and also abuses a legitimate EaseUS Partition Master driver to gain raw disk access and manipulate the disk to make the system inoperable.

The CrowdStrike Falcon platform provides continuous protection against DriveSlayer and wiper-style threats by delivering real-time visibility across workloads to protect customers.

Technical Analysis

Unlike WhisperGate, which uses higher-level API calls, DriveSlayer uses raw disk access to destroy data.

Upon initialization, two optional command-line parameters may be used to specify how long the malware will sleep before destruction begins and the system is restarted. If none are specified it will default to 20 and 35 minutes, respectively.

Next, the malware will ensure it has the proper privileges to perform its actions. It uses the API `AdjustTokenPrivileges` to give itself the following privileges: `SeShutdownPrivilege`, `SeBackupPrivilege` and `SeLoadDriverPrivilege`.

Privilege Name	Description
SeShutdownPrivilege	Provides the ability to shut down a local system
SeBackupPrivilege	Provides the ability to perform system backup operations
SeLoadDriverPrivilege	Provides the ability to load or unload a device driver

Different drivers will be loaded based on the system version. The malware uses `IsWow64Process` to determine which driver version to load. These drivers are stored in the resource section of the binary and are compressed with the Lempel-Ziv algorithm. The driver file is written to system32\drivers with a 4-character, pseudo-randomly generated name. This file is then decompressed using LZCopy to a new file with a ".sys" extension.

Example File Name	Description
C:\Windows\System32\drivers\bpdr	Lempel-Ziv compressed driver
C:\Windows\System32\drivers\bpdr.sys	Decompressed driver

Before the driver is loaded, the malware disables crash dump by setting the following registry key:

Registry	Value	Description
HKLM:\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled	0	Disables crash dump

To load the driver, a new service is created using the API `CreateServiceW`. The name and display name for this service is the 4-character name used for the file name. Next, `StartServiceW` is called in a loop five times to ensure the driver is loaded. Immediately after the driver is loaded, the service is removed by deleting the entire registry key.

After the driver is loaded, the VSS service is disabled using the Control Service Manager. Following this, a number of additional threads are created. A thread is created to handle the system reboot. It will sleep for the time specified by a command line parameter of 35 minutes, at which point the system will be restarted by an API call to `InitializeSystemShutdownExW`.

Another thread disables features in the UI that could alert the user of suspicious activity occurring on the system before iterating through attached drives.

Registry	Value	Description
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor	0	Disables colors for compressed and encrypted NTFS files
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip	0	Disables pop-up information about folders and desktop items

Finally, the malware begins its destructive routine by spawning multiple additional threads that overwrite the files on disk and destroy the partition tables. Once the system is rebooted, the user will see a blank screen with the words “Missing operating system.”

The Falcon Platform’s Continuous Monitoring and Visibility Stop Destructive Malware

The Falcon platform takes a layered approach to protect workloads. Using on-sensor and cloud-based machine learning, behavior-based detection using indicators of attack (IOAs), and intelligence related to tactics, techniques and procedures (TTPs) employed by threats and threat actors, the Falcon platform enables visibility, threat detection and continuous monitoring for any environment, reducing time to detect and mitigate threats including destructive malware.

As shown in Figure 1, the Falcon platform uses cloud-based machine learning to detect DriveSlayer and prevent the malware from performing additional malicious actions, such as loading additional components.

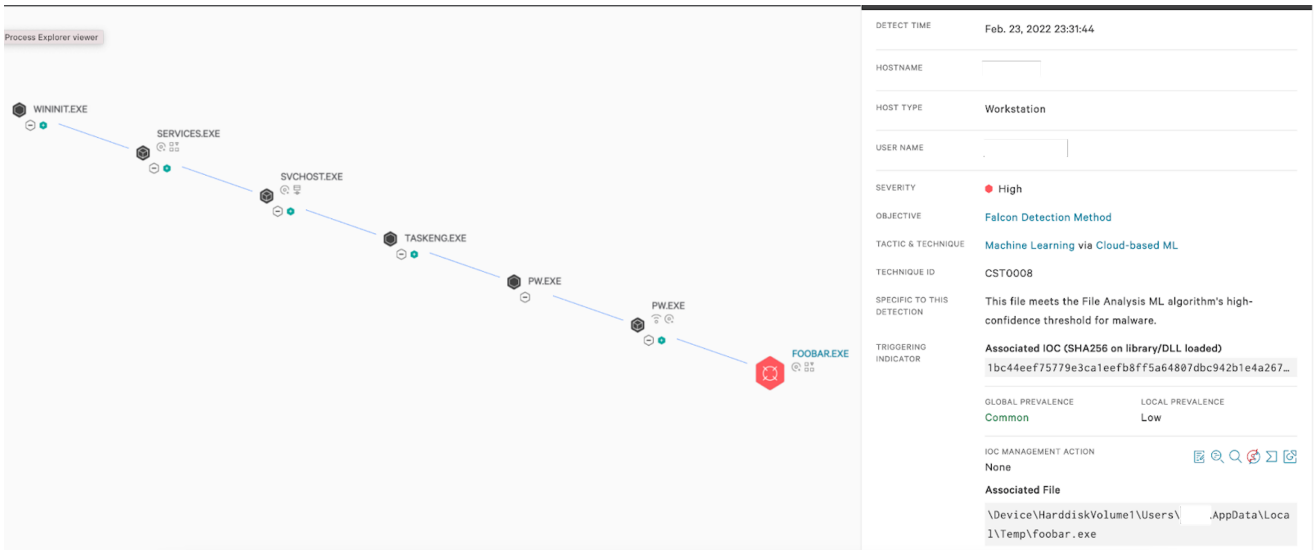


Figure 1. The Falcon platform's cloud-based machine learning detects DriveSlayer wiper (Click to enlarge)

The Falcon platform's behavior-based IOAs can detect and prevent suspicious processes from executing or loading additional components, as well as other behaviors that indicate malicious intent. For example, Falcon detects and prevents DriveSlayer behavior such as tampering with specific registry keys. The behavior-based detection is further layered with a traditional indicator of compromise (IOC)-based hash detection (see Figure 2).

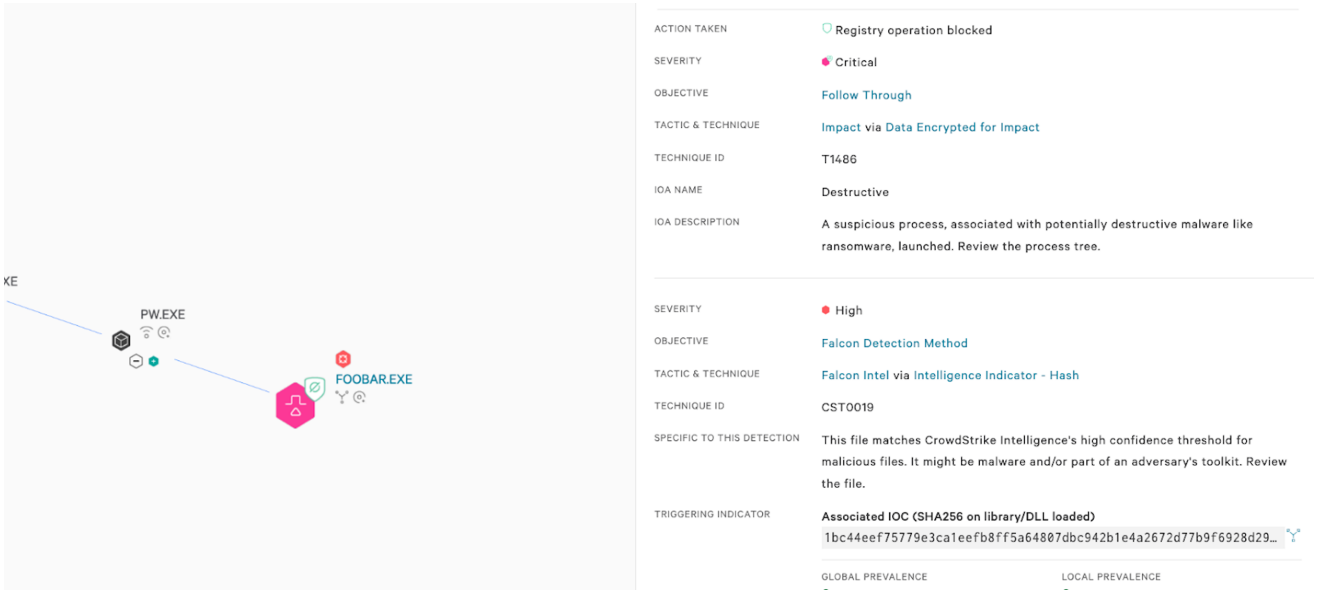


Figure 2. CrowdStrike Falcon detects and prevents DriveSlayer destructive behavior (Click to enlarge)

Because DriveSlayer has no built-in propagation methods for spreading across infrastructures, and because reports of it being used to target Ukraine have so far been limited, the risk of organizations encountering this data-wiping threat may be low at present. CrowdStrike will continue to monitor and report on the situation as it unfolds.

CrowdStrike Falcon customers can proactively monitor their environments by using hunting queries to reveal indicators of DriveSlayer's presence. Read our summary on DriveSlayer, and how to hunt for it in our Support Portal.

Companies facing cyber incident risks, including data-wiping threats, are encouraged to take steps to increase their operational resilience. Security solutions that can protect them from malware and other threats must provide visibility into their environments and intelligent monitoring of cloud resources to help detect and respond to potential threats — including destructive threats — and limit potential damages.

Note: More detailed intelligence and technical information about DriveSlayer is available to CrowdStrike customers through the Falcon console and Support Portal.

Indicators of Compromise (IOCs)

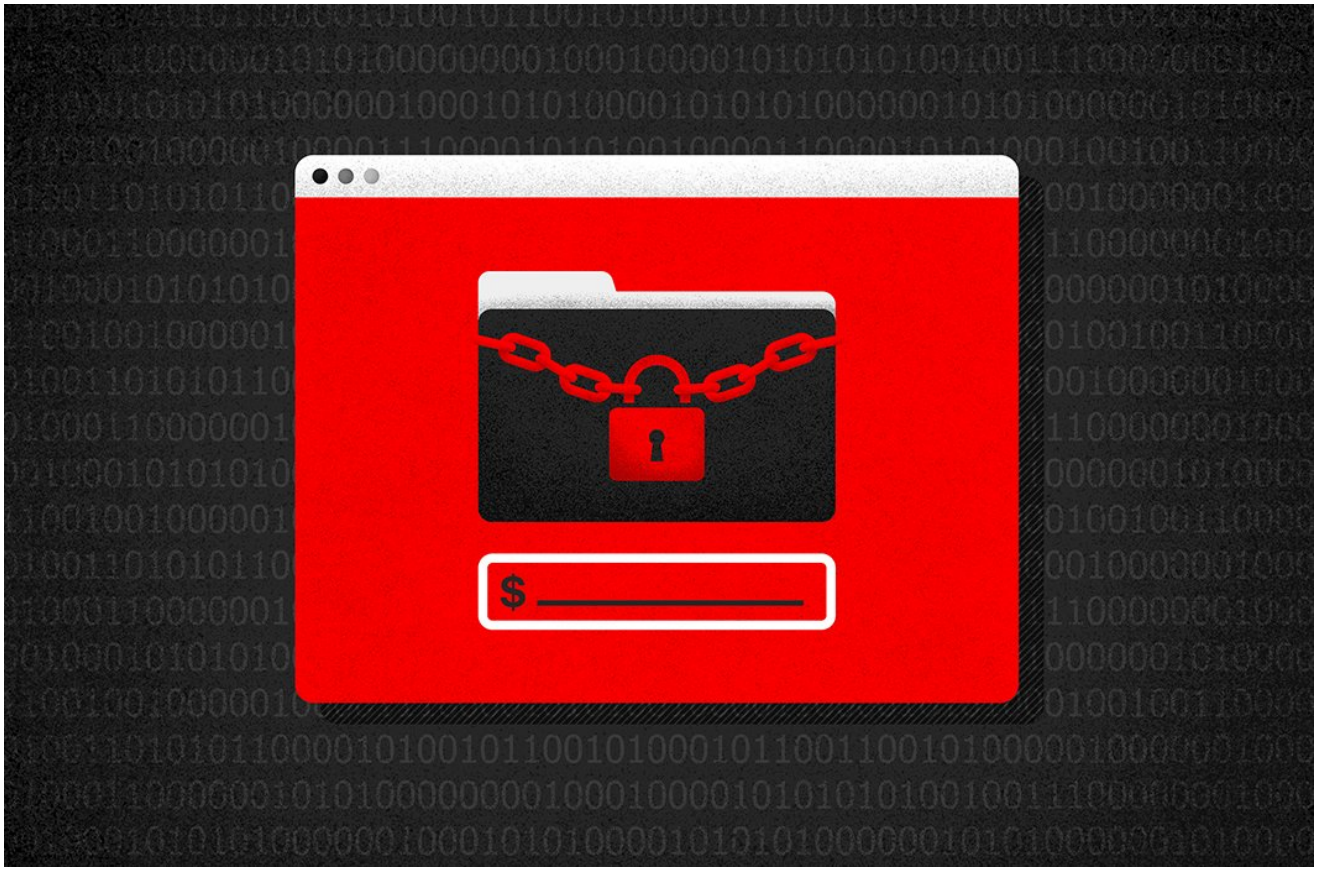
File	SHA256
DriveSlayer	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

Additional Resources

- *Read more about successive use of offensive cyber operations against Ukraine: Lessons Learned From Successive Use of Offensive Cyber Operations Against Ukraine and What May Be Next.*
- *Learn more about WhisperGate in this CrowdStrike Intelligence blog: Technical Analysis of the WhisperGate Malicious Bootloader.*
- *Learn more about the powerful, cloud-native CrowdStrike Falcon platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent to see for yourself how true next-gen AV performs against today's most sophisticated threats.*
- *Follow all related content in Trending Threats & Vulnerabilities: New Wiper used in Ukraine Cyberattacks.*

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell

At the start of 2022, CrowdStrike Intelligence and CrowdStrike Services investigated an incident in which PROPHET SPIDER exploited CVE-2021-22941 — a remote code execution (RCE) vulnerability impacting Citrix ShareFile Storage Zones Controller — to compromise a Microsoft Internet Information Services (IIS) web server. The adversary exploited the vulnerability to deploy a webshell that enabled the […]



Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities

Summary On Feb. 23, 2022, destructive attacks were conducted against Ukrainian entities. Industry reporting has claimed the Go-based ransomware dubbed PartyTicket (or HermeticRansom) was identified at several organizations affected by the attack,1 among other families including a sophisticated wiper CrowdStrike Intelligence tracks as DriveSlayer (HermeticWiper). Analysis of the PartyTicket ransomware indicates it superficially encrypts files […]

Access Brokers: Who Are the Targets, and What Are They Worth?

Access brokers have become a key component of the eCrime threat landscape, selling access to threat actors and facilitating myriad criminal activities. Many have established relationships with big game hunting (BGH) ransomware operators and affiliates of prolific ransomware-as-a-Service (RaaS) programs. The CrowdStrike Intelligence team analyzed the multitude of access brokers' advertisements posted since 2019 and […]