How CrowdStrike Protects Against Data-Wiping Malware

crowdstrike.com/blog/how-crowdstrike-protects-against-data-wiping-malware/

Sarang Sonawane - Liviu Arsene January 31, 2022

- The Cybersecurity and Infrastructure Security Agency (CISA) warns of potential critical threats similar to recent cyberthreats targeting Ukraine
- U.S. companies are advised to implement cybersecurity measures to maximize resilience
- The CrowdStrike Falcon® platform provides continuous protection against wiper-style threats and real-time visibility across workloads

CISA recently advised U.S. business leaders to protect their companies from destructive malware that has been seen targeting Ukraine. This emphasizes the importance of having the right technologies in place. The automated detection and protection capabilities of the CrowdStrike Falcon platform protect customers from this malware, provide them with visibility into their environments and allow for intelligent monitoring of cloud resources. Falcon customers gain insights into overall security posture and the actions required to prevent potential security incidents.

Following mid-January 2022 incidents involving a series of Ukrainian website defacements and the deployment of data-wiping WhisperGate malware, CISA issued guidance on how companies can maximize resilience against similar incidents.

To better understand how WhisperGate malware operates, CrowdStrike Intelligence recently performed a technical analysis of the malicious bootloader and how the destructive wiping operation occurs.

The Falcon platform uses machine learning and behavior-based detections to provide continuous protection from threats — including data-wiping malware — and deliver real-time visibility across workloads.

A Primer on Destructive Malware

Destructive malware includes threats that render compromised systems inoperable by deleting or wiping critical data instead of making it inaccessible through encryption.

In 2017, two destructive ransomware outbreaks — NotPetya and WannaCry — leveraged the EternalBlue vulnerability in the Server Message Block (SMB) protocol to quickly spread and infect vulnerable systems worldwide.

The NotPetya ransomware outbreak started in Ukraine, and shortly after security researchers found that a faulty encryption routine made file recovery impossible regardless of whether victims paid. The WannaCry ransomware outbreak that followed also made data recovery impossible, as the ransomware could not tie payment to a particular victim machine.

The recent WhisperGate threat targeting Ukraine features no decryption or data-recovery mechanism, and only performs destructive wiping operations on the infected host's hard drives. While the threat attempts to masquerade as genuine modern ransomware operations, it irrevocably corrupts the affected host's data. The CISA alert urges companies to immediately implement cybersecurity measures to protect their infrastructures.

Gain Visibility and Stop Threats with the Falcon Platform

The Falcon platform offers unified visibility, threat detection and continuous monitoring and compliance for any environment, enabling security teams to reduce the time it takes to detect and mitigate security risks.

The Falcon sensor employs behavior-based detections using indicators of attack (IOAs) and on-sensor and in-the-cloud machine learning to identify and block threats while incorporating intelligence derived by continuously monitoring tactics, techniques and procedures (TTPs) related to threats and threat actors.

Data-wiping threats, including the recent WhisperGate, perform destructive operations on the infected host's hard drive, making data unrecoverable. CrowdStrike Intelligence performed an analysis on the malicious bootloader, but WhisperGate also uses a downloader to retrieve

the final data-wiping payload. The Falcon platform uses on-sensor machine learning to detect and prevent the downloader before fetching the data-wiping component, as seen in the screenshot below.

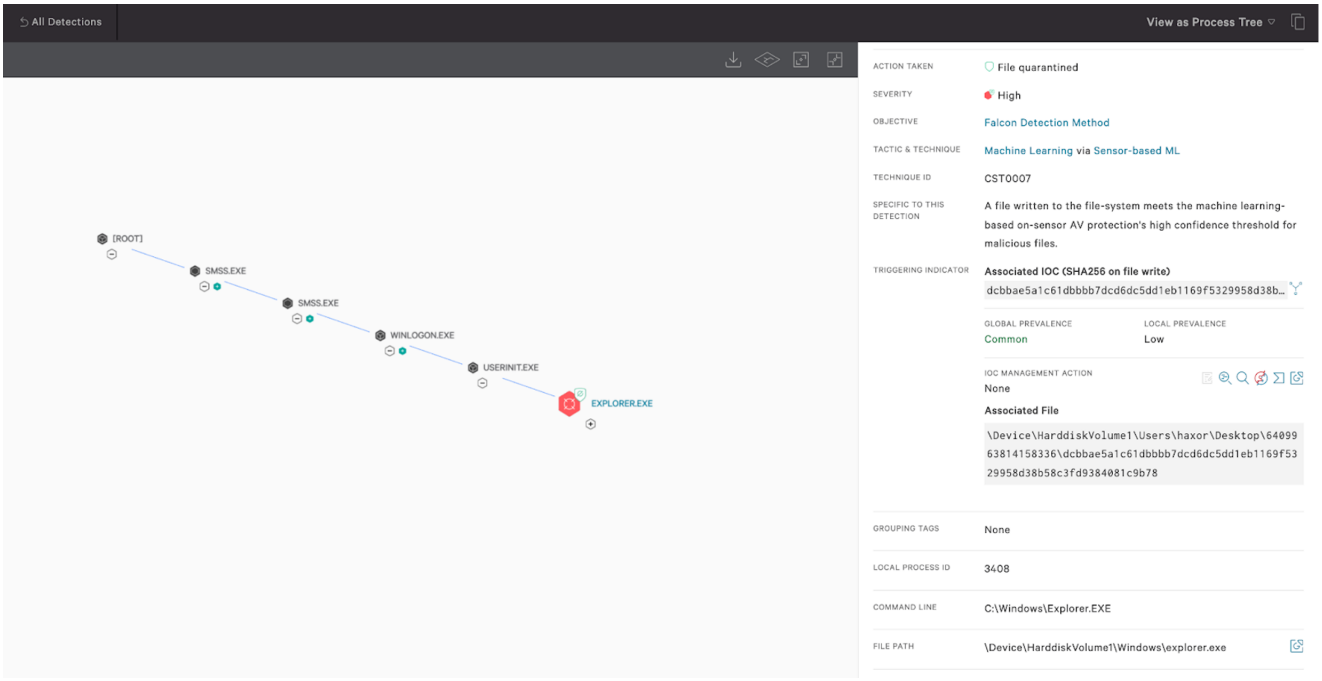

Figure 1. Falcon on-sensor machine learning coverage for the WhisperGate downloader component (Click to enlarge)

The data-wiping payload reads the file name and adds a random integer at the end of file. It then replaces the 0x100000 bytes of the file with hex 0xcc and renames the file, making the data unrecoverable, as seen in Figure 2.

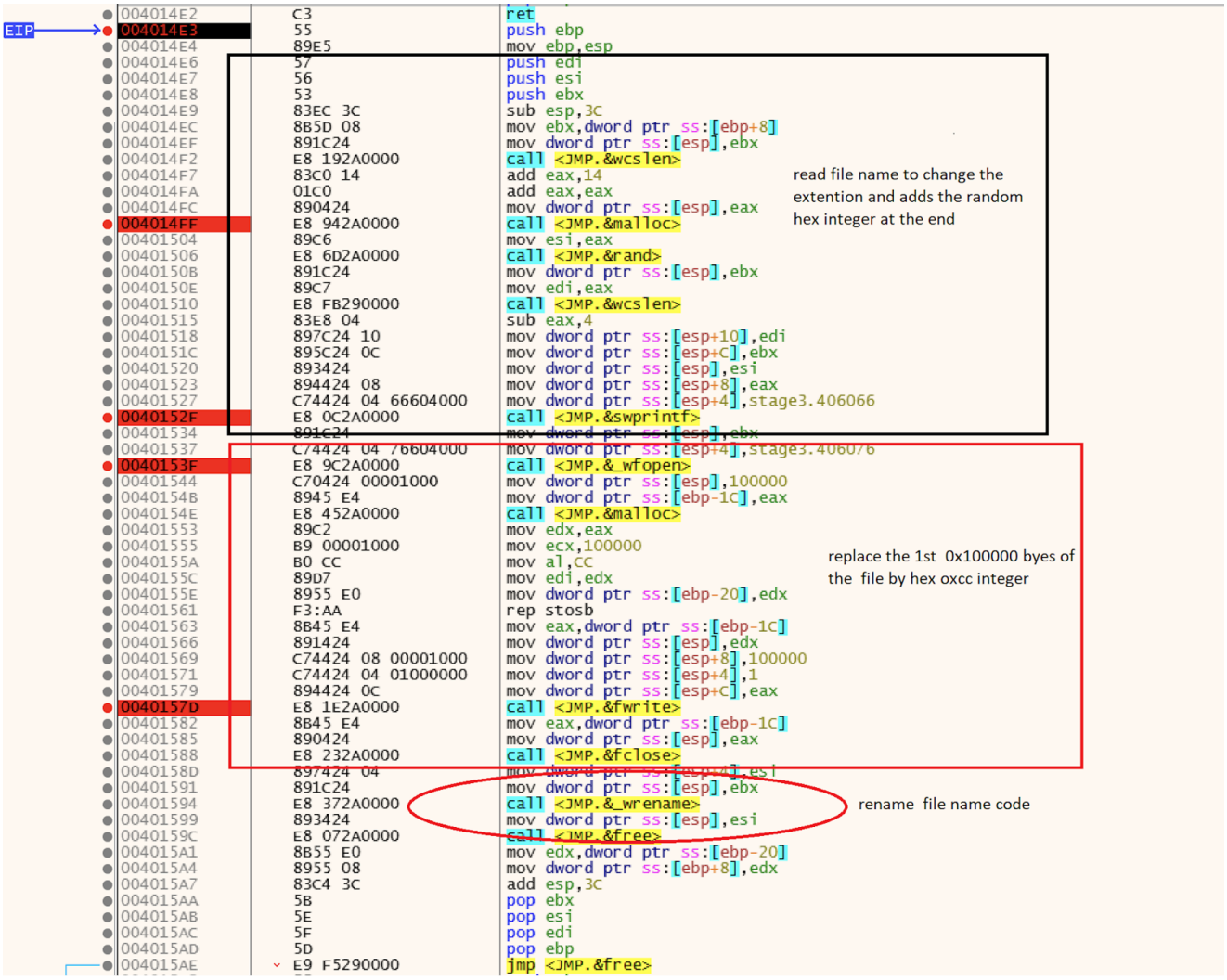

Figure 2. Data-wiping and file-renaming code (Click to enlarge)

The Falcon platform automatically detects and prevents the final data-wiping payload, using machine learning and behavior-based detection. Figure 3 reveals that the Falcon sensor immediately detects and protects from any data-wiping activity.

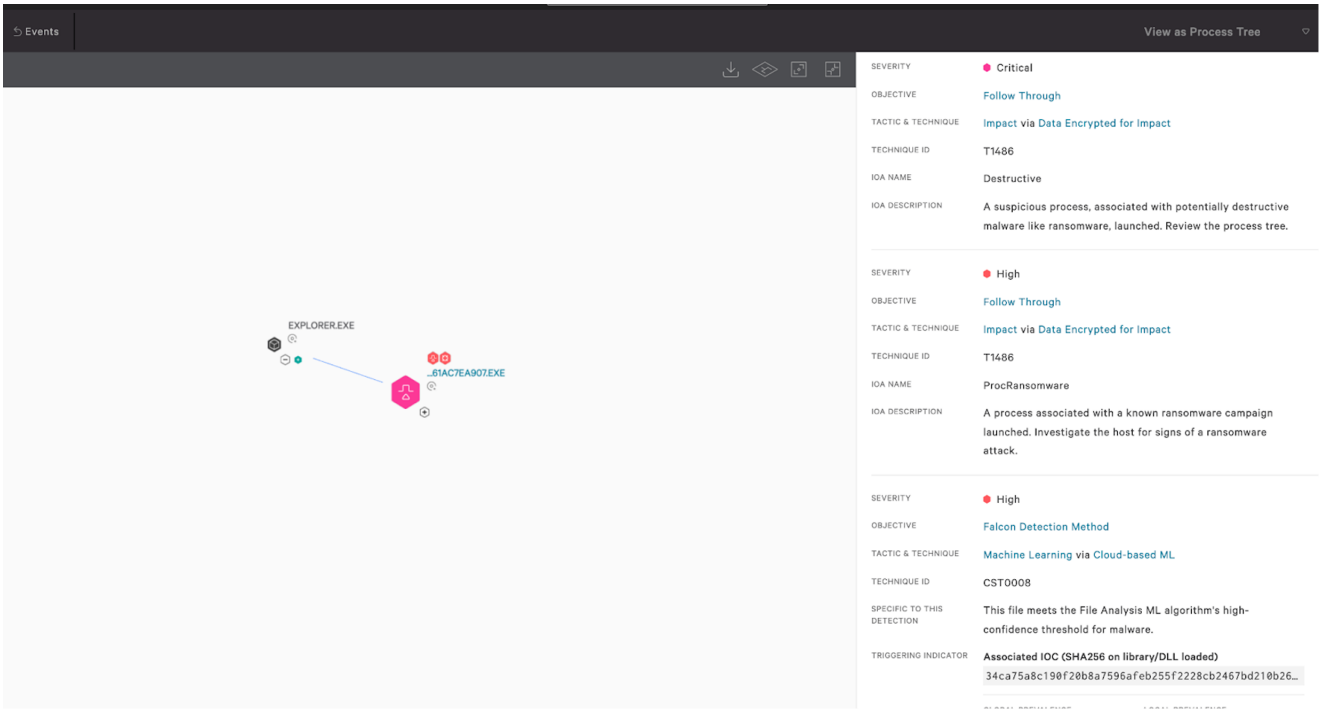

Figure 3. Falcon machine learning and IOA coverage for the data-wiping payload (Click to enlarge)

By accurately identifying malicious activity, gaining visibility into suspicious behaviors and prioritizing threats, the Falcon platform eliminates noise and reduces alert fatigue, allowing organizations to respond faster to potential threat incidents and gain deep visibility of potential security blind spots.

Maximize Resilience

Organizations that face risk from cyber incidents, including data-wiping threats, are strongly encouraged to take appropriate measures to protect their business from any significant impact on their operations.

CISA recommends that organizations take cyber risk and operational resilience seriously and take steps to reduce potential damages, detect intrusions and respond to potential threats.

The Falcon platform protects customers against sophisticated adversaries and sophisticated threats, accelerating response and offering visibility into the overall security posture of the organization. Organizations leveraging the power of the Falcon platform can detect and protect themselves from ransomware, data-wiping malware and other sophisticated threats and adversaries.

Additional Resources

- *Read more about WhisperGate in this CrowdStrike Intelligence blog: Technical Analysis of the WhisperGate Malicious Bootloader.*
- *Learn 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.*