

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.

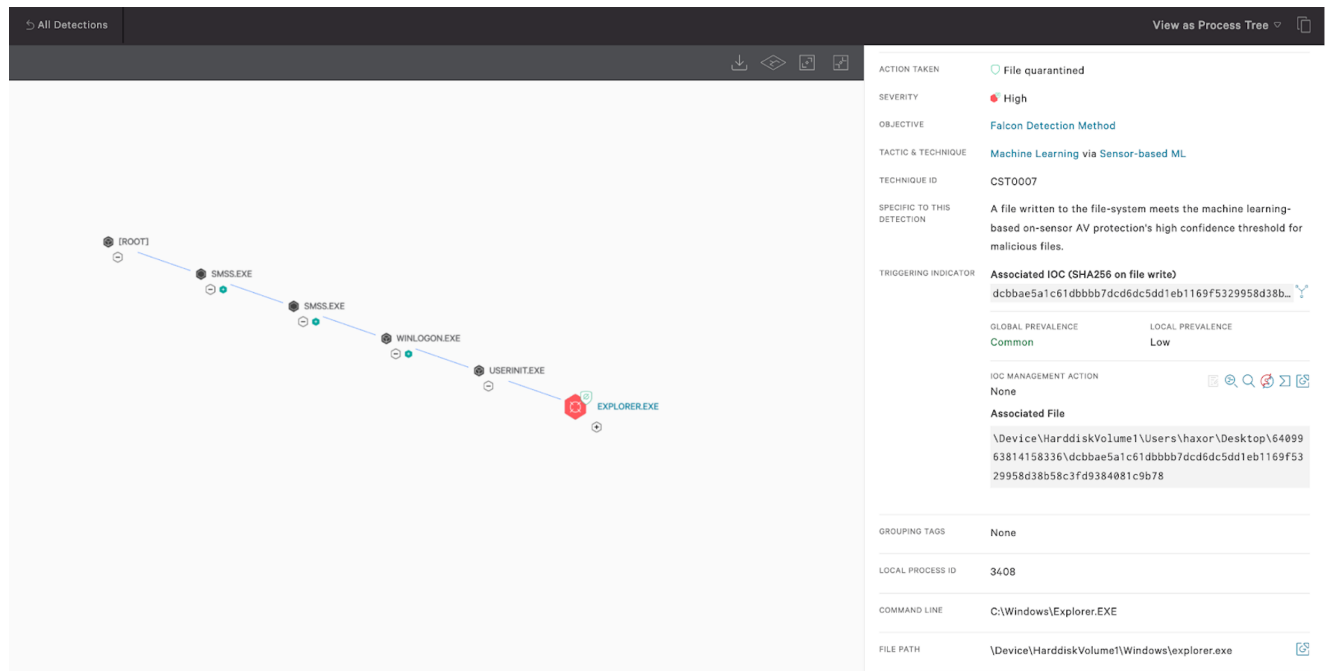


Figure 1. Falcon on-sensor machine learning coverage for the WhisperGate downloader component (Click to enlarge)

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.

004014E2	C3	ret	
004014E3	55	push ebp	
004014E4	89E5	mov ebp,esp	
004014E6	57	push edi	
004014E7	56	push esi	
004014E8	53	push ebx	
004014E9	83EC 3C	sub esp,3C	
004014EC	8B5D 08	mov ebx,dword ptr ss:[ebp+8]	
004014EF	891C24	mov dword ptr ss:[esp],ebx	
004014F2	E8 192A0000	call <JMP.&wcslen>	
004014F7	83C0 14	add eax,14	read file name to change the
004014FA	01C0	add eax,eax	extention and adds the random
004014FC	890424	mov dword ptr ss:[esp],eax	hex integer at the end
004014FF	E8 942A0000	call <JMP.&malloc>	
00401504	89C6	mov esi,eax	
00401506	E8 6D2A0000	call <JMP.&rand>	
0040150B	891C24	mov dword ptr ss:[esp],ebx	
0040150E	89C7	mov edi,eax	
00401510	E8 FB290000	call <JMP.&wcslen>	
00401515	83E8 04	sub eax,4	
00401518	897C24 10	mov dword ptr ss:[esp+10],edi	
0040151C	895C24 0C	mov dword ptr ss:[esp+C],ebx	
00401520	893424	mov dword ptr ss:[esp],esi	
00401523	894424 08	mov dword ptr ss:[esp+8],eax	
00401527	C74424 04 66604000	mov dword ptr ss:[esp+4],stage3.406066	
0040152F	E8 0C2A0000	call <JMP.&swprintf>	
00401534	891C24	mov dword ptr ss:[esp],ebx	
00401537	C74424 04 76604000	mov dword ptr ss:[esp+4],stage3.406076	
0040153F	E8 9C2A0000	call <JMP.&w fopen>	
00401544	C70424 00001000	mov dword ptr ss:[esp],100000	
00401548	8945 E4	mov dword ptr ss:[ebp-1C],eax	
0040154E	E8 452A0000	call <JMP.&malloc>	
00401553	89C2	mov edx,eax	
00401555	B9 00001000	mov ecx,100000	replace the 1st 0x100000 bytes of
0040155A	B0 CC	mov al,CC	the file by hex 0xcc integer
0040155C	89D7	mov edi,edx	
0040155E	8955 E0	mov dword ptr ss:[ebp-20],edx	
00401561	F3:AA	rep stosb	
00401563	8B45 E4	mov eax,dword ptr ss:[ebp-1C]	
00401566	891424	mov dword ptr ss:[esp],edx	
00401569	C74424 08 00001000	mov dword ptr ss:[esp+8],100000	
00401571	C74424 04 01000000	mov dword ptr ss:[esp+4],1	
00401579	894424 0C	mov dword ptr ss:[esp+C],eax	
0040157D	E8 1E2A0000	call <JMP.&fwrite>	
00401582	8B45 E4	mov eax,dword ptr ss:[ebp-1C]	
00401585	890424	mov dword ptr ss:[esp],eax	
00401588	E8 232A0000	call <JMP.&fclose>	
0040158D	897424 04	mov dword ptr ss:[esp+4],esi	
00401591	891C24	mov dword ptr ss:[esp],ebx	
00401594	E8 372A0000	call <JMP.&wrename>	rename file name code
00401599	893424	mov dword ptr ss:[esp],esi	
0040159C	E8 072A0000	call <JMP.&free>	
004015A1	8B55 E0	mov edx,dword ptr ss:[ebp-20]	
004015A4	8955 08	mov dword ptr ss:[ebp+8],edx	
004015A7	83C4 3C	add esp,3C	
004015AA	5B	pop ebx	
004015AB	5E	pop esi	
004015AC	5F	pop edi	
004015AD	5D	pop ebp	
004015AE	E9 F5290000	jmp <JMP.&free>	

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.

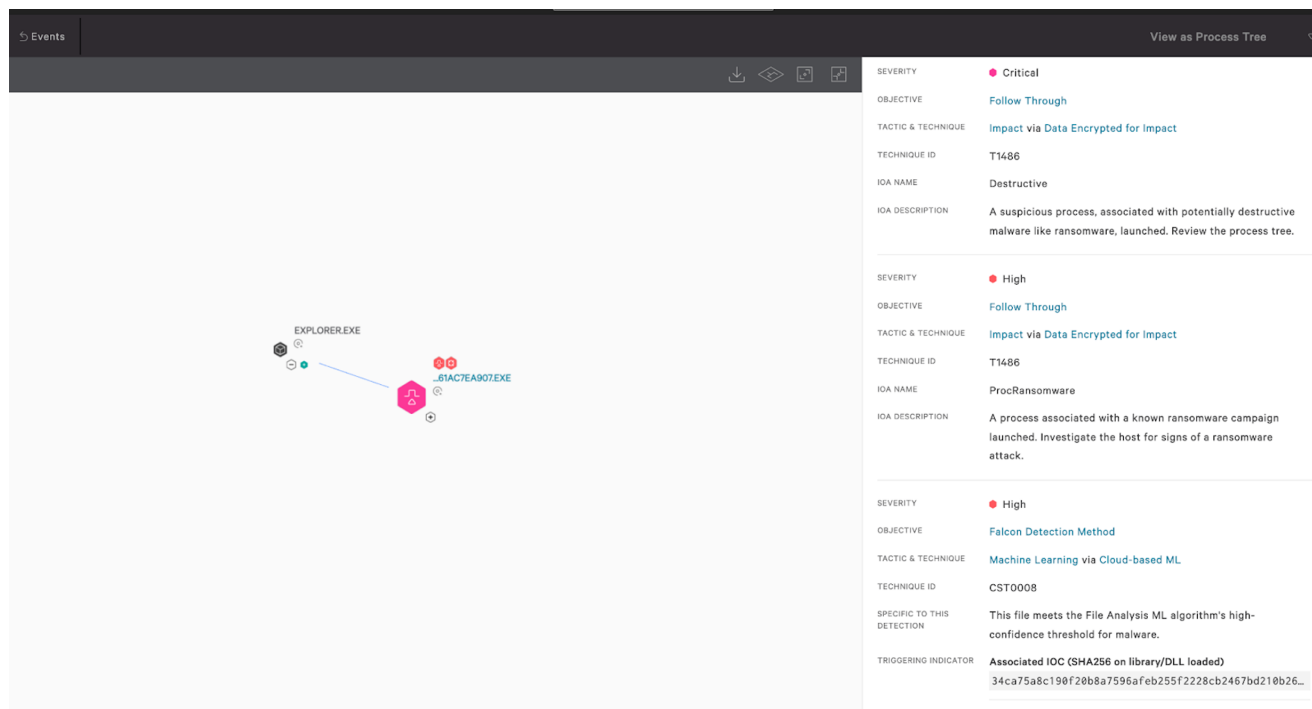


Figure 3. Falcon machine learning and IOA coverage for the data-wiping payload (Click to enlarge)

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.