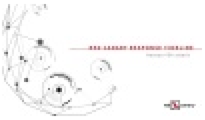
See what it's like to have a partner in the fight.

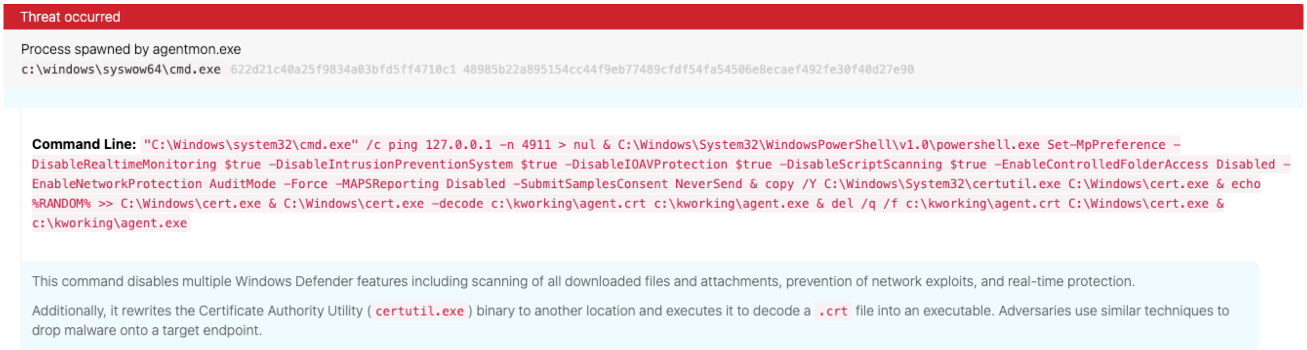
redcanary.com/blog/uncompromised-kaseya/

We’re rewinding the clock a bit to tell the tale of how we detected and helped prevent REvil (aka Sodinokibi) activity associated with zero days in Kaseya’s IT management software last year, before we or anyone else knew about the vulnerabilities, their impact, or the severity of follow-on ransomware attacks. For some, this story is a stark reminder of the importance of incident response planning and intelligence. For others—practitioners tasked with defending networks large and small—it also brings into focus the efficacy of developing broad, behavior-based detections.



How it started

Just after 1 PM (ET) on July 2, 2021, an adversary leveraged the Kaseya Virtual System Administrator (VSA) agent `agentmon.exe` to launch the command processor and execute a variety of malicious actions. Within five minutes, the Red Canary detection engineering team was investigating events generated by this suspicious activity.



Threat occurred

Process spawned by agentmon.exe

```
c:\windows\syswow64\cmd.exe 622d21c40a25f9834a03bfd5ff4710c1 48985b22a895154cc44f9eb77489cfdf54fa54506e8ecaef492fe30f40d27e90
```

Command Line: `"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 4911 > nul & C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %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.exe & c:\kworking\agent.exe`

This command disables multiple Windows Defender features including scanning of all downloaded files and attachments, prevention of network exploits, and real-time protection.

Additionally, it rewrites the Certificate Authority Utility (`certutil.exe`) binary to another location and executes it to decode a `.crt` file into an executable. Adversaries use similar techniques to drop malware onto a target endpoint.

The command-line arguments in question included two groupings of conspicuously suspicious actions, both of which were caught by existing Red Canary detection analytics:

1.
    1. Multiple commands designed to disable Windows Defender security features
    2. The relocation and execution of the Windows Certificate Authority Utility (`certutil.exe`) to decode a `.crt` file

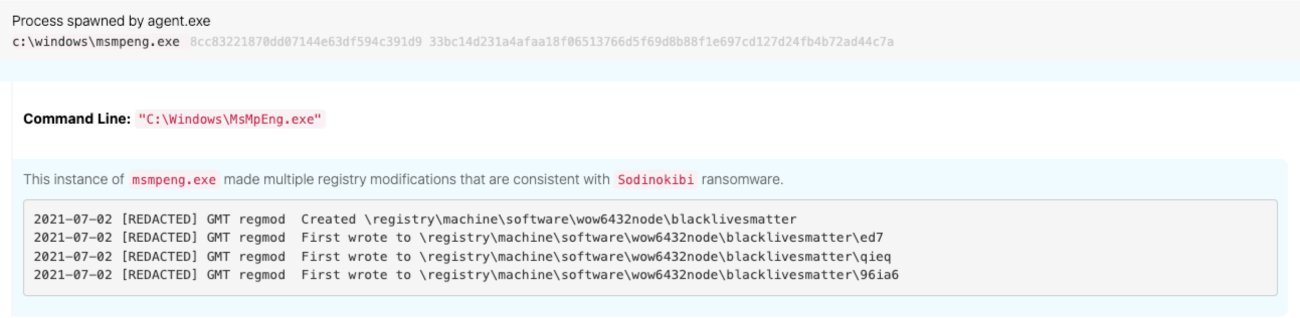
While the purpose of the former commands is self-evident (the adversary wanted to evade defensive controls), the latter activity requires some explanation.

Sidebar: Decoding malicious payloads with `certutil.exe`

Nearly five years ago, then detection engineer manager Joe Moles committed a new detection analytic to our detector repo that looked for adversaries leveraging `certutil.exe` to decode malicious payloads. Adversaries consistently use this utility to deliver malicious payloads, and we've observed this behavior in hundreds of confirmed threat detections since initially developing the detection analytic.

The ultimate payload

All of this activity was merely pretense. Less than an hour after detecting the initial defense evasion and execution activity, we observed a series of malicious registry modifications.



Process spawned by agent.exe

```
c:\windows\msmpeng.exe 8cc83221870dd07144e63df594c391d9 33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a
```

Command Line: `"C:\Windows\MsMpEng.exe"`

This instance of `msmpeng.exe` made multiple registry modifications that are consistent with `Sodinokibi` ransomware.

```
2021-07-02 [REDACTED] GMT regmod  Created \registry\machine\software\wow6432node\blacklivesmatter
2021-07-02 [REDACTED] GMT regmod  First wrote to \registry\machine\software\wow6432node\blacklivesmatter\ed7
2021-07-02 [REDACTED] GMT regmod  First wrote to \registry\machine\software\wow6432node\blacklivesmatter\qieq
2021-07-02 [REDACTED] GMT regmod  First wrote to \registry\machine\software\wow6432node\blacklivesmatter\96ia6
```

Thanks to research conducted by our Intelligence team in late 2020 and open source reports by the likes of Unit 42, we were immediately able to associate these registry modifications with a known ransomware threat called REvil, based on the following registry modification paths:

- `Software\blacklivesmatter`
- `software\wow6432node\blacklivesmatter`

Within 12 minutes of this threat occurring, the Red Canary Incident Handling team was proactively reaching out to the affected customer to help them begin responding to the incident. Unfortunately, the customer's security team was off for the holiday weekend and were part of a legacy customer group that hadn't upgraded their contract to include access to Automate. Recognizing the severity of the situation, we activated Automate, developed some custom playbooks, and started automatically banning hashes, collecting forensics packages, and isolating endpoints within roughly two hours of the initial threat occurring.

Additional detections

In isolation, this was just a single instance of an adversary using the Kaseya IT management platform to deliver a malicious payload. In fact, this wasn't the first time we'd observed adversaries abusing Kaseya in an effort to deliver ransomware.

However, just 23 minutes after the first threat occurred, we observed the same behavior in a second customer environment. Roughly an hour after the initial threat, we detected this behavior in a third environment. This process—excepting the response complications for the first customer—effectively repeated itself across two more customers and dozens of endpoints over the span of three days.

Internal and external intelligence

Less than an hour and a half after the initial threat occurred, the Red Canary Threat Research and Intelligence teams had finished reverse engineering the ransomware payload and began drafting up their findings.

While we were working incidents across multiple customers, initial public information started to appear on Reddit and Twitter roughly an hour after we initially detected the threat. Kaseya eventually acknowledged the incidents in a formal announcement roughly two-and-a-half hours after our first detections.

Customer communication

A little more than six hours after the initial threat occurred, the Red Canary Threat Intelligence team had compiled everything we knew about this incident—information drawn from customer detections, reverse engineering, and open source reporting, to name a few sources—into a bulletin that we promptly sent to every Red Canary customer.

In retrospect

In the days that followed the incident, we learned that REvil had exploited a series of four zero-day vulnerabilities in Kaseya, which ultimately enabled the group to gain initial access, upload the malicious payload, bypass security controls, and execute the payload. Kaseya would eventually patch these vulnerabilities on July 11.

A zero day is just a means to an end. It might provide an adversary access, elevate their privileges, or help them perform a variety of other actions. That aside, the exploitation of any vulnerability—known or unknown—is just one part of a much broader campaign that almost certainly involves other activity. By developing a robust behavioral detection program, security teams can achieve a level of defense in depth that offers visibility into—and protection against—a wide variety of threats, regardless of the techniques at hand.

Related Articles

Detection and response

ChromeLoader: a pushy malvertiser

Detection and response

Intelligence Insights: May 2022

Detection and response

The Goot cause: Detecting Gootloader and its follow-on activity

Detection and response

Marshmallows & Kerberoasting

This website uses cookies to improve your experience while you navigate through the website. Out of these cookies, the cookies that are categorized as necessary are stored on your browser as they are essential for the working of basic functionalities of the website. We also use third-party cookies that help us analyze and understand how you use this website. These cookies will be stored in your browser only with your consent. You also have the option to opt-out of these cookies. But opting out of some of these cookies may have an effect on your browsing experience.

Necessary cookies are absolutely essential for the website to function properly. This category only includes cookies that ensures basic functionalities and security features of the website. These cookies do not store any personal information.

Any cookies that may not be particularly necessary for the website to function and is used specifically to collect user personal data via analytics, ads, other embedded contents are termed as non-necessary cookies. It is mandatory to procure user consent prior to running these cookies on your website.