Kaseya Ransomware Supply Chain Attack: What You Need To Know

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/kaseya-ransomware-supply-chain

UPDATE July 5 2021: *Our blog has been updated with more details on how the ransomware was executed along with additional protection information.*

Several hundred organizations have been targeted by the REvil (aka Sodinokibi) ransomware in a supply chain attack involving Kaseya VSA software and multiple Managed Service Providers (MSPs) who use it. News of the attack broke yesterday (Friday 3 July), prompting Kaseya to urge VSA users to shut down their VSA servers to prevent them from being compromised. The attack may have been timed to coincide with the 4th of July holiday weekend in the U.S., where many organizations may be lightly staffed.

Are Symantec customers protected?

Yes, Symantec Endpoint products proactively blocked tools used to deliver the ransomware payload in this wave of attacks.

How many organizations are affected?

According to Kaseya only a very small percentage of their customers were affected, “currently estimated at fewer than 40 worldwide”. However, each of those organizations may be MSPs with multiple customers. Current reports suggest hundreds of victims.

How was REvil delivered to computers during these attacks?

While the exploit used to breach Kaseya VSA server side has not yet been fully documented, it is known that the attackers delivered a malicious script and an ASCII PEM named agent.crt to Kaseya VSA clients. The dropper masqueraded inside the ASCII PEM file, which was decoded using certutil after attempts to disable Microsoft Defender. It dropped two resources, an old, but legitimate copy of Windows Defender (MsMpEng.exe) and custom malicious loader. The dropper writes the two files to disk and executes MsMpEng.exe which then side loads and executes the custom loader's export (mpsvc.dll).

What was the motivation for the attacks?

REvil attacks are usually financially motivated. However, there are some signs that the attacks may be politically motivated disruption. The attackers have, on occasion, appeared to have a political motive in their selection of targets.

In this attack, strings in the payload made references to President Joe Biden, ex-president Donald Trump, and Black Lives Matter. The attackers demanded a ransom of $45,000, which may be another reference to Trump, who was the 45th president of the U.S.

Furthermore, REvil’s Tor payment site is down at the time of writing, meaning victims will have no way of paying a ransom. Whether the group is having technical difficulties or whether it never intended to collect a ransom remains unclear.

What is REvil/Sodinokibi?

REvil (detected as Ransom.Sodinokibi) is a family of ransomware developed by a cybercrime group Symantec calls Leafroller. The ransomware is used in targeted attacks, where the attackers attempt to encrypt all computers on the victim’s network in the hope of extorting a large ransom. The group is known to steal victim data prior to encryption and threaten to release it unless a ransom is paid.

Leafroller is one of the most established and prolific targeted ransomware groups in operation. Prior to its development of REvil, the group was associated with an older ransomware family known as Gandcrab. Leafroller is known to operate a Ransomware-as-a-Service, where its sells its tools to collaborators known as affiliates in exchange for a cut of any ransom payments they obtain.

Protection/Mitigation

Tools associated with these attacks will be detected and blocked on machines running Symantec Endpoint products.

File-based protection:

- Downloader
- Heur.AdvML.C
- Packed.Generic.618
- Ransom.Sodinokibi
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

Network-based protection:

- Ransom.Gen Activity 29
- Audit: Ransom.Gen Activity 55

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e - Dropper

df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e - Dropper

dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f - Dropper

aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7 - Dropper

66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8 - Dropper

81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471 - Dropper

1fe9b489c25bb23b04d9996e8107671edee69bd6f6def2fe7ece38a0fb35f98e - Dropper

8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd - Sodinokibi

e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2 - Sodinokibi

d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20 - Sodinokibi

d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f - Sodinokibi

cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6 - Sodinokibi

0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402 - Sodinokibi

8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f - Sodinokibi