Netskope Threat Coverage: REvil

By Gustavo Palazolo

Published: 2021-07-07 · Archived: 2026-04-06 00:31:42 UTC

Summary

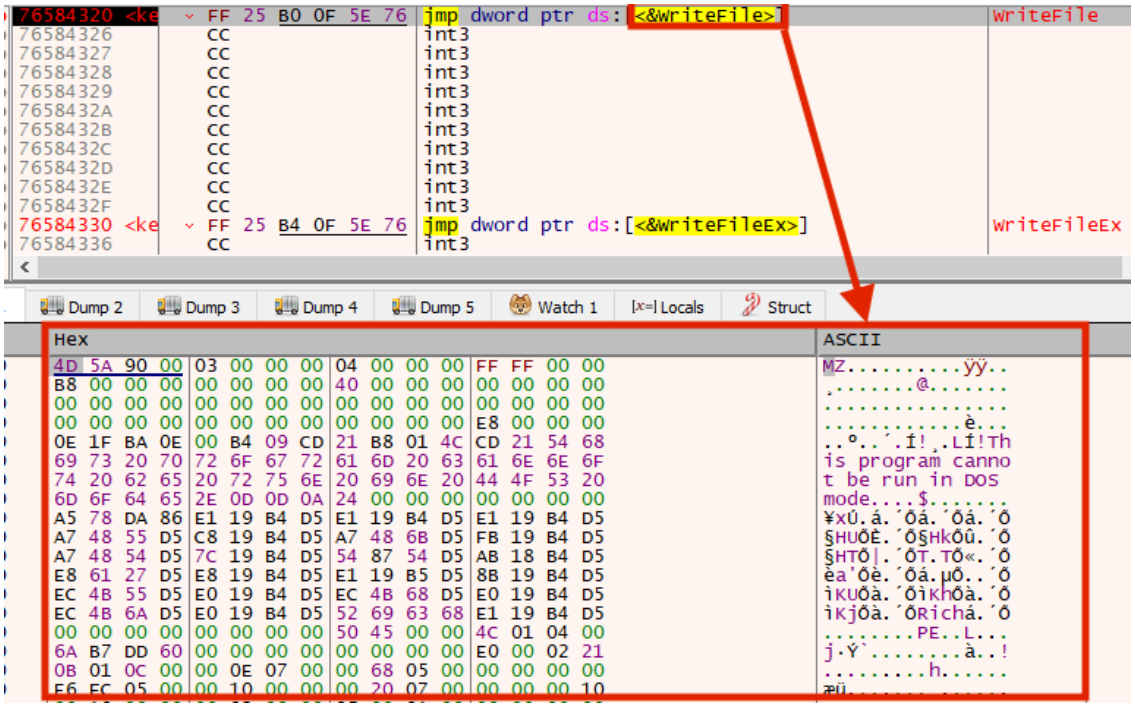
The REvil ransomware (a.k.a Sodinokibi) is a threat group that operates in the RaaS (Ransomware-as-a-Service) model, where the infrastructure and the malware are supplied to affiliates, who use the malware to infect target organizations. On July 2, the REvil threat group launched a supply chain ransomware attack using an exploit in Kaseya's VSA remote management software. REvil claims to have infected more than one million individual devices around the world. The attackers demanded $45,000 USD to restore the files from a single infected device, or $70 million USD paid in BTC for a universal decrypter that will allegedly work for all of the victims of the Kaseya attack. This threat is targeting anyone with Kaseya's VSA Remote Management Platform agent installed on Microsoft Windows systems (any version).

Threat

The REvil group has likely used a zero-day exploit against Kaseya's management server, allowing the attackers to deploy the malware remotely on Windows devices running the VSA agent application. The first step executed by the group was to deploy a base64-encoded file to Kaseya's working directory, which was probably ignored by anti-virus engines as recommended by Kaseya.

Once the encoded file (`agent.crt`) was deployed, the attacker executed a set of shell commands remotely to decode and execute the payload, as well as to disable the Windows Defender protections. The decoded file (`agent.exe`) is a malware dropper that writes to disk two different files:

1. `MsMpEng.exe` : This is an outdated version of Microsoft's Antimalware Service that is vulnerable to a technique known as DLL Hijacking.
2. `mpsvc.dll` : This is the packed REvil payload, which is loaded by `MsMpEng.exe` through the DLL Hijacking technique.



“Agent.exe” writing REvil packed payload “mpsvc.dll” to disk

Once executed, the REvil packed sample loads and executes a small shellcode, which is responsible for unpacking and executing the final payload, which contains an encrypted configuration within the binary.

REvil ransomware encrypted configuration

The data is encrypted with RC4, so we can use a small Python script to decrypt it:

Decrypting REvil configuration using Python

After decrypting the configuration, we can obtain more detailed information about the sample, such as the “affiliate” ID, ignored folders, C2 domains, etc.

Part of the decrypted REvil configuration

In this case, the “net” option is set to “false” in the configuration, which tells the ransomware to ignore the C2 addresses. However, in case this option is set to “true,” the malware sends a POST request to available addresses with information about the infected machine, such as the encryption key and the machine name.

REvil ransomware preparing to send the POST request to the C2

Within this REvil configuration, we have found 1,221 unique domains that could be used for network communication.

After encrypting the files, REvil changes the user's background:

Image set by REvil as the user's background

Also, the ransom note is created in the directories where there are encrypted files:

Part of REvil ransom note

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured coverage for all known threat indicators and payloads.

- **Netskope Threat Protection**
  - `Generic.Ransom.Sodinokibi.B.8FB3E6FD`
  - `Gen:Variant.Ransom.Sodinokibi.61`
  - `Gen:Variant.Razy.525651`
- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
  - `Gen.Malware.Detect.By.StHeur` indicates a sample that was detected using static analysis
  - `Gen.Malware.Detect.By.Sandbox` indicates a sample that was detected by our cloud sandbox

Sample Hashes

Name	sha256
agent.exe	d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
mpsvc.dll	e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
mpsvc.dll	8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
unpacked	5286889a725a109df74bdee612ce2c288a61970d3126c466c4e8c5cde1cc23c3

A full list of sample hashes, domains, and a tool to extract and decrypt the config from a REvil sample are available in our Git repo.
