

# Netskope Threat Coverage: REvil

---

 [netskope.com/blog/netskope-threat-coverage-revil](https://netskope.com/blog/netskope-threat-coverage-revil)

Gustavo Palazolo

July 7, 2021



## 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 `MsMpEng.exe` : This is an outdated version of Microsoft's Antimalware Service that is vulnerable to a technique known as DLL Hijacking.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.

```

76584320 <ke > FF 25 B0 0F 5E 76 jmp dword ptr ds: [<&writeFile>] writeFile
76584326 CC int3
76584327 CC int3
76584328 CC int3
76584329 CC int3
7658432A CC int3
7658432B CC int3
7658432C CC int3
7658432D CC int3
7658432E CC int3
7658432F CC int3
76584330 <ke > FF 25 B4 0F 5E 76 jmp dword ptr ds: [<&writeFileEx>] writeFileEx
76584336 CC int3
  
```

Hex	ASCII
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	.....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00	.....è.....
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..°..'i!..L!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....\$......
A5 78 DA 86 E1 19 B4 D5 E1 19 B4 D5 E1 19 B4 D5	¥xÙ.á. 'óá. 'óá. 'ó
A7 48 55 D5 C8 19 B4 D5 A7 48 6B D5 FB 19 B4 D5	§HUÓÈ. 'Ó§HKÓÙ. 'Ó
A7 48 54 D5 7C 19 B4 D5 54 87 54 D5 AB 18 B4 D5	§HTÓ  . 'ÓT. TÓ«. 'Ó
E8 61 27 D5 E8 19 B4 D5 E1 19 B5 D5 8B 19 B4 D5	èa'òè. 'óá. μó. 'ó
EC 4B 55 D5 E0 19 B4 D5 EC 4B 68 D5 E0 19 B4 D5	ìKUòá. 'óìKHòá. 'ó
EC 4B 6A D5 E0 19 B4 D5 52 69 63 68 E1 19 B4 D5	ìKjòá. 'óRìchá. 'ó
00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00	.....PE..L...
6A B7 DD 60 00 00 00 00 00 00 00 00 E0 00 02 21	j.ÿ'.....à..!
0B 01 0C 00 00 0E 07 00 00 68 05 00 00 00 00 00	.....h.....
E6 FC 05 00 00 10 00 00 00 20 07 00 00 00 00 10	πü.....

“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.

Legend:

- Decryption Key
- Encrypted Config
- PE Section

Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Nur
>	400	C400	1000	C324	60000020	0	0	0
>	C800	2E00	E000	2DA8	40000040	0	0	0
>	F600	2200	11000	25E0	C0000040	0	0	0
>	11800	C800	14000	C800	C0000040	0	0	0
>	1E000	800	21000	74C	42000040	0	0	0

### REvil ransomware encrypted configuration

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

```
>>> enc_data = pefile.PE(fp).sections[3].get_data()
>>> dec_key = enc_data[0:0x20]
>>> dec_data = ARC4(dec_key).decrypt(enc_data[0x28:0x28 + struct.unpack('<I', enc_data[0x24:0x28])[0] - 1])
>>> dec_data[:200]
b'{"pk": "9/AgyLvWEviWbvuyR2k0Q140e9LZJ5hwrmt0/zCyFM=", "pid": "$2a$12$pr0X/4eKl8zrp6SC5lnHPecev5N0ck0UW5r3s4JJYDnZZSghvBkq", "sub": "8254", "dbg": false, "et": 0, "wipe": true, "wht": {"fld": ["program files", "app'
```

### 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.

```

],
"dmn": "boisehosting.net;fotoideaymedia.es;dubnew.com;
"net": false,
"svc":
[
  "veeam",
  "memtas",
  "sql",
  "backup",
  "vss",
  "sophos",
  "svc$",
  "mepocs"
],
"nbody": "LQAtAC0APQA9AD0AIABXAGUAbABjAG8AbQB\AC4AIABB
"name": "{EXT}-readme.txt",
"exp": false,
"img": "QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzAC
"arn": false,
"rdmcnt": 0

```

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.

```

push eax
push esi
push esi
push dword ptr ss:[ebp+8]
inc ecx
mov dword ptr ss:[ebp-44],esi
mov dword ptr ss:[ebp-40],esi
mov dword ptr ss:[ebp-3c],esi
mov dword ptr ss:[ebp-38],esi
mov dword ptr ss:[ebp-34],ecx
mov dword ptr ss:[ebp-2c],esi
mov dword ptr ss:[ebp-28],esi
mov dword ptr ss:[ebp-24],esi
mov dword ptr ss:[ebp-20],esi
mov dword ptr ss:[ebp-1c],esi
mov dword ptr ss:[ebp-18],ecx
mov dword ptr ss:[ebp-14],esi
mov dword ptr ss:[ebp-10],esi
call dword ptr ds:[<&winHttpCrackur1>]

```

[ebp+8]:L"https://eraorastudio.com/admin/pics/yabxwciiphsh.gif"

*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:

All of your files are encrypted!

Find 77s9x27u-readme.txt and follow instructions

*Image set by REvil as the user's background*

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

```
---=== Welcome. Again. ===---
```

```
[-] Whats HapPen? [-]
```

```
Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 77s9x27u.
```

```
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).
```

```
[+] What guarantees? [+]
```

```
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
```

```
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
```

```
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.
```

```
[+] How to get access on website? [+]
```

```
You have two ways:
```

*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](#).