Kaseya: Attacked with Ransomware

7/6/2021

What Happened?

On Friday July 2nd, a ransomware group launched a widespread crypto-extortion attack, targeting MSPs and ultimately their largest customers. A comprehensive technical write-up of the attack and how it was perpetrated is available from our partners at Sophos. You can read it here: https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

What do I need to know?

A vulnerability in the Kaseya software was leveraged to deploy what is known as a 'supply chain ransomware attack'. If successful, any client machine accessible via Kaseya could eventually fall victim to this ransomware attack.

What is Kaseya?

Kaseya is the maker of a very popular remote management and monitoring software, used by over 4000 managed service providers and internal IT departments. It provides automation of IT tasks like software deployment and patch management and allows remote access for support technicians who are logged in to the Kaseya VSA. Packet Fusion uses Kaseya VSA to remotely monitor and manage your unified communication and contact center environments.

Kaseya VSA?

Kaseya VSA refers to the servers in our datacenter that run the Kaseya server software and work with the agents (Kaseya client software installed on your servers that are managed by Packet Fusion).

What is Packet Fusion doing to protect me?

Packet Fusion took swift action to minimize the spread of this attack - we immediately shut down our Kaseya server which would prevent it from propagating any harmful software out to our other managed servers, and subsequently our customers' environments.

Is my environment in danger?

No. We have been provided with tools to scan our systems and detect whether we were impacted by this attack, and our scans report that our systems are clean. Since our Kaseya VSA was not impacted, we can confidently state your systems are safe and you will not be impacted by this attack.*

So, business as usual, then?

Not exactly. We are proceeding cautiously and keeping our Kaseya platform offline for the time being. This will give Kaseya plenty of time to fully investigate and mitigate this attack. With Kaseya unavailable we will not be able to remotely monitor for signs of trouble in your environment, deploy patches, or remotely access your environment without a "knock and enter" style remote access mechanism, such as LogMeIn Rescue.

What's next?

Kaseya has published a runbook of changes to make to VSA servers. Indicated within the runbook, a patch will be issued this week to correct the vulnerability exploited to carry out this ransomware attack. Packet Fusion will follow the runbook's guidance to add additional layers of security to our environment,

and we will apply the patch from Kaseya when they release it on Sunday, July 11. However, we will not be immediately returning our Kaseya VSA to service. We are still evaluating activating our Kaseya environment and resuming operations, as well as other options to reinstate our proactive monitoring and remote access abilities.

I still have questions

We'd love to hear from you. Feel free to reach out to Packet Fusion Support – you can always open a case in our support portal or give us a call at 925-701-2020. When calling for support, please note we've added a new option in our support menu. When prompted, press 1 to access our Kaseya group for all of your Kaseya related issues.

*This does not apply to our customers who maintain their own premises based Kaseya VSA for internal IT departments' use