Kaseya suffers a supply chain cyber-attack resulting in up to 1,500 businesses being affected.

Author by Jeremiah Cristobal; Security Television Network

FULL TEXT

September 2, 2021 (Security Television Network) -- Kaseya suffers a supply chain cyber-attack resulting in up to 1,500 businesses being affected.

On July 2, 2021, Kaseya was targeted by a ransomware attack that resulted in between 800 and 1,500 businesses all around the world being affected. This ranged with their clients being inconvenienced to outright being closed down due to the seriousness of the situation.

Kaseya is an IT Management Software company that is known for their Unified Remote Monitoring &Management software platform, or Kaseya VSA. This type of software helps out with organizing and managing a company's IT whether that be a small start-up or a well-known company. The company is able to increase the efficiency of IT departments by implementing automated IT management software (Kaseya Home Page, 2021).

On July 2, 2021, Kaseya was hit by a ransomware attack that spread to not only the company but to their clients as well. The clients would range from around 800 to 1500 businesses all around the world. Some of the businesses were merely inconvenienced for dentists' offices or accountants but the effect was felt the most by the Swedish supermarket company COOP. Hundreds upon hundreds of supermarkets were closed due to their cash registers not working. Other businesses that were affected greatly were schools in New Zealand, not having any internet (Satter, 2021).

The culprits came out with a ransom note following the attack. This was targeted to the clients of Kaseya and would confuse the business owners on what to do. The ransomware attack was identified as a REvil ransomware attack, a hacker group based in Russia who encrypted businesses' files.

The hacker group had asked for $70 million in exchange for the restoration of the encrypted files and were willing to negotiate a better price if the company were to entertain the idea of negotiation (Panettieri, 2021).

The CEO of Kaseya, Fred Voccola, had stated that "I can't comment 'yes,' 'no,' or 'maybe', No comment on anything to do with negotiating with terrorists in any way. In the topic of Voccola, he also got in contact with the White House, the FBI, and the Department of Homeland Security to reassure them that the breach did not introduce any "national risk".

Fred Voccola, Source: KaseyaFrom July 6 until July 13, Kaseya had been slowly but surely getting their infrastructure back on track. They had encountered a few setbacks with vulnerability issues, leaks in their security, and fake emails.

Due to the quick response of Kaseya and help from third parties, on July 13 Kaseya was able to say to their clients that their VSA has been restored with some guidance from the Cybersecurity and Information Security Agency. Moreover REvil, the group responsible for the hack had mysteriously disappeared leaving the threat not as scary as before. Some have speculated that the U.S. Government was able to track them down or Vladimir Putin himself was able to call them off after President Joe Biden called up Putin in an effort to put an end to the ransomware group. Overall, this must have cost Kaseya and their clients millions upon millions and it is nice to see that it has been resolved. A tighter grip on their security will be needed and a sense of trust will be built right up for their clients.

References

Panettieri, J., 2021. Kaseya VSA Supply Chain Cyberattack Details, RMM Recovery Timeline - MSSP Alert. [online]

MSSP Alert. Available at: msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning [Accessed 13 July 2021].
Kaseya. 2021. Kaseya Home Page. [online] Available at: kaseya.com [Accessed 13 July 2021].Satter, R., 2021. Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says. [online] Reuters. Available at: reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05 [Accessed 13 July 2021].

Dr. James Halldrhall@security20.com(202) 607-2421
By Author: by Jeremiah Cristobal, Security Television Network

DETAILS

Subject:	Supply chains; Data encryption; Network security; Computer security; Ransomware; Television networks
Business indexing term:	Subject: Supply chains Ransomware
Location:	United States--US
Company / organization:	Name: Kaseya; NAICS: 541511
Publication title:	CNN Wire Service; Atlanta
Publication year:	2021
Publication date:	Sep 2, 2021
Section:	Regional
Publisher:	CNN Newsource Sales, Inc.
Place of publication:	Atlanta
Country of publication:	United States, Atlanta
Publication subject:	General Interest Periodicals--United States
Source type:	Wire Feed
Language of publication:	English
Document type:	News
ProQuest document ID:	2568312108
Document URL:	https://www.proquest.com/wire-feeds/kaseya-suffers-supply-chain-cyber-attack/docview/2568312108/se-2?accountid=38945

Copyright:	Copyright 2021 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.
Last updated:	2021-09-02
Database:	ProQuest Central