July 2021

Mendes Insights

Supply Chain Attacks: Kaseya and More

A software vendor suffers an attack and thousands downstream bear the brunt.

Cyber/Data Privacy and Security

The Rise of Supply Chain Attacks

At the end of 2020, it was SolarWinds and Microsoft Exchange. In May 2021, it was the Colonial Pipeline. For the 4th of July in 2021, it was Kaseya. The Department of Homeland Security, CISA (Cybersecurity & Infrastructure Security Agency) and the FBI distinguish supply chain attacks as events where software is compromised through cyber attacks, insider threats, or other malign activities at any stage throughout the software's entire lifecycle.[1] More simply put, these are a type of cyberattack where criminals target software vendors or IT service companies with the added objective of impacting their clients.

[1] https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf

In the SolarWinds scenario, the compromised stage was at “development” (infrastructure) and the initial impact appeared to be espionage. The source code compromise impacted enterprise networks across the private sector, federal, state, and local governments. The attacks often use simple deception techniques disguising malware as legitimate products.[2] In other scenarios the attackers access and modify the source code of genuine products. For Microsoft, it was an espionage group exploiting flaws in Microsoft Exchange Server email software, affecting 30,000 organizations in the U.S.[3] Then with the Colonial Pipeline attack, the group known as DarkSide forced one of the largest U.S. pipeline operators to shutdown operations, due to concerns that an attack on its business systems (not its operational systems) would have broader implications.

Supply chain attacks rose 42% in the first quarter of 2021 in the U.S.[4] The result can be a magnifier or multiplier effect of a single attack – instead of getting just one hospital or one plant, the attackers attempt to infiltrate numerous organizations’ systems via the common software utilized across sectors. While some of these attacks wreak widespread havoc, the financial impact may have been disparate, causing headaches for a few CISOs providing real-time updates to their boards plus some spending on investigation and systems hardening. The latest of these attacks illustrates the increasing potential for the scale of such events, impacting more and varying types of entities.

Kaseya Timeline

On Friday, July 2, 2021, Kaseya, a software vendor, was alerted to a potential attack involving its remote management software, VSA. Kaseya provides technology services to organizations around the world, including many managed service providers. Kaseya first notified its on-premises customers to immediately shutdown their VSA servers. Kaseya shutdown its SaaS Servers as a precautionary measure, even though it had not received any reports of compromise from any SaaS or hosted customers. Kaseya started receiving reports from customers that they were experiencing ransomware and Kaseya advised that if a customer received a communication from an attacker, they should not click on any links as they may be weaponized.

Kaseya advised by July 6, 2021 that they were aware of fewer than 60 Kaseya customers, all of whom were using the VSA on-premises product, who were directly compromised by the attack. They subsequently described these customers as “a very small number.” Kaseya noted that these customers provide IT services

[2] In subsequent reports, SolarWinds “blamed” an intern for a critical password lapse that went unnoticed for several years. https://www.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html

[3] Supply chain attacks are not just for Russians any more as Microsoft blamed a Chinese-backed hacking group:: https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world

[4] https://www.cips.org/supply-management/news/2021/april/troubling-rise-in-supply-chain-cyber-attacks/

to multiple other companies, and they understood the total impact thus far had been to "fewer than 1,500 downstream businesses." (No SaaS customers were compromised and VSA was the only product affected).

Reports are that the Russian-based cybercriminal organization REvil claimed responsibility for the attack as of July 4, 2021 and were asking $45,000 for each computer system impacted. REvil also said it would publish a tool that would allow all infected companies to recover their data if it were paid $70 million in Bitcoin. One researcher reached out to REvil and reported that the group was willing to negotiate down to $50 million.

Outside Resources and Reporting

Kaseya retained FireEye Mandiant IR and reportedly other firms to assess the manner and impact of the attack and to ensure that they have properly identified and mitigated the vulnerability.

Kaseya also was working with the FBI and Department of Homeland Security. Kaseya met with the FBI and CISA on July 5, 2021 to discuss systems and network hardening requirements prior to service restoration.

Remediation and Status

Kaseya rolled out a Compromise Detection Tool to 900 customers who requested it as of July 4, 2021. As of July 6, 2021, Kaseya initially estimated bringing SaaS servers online before the end of that day and then the on-premises patch would follow within 24 hours. However, as of July 7th, they continued to work on patch releases and restoring SaaS services.[5]

Outside Investigators - DIVD

The Dutch Institute for Vulnerability Disclosure (DIVD) had been investigating the Kaseya VSA product. As of July 2, 2021, they discovered server vulnerabilities in Kaseya VSA and reported them to Kaseya. As of July 6, 2021, DIVD reports a "steady decrease in the number of online servers" subject to the vulnerability. (From about 2238 suspected instances to 68).

DIVD advises that all on-premises VSA Servers should continue to remain offline until further instructions from Kaseya. DIVD also issued general security advice:

- Use MFA where available
- Remove admin interfaces from the public internet, for instance by placing them behind a VPN

[5] https://www.kaseya.com/potential-attack-on-kaseya-vsa/

- If something has to be on the Internet, work with an allowed list for authorized addresses

Governmental Guidance

CISA and the FBI issued "Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack" (last updated July 6, 2021). These include recommendations for MSPs and customers to download the detection tool, enable MFA, implement "allow listing" to limit communication with remote monitoring and management capabilities to known IP addresses or place admin interfaces behind a virtual private network (VPN), or firewall on a dedicated admin network. The guidance also recommends that MSP customers should ensure backups are up to date (stored in easily retrievable locations), install patches as available, and implement MFA as well as the principle of least privilege on key network resources.

Businesses/Entities Impacted

Companies in the U.S., Germany, Australia, Sweden, and Brazil were known to be impacted. A retailer in Sweden was forced to close 800 stores as of July 3, 2021. A Swedish railway and pharmacy chain were affected.

Comparison Figures

SolarWinds reported that the attack cost the company at least $18 million in the first three months of 2021. This figure did not include legal and "other professional services expenses" to be incurred "in future periods."[6] On a global basis, some estimates were reported of up to a billion dollars for entities to investigate and remediate the problem as well as increased insurance premiums, even though most organizations were not actually exploited.[7]

There are estimates that there are over 250,000 organizations around the world that were impacted by the Microsoft Exchange Server vulnerability. Again, each organization had to assess their exposure and spent a great deal of time to "track down, clean and ensure they were not affected."[8] Many certainly used outside vendors to assist and notified their insurers out of an abundance of caution. That event broadly impacted smaller businesses as well as schools and governments. Meanwhile, there are ongoing reports that Exchange Servers remain vulnerable.

[6] https://www.reuters.com/technology/solarwinds-says-dealing-with-hack-fallout-cost-least-18-million-2021-04-13/

[7] https://financialpost.com/technology/tech-news/experts-say-worldwide-cost-of-investigating-solarwinds-orion-hack-could-be-in-the-billions

[8] *See supra* note 3.

Colonial Pipeline reportedly paid $4.4 million in ransom and then faced class litigation from businesses and consumers. Apparently, gas stations were without fuel for a period of time and airlines and tracking companies likewise suffered losses.[9]

The Kaseya impact on the number of entities may not rise to the scale of SolarWinds or Microsoft but the types of entities impacted could look similar to some of the smaller businesses affected by the Colonial Pipeline attack. In other words, each organization that suffered an actual or attempted ransomware attack will incur its own investigation and remediation expenses as well as potential downtime losses and the redirection and redeployment of internal resources. Also, it appears that businesses have not just had to investigate for and attend to potential vulnerabilities but actually have reported ransomware attacks. Such entities thus likely would immediately incur forensic, legal and remedial expenses but also may have to notify or report the incident depending upon the exposure of any confidential or sensitive data. Some initial analysis of the malware, though, is that there do not appear to be any attempts to exfiltrate data. In sum, the Kaseya incident may impact more "little guy" types, although fewer in numbers than other supply chain incidents, but with the potential for greater per entity losses and expenses.

[9] https://www.insurancejournal.com/news/national/2021/06/24/619899.htm

July 2021

Contacts:

Kevin G. Flynn
kevin.flynn@mendes.com
1.212.261.8321

Lauren B. Prunty
lauren.prunty@mendes.com
1.212.261.8303

Margaret A. Reetz
margaret.reetz@mendes.com
1.212.261.8726

Gregory S. Mantych
gregory.mantych@mendes.com
1.212.261.8091

Mendes & Mount publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication without the prior written consent of the Firm. The distribution of these materials is not intended to create, and receipt of such does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the firm.