Contrast SECURITY

Kaseya Ransomware Attack: What You Should Know

Near the end of the U.S. business day on Friday, July 2, hundreds of organizations around the world were hit with a coordinated ransomware attack just as employees were winding down for a holiday weekend.[1] The victims all used managed service providers (MSPs) to run their IT networks and devices, and those MSPs all used virtual system/server administrator (VSA) software from Florida-based Kaseya to provide this remote service. It is possible that many of the end-user victims were unaware that Kaseya was even a part of their software supply chain.

REvil, a Ransomware-as-a-Service group with ties to the Russian government (see "REvil: Many Attacks Over a Short History"), claimed responsibility for the attack. Soon after the attack, Kaseya warned all its customers to immediately shut down their on-premises servers until a patch is completed and also disabled its cloud service as a precaution.[2] But it was too late for some: Attackers disabled victims' entire IT networks, forcing hundreds of organizations to close their doors due to a complete lack of operational devices and networks.

WHAT WE KNOW

At this writing, only a few days have elapsed and full details about the attack have not been released. Here are some things we do know:

- *The vulnerability.* The Dutch Institute for Vulnerability Disclosure (DIVD) notified Kaseya of zero-day vulnerabilities it had discovered in the company's VSA software (CVE-2021-30116).[3] Kaseya was working on patches when the attack occurred. While there has been speculation that REvil may have monitored internal communications about the vulnerability, Kaseya indicates its systems were not compromised.[4]

- *Attack methodology.* REvil apparently did not infiltrate Kaseya's network, and this supports the theory that the group attacked the MSPs separately but simultaneously using a "compromise-once-infect-many" approach.[5] In this case, there are two layers that multiply the number of victims: A hack of a single MSP infects multiple MSP customers, and the existence of a vulnerability in Kaseya software enabled the adversaries to attack dozens of MSPs simultaneously.

- *Number of victims.* Kaseya said on July 5 that around 60 Kaseya customers (mostly MSPs) were impacted and fewer than 1,500 companies were downstream victims—that is, customers of those MSPs. In addition to the United States, victims have been identified in 17 countries, including the United Kingdom, South Africa, Canada, New Zealand, Kenya, and Indonesia. Most of the victims are small and midsize organizations, but hundreds of Coop supermarkets in Sweden were forced to close due to the attack.[6]

- *Ransom demands.* REvil claimed responsibility for the attack and has demanded $70 million in bitcoin in exchange for publicly posting a universal decryptor to unlock all systems.[7] Kaseya CEO Fred Voccola declined to disclose whether his company has paid, or is in negotiations to pay, the ransom. He did say that he is coordinating with the U.S. Federal Bureau of Investigation and other law enforcement agencies.[8]

RECOMMENDATIONS

Attacks on the software supply chain have generated numerous headlines in recent months, from the massive SolarWinds attack[9] to the exploits against Microsoft Exchange Server.[10] The Kaseya attack is another reminder that organizations must protect their entire software supply chain. The victims in this attack were not even Kaseya customers, but their IT networks were being managed by Kaseya technology.

While many organizations think of application security only in connection with internally developed software, today's threat landscape requires an emphasis across all four dimensions of application security in the software supply chain:

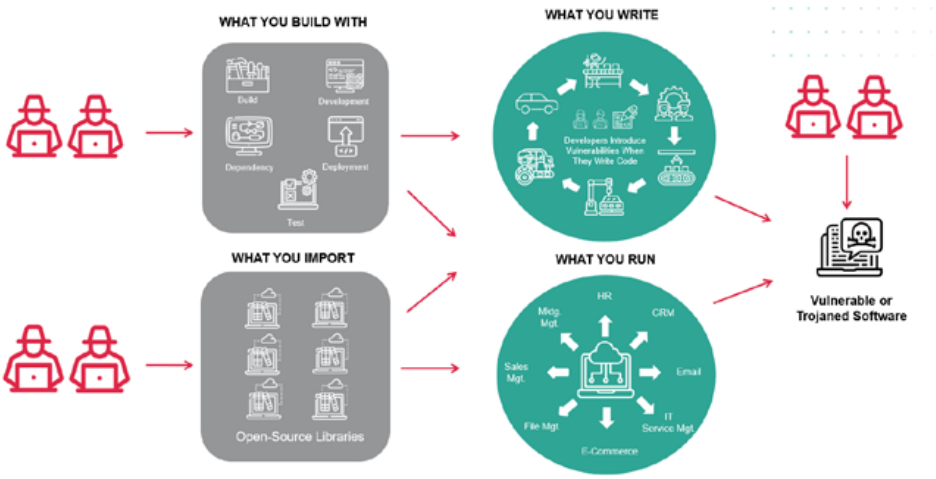
- *What you write:* Internally developed software, including custom code and open-source libraries
- *What you build with:* Numerous development tools used by DevOps team members
- *What you run:* Commercial off-the-shelf (COTS) software used by an organization *and/or* by connected partners and suppliers
- *What you import:* Third-party libraries contained in internally developed software

The victims of this attack were hit through software in the "what you run" category—in this case, what their MSP runs. How can an organization protect against attacks on software that it does not even own or use, but is instead utilized by a third-party partner or service provider? Naturally, they should ensure that third parties have adequate application security policies and practices, are deploying patches and updates in a timely manner, and have adequate tools for real-time threat response.

To achieve the above, third-party software providers must have safeguards in place for the applications they provide to customers. Using a software composition analysis (SCA) solution like **Contrast OSS** that delivers real-time, continuous monitoring of third-party libraries helps alleviate the visibility gaps that come with using open-source software. To fight against zero-day attacks like this one, the third party will ideally need a runtime protection and observability solution, such as **Contrast Protect**, that detects attacks while they are in progress and stops them before they can cause damage. Finally, for third-party providers, they should continuously monitor their applications in development using an integrated application security testing (AST) solution such as **Contrast Assess**.

For organizations that have software in all four categories above, a comprehensive approach to application security is nonnegotiable. One way to get a rough idea of how well a specific organization is doing is to refer to the proposed application security scoring system by Jeff Williams.[11] Further, the best way to ensure security across the software supply chain is through instrumentation, which builds security monitoring into the software itself. The **Contrast Application Security Platform** enables full observability and protection throughout the software development life cycle (SDLC).

4 Dimensions of Modern Application Security



REVIL: MANY ATTACKS OVER A SHORT HISTORY

REvil, pronounced R-evil, became active soon after the developers of GandCrab ransomware announced their retirement in 2019 after collecting an estimated $2 billion in ransoms.[12] Due to similarities in their code, it is believed that the same people were behind the development of both products.

REvil specializes in supply chain attacks that use a "compromise-once-infect-many" approach.[13] The group is mostly made up of native Russian speakers and is believed to be protected by the Russian government. In an ironic twist, the group posts its stolen information on a dark web site called "Happy Blog."[14]

Early REvil victims included two dozen Texas municipalities and hundreds of dentist offices.[15] Since then, they have been responsible for a number of high-profile attacks:

- May 2020: A demand for $42 million from then-U.S. President Donald Trump to prevent posting of stolen files from the Grubman Shire Meiselas & Sacks law firm[16]
- March 2021: 37,000 students in the Harris Federation, a group of primary and secondary academies in the London area, were locked out of their email and coursework[17]
- April 2021: A $50 million demand from Apple after stealing product development plans from partner Quanta Computer[18]
- May 2021: An $11 million ransom paid by JBS S.A., a Brazilian-based meat processing company with operations in the United States, Canada, and Australia, after slaughterhouses were closed around the world[19]

1 Zack Wittaker, "Kaseya hack floods hundreds of companies with ransomware," TechCrunch, July 5, 2021.
2 "Updates Regarding VSA Security Incident," Kaseya, July 2-6, 2021.
3 Victor Gevers, "Kaseya Case Update 2," DIVD, July 4, 2021.
4 Zack Wittaker, "Kaseya hack floods hundreds of companies with ransomware," TechCrunch, July 5, 2021.
5 Ibid.
6 Ibid.
7 Catalin Cimpanu, "REvil gang asks for $70 million to decrypt systems locked in Kaseya attack," The Record, July 4, 2021.
8 Raphael Satter, "Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says," Reuters, July 6, 2021.
9 Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," NPR, April 16, 2021.
10 Jordan Novet, "Microsoft's big email hack: What happened, who did it, and why it matters," CNBC, March 9, 2021.
11 Jeff Williams, "It's High Time for a Security Scoring System for Applications and Open Source Libraries," Dark Reading, July 6, 2021.
12 Jai Vijayan, "GandCrab Developers Behind Destructive REvil Ransomware," Dark Reading, September 25, 2019.
13 Ibid.
14 Eamon Javers, "Axis of REvil: What We Know about the Hacker Collective Taunting Apple," CNBC, April 23, 2021.
15 Jai Vijayan, "GandCrab Developers Behind Destructive REvil Ransomware," Dark Reading, September 25, 2019.
16 Kevin Collier and Diana Dasrath, "Criminal group that hacked law firm threatens to release Trump documents," NBC News, May 15, 2020.
17 Sabina Weston, "Evidence suggests REvil behind Harris Federation ransomware attack," ITPro, April 9, 2021.
18 Eamon Javers, "Axis of REvil: What we know about the hacker collective taunting Apple," CNBC, April 23, 2021.
19 Tom Polansek and Nandita Bose, "JBS meat plants reopen as White House blames Russia-linked group over hack," Reuters, June 2, 2021.

Contrast SECURITY

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com