UPDATED: Kaseya hijacked, thousands attacked by REvil, fix delayed again

By Mark Stockley

Published: 2021-07-01 · Archived: 2026-04-05 17:41:33 UTC

Malwarebytes does not use Kaseya products. Malwarebytes detects the REvil ransomware used in this attack as Sodinokibi.

Latest updates

- July 7, 8:30 am, Kaseya **VSA SaaS platform still offline**, not updated as planned
- July 6, 3:40 pm, **malspam** using **fake Kaseya security update**
- July 6, 3:15 am, Malwarebytes telemetry reveals **global scale** of the attack
- July 6, 2:45 am, **Ransom demand drops to $50 million**, REvil branded "terrorists"
- July 5, 5:00 am, Kaseya flaw part of larger **structural weakness in admin tools**
- July 5, 4:30 am, Kaseya releases **compromise detection tool**
- July 4, 8:50 pm, **REvil asks for $70 million**
- July 4, 4:00 pm, Malwarebytes telemetry shows **surge in REvil detections**
- July 4, 5:00 am, "**Thousands affected**", zero-day blamed
- July 3, Two MSPs named, **hundreds of Coop stores closed**
- July 2, **Shutdown Kaseya VSA** immediately
- **IOCs**

Shutdown Kaseya VSA immediately

A severe ransomware attack reportedly taking place now against the popular Remote Monitoring and Management software tool Kaseya VSA has forced Kaseya into offering urgent advice: **Shutdown VSA servers immediately**.

"We are experiencing a potential attack against the VSA that has been limited to a small number of on-premise customers only as of 2:00 PM EDT today," Kaseya wrote on Friday afternoon.

> "We are in the process of investigating the root cause of the incident with an abundance of caution but we recommend that you IMMEDIATELY shutdown your VSA server until you receive further notice from us.
>
> It's critical that you do this immediately, because one of the first things the attacker does is shutoff administrative access to the VSA."

The attack is reportedly delivered through a Kaseya VSA auto-update that maliciously pushes the Revil ransomware onto victims' machines. Kaseya is a popular software developed for Managed Service Providers that provide remote IT support and cybersecurity services for small- to medium-sized businesses that often cannot afford to hire full-time IT employees, due to their limited size or budgets.

Complicating the attack is the fact that, according to cybersecurity researcher Kevin Beaumont, the malicious update carries administrator rights for clients' systems, "which means that Managed Service Providers who are infected then infect their client's systems."

For a company that says it has 40,000 customers, this could be a disaster.

During the attack, the cybercriminals reportedly shut off administrative access to VSA, and several protections within Microsoft Defender are disabled, including Real-Time Monitoring, Script Scanning, and Controlled Folder Access.

A screenshot from Malwarebytes reveals a ransom note delivered to an infected Windows machine. In the note, attackers warn:

Malwarebytes customers are currently protected from REvil, as shown in the screenshots below, and Malwarebytes is committed to continuing this protection. (Malwarebytes detects REvil as Sodinokibi)

We will update this post with more information as it becomes available, but the immediate guidance from Kaseya cannot be overstated: Shutdown VSA servers immediately.

Update July 3, 2021

Kaseya has released a new statement confirming they were the victim of a sophisticated cyberattack. At this time they are still urging customers to keep their on-premise VSA servers offline.

According to Bloomberg two of the affected managed service providers (MSPs) are Synnex Corp. and Avtex LLC. While Kaseya is a US-based company, some of of the MSPs' customers are businesses in Europe. According to the BBC, Swedish supermarket chain Coop had to close more than 400 stores on Friday after the point-of-sale terminals and checkouts stopped working.

Victims of this attack would have downloaded a malicious update called 'Kaseya VSA Agent HotFix' which was in fact meant to disable Windows Defender and push the file encryptor payload.

Update July 4, 2021, 5:00 am, PT

More details of the vast scope of the attack have emerged. Huntress has been maintaining a comprehensive Reddit thread on the incident since Friday. In an accompanying blog post, the organization says it is tracking about 30 MSPs in four continents "where Kaseya VSA was used to encrypt well over 1,000 businesses".

One of the affected organizations is St Peter's School, Cambridge, New Zealand, which has confirmed that it is one of eleven schools in the country affected by this supply-chain attack.

Security company HuntressLabs has analyzed the original attack vector and believes a REvil/Sodinokibi affiliate exploited a zero-day for an authentication bypass in the Kaseya's web interface.

Today, Victor Gevers of the Dutch Institute for Vulnerability Disclosure (DIVD) revealed on Twitter that it was in a "coordinated vulnerability disclosure process" with Kaseya at the time of the attack.

In other words, Kaseya was aware of a problem and it was actively working to fix it. According to Gevers, this explains why on-premise version of VSA was vulnerable and the SaaS version was not. It seems that, sensibly, the SaaS version of VSA receives patches before the on-premise version.

It seems the attack was remarkably well timed. Had that process moved a little more quickly, infosec folks would now be enjoying their weekends and we'd be writing about what might have been, rather about what Gevers describes as "the single largest ransomware spree in history".

Given the way 2021 is unfolding, we can't help wondering how long it will keep that title.

Update: July 4, 4:00 pm, PT

Malwarebytes' telemetry shows a major increase in Ransom.Sodinokibi (REvil) detections and not just in the US. In fact, we have a number of hits in India, France, Chile, Taiwan, Australia, Colombia and Argentina.

Update: July 4, 8:50 pm, PT

The REvil gang has claimed the attack on MSPs and is asking for $70M in exchange for a universal decryptor. In a new post on their 'Happy Blog' hosted on the dark web, they say that more than a million systems were infected. They also mention that the universal decryptor would help recover from the attack in less than an hour. Both claims are highly controversial.

Update: July 5, 4:30 am, PT

Kaseya has created a Compromise Detection Tool that can be download from the company's Box account. The tool will scan VSA servers or managed endpoints and determine whether any indicators of compromise (IoC) are present. However, Kaseya says its customers should keep VSA turned off for now:

> All on-premises VSA Servers should continue to remain offline until further instructions from Kaseya about when it is safe to restore operations. A patch will be required to be installed prior to restarting the VSA and a set of recommendations on how to increase your security posture.

Cado Security has created a GitHub repository of tools for DFIR professionals who are dealing with the fallout from the attack.

Update: July 5, 4:45 am, PT

DIVD reveals that Kaseya's instruction to shutdown VSA servers, and the subsequent efforts of organizations like theirs has drastically reduced the number of Kaseya VSA instances that are reachable from the internet from "over 2,200 to less than 140" in 48 hours.

The organization also sheds a little more light on the root cause of the incident, saying "DIVD researcher, has previously identified a number of the zero-day vulnerabilities [CVE-2021-30116] which are currently being used in the ransomware attacks." As we explained in an earlier update, DIVD was in the process of working with Kaseya to resolve the vulnerabilities when REvil struck. "Unfortunately, we were beaten by REvil in the final sprint."

Ominously, it explains that this is part of a broader effort looking at the administration interfaces of tools used for system administration, saying: "we spotted a trend where more and more of the products that are used to keep networks safe and secure are showing structural weaknesses."

Update: July 6, 2:45 am, PT

Reuters reports that the REvil affiliate behind the attack "has indicated a willingness to temper their demands in private conversations with a cybersecurity expert and with Reuters." According to the news organization, the attackers told Jack Cable of the Krebs Stamos Group, that it was prepared to lower the asking price for a universal decryptor from $70 million to $50 million. A universal decryptor could be used to free all of the victims—all the customers of Kaseya's customers—and save the attackers the bother of negotiating with each of up to 1,500 victims separately.

Ransomware gangs typically negotiate with one, or a small number of victims at a time. The REvil affiliate behind this attack may simply be unequipped to communicate with so many victims. They may also be wary of creating thousands of separate 'paper trails' on the Bitcoin blockchain, since cryptocurrency payments are where recent law enforcement efforts seem to have focussed. About a month ago, the DOJ recovered the majority of the ransom paid in the Colonial Pipeline attack. A week later, police in Ukraine arrested several individuals believed to be engaged in money laundering for the Cl0p ransomware group.

The question now, is whether Kaseya will pay. Reuters reports that in an interview with Kaseya CEO Fred Voccola, he responded to a question about whether the company would pay by saying "I can't comment 'yes,' 'no,' or 'maybe' … No comment on anything to do with negotiating with terrorists in any way."

Update: July 6, 3:15 am, PT

Malwarebytes Threat Intelligence has released an image showing the global scale of the event. Telemetry from Malwarebytes reveals detections for REvil on four continents following Friday's attack.

Update: July 6, 3:40 pm, PT

Malwarebytes Threat Intelligence has seen a malicious spam campaign trying to take advantage of the Kaseya VSA attack. The email asks recipients to "please install the update from Microsoft to protect against ransomware" and a carries an attachment called `SecurityUpdates.exe`.

Update: July 7, 8:30 am, PT

Kaseya has updated its incident page to explain that its planned update to the Kaseya VSA SaaS platform has still not taken place, due to an unspecified issue.

> …during the deployment of the VSA update an issue was discovered that has blocked the release. We have not yet been able to resolve the issue

The SaaS platform's continued unavailability is a mystery. Kaseya maintains that unlike the on-premises version of its VSA product, the SaaS platform was not vulnerable to the zero-day issue used to launch Friday's attack. However, the SaaS platform was taken offline as a precaution and will remain so until it can be updated.

Indicators of Compromise (IoCs)

Loader

REvil/Sodinoki DLL

File paths

Additional IOCs from configuration file (source)

Process list to kill

Services to stop and delete
