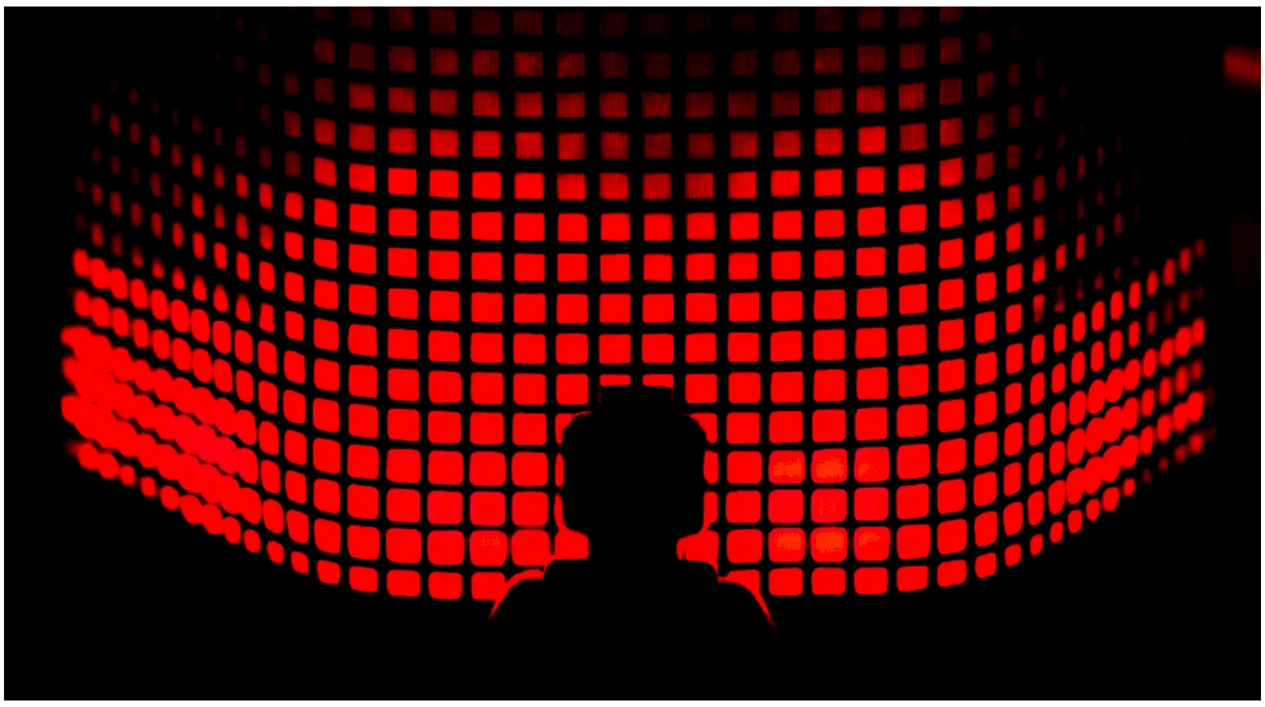
The Record.
Recorded Future® News



RANSOMWARE-HACKER|KASEYA-NOTICE|KASEYA-RESPONSE

Catalin Cimpanu

July 2nd, 2021

Malware News Cybercrime

REvil ransomware gang executes supply chain attack via malicious Kaseya update

The REvil ransomware gang appears to have gained access to the infrastructure of Kaseya, a provider of remote management solutions, and is using a malicious update for the VSA software to deploy ransomware on enterprise networks.

The incident, believed to have impacted thousands of companies across the world, first came to light earlier today in a Reddit section dedicated to managed service providers (MSPs) -- companies that provide remote IT services to smaller businesses lacking an IT department and which are usually Kaseya's primary customerbase.

According to security firm Sophos and Kaseya customers who spoke with The Record, the malicious Kaseya update is reaching VSA on-premise servers, from where, using the internal scripting engine, the ransomware is deployed to all connected client systems.

Per Mark Loman, a Sophos malware analyst, on a host systems, the REvil gang disables local antivirus solutions and then deploys a fake Windows Defender app that runs the actual ransomware binary that encrypts a victim's files.

BRIEFS

German police arrest two for alleged ties to DDoS-for-hire platform | November 1st, 2024

California court suffering from tech outages after cyberattack | November 1st, 2024

Russia behind latest election disinformation video, US intel agencies say | November 1st, 2024

Ransomware attack hits German pharmaceutical wholesaler, disrupts medicine supplies | November 1st, 2024

Los Angeles housing agency confirms another cyberattack after 2023 ransomware incident | November 1st, 2024

Young people's data feared stolen in cyberattack on French government contractor | November 1st, 2024

Shopping scam sprawled across thousands of websites, bilked 'tens of millions of dollars' | October 31st, 2024

Russia to ban cryptocurrency mining in some regions due to electricity shortages | October 31st, 2024

Suspected pro-Ukraine cyberattack knocks out parking enforcement in Russian city | October 31st, 2024

> **We are monitoring a REvil 'supply chain' attack outbreak, which seems to stem from a malicious Kaseya update. REvil binary C:\Windows\mpsvc.dll is side-loaded into a legit Microsoft Defender copy, copied into C:\Windows\MsMpEng.exe to run the encryption from a legit process.— Mark Loman (@markloman)** July 2, 2021

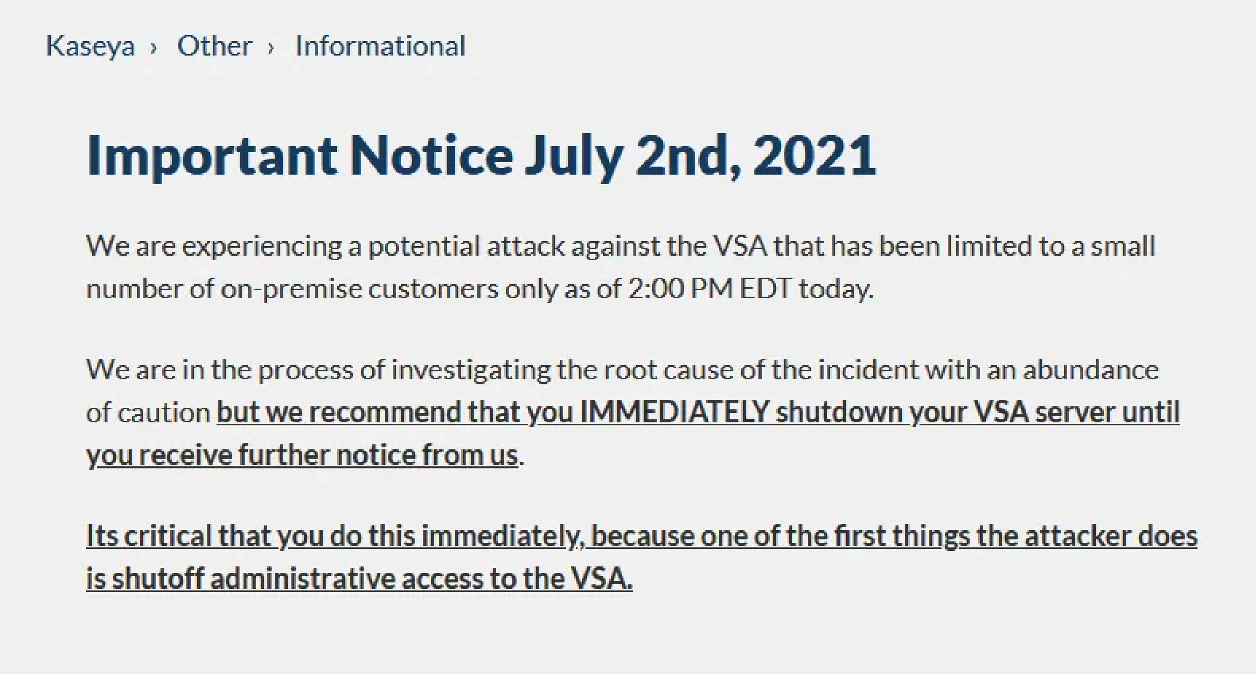
In a Zoom call today, Mark Loman, malware analyst for security firm Sophos, told The Record that the attack is massive in nature, based on the company's telemetry, which helped the Sophos team spot the attack early on.

Loman said that companies who have been impacted are seeing ransom notes of $50,000 (if their infected systems is not domain joined) or $5 million (if the computer is domain joined, and a clear sign the system is part of a large corporate network).

In a Reddit post, security firm Huntress Labs said it is aware of at least eight MSPs that have been impacted by today's incident, and at least 200 businesses that have had networks encrypted, based on its visibility alone.

Kaseya tells customers to take VSA servers offline

In an email earlier today, a Kaseya representative confirmed the attacks to The Record, pointing us to a support page that was urging all VSA owners to take their systems offline until further notice.



Kaseya › Other › Informational

Important Notice July 2nd, 2021

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.

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.

Its critical that you do this immediately, because one of the first things the attacker does is shutoff administrative access to the VSA.

In addition, besides advising customers to shut off their VSA servers, Kaseya has also shut down its own cloud infrastructure in what looks like an attempt to stop the malicious updates going out and an attempt to root out the REvil gang off its systems.

> **Kaseya is advising onprem users to shut their servers off. They brought their entire cloud offline. Short of screaming "We've been hacked!" it's pretty certain that they feel it's origin is them.— CONDITION.BLACK | RESEARCH AND INTELLIGENCE (@Shadow0pz)** July 2, 2021

Following news of today's massive supply chain attack via Kaseya's software, the US Cybersecurity and Infrastructure Security Agency said it was looking into the incident and how to address it.

Today's incident also marks the third time that a ransomware gang abused Kaseya products to deploy ransomware.

In February 2019, the Gandcrab ransomware gang abused a vulnerability in a Kaseya plugin for the ConnectWise Manage software to deploy ransomware on the networks of MSPs' customer networks.

After the Gandcrab gang rebranded as REvil, they pulled a second attack against MSPs in June 2019, when they abused Webroot SecureAnywhere and Kaseya VSA products to deploy ransomware again from MSPs to their customer networks.

Indicators of compromise (IOCs) from today's attack are currently available in a Sophos

RUSSIAN STRATEGIC INFORMATION ATTACK FOR CATASTROPHIC EFFECT

OPERATION OVERLOAD IMPERSONATES MEDIA TO INFLUENCE 2024 US ELECTION

OPERATION OVERLOAD IMPERSONATES MEDIA TO INFLUENCE 2024 US ELECTION

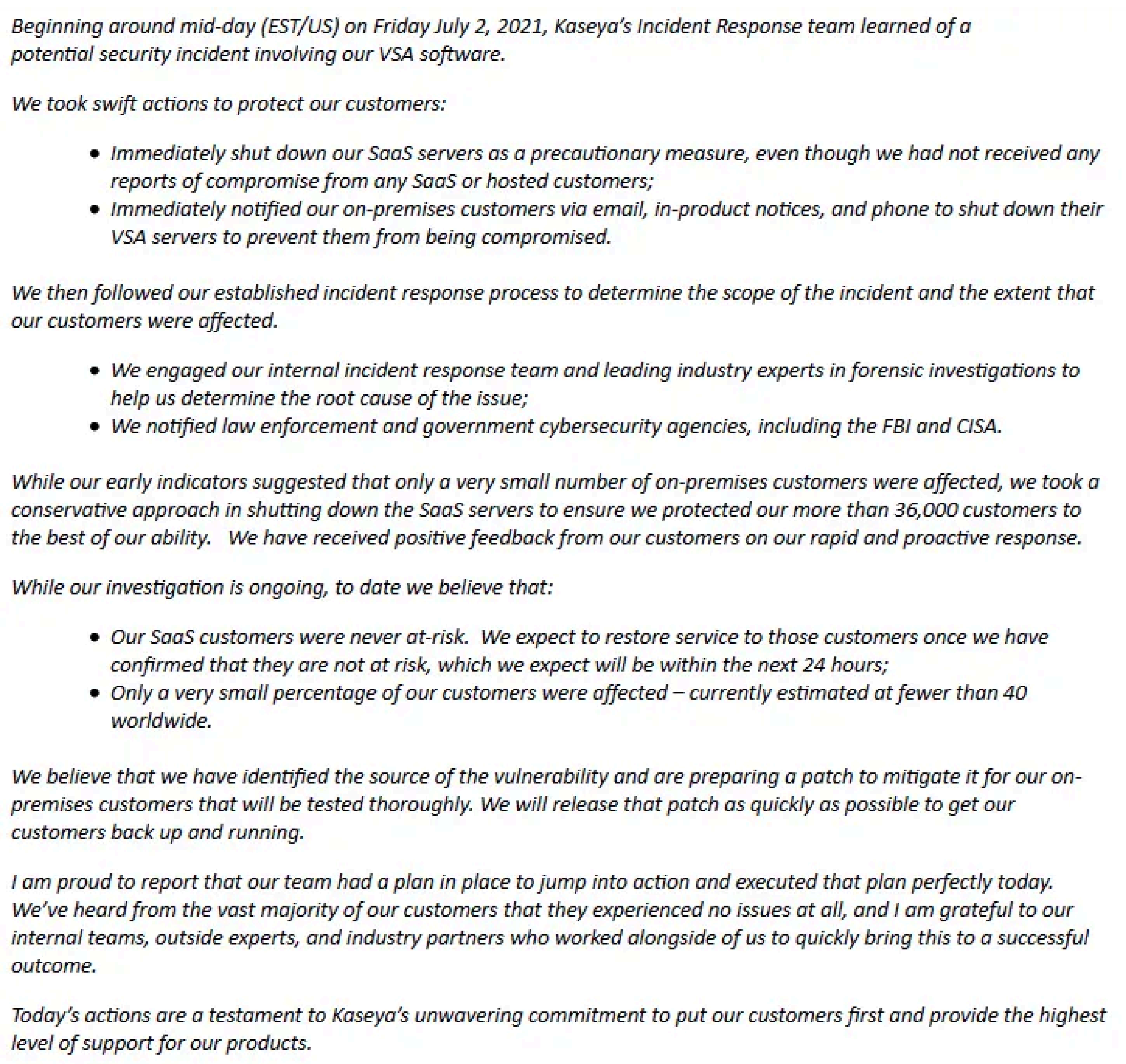
OUTMANEUVERING RHYSIDA: HOW ADVANCED THREAT INTELLIGENCE SHIELDS CRITICAL INFRASTRUCTURE FROM RANSOMWARE

OUTMANEUVERING RHYSIDA: HOW ADVANCED THREAT INTELLIGENCE SHIELDS CRITICAL INFRASTRUCTURE FROM RANSOMWARE

RHADAMANTHYS STEALER ADDS INNOVATIVE AI FEATURE IN VERSION 0.7.0

RHADAMANTHYS STEALER ADDS INNOVATIVE AI FEATURE IN VERSION 0.7.0

TARGETS, OBJECTIVES, AND EMERGING TACTICS OF POLITICAL DEEPFAKES



Beginning around mid-day (EST/US) on Friday July 2, 2021, Kaseya's Incident Response team learned of a potential security incident involving our VSA software.

We took swift actions to protect our customers:

- *Immediately shut down our SaaS servers as a precautionary measure, even though we had not received any reports of compromise from any SaaS or hosted customers;*
- *Immediately notified our on-premises customers via email, in-product notices, and phone to shut down their VSA servers to prevent them from being compromised.*

We then followed our established incident response process to determine the scope of the incident and the extent that our customers were affected.

- *We engaged our internal incident response team and leading industry experts in forensic investigations to help us determine the root cause of the issue;*
- *We notified law enforcement and government cybersecurity agencies, including the FBI and CISA.*

While our early indicators suggested that only a very small number of on-premises customers were affected, we took a conservative approach in shutting down the SaaS servers to ensure we protected our more than 36,000 customers to the best of our ability. We have received positive feedback from our customers on our rapid and proactive response.

While our investigation is ongoing, to date we believe that:

- *Our SaaS customers were never at-risk. We expect to restore service to those customers once we have confirmed that they are not at risk, which we expect will be within the next 24 hours;*
- *Only a very small percentage of our customers were affected – currently estimated at fewer than 40 worldwide.*

We believe that we have identified the source of the vulnerability and are preparing a patch to mitigate it for our on-premises customers that will be tested thoroughly. We will release that patch as quickly as possible to get our customers back up and running.

I am proud to report that our team had a plan in place to jump into action and executed that plan perfectly today. We've heard from the vast majority of our customers that they experienced no issues at all, and I am grateful to our internal teams, outside experts, and industry partners who worked alongside of us to quickly bring this to a successful outcome.

Today's actions are a testament to Kaseya's unwavering commitment to put our customers first and provide the highest level of support for our products.

Tags Ransomware Cyberattack Kaseya Sodinokibi supply chain attack REvil

Previous article
← **Mysterious Node.js malware puzzles security...**

Next article
TrickBot: New attacks see the botnet deploy new... →

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

The Record. Recorded Future® News

Privacy About Contact Us