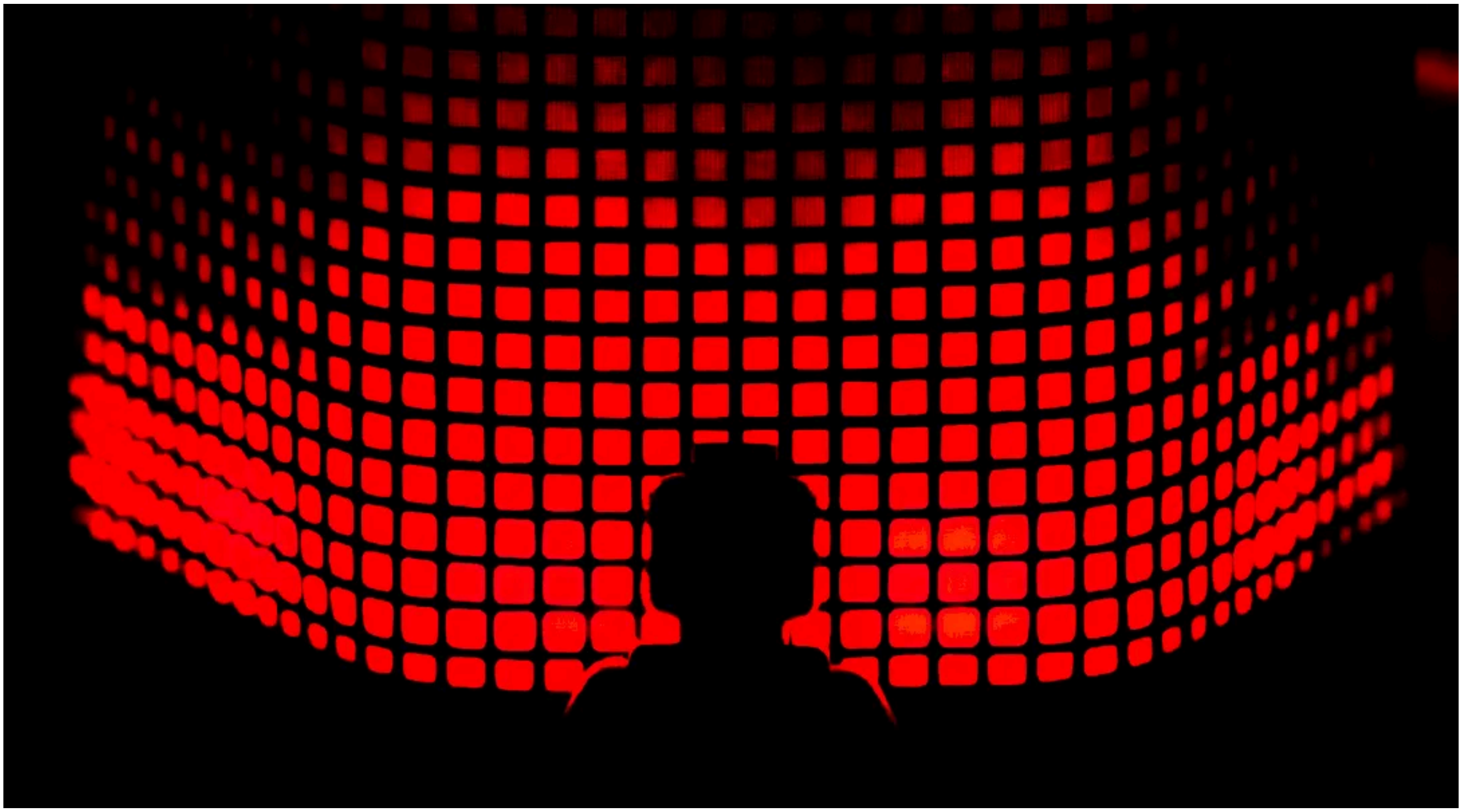
The Record.
Recorded Future® News



RANSOMWARE-HACKER|KASEYA-NOTICE|KASEYA-RESPONSE

Catalin Cimpanu

July 2nd, 2021

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.

> **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.

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 Community page.

Update: Five hours after this article was published, Kaseya CEO Fred Voccola provided the following statement to The Record in regards to today's incident (reproduced in full with no alterations):

Malware News Cybercrime

Tags Ransomware Cyberattack Kaseya Sodinokibi supply chain attack REvil

No previous article

No new articles

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.

BRIEFS

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

UnitedHealth hires cybersecurity veteran as new CISO
| October 30th, 2024

Texas county says 47,000 had SSNs, medical treatment info leaked during May cyberattack | October 28th, 2024

UK sanctions Russians over anti-Ukrainian disinformation campaigns | October 28th, 2024

EU president denounces Russian influence campaigns targeting Western Balkans | October 28th, 2024

Free, France’s second-largest telecoms company, confirms being hit by cyberattack | October 28th, 2024

'All servers' for Redline and Meta infostealers hacked by Dutch police and FBI | October 28th, 2024

RUSSIAN STRATEGIC INFORMATION ATTACK FOR CATASTROPHIC EFFECT

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

TARGETS, OBJECTIVES, AND EMERGING TACTICS OF POLITICAL DEEPFAKES

The Record.
Recorded Future® News

Privacy **About** **Contact Us**