Menu

Threat Brief: Kaseya VSA Ransomware Attacks

3,854 people reacted

13 < 1 min. read

SHARE

By Unit 42
July 3, 2021 at 3:15 PM
Category: Threat Brief, Unit 42
Tags: Kaseya, ransomware, REvil

This post is also available in: 日本語 (Japanese)

Executive Summary

On July 2nd, attackers reportedly launched attacks against users of the Kaseya VSA remote monitoring and management software as well as customers of multiple managed service providers (MSPs) that use the software. They used access to the VSA software to deploy ransomware associated with the REvil/Sodinokibi ransomware-as-a-service group, according to reports. Kaseya has stated that the attack was conducted by exploiting a vulnerability in its software, and said they are working on a patch. The company has not released further information on the vulnerability. Kaseya recommends that any organization using VSA shut the system down immediately. CISA has also issued a bulletin asking organizations using the software to follow Kaseya guidance.

The full extent of the attack is currently unknown. Kaseya states that fewer than 40 of its customers are impacted. If those customers include MSPs, many more organizations could have been attacked with the ransomware. Kaseya VSA's functionality allows administrators to remotely manage systems. If a MSP's VSA system was compromised, that could allow the attacker to deploy malware into multiple networks managed by that MSP.

There has been much speculation about the nature of this attack on social media and other forums. We have not been able to independently determine how these attacks were conducted.

Multiple sources have stated that the following three files were used to install and execute the ransomware attack on Windows systems:

agent.exe | d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

mpsvc.dll | e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2

mpsvc.dll | 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

WildFire, Threat Prevention detect and Cortex XDR detect these files as malicious.

As more information becomes available on the nature of this attack, we will update this brief to provide additional details.

Indicators of Compromise

Kaseya Connected REvil Executables

d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2