Severity

High

Analysis Summary

On the Fourth of July weekend, around 200 organizations all over the world were hit with a ransomware attack. Investigators are calling this the “largest ransomware attack in history.” The REvil ransomware group exploited the Kaseya VSA tool used to perform client monitoring and patch management by MSPs. The gang initially compromised the VSA software, and then deployed their ransomware on the on-premise servers of enterprise networks. This is an ongoing attack and more than1500 organizations have been compromised as of yet. FBI is helping the company investigate this incident and organizations and vendors affected by the attack have also released advisories on patches and remediations for the attack. They are demanding $70 million.

Impact

- Data Encryption

Indicators of Compromise

MD5

- ad49374e3c72613023fe420f0d6010d9

SHA-256

- ad49374e3c72613023fe420f0d6010d9

SHA-1

- eb563ab4caca7e19bdeee807b025ab2d54e23624

Remediation

- Block all threat indicators at your respective controls
- Search for IOCs in your environment.