GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

July 2021

Kaseya Ransomware Attack – Considerations for Those Affected

The Fourth of July is usually reserved for fireworks, and this year was no different. On July 2, 2021, Kaseya, a provider of IT and security-management solutions, announced that it was the target of a supply-chain ransomware attack by the REvil/Sodinokibi (REvil) organized ransomware group. Kaseya's virtual systems/server administrator (VSA) is a server and cloud-based remote monitoring and management system that combines endpoint management and network monitoring into a single, automated system.

Up to 1,500 organizations are believed to have been directly impacted by the attack, including both Managed Services Providers (MSPs) and small-to-medium-size businesses, impacting thousands of computer systems and rivaling the scope of the ransomware attack known as "WannaCry" that hit hospitals, telcoms, and shipping and logistic systems worldwide in 2017.

Some weak links in defending against many cyberattacks may include software patch management, a lack of multifactor authentication, and management of backups and antivirus/antimalware. Kaseya VSA automates those functions, and REvil's attack took advantage of several vulnerabilities in the VSA software to facilitate its attack. As of today, it appears the attack was limited to only the software being run on customer servers rather than users of Kaseya's online service. On July 11, Kaseya announced that it had begun rollout of its patch for the software program.

REvil is demanding from between $25,000 - $150,000 from individual companies to $5 million from MSPs and has made a single demand of $70 million to Kaseya to provide a universal decryptor to unlock

all the impacted computer systems. While known for negotiating and discounting their ransom demands, REvil's online footprint disappeared early July 13, prompting questions of whether actions are being taken against one of the most prolific cybercriminal organizations in the world.

Who Is Impacted?

1. Companies who have Kaseya VSA in their environment.
2. Companies whose IT services are managed by an MSP that uses Kaseya VSA.

Considerations for Those Who Are Impacted

1. Shut down the VSA server or request your MSP shut down its VSA server.
2. You may wish to preserve or request preservation of Kaseya and firewall traffic logs for the past 30 days.
3. Many cyber professionals suggest isolating backups, if they are unaffected.
4. Your cyber-insurance carrier may be able to provide further guidance.
5. Consider retaining legal counsel experienced in ransomware attacks.
6. A forensic investigator may assist you with investigations and restoration.
7. Follow your company's incident response plan (IRP), if it has one.
8. Do not reboot, restore, or wipe machines before conferring with outside cybersecurity legal counsel and forensic vendor.

Fortunately, unlike many ransomware attacks committed these days, to date, it does not appear REvil tried to steal sensitive data before locking victims out of their systems (but this fact should be confirmed through forensics). Nonetheless, companies should consider working with legal counsel to address potential legal, contractual, and regulatory requirements that may be applicable to their business.

Author

This GT Alert was prepared by:

- Kevin M. Scott | +1 312.456.1040 | scottkev@gtlaw.com