Kaseya VSA Supply Chain Ransomware Attack

On 2 July 2021, Kaseya sustained a ransomware attack in which the attackers leveraged Kaseya VSA software to release a fake update that propagated malware through Kaseya's managed service provider (MSP) clients to their downstream companies. Kaseya VSA is a cloud-based MSP platform for patch management and client monitoring.

As of 5 July, Kaseya reported the attack affected fewer than 60 direct clients and not more than 1500 businesses supported by those clients. The attackers gained initial entry via a known vulnerability in VSA while Kaseya was still in the process of developing a fix.

The Russia-based REvil group issued a statement 5 July claiming responsibility and initially demanding US$70 million in exchange for decrypting all affected systems. As of 23 July, Kaseya announced it acquired a universal decryption key and was offering it to customers. Many firms had already restored their systems from backups, and some reportedly already negotiated individual ransoms, paying between $40,000 and $220,000.

REvil, also known in cyber security circles as Sodinokibi, is a ransomware-as-a-service (RaaS) group that provides cyber tools in exchange for a cut of the ransoms it collects for affiliates who execute the actual attacks. Affiliates receive credit for attacks through unique IDs embedded in the malware they use, allowing investigators to associate individual attacks with broader campaigns.

- **Type:** Ransomware; software-enabled supply chain attack.
- **Vector:** Zero-day vulnerability in Kaseya VSA remote management software.
- **Impact:** Approximately 1,500 businesses affected; Russia-based REvil group demanded US$70 million to decrypt all devices.
- **Mitigations:** On 04 July 2021, CISA and FBI issued joint advisory and additional best-practice recommendations. ODNI's Intelligence Community Security Coordination Center (IC-SCC) provided updates through its blog on 6 July 2021. Kaseya was already patching the VSA vulnerability when REvil struck. No evidence of malicious changes to the Kaseya VSA codebase. Kaseya provided security updates on 11 July and obtained a universal decryption key 21 July.