The REvil ransomware attack on **Kaseya VSA**

How behavioral analytics and Collective Defense can provide detection before the ransom

Background

On July 2, an auto update with REvil ransomware was delivered to Kaseya VSA, a common software used by MSPs (managed service providers) to manage their clients' systems. By design, VSA has administrator rights to its client systems, so MSPs that became infected via the auto update unknowingly pushed the ransomware to its clients, resulting in REvil hitting 1,000 companies in this MSP supply chain attack, raising another alarm across the industry for scrutinizing supply chain security.

It appears as if the initial payload was delivered via a software update that the actor manipulated via a vulnerability within the Kaseya software. The malicious update was not delivered directly from Kaseya but rather was enabled through a suspected authentication bypass zero day vulnerability that allowed the attacker to push the malicious ransomware payload to all connected clients.

REvil is a private, notorious Russian ransomware-as-a-service (RaaS) group that uses ransomware attacks as a money-making scheme. The group is responsible for the JBS cyberattack, which resulted in an $11 million payout.

IronNet's analysis of the attack

According to IronNet Threat Intelligence Analyst Joey Fitzpatrick, Remote Monitoring & Management software (RMMs) is "the new insider threat." As demonstrated with SolarWinds, instead of focusing effort on a single entity, if adversaries can determine which management software its target uses, it becomes much easier for them to exploit this third-party point of entry.

Unfortunately, SolarWinds proved how devastating supply chain attacks can be with network management tools. Even the most well-patched environment is susceptible to these types of attacks because a trusted process or program is being exploited.

The ransomware portion of the Kaseya attack by REvil targets backup systems first to stop any attempt to restore critical business files to ensure that a ransom becomes a viable opportunity. As Bleeping Computer noted, "MSPs are a high-value target for ransomware gangs as they offer an easy channel to infect many companies through a single breach, yet the attacks require intimate knowledge about MSPs and the software they use. REvil has an affiliate well versed in the technology used by MSPs as they have a long history of targeting these companies and the software commonly used by them."

RMMs allow both Managed Service Providers and large-scale businesses to monitor and manage thousands of devices with ease. But, because of the wide breadth of customers that MSPs serve and the domain admin level access these tools inherently have, MSPs have become prime targets for adversaries. Even with the most sophisticated defenses, MSPs and the enterprise end-users they support are challenged: Once an adversary gains access to one's RMM, they do not need to evade defense or escalate privileges. In other words, they already have become "king of the castle" and can dominate their targets' crown jewels as they please.

Although infrequent, supply chain attacks like this further stress the notion that it's not ***if*** your company is going to be breached, it's ***when***.

How IronNet Delivers Collective Defense through NDR and the power of real-time threat intelligence sharing

Well-defined data boundaries no longer exist and traditional data protections can't protect and secure such vast ecosystems. With IronNet's Collective Defense your entire supply-chain network can operate collectively to defend against threats in real time. Now you have broader visibility of the threat landscape across your company's value chain helping you more proactively defend against incoming attacks.

Here's the truth: Signature-based detections fall short

Given the growing threat of supply chain attacks, detection toolsets such signature-based endpoint solutions or traditional network security tools would not have caught this latest REvil effort. Much like the SolarWinds attack, which was detected by IronNet behavioral analytics, endpoint security tools that are monitoring interesting behaviors of **ALL** software with broad detection capabilities/queries would be the first to alert on this behavior. Immediate notification of powershell running a command to disable Microsoft Defender should have sent off the alarms in any SOC, which the adversary did do. It ran powershell to disable many of the defenses in place to defend against ransomware.

Tracking early intrusions with behavioral analytics

IronNet's behavioral analytics are designed to detect these behavior indicators in advance of the ransom, alerting IronNet's customers of early indicators before the ransom stage. The lifecycle of ransomware includes six phases: the attack, embedding and persistence, scanning, encryption, and the ransom itself. Implementing 360° visibility into your network traffic increases your chances of catching ransomware early in the kill chain. Applying behavioral analytics to look for anomalies in your network allows our analysts and threat hunters to detect, prevent, and mitigate the attack lifecycle of ransomware early in the process of a typical ransomware attack's six phases:

social engineering:
spear-phishing

"legitimate" user credentials:
for services such as remote desktop protocols and remote file sharing

exploitation:
for example via publicly known, but unpatched, software vulnerabilities

command and control:
domain generation

encryption:
files are encrypted after backup files are removed

Learn more about how to catch a ransomware attack early with IronNet with IronDefense network detection and response, upping the defense game even more with a Collective Defense approach that correlates adversarial campaigns across sectors in real time via a cyber radar view.

Network detection and response – and AI-based technologies like behavioral analytics – can go further to detect the unknown and sophisticated attacks as part of a defense-in-depth strategy. Collective Defense then provides the next-level proactive layer of defense. When those previously unknown threats are shared anonymously — and in real time — in a Collective Defense ecosystem, then all members of a Collective Defense community – both public and private sectors – can benefit from a radar-like view of incoming attacks.

IronNet™

Experience Collective Defense.

Request a live demo

IronNet's Collective Defense capabilities for sharing anonymized threat data quickly operationalize advanced detection, information sharing, and collaboration to identify adversaries such as REvil **before they attack.**

IronNet.com | info@IronNet.com | (443) 300-6761