Kaseya Ransomware Attack

Overview

Kaseya, which provides IT management software services to thousands of businesses across various verticals, recently fell victim to a ransomware attack executed by the REvil group. REvil was also responsible for the ransomware attack on meat provider JBS, which came on the heels of the Colonial Pipeline attack. This attack exploited an authentication vulnerability in the web interface of Kaseya's VSA service, which allowed the attackers to circumvent security measures and execute their attack. In all, about 50 direct customers and between 800 and 1,500 businesses down the chain were affected by this attack.

Recommendation for Lookout Admins

While there is no silver bullet against ransomware, combining Lookout Zero Trust Network Access, Modern Endpoint Protection, and User & Entity Behavior Analytics will help mitigate the risk. By doing this, Lookout admins can continuously assess risk across endpoints, protect employees from account compromise, identify anomalous user and device behavior, and modernize access policies to cloud and on-premises infrastructure. Adopting a well-rounded strategy based in Zero Trust will help mitigate the risk of unauthorized users gaining access to your infrastructure, exfiltrating data, and locking down resources for ransom.

Lookout Analysis

Reminiscent of Solarwinds, this attack was carried out as a supply chain attack by pushing the ransomware through a malicious software update. Since VSA is such a trusted service, integrated systems will generally accept any requests from it. However, the base issue of this incident is unauthorized access to the VSA backend itself.

It can be incredibly difficult to have enough visibility into your infrastructure and understand indications of a compromised account or service – especially in the cloud. Therefore, it's so important to have context-based login and access policies that can observe and baseline user behavior to detect anomalous activity such as an abnormal login location or massive data exfiltration.

Lookout Cloud Access Security Broker (CASB)

Lookout Cloud Access Security Broker (CASB) provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls. With continuous monitoring of user and entity behavior analytics (UEBA), you can detect and respond to insider threats and advanced cyberattacks. We provide advanced data loss prevention that can classify, encrypt and restrict sharing of your data on the fly so that only authorized users have access.

Click here to learn more about Lookout CASB