Scattered Spider

Overview

Scattered Spider, aka UNC3944, was able to successfully target and gain access to the infrastructure of Caesars Entertainment in its latest campaign. In addition, the group was implicated in a ransomware attack by the ALPHV/BlackCat group on MGM resorts just days before. This financially motivated threat actor has been active since March 2022 and historically targeted telecommunications, cryptocurrency, and business process outsourcing (BPO) organizations. The group compromises data by targeting users in social engineering attacks directed at the user's phones to steal their credentials and use them to gain access to systems that host sensitive data.

By socially engineering targets through mobile form factors such as SMS phishing, voice phishing, phishing using Telegram, SIM swapping, and MFA fatigue, the group has a track record of impersonating IT or contractor personnel and stealing login credentials. They are known to attack the mobile device to steal credentials and gain initial access, then create virtual machines in cloud and on-prem infrastructure to execute malicious activity. In particular, they are known to take advantage of systems that lack EDR capabilities. Its victims now span hundreds of organizations in technology, hospitality, transportation, and entertainment.

Coverage and Recommendation for Lookout Admins

Lookout strongly suggests all Mobile Endpoint Security (MES) customers enable phishing and content protection to mitigate the risk of being socially engineered and sharing login credentials with malicious actors. This will help protect employee credentials from being compromised. In addition, Lookout Secure Cloud Access customers can enable user and entity behavior analytics (UEBA) policies to detect anomalous login activity, such as an irregular location or multiple attempts, and anomalous data activity such as large data transfers or copies. These activities could be indicative of an attacker using stolen credentials to access and handle corporate data.

Lookout Analysis

Social engineering attacks that target users on mobile devices have become more successful in recent years as attackers have become more proficient in leveraging SMS and messaging apps against employees to impersonate IT and support staff. In addition, iOS and Android devices are relied upon as the second form of authentication for MFA solutions despite the fact that users are more susceptible to social engineering when using them. Threat actors that carry out these attacks will frequently target individuals who have access to sensitive data – using sites like LinkedIn to identify employees in positions that typically have this type of access.

Scattered Spider has formulated a vicious attack chain where they leverage SMS phishing (smishing), voice phishing (vishing), and other mobile-specific tactics to reliably steal credentials from targeted individuals within an organization. With those credentials, they're then able to access sensitive corporate data stored across the organization's cloud infrastructure under the guise of being a legitimate user who might typically have access to that data. Their attack chain is exemplary of the critical role that mobile devices now play in any organization's data security strategy, and we are likely to see a spike in copycats as Scattered Spider's successful attacks become well-known.

For additional analysis, we suggest these resources from BushidoToken and Security Scorecard.

Click here to learn more about Lookout Threat Intelligence