



How Lookout Protects Against Scattered Spider

What is Scattered Spider?

Scattered Spider, aka UNC3944, is a financially motivated threat actor that 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.

The group became more widely known after it successfully targeted and gained access to the infrastructure of Caesars Entertainment in 2023.

What tactics are in use?

By socially engineering targets through mobile form factors such as SMS phishing, voice phishing, Telegram, SIM swapping, and MFA fatigue, Scattered Spider 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, bypass MFA solutions and gain initial access.

Once the actor has compromised a user’s account, they create virtual machines in cloud and on-prem infrastructure to carry out the data-focused attacks and exfiltration. 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.

How Does Lookout Protect Against Scattered Spider?

Tactic	How Lookout Protects
Mobile phishing and social engineering	Lookout is constantly identifying new URLs that match the patterns that threat actors use and implements protection against those URLs as part of our Mobile Endpoint Security (MES) solution.
Desktop phishing and social engineering	Lookout Secure Internet Access, a SWG solution, can also block malicious domains. This is particularly important to address as messaging solutions evolve beyond mobile to be used on desktops.
Credential compromise and unauthorized data access	Lookout Secure Cloud Access, a CASB solution, detects anomalous user behavior indicative of a compromised account such as irregular login locations, access to apps atypical apps, and large data transfers or copies.

Protect Your Organization From Evolving Cyber Threats —
 Try **Lookout Mobile Endpoint Security Free For 90 Days** or **Contact Us Today**

“Lookout mobile endpoint provides services that solve an ever-growing need for advanced security for mobile devices that are most vulnerable to attacks, as user tends to open various links/ website across any Wi-Fi.”

Engineering, Software Industry



- Lookout Mobile Endpoint Security

“We had a great experience with the Lookout endpoint security solution in our organization. It protects our mobile devices from advanced threats and scans devices very well. It allows us to browse safely and track device locations for advanced security.”

Product Management, Healthcare and Biotech Industry



- Lookout Mobile Endpoint Security

Gartner
Peer Insights™



About Lookout

Lookout, Inc. is the data-centric cloud security company that uses a defense in-depth strategy to address the different stages of a cybersecurity attack. Data is at the core of every organization, and our approach to cybersecurity is designed to protect that data in the modern threat landscape. With a focus on people and their behavior, the Lookout Cloud Security Platform ensures real-time threat visibility, and quickly halts breaches from initial phishing attempts to data extraction. To learn more, visit www.lookout.com and follow Lookout on our [blog](#), [LinkedIn](#) and [X](#).

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo

© 2024 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.

lookout.com