Lookout

Mobile Threat of the Month

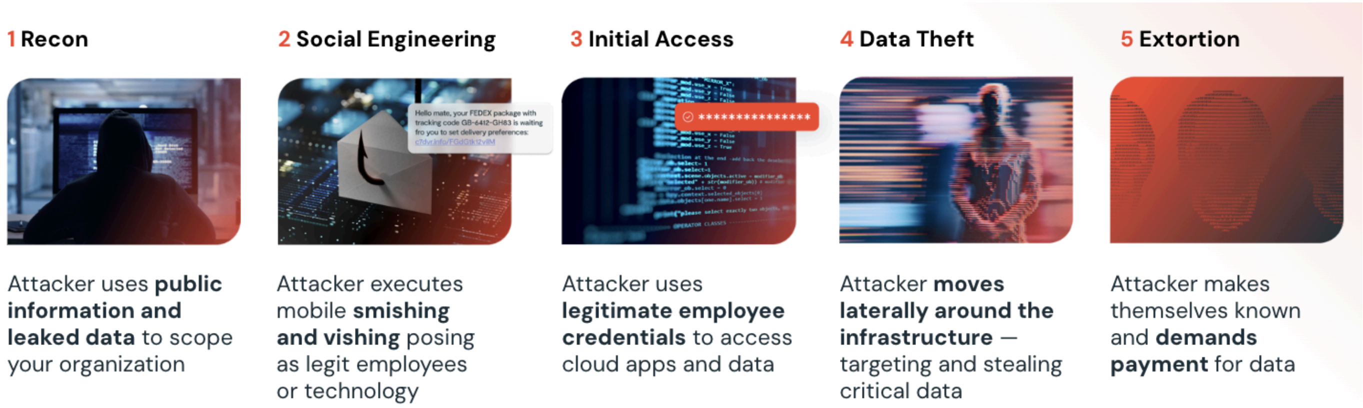
September 2025

ShinyHunters: The Latest Threat Actor Group Exploiting the Modern Kill Chain

About ShinyHunters

ShinyHunters is a financially motivated cybercriminal group, becoming increasingly notorious for its large-scale data breaches. Their tactics have evolved to include extortion and sophisticated social engineering schemes.

ShinyHunters employ a variety of tactics to infiltrate their targets' networks and exfiltrate sensitive information. Operational methods have shifted from purely technical exploits to leveraging human vulnerabilities to move through the five steps of the modern kill chain:



1 Recon

Attacker uses **public information and leaked data** to scope your organization

2 Social Engineering

Hello mate, your FEDEX package with tracking code GB-6412-GH83 is waiting fro you to set delivery preferences: c7dvr.info/FGdG1k12vllM

Attacker executes mobile **smishing and vishing** posing as legit employees or technology

3 Initial Access

Attacker uses **legitimate employee credentials** to access cloud apps and data

4 Data Theft

Attacker **moves laterally around the infrastructure** — targeting and stealing critical data

5 Extortion

Attacker makes themselves known and **demands payment** for data

Victims of ShinyHunters

Human resources platform provider Workday recently fell victim to a cyber attack originating through a third-party supplier – likely orchestrated through Salesforce. The breach of Workday's systems puts it among a growing number of companies to have been compromised by ShinyHunters in the past few weeks, including Adidas, Air France-KLM, Allianz, Google and various Moët Hennessy Louis Vuitton brands. These campaigns closely mirror a series of cyber attacks conducted by the Scattered Spider group whose victims included Marks & Spencer and Jaguar Land Rover.

Securing the Blind Spot

Threat actor groups such as ShinyHunter have shifted their focus to mobile devices and the humans behind them through sophisticated social engineering tactics. Smartphones have become the central tool for modern workforces and our constant connectivity and reliance on mobile makes it an attractive, high-reward target for cybercriminals. As the most personal, portable, and increasingly targeted endpoint, treating mobile as an afterthought is no longer an option.

Lookout's Mobile Threat Defense (MTD) solution is purpose-built to meet these modern security challenges, protecting iOS and Android devices from becoming the entry point of cyberattacks. Lookout's AI-first social engineering defends against these human-targeted attacks - preventing account takeovers and resulting data breaches. Lookout's mobile protection also addresses the broader spectrum of mobile risk, actively identifying and preventing mobile phishing, app-based malware, exploitable vulnerabilities, and insecure network connections.