DATASHEET

SpyCloud

SESSION IDENTITY PROTECTION

PREVENT AUTHENTICATION BYPASS & STOP SESSION HIJACKING BY SECURING YOUR CONSUMERS' ACCOUNTS

THE CHALLENGE

Cybercriminals excel at concealing malware within enticing links and downloads, causing a surge in consumers falling victim to infections – with more modern and sophisticated malware executing and auto-deleting before antivirus tools can even detect it. Upon infection, cybercriminals perceive session cookies as the most actionable and highest value authentication data stolen, due to their potential for session hijacking – an advanced method of ATO that extends beyond the realm of traditional credentials.

Session hijacking bypasses all forms of authentication by using malware-exfiltrated cookies in anti-detection tools to mimic a trusted consumer's device – defeating the need for a password, passkey, or any form of MFA. As long as a cookie stays valid, the gate to that consumer's account remains wide open.

THE SOLUTION

SpyCloud Session Identity Protection helps businesses proactively safeguard their customer base from "next-generation" account takeover by identifying malware-infected consumers with exposed authentication data – allowing security teams to intervene quickly to invalidate active sessions and lock criminals out of accounts to prevent fraud.

SpyCloud's security researchers constantly recover malware logs from the criminal underground. From this data, we parse out the compromised cookies relevant to your application, enrich it with information to help you identify the affected consumers, and deliver results via our high-volume, REST-based API. SpyCloud rapidly alerts your business, so you can act swiftly to protect your highest-risk accounts.

Using SpyCloud Session Identity Protection you can:

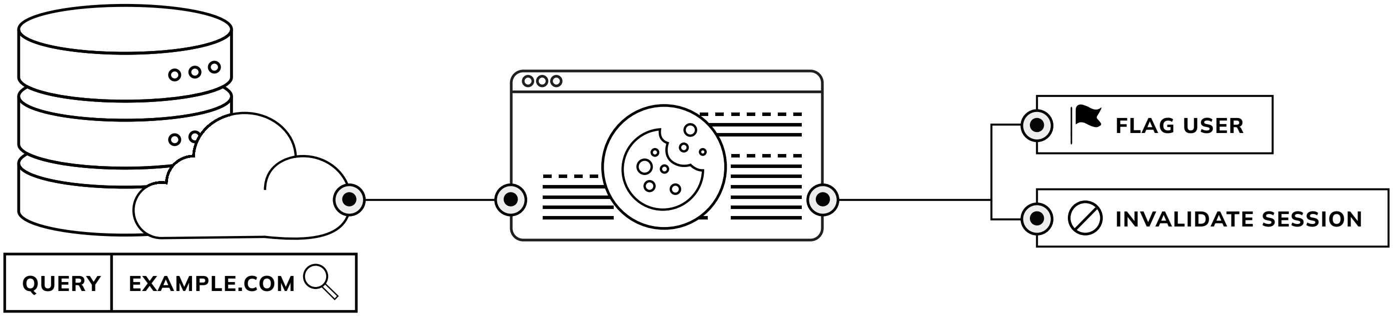
- **Stop targeted account takeover attacks** by invalidating compromised sessions, negating the value of the original cookie in criminal hands
- **Prevent authentication bypass** by identifying valid authentication cookies criminals can use to emulate a consumer's session and bypass security controls
- **Identify malware-infected consumers** to safeguard high-value accounts and notify users of infections, building trust and advising on how to further avoid the potential for fraud

SpyCloud

HOW IT WORKS

SpyCloud specializes in recapturing data from the deepest layers of the darknet — curating, analyzing, and enriching it with actionable insights to deliver only the most relevant and high quality information to security teams. Businesses can in turn increase operational efficiency by reducing noise and streamlining otherwise manual processes.

SpyCloud operationalizes the malware-siphoned authentication data containing compromised cookies tied to your domain and delivers alerts via our REST-based API. By integrating SpyCloud Session Identity Protection into your existing ATO prevention workflows, you can reduce your consumer's exposure window by invalidating active sessions and preventing criminals from accessing their accounts.



1. Query the Session Identity Protection API for your target application domain. Query options include:
   - Cookie Domain (required)
   - Cookie Name
   - Cookie Expiration Date
   - Source ID
   - SpyCloud Publish Date

2. SpyCloud returns compromised cookie data associated with your application domain, including the information you need to identify which accounts are vulnerable. Results include:
   - Source ID
   - Cookie Domain
   - Cookie Name
   - Cookie Value
   - Cookie Expiration
   - SpyCloud Publish Date
   - Infected Machine ID
   - IP Addresses
   - User Hostname
   - User System Registered Owner

3. Choose how and when to intervene to protect these accounts. SpyCloud recommends you invalidate the compromised cookies, or flag consumer accounts with known compromised devices for increased scrutiny.

> *"This was amazing. We were able to respond quickly, invalidate cookies, and protect millions of customer dollars."*
>
> **FINANCIAL SERVICES COMPANY**