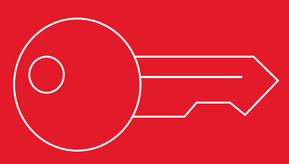
A PASSKEY-AUTHENTICATED SESSION HIJACKING

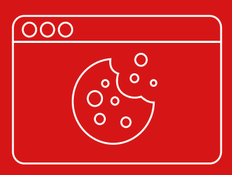
STEP 1 ⊙ MALWARE INFECTS DEVICE

Malware is mistakenly downloaded on a device Jill uses to access her online marketplace account. This could also occur after Jill authenticates, given that some infostealers exfiltrate everything already stored in the browser – including cookies – and delete themselves within seconds.



STEP 2 ⊙ PASSKEY AUTHENTICATION

Jill uses a passkey to initiate a session in the marketplace.



STEP 3 ⊙ SESSION COOKIE ISSUED

The app issues a cookie to remember Jill with a 30-day time-to-live, making it easier for her to visit again without re-authenticating.

STEP 4 ⊙ DATA EXFILTRATED

The malware exfiltrates Jill's browser data, including the cookie for the marketplace.

WITH SPYCLOUD...

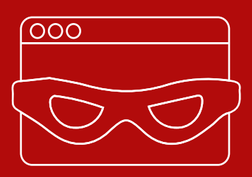
⊙ INVALIDATE COOKIE TO STOP SESSION HIJACKING

As a customer of SpyCloud, we would alert the marketplace of the stolen cookie so it can be immediately invalidated. Even expired stolen cookies can be used to identify accounts that should be monitored for suspicious behavior.

WITHOUT SPYCLOUD...

STEP 5 ⊙ DATA SOLD ON DARKNET

Jill's malware-exfiltrated data is packaged and sold to other criminals on the darknet.



STEP 6 ⊙ SESSION HIJACKED

Using Jill's stolen cookie and an anti-detect browser, the criminal hijacks the active marketplace session. The criminal appears to the app as Jill, setting off no red flags.

STEP 7 ⊙ CRIMINAL INVADES

From here, the criminal can see and do everything Jill is authorized to do, as long as the cookie remains valid.

SpyCloud