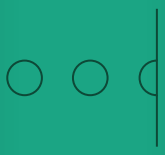
JON

HOW A MALWARE INFECTION LEADS TO RANSOMWARE

STEP 1 MALWARE INFECTS DEVICE

Malware is mistakenly downloaded on a device used to access corporate resources.



STEP 2 DATA SIPHONED

The malware siphons Jon's passwords, cookies, device information, browser fingerprint, and other data that can be used to impersonate him.

STEP 3 DATA SOLD ON DARKNET

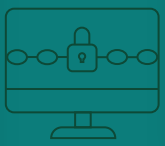
Jon's stolen data is bought or traded in the darknet, where initial access brokers or ransomware operators find it.

STEP 4 BUSINESS BECOMES A TARGET

Initial access brokers identify that Jon's data included personal and corporate assets. They provide the data to ransomware operators who target Jon's employer.

STEP 5 CRIMINALS INVADE COMPANY

Ransomware operators use Jon's compromised authentication data to log into corporate resources, bypass MFA, and move laterally to increase their access while evading detection.



STEP 6 RANSOMWARE DEPLOYED

Ultimately, the bad actors use their illegitimate access to deploy ransomware and demand a ransom payment in exchange for access to the enterprise's files.

SpyCloud