See No ®Evil: The New Approach to Ransomware Prevention

Doug Lingenfelter
Federal Sales, Account Manager
SpyCloud

Threat actors have direct access to valid credentials obtained through infostealer malware at a scale that's unimaginable – according to SpyCloud data, 24,000 infections alone in 2022 among just a sample of defense contractors. It's putting admin credentials and other forms of identity and authentication data in the wrong hands. Even on CAC protected systems, infostealers are extracting cyber vulnerabilities valuable to our adversaries to understand infrastructure, hidden IP addresses and the online activity of service members and contractors.

The DoD and DIB Supply Chain must better prepare for the threat of malware, and threat actors' increasing reliance on it for fresh data that enables MFA bypass, theft of mission-critical data from third-party applications, and ultimately – ransomware deployment. Anti-ransomware frameworks now need to focus on proper remediation of that common precursor, infostealer malware.

Demonstrating the visibility that now exists into the malware-infected devices used by service members and contractors and the networks and applications they access while infected, we'll walk through the new, necessary steps for malware infection response that's inclusive of remediating stolen identity data exfiltrated from infostealer malware-infected devices.