Learn: Command and Control (C2)

How attackers and autonomous agents keep control of compromised systems and move data out without tripping domain blocklists. The C2 and evasion techniques seen in modern, machine-speed intrusions.

HOW IT WORKS

01 Topics

How attackers and autonomous agents keep control of compromised systems and move data out without tripping domain blocklists. The C2 and evasion techniques seen in modern, machine-speed intrusions.

- What is a Dead Drop Resolver?: Instead of a hardcoded C2 domain, malware reads the real server's address from content on
- What is Living-off-Trusted-Services C2?: Run command and control through platforms the network already trusts, paste sites, code ho
- What is a Staged Payload Loader?: A tiny first-stage component fetches and runs the real second-stage payload at runtime, ke
- What is Payload Obfuscation?: Hide the content and intent of malicious code or data with compression, encoding, encrypti

SOURCES

[1] MITRE ATT&CK: Command and Control (TA0011)

Find the C2 and exfiltration paths before an attacker does.

securelayer7.net/learn/command-and-control

Open online