What is a dead drop resolver?

A dead drop resolver is a command-and-control technique that hides the address of the real C2 server inside content on a legitimate, trusted third-party service. Malware reads that content, a profile bio, a paste, or a dataset, to learn where to connect, so there is no hardcoded C2 domain to block and the traffic to a well-known service looks normal. In agentic intrusions, attacker-controlled datasets on a compromised platform act as the dead drop.

HOW IT WORKS

01 How it works and example

The attacker plants the C2 location, often encoded, in an ordinary-looking place: a social profile field, a paste, a repository file, or a dataset. The implant reads it and connects, so its only visible traffic is to a reputable service. In a 2026 agentic intrusion, attacker-controlled datasets on the compromised platform served as asynchronous message queues, a dead drop for commands and results.

SOURCES

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

[2] HuggingFace, Agent intrusion technical timeline

[3] MITRE ATT&CK: Web Service (T1102)

Find the C2 and exfiltration paths before an attacker does.

securelayer7.net/learn/command-and-control/dead-drop-resolver

Open online