What is living-off-trusted-services C2?

Living-off-trusted-services is running command-and-control and exfiltration through legitimate platforms a network already trusts, such as paste sites, code hosts, dataset hubs, or request-capture services. Because the traffic goes to allowlisted, reputable domains, blocklists and reputation filters do not flag it. A single C2 message envelope can be carried interchangeably over HTTP, dataset commits, error messages, or raw sockets. Defend with behavioural detection, not domain reputation.

HOW IT WORKS

01 How it works and example

The attacker layers a message envelope, with type, channel, sequence, and checksum fields, over trusted services, and carries the same protocol over whatever transport is available: an HTTP request to a paste site, a commit to a dataset, text hidden in an error message, or a raw socket. In a 2026 intrusion this multi-transport approach kept C2 alive as individual channels were closed.

02 What to do about it

Do not rely on domain reputation. Detect on behaviour and volume: unusual programmatic use of content and capture services from server workloads, abnormal request timing, and data leaving through error channels or raw sockets. Restrict which workloads may reach these services, apply data-loss controls, and treat the ability to carry the same protocol over many transports as a strong signal.

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/living-off-trusted-services

Open online