What is a staged payload loader?

A staged payload loader is a small first-stage component that fetches and runs a larger second-stage payload from a remote source at runtime. It keeps the initial footprint tiny, lets the attacker update the real payload without re-accessing the victim, and re-arms on every run, which matters in ephemeral, rebuilt-each-time environments. In a 2026 intrusion, a loader fetched code from a paste site on each code-submission sandbox to persist across throwaway environments.

HOW IT WORKS

01 How it works and example

The loader is injected into a harness or startup path, and on each execution it fetches the second stage, often from a trusted content service, and runs it. In ephemeral environments that rebuild on every job, this re-arms the attack each time, giving persistence without a persistent file. A 2026 sandbox intrusion used exactly this to survive throwaway evaluation environments.

SOURCES

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

[2] HuggingFace, Agent intrusion technical timeline

[3] MITRE ATT&CK: Ingress Tool Transfer (T1105)

Find the C2 and exfiltration paths before an attacker does.

securelayer7.net/learn/command-and-control/staged-payload-loader

Open online