

Advanced Reconnaissance

TACTICAL INTELLIGENCE REPORT // 2026

The Silent Phase

Reconnaissance is no longer just pinging servers. It is a multi-dimensional analysis of a company's soul—its people, its third-party vendors, and its forgotten digital crumbs.

Case Study: The 2024 U.S. Treasury Vendor Breach

ADVERSARY TACTIC: SUPPLY CHAIN STALKING

In December 2024, state-sponsored actors bypassed the Treasury's hardened perimeter entirely. Instead, they spent months performing reconnaissance on a niche IT contractor. By identifying a single unpatched VPN on the vendor's side, they gained a trusted tunnel into the Treasury's network, exfiltrating 3,000 sensitive documents before a single alarm was raised.

Advanced Tactics

AI-Powered Footprinting

Modern attackers use LLM-based scrapers to build 'Influence Maps.' They cross-reference GitHub commits with LinkedIn profiles to find developers who accidentally leaked internal API keys.

Operational Best Practices

Counter-Recon Strategy

- **DNS Sinkholing:** Monitor and block queries for suspicious, newly registered domains.

- **Bait Infrastructure:** Deploy 'Honey-Tokens' (fake AWS keys) in public repos to alert you the moment they are used.