Proxy: Multi-hop Proxy, Sub-technique T1090.003 - Enterprise

Archived: 2026-04-02 11:21:05 UTC

Adversaries may chain together multiple proxies to disguise the source of malicious traffic. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.

For example, adversaries may construct or use onion routing networks – such as the publicly available Tor network – to transport encrypted C2 traffic through a compromised population, allowing communication with any device within the network.[1] Adversaries may also use operational relay box (ORB) networks composed of virtual private servers (VPS), Internet of Things (IoT) devices, smart devices, and end-of-life routers to obfuscate their operations.[2]

In the case of network infrastructure, it is possible for an adversary to leverage multiple compromised devices to create a multi-hop proxy chain (i.e., Network Devices). By leveraging Patch System Image on routers, adversaries can add custom code to the affected network devices that will implement onion routing between those nodes. This method is dependent upon the Network Boundary Bridging method allowing the adversaries to cross the protected network boundary of the Internet perimeter and into the organization’s Wide-Area Network (WAN). Protocols such as ICMP may be used as a transport.

Similarly, adversaries may abuse peer-to-peer (P2P) and blockchain-oriented infrastructure to implement routing between a decentralized network of peers.[3]

Source: https://attack.mitre.org/techniques/T1090/003