Proxy

Sub-techniques (4)

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. [1] Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

ID: T1090

Sub-techniques: T1090.001, T1090.002, T1090.003, T1090.004

ⓘ Tactic: Command and Control

ⓘ Platforms: Linux, Network, Windows, macOS

Contributors: Heather Linn; Jon Sheedy; Walker Johnson

Version: 3.1

Created: 31 May 2017

Last Modified: 30 August 2021

Version Permalink

Procedure Examples

ID	Name	Description
G0096	APT41	APT41 used a tool called CLASSFON to covertly proxy network communications.[2]
S0456	Aria-body	Aria-body has the ability to use a reverse SOCKS proxy module.[3]
S0347	AuditCred	AuditCred can utilize proxy for communications.[4]
S0245	BADCALL	BADCALL functions as a proxy server between the victim and C2 server.[5]
S1081	BADHATCH	BADHATCH can use SOCKS4 and SOCKS5 proxies to connect to actor-controlled C2 servers. BADHATCH can also emulate a reverse proxy on a compromised machine to connect with actor-controlled C2 servers.[6]
S0268	Bisonal	Bisonal has supported use of a proxy server.[7]
G0108	Blue Mockingbird	Blue Mockingbird has used FRP, ssf, and Venom to establish SOCKS proxy connections.[8]
C0017	C0017	During C0017, APT41 used the Cloudflare CDN to proxy C2 traffic.[9]
C0027	C0027	During C0027, Scattered Spider installed the open-source rsocx reverse proxy tool on a targeted ESXi appliance.[10]
S0348	Cardinal RAT	Cardinal RAT can act as a reverse proxy.[11]
G1021	Cinnamon Tempest	Cinnamon Tempest has used a customized version of the Iox port-forwarding and proxy tool.[12]
G0052	CopyKittens	CopyKittens has used the AirVPN service for operational activity.[13]