Proxy, Technique T1090 - Enterprise

Archived: 2026-04-05 16:21:37 UTC

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]

G1052 Contagious Interview

Contagious Interview has leveraged Astrill VPN for C2.[13]

G0052 CopyKittens

CopyKittens has used the AirVPN service for operational activity.[14]

S0384 Dridex

Dridex contains a backconnect module for tunneling network traffic through a victim's computer. Infected computers become part of a P2P botnet that can relay C2 traffic to other infected peers.[15][16]

G1006 Earth Lusca

Earth Lusca adopted Cloudflare as a proxy for compromised servers.[17]

G0117 Fox Kitten

Fox Kitten has used the open source reverse proxy tools including FRPC and Go Proxy to establish connections from C2 to local servers.[18][19][20]

S1144 FRP

FRP can proxy communications through a server in public IP space to local servers located behind a NAT or firewall.[21]

S1044 FunnyDream

FunnyDream can identify and use configured proxies in a compromised network for C2 communication.[22]

G0047 Gamaredon Group

Gamaredon Group has used the Cloudflare Tunnel client to proxy C2 traffic.[23]

S1197 GoBear

GoBear implements SOCKS5 proxy functionality.[24]

S0690 Green Lambert

Green Lambert can use proxies for C2 traffic.[25][26]

S0246 HARDRAIN

HARDRAIN uses the command `cmd.exe /c netsh firewall add portopening TCP 443 "adp"` and makes the victim machine function as a proxy server.[27]

S1229 Havoc

Havoc has the ability to route HTTP/S communications through designated proxies.[28]

S0376 HOPLIGHT

HOPLIGHT has multiple proxy options that mask traffic between the malware and the remote operators.[29]

S0040 HTRAN

HTRAN can proxy TCP socket connections to obfuscate command and control infrastructure.[30][31]

S0283 jRAT

jRAT can serve as a SOCKS proxy server.[32]

S1190 Kapeka

Kapeka can identify system proxy settings via `WinHttpGetIEProxyConfigForCurrentUser()` during initialization and utilize these settings for subsequent command and control operations.[33]

S0487 Kessel

Kessel can use a proxy during exfiltration if set in the configuration.[34]

S1051 KEYPLUG

KEYPLUG has used Cloudflare CDN associated infrastructure to redirect C2 communications to malicious domains.[9]

S0669 KOCTOPUS

KOCTOPUS has deployed a modified version of Invoke-Ngrok to expose open local ports to the Internet.[35]

G1004 LAPSUS$

LAPSUS$ has leverage NordVPN for its egress points when targeting intended victims.[36]

S1121 LITTLELAMB.WOOLTEA

LITTLELAMB.WOOLTEA has the ability to function as a SOCKS proxy.[37]

S1141 LunarWeb

LunarWeb has the ability to use a HTTP proxy server for C&C communications.[38]

G0059 Magic Hound

Magic Hound has used Fast Reverse Proxy (FRP) for RDP traffic.[39]

G1019 MoustachedBouncer

MoustachedBouncer has used a reverse proxy tool similar to the GitHub repository revsocks.[40]

S1189 Neo-reGeorg

Neo-reGeorg has the ability to establish a SOCKS5 proxy on a compromised web server.[41]

S0108 netsh

netsh can be used to set up a proxy tunnel to allow remote host access to an infected host.[42]

S0198 NETWIRE

NETWIRE can implement use of proxies to pivot traffic.[43]

S0508 ngrok

ngrok can be used to proxy connections to machines located behind NAT or firewalls.[44][45]

C0048 Operation MidnightEclipse

During Operation MidnightEclipse, threat actors used the GO Simple Tunnel reverse proxy tool.[46]

C0013 Operation Sharpshooter

For Operation Sharpshooter, the threat actors used the ExpressVPN service to hide their location.[47]

C0014 Operation Wocao

During Operation Wocao, threat actors used a custom proxy tool called "Agent" which has support for multiple hops.[48]

S0435 PLEAD

PLEAD has the ability to proxy network communications.[49]

G1005 POLONIUM

POLONIUM has used the AirVPN service for operational activity.[14]

S0378 PoshC2

PoshC2 contains modules that allow for use of proxies in command and control.[50]

S0262 QuasarRAT

QuasarRAT can communicate over a reverse proxy using SOCKS5.[51][52]

S0629 RainyDay

RainyDay can use proxy tools including boost_proxy_client for reverse proxy functionality.[53]

S1212 RansomHub

RansomHub can use a proxy to connect to remote SFTP servers.[54]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda proxied communication through the Cloudflare CDN service during RedDelta Modified PlugX Infection Chain Operations.[55]

C0056 RedPenguin

During RedPenguin, UNC3886 used malware capable of establishing a SOCKS proxy connection to a specified IP and port.[56][57]

S1187 reGeorg

reGeorg can establish an HTTP or SOCKS proxy to tunnel data in and out of a network.[58][59][60]

S0332 Remcos

Remcos uses the infected hosts as SOCKS5 proxies to allow for tunneling and proxying.[61]

S1210 Sagerunex

Sagerunex uses several proxy configuration settings to ensure connectivity.[62]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors used Mullvad VPN IPs to proxy voice phishing calls.[63]

S1099 Samurai

Samurai has the ability to proxy connections to specified remote IPs and ports through a a proxy module.[64]

G0034 Sandworm Team

Sandworm Team's BCS-server tool can create an internal proxy server to redirect traffic from the adversary-controlled C2 to internal servers which may not be connected to the internet, but are interconnected locally.[65]

G1015 Scattered Spider

Scattered Spider has used proxy networks to hamper detection and has installed legitimate proxy tools on VMware vCenter and adversary-controlled VMs.[66][67]

S0461 SDBbot

SDBbot has the ability to use port forwarding to establish a proxy between a target host and C2.[68]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors used Fast Reverse Proxy to communicate with C2.[69][70]

S0273 Socksbot

Socksbot can start SOCKS proxy threads.[71]

S0615 SombRAT

SombRAT has the ability to use an embedded SOCKS proxy in C2 communications.[72]

S0436 TSCookie

TSCookie has the ability to proxy communications with command and control (C2) servers.[73]

G0010 Turla

Turla RPC backdoors have included local UPnP RPC proxies.[74]

S0263 TYPEFRAME

A TYPEFRAME variant can force the compromised system to function as a proxy server.[75]

S0386 Ursnif

Ursnif has used a peer-to-peer (P2P) network for C2.[76][77]

S0207 Vasport

Vasport is capable of tunneling though a proxy.[78]

G1017 Volt Typhoon

Volt Typhoon has used compromised devices and customized versions of open source tools such as FRP (Fast Reverse Proxy), Earthworm, and Impacket to proxy network traffic.[79][80][81]

S0670 WarzoneRAT

WarzoneRAT has the capability to act as a reverse proxy.[82]

G0124 Windigo

Windigo has delivered a generic Windows proxy Win32/Glubteta.M. Windigo has also used multiple reverse proxy chains as part of their C2 infrastructure.[83]

S0117 XTunnel

XTunnel relays traffic between a C2 server and a victim.[84]

S1114 ZIPLINE

ZIPLINE can create a proxy server on compromised hosts.[85][86]

S0412 ZxShell

ZxShell can set up an HTTP or SOCKS proxy.[2][87]
