# Protocol Tunneling, Technique T1572 - Enterprise

Archived: 2026-04-05 13:40:38 UTC

C0034 2022 Ukraine Electric Power Attack

During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the GOGETTER tunneler software to establish a "Yamux" TLS-based C2 channel with an external server(s).[4]

S1063 Brute Ratel C4

Brute Ratel C4 can use DNS over HTTPS for C2.[5][6]

C0027 C0027

During C0027, Scattered Spider used SSH tunneling in targeted environments.[7]

C0032 C0032

During the C0032 campaign, TEMP.Veles used encrypted SSH-based PLINK tunnels to transfer tools and enable RDP connections throughout the environment.[8]

G0114 Chimera

Chimera has encapsulated Cobalt Strike's C2 protocol in DNS and HTTPS.[9]

G1021 Cinnamon Tempest

Cinnamon Tempest has used the Iox and NPS proxy and tunneling tools in combination create multiple connections through a single tunnel.[10]

G0080 Cobalt Group

Cobalt Group has used the Plink utility to create SSH tunnels.[11][12][13]

S0154 Cobalt Strike

Cobalt Strike uses a custom command and control protocol that is encapsulated in HTTP, HTTPS, or DNS. In addition, it conducts peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.[14][15]

C0004 CostaRicto

During CostaRicto, the threat actors set up remote SSH tunneling into the victim's environment from a malicious domain.[16]

C0029 Cutting Edge

During Cutting Edge, threat actors used Iodine to tunnel IPv4 traffic over DNS.[17]

S0687 Cyclops Blink

Cyclops Blink can use DNS over HTTPS (DoH) to resolve C2 nodes.[18]

S0038 Duqu

Duqu uses a custom command and control protocol that communicates over commonly used ports, and is frequently encapsulated by application layer protocols.[19]

G1003 Ember Bear

Ember Bear has used ProxyChains to tunnel protocols to internal networks.[20]

G1016 FIN13

FIN13 has utilized web shells and Java tools for tunneling capabilities to and from compromised assets.[21]

G0037 FIN6

FIN6 used the Plink command-line utility to create SSH tunnels to C2 servers.[22]

G0046 FIN7

FIN7 has tunneled C2 traffic via OpenSSH.[23]

S0173 FLIPSIDE

FLIPSIDE uses RDP to tunnel traffic from a victim environment.[24]

G0117 Fox Kitten

Fox Kitten has used protocol tunneling for communication and RDP activity on compromised hosts through the use of open source tools such as ngrok and custom tool SSHMinion.[25][26][27]

S1144 FRP

FRP can tunnel SSH and Unix Domain Socket communications over TCP between external nodes and exposed resources behind firewalls or NAT.[28]

S1044 FunnyDream

FunnyDream can connect to HTTP proxies via TCP to create a tunnel to C2.[29]

S1027 Heyoka Backdoor

Heyoka Backdoor can use spoofed DNS requests to create a bidirectional tunnel between a compromised host and its C2 servers.[30]

S0604 Industroyer

Industroyer attempts to perform an HTTP CONNECT via an internal proxy to establish a tunnel.[31]

S1020 Kevin

Kevin can use a custom protocol tunneled through DNS or HTTP.[32]

G0065 Leviathan

Leviathan has used protocol tunneling to further conceal C2 communications and infrastructure.[33]

S1141 LunarWeb

LunarWeb can run a custom binary protocol under HTTPS for C2.[34]

G0059 Magic Hound

Magic Hound has used Plink to tunnel RDP over SSH.[35]

S1015 Milan

Milan can use a custom protocol tunneled through DNS or HTTP.[32]

G0129 Mustang Panda

Mustang Panda has leveraged OpenSSH (sshd.exe) to execute commands, transfer files and spread across the environment communicating over SMB port 445.[36]

S0699 Mythic

Mythic can use SOCKS proxies to tunnel traffic through another protocol.[37]

S1189 Neo-reGeorg

Neo-reGeorg can tunnel data in and out of targeted networks.[38]

S0508 ngrok

ngrok can tunnel RDP and other services securely over internet connections.[39][40][41][42]

G0049 OilRig

OilRig has used the Plink utility and other tools to create tunnels to C2 servers.[43][44][45][46]

S0650 QakBot

The QakBot proxy module can encapsulate SOCKS5 protocol within its own proxy protocol.[47]

S1187 reGeorg

reGeorg can tunnel TCP sessions including RDP, SSH, and SMB through HTTP.[48][49][50]

G1045 Salt Typhoon

Salt Typhoon has modified device configurations to create and use Generic Routing Encapsulation (GRE) tunnels.[51]

G1015 Scattered Spider

Scattered Spider has installed protocol-tunneling tools on VMware vCenter and adversary-controlled VMs, including Teleport.sh, Chisel (configured to communicate with trycloudflare[.]com subdomains), MobaXterm, ngrok, Pinggy, and Teleport.[52][53]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors utilized ngrok tunnels to deliver PowerShell payloads.[54]

S0022 Uroburos

Uroburos has the ability to communicate over custom communications methodologies that ride over common network protocols including raw TCP and UDP sockets, HTTP, SMTP, and DNS.[55]

---