

NOTABLE TUNNELING TOOLS LEVERAGED BY STATE-SPONSORED / RANSOMWARE ACTORS

Tool Name	Description	Capabilities	Opens source \Premium	Used in Ransomware Campaign	Used by Threat Actor
NPS	Tunneling tool used for command and control traffic and infrastructure management.	<ol style="list-style-type: none"> 1. Compatible with all platforms. 2. Supports all type of protocols traffic forwarding such as TCP, UDP, SOCKS5, HTTP, etc. 3. Provides compression, encryption, and port reuse. 	Open Source	Yes(RA World)	Yes(Red Lima/APT15-CN)
Fast Reverse Proxy (FRP)	Used to expose a local server behind a NAT or firewall to the internet.	<ol style="list-style-type: none"> 1. Supports authentication and encrypted connection facility. 2. It currently supports TCP and UDP, as well as HTTP and HTTPS protocols, enabling requests to be forwarded to internal services via domain name. 	Open Source	Unknown	Yes(Pioneer Kitten-IRN, Volt Typhoon-CN)
Chisel	Used for tunneling TCP and UDP connections traffic via HTTP.	<ol style="list-style-type: none"> 1. Reverse port forwarding (Connections go through the server and out the client) 2. Supports multiple tunnel endpoints over one TCP connection 3. Supports authentication and encrypted connection facility. 	Open Source	Yes(Royal Ransomware, BlackSuit Ransomware)	Yes(Red Hotel-CN)
Ligolo-ng	Tunneller written in Go that provides encrypted reverse TCP/TLS connections to a remote host.	<ol style="list-style-type: none"> 1. Reverse/Bind Connection 2. Tun interface (No more SOCKS/Proxymchains) 3. Supports multiple platforms and multiple tunnel connection. 	Open Source	Unknown	Yes

Detection Mechanism

1. Port Scanning & Service Identification

Custom Ports: If custom ports are used, identifying specific ports through scanning tools may still detect unusual traffic patterns that suggest a reverse proxy. If any tunnelling is detected using non-standard ports (or multiple ports for various services), it could be flagged during scans.

Unusual Port Usage: Tunnelling tool typically operates on ports 80 (HTTP) or 443 (HTTPS) to bypass network restrictions. While these ports are standard for web traffic, constant connections or data transfer on these ports without legitimate HTTP/S traffic could suggest tunnelling activity.

2. Traffic Pattern and Behavior Analysis

Tunnel Traffic Signatures: Major tunnelling tool establishes an encrypted tunnel between a client and server, which can exhibit unique patterns in the traffic. This traffic is often different from regular HTTP/HTTPS traffic in terms of packet size, timing, and consistency.

High Traffic Over Unusual Hours: Attacker mainly exfiltrate data from victim environment during Unusual Hours. Activity like unusually high traffic volumes at certain times, particularly during off-hours or without a corresponding increase in legitimate user activity, could raise suspicion. A rapid increase in traffic (especially during network audits or while performing security checks) may indicate that tunnelling tools are being used to transmit large amounts of data covertly.

3. Connection Analysis

Long-Lived Connections: Any long-lived, persistent connections or Single Endpoint with Multiple Services to the server is sign of tunnelling activity. This can be different from typical short-lived HTTP connections. Long sessions with little or no web traffic activity on standard ports could indicate tunnelling.

4. DNS Analysis

Attacker configured the tunnelling tool to dynamically choose domains for its traffic, unusual DNS request patterns (e.g., frequent requests to non-standard or obscure domains). Any such request in traffic logs might indicate presence of Tunnelling tool.

Mitigation

1. Monitor network traffic for unexpected and unapproved protocols, especially outbound to the internet (e.g., SSH, SMB, RDP).
2. Implement multi-factor authentication, especially for privileged accounts.
3. Deploy endpoint defense tools on all endpoints; ensure they work and are up to date.
4. Regularly update and patch all software, applications, and firmware.
5. Use network segmentation to limit lateral movement within the network and protect sensitive data.
6. Enforce strict access controls and monitor for unusual activity to prevent unauthorized access.
7. Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security for accessing critical systems.
8. Endpoint Protection: Deploy advanced endpoint protection solutions to detect and block malicious activities.
9. Incident Response: Establish a comprehensive incident response plan and conduct regular drills.