CxO Corner

Your Executive Edge

Liminal Panda: A Threat to the Telecommunications Sector

Liminal Panda is a China-linked cyber espionage group that has been targeting telecommunications entities in South Asia and Africa since at least 2020. The group's goal is to collect intelligence, and it possesses a deep understanding of telecommunications networks, protocols, and interconnections between providers.

Impacts on the Telecommunications Sector

- **Data Exfiltration:** Liminal Panda uses custom tools to gain access to telecom networks, establish command and control, and steal sensitive data. This includes:
  - Network telemetry
  - Subscriber information
  - Call metadata
  - Text messages (SMS)
- **Breaching Other Telecom Entities:** Liminal Panda exploits trust relationships and security gaps between providers to gain access to core infrastructure and potentially breach other telecom entities.
- **SIGINT Collection:** The group's activities, particularly the development and deployment of telecom-specific tools, point to signals intelligence (SIGINT) collection operations for intelligence gathering.
- **Targeting the Belt and Road Initiative:** Liminal Panda has focused on telecom providers in regions associated with China's Belt and Road Initiative, suggesting alignment with China's national objectives

Tactics and Techniques

- **Exploiting Trust Relationships:** Liminal Panda abuses trust relationships between telecom providers and exploits gaps in security policies to gain access to core infrastructure from external hosts.
- **Password Spraying:** The group uses password spraying with weak and third-party-focused passwords to infiltrate external DNS (eDNS) servers.
- **Emulating GSM Protocols:** Liminal Panda uses techniques like emulating global system for mobile communications (GSM) protocols to enable command and control (C2) and data exfiltration.
- **Custom and Publicly Available Tools:** Liminal Panda's arsenal includes both custom malware and publicly available tools for C2 communication. Some of these tools include:
  - **SIGTRANslator:** A tool designed to send and receive data using SIGTRAN protocols.

    - **CordScan:** A utility for network scanning and packet capture, specifically designed to retrieve data related to common telecommunication protocols.
    - **PingPong:** A backdoor that sets up a reverse shell connection for remote access.
    - **TinyShell:** An open-source Unix backdoor used in conjunction with an SGSN emulator for C2 communications.
    - **Publicly available proxy tools:** Liminal Panda uses various public proxy tools to route C2 communications, often through compromised SOHO routers (Operational Relay Boxes).

Indicators of Compromise for Liminal Panda Activity

There are several indicators of compromise (IOCs) that organisations, particularly those in the telecommunications sector, can use to detect potential Liminal Panda activity:

Network Activity:

- **Anomalous SSH Connections:** Monitor SSH connections between internal servers, particularly connections originating from eDNS servers or other servers that accept connections from external organisations. Liminal Panda uses password spraying to compromise eDNS servers and may use these compromised servers as pivots to access other internal systems.
- **Suspicious Inbound Firewall Rules:** Regularly check firewall rules for any abnormal entries that allow inbound access from unexpected external IP addresses. Liminal Panda may modify firewall rules to enable persistent access or data exfiltration.
- **Unusual Network Traffic Patterns:** Look for unusual traffic patterns, especially those associated with GSM protocol emulation or traffic routed through known public proxy tools. Liminal Panda leverages GSM emulation for C2 and uses various public proxy tools, often via compromised SOHO routers, to obfuscate their C2 communications.

File and System Changes:

- **Modified System Binaries:** Employ file integrity monitoring on critical system service binaries, like `iptables`, to detect any unauthorised modifications or replacements. Liminal Panda may modify these binaries to maintain persistence or evade detection.
- **Presence of Custom Tools:** Look for the presence of Liminal Panda's custom tools, such as SIGTRANslator, CordScan, and PingPong, on your systems. These tools are specifically designed to interact with telecommunications protocols and infrastructure.
- **Presence of Publicly Available Tools:** Be aware of the usage of publicly available tools like TinyShell, Fast Reverse Proxy, ProxyChains, and Microsocks Proxy on systems that don't typically require them. While legitimate uses for these tools exist, their presence, especially in conjunction with other suspicious activity, may warrant further investigation.

Other Indicators:

- **Compromised Credentials:** Regularly audit user accounts for signs of compromise, such as password changes, unusual login times, or access from unexpected locations. Liminal Panda uses password spraying and may target user accounts with weak or third-party-focused passwords.
- **Targeting of Specific Regions:** Be particularly vigilant if your organisation operates in South Asia or Africa, regions where Liminal Panda has historically concentrated its activities. The group's

targeting may expand to other regions depending on their collection requirements, but these regions remain primary areas of focus.

- **Exploitation of Trust Relationships:** Review security policies and configurations related to trust relationships between your organisation and other telecom providers. Ensure strong authentication mechanisms are in place and access from external partners is appropriately restricted.

Attribution to China

While the exact motives of Liminal Panda are still under investigation, its activities are consistent with state-linked operations, particularly intelligence gathering for national objectives rather than financial gain. CrowdStrike assesses with low confidence that Liminal Panda's activity aligns with China-nexus cyber operations based on several factors:

- Targeting organizations in countries associated with China's Belt and Road Initiative.
- Using Pinyin strings for malware keys and passwords.
- Utilizing domain names that overlap with Chinese infrastructure.
- Employing tools like *Fast Reverse Proxy* and *TinyShell*, commonly used by Chinese adversaries.
- Using VPS infrastructure provided by Vultr, a provider frequently used by China-nexus actors.

It is important to note that the attribution of cyberattacks can be complex and challenging, and definitive attribution may not always be possible. CrowdStrike acknowledges a past misattribution of some of Liminal Panda's activities to another group, LightBasin, due to multiple actors operating on a contested compromised network.

Recommendations for Protection

CrowdStrike offers several recommendations for organisations to protect themselves from threats like Liminal Panda, particularly for telecom providers:

- **Deploy advanced endpoint protection solutions.**
- **Implement secure authentication methods, avoiding weak or default passwords.**
- **Regularly monitor network traffic for anomalies.**
- **Limit public accessibility of sensitive services.**
- **Enforce strict network access control policies.**
- **Log and monitor SSH connections for suspicious activity.**
- **Verify and monitor firewall rules for unauthorised inbound access.**
- **Implement file integrity checking mechanisms on critical system binaries.**