SecurityGen
Telecom Security. Transcending Generations.

Liminal Panda Unveiled by CrowdStrike: What It Means for Telcos

Threat Intelligence Report, 27.11.24

1. Executive Summary

On 19 November, CrowdStrike shed light on a newly identified advanced persistent threat (APT) group called Liminal Panda, which has been active since at least 2020. The group specializes in targeting telecom networks for signals intelligence (SIGINT) operations. Recent analysis reattributes past LightBasin linked events to Liminal Panda, revealing multiple threat actors conducting malicious activities on the same compromised networks. This overlap highlights significant detection gaps in many mobile network operators (MNOs), emphasizing the urgent need for enhanced monitoring and threat visibility across critical telecom infrastructures.

This report primarily focuses on the group's tactics, techniques, and procedures (TTPs) related to the exploitation of telecom-specific protocols and infrastructure. It assesses the potential impact on the telecom sector and provides actionable recommendations for mitigation.

2. Technical Details

2.1 Description

Liminal Panda exhibits a deep understanding of telecom networks, including the interconnections between providers and the protocols supporting mobile telecommunications. The group uses a combination of publicly available and custom-developed tools to fingerprint networks, extract data from telecom protocols, and tunnel command-and-control (C2) traffic through less-monitored protocols like **SIGTRAN** and **GTP**. By compromising networks within a single provider, Liminal Panda can attack interconnected providers globally via the **GRX/IPX** network.

2.2 Attack Vector

To execute the attack, the intruder must gain access to the international, national, or adjacent GRX/IPX network.

2.3 APT Actions

2.3.1 Initial Access and Execution

Liminal Panda compromised multiple telecom providers by targeting their external DNS (eDNS) servers, which are integral to the General Packet Radio Service (GPRS) network and facilitate roaming between mobile operators. The group gained access through password spraying weak SSH credentials, exploiting trust relationships between providers, and leveraging poor security configurations.

2.3.2 Persistence and Defence Evasion

After gaining initial access, the group deploys a backdoor known as **PingPong**, which listens for inbound magic ICMP echo requests from other compromised telecom providers and establishes a TCP reverse shell connection to a remote C2 server on TCP port 53 — the port typically used for DNS — in order to disguise their activity as legitimate traffic. To maintain access and evade detection, the group adds iptables rules to the eDNS server, ensuring continued SSH access from five other compromised telecom providers. They also replace the legitimate iptables binary with a wrapper to conceal the created rules from iptables queries.

2.3.3 Discovery, Collection and Exfiltration

The group employs a network-scanning and packet-capture utility called **CordScan** to fingerprint networks and extract sensitive subscriber data, including traffic and location information, from network elements such as **SGSNs**, which handle packet-data delivery to and from mobile stations. To further evade detection, the group tunnels all C2 communications and data exfiltration over **GTP** and SIGTRAN protocols. Liminal Panda uses the **sgsnemu** SGSN emulator to establish Packet Data Protocol (PDP) context requests for nine pairs of international IMSI/MSISDN numbers, disguising all communications as legitimate subscriber data traffic. Additionally, the group employs the **SIGTRANslator** utility, capable of sending and receiving data over the SIGTRAN protocol in an encrypted format using the hard-coded XOR key, wuxianpinggu507.

2.4 Affected Systems/Technology

The group targets core telecom infrastructure, including systems that support interconnection such as eDNS servers.

2.5 Tactics, Techniques, and Procedures (TTPs)

The following table maps observed TTPs for Liminal Panda to relevant techniques in the MITRE ATT&CK, MITRE FiGHT, and GSMA MoTIF frameworks to provide comprehensive context.

Tactics	Attack Technique	Fight Equivalent	Motif Equivalent
Initial Access	T1199 - Trusted Relationship	FGT1199.501 - MNO Roaming Partners	MOT 1199.301 - Exploit Interconnection Agreements
	T1078.003 —Local Accounts	FGT1078.003 - Local Accounts	NA
Execution	T1059.004 - Unix Shell	NA	NA
Persistence	T1543 - Create or Modify System Process	NA	NA
Defense Evasion	T1562.004 - Disable or Modify System Firewall	NA	NA
	T1562.001 - Disable or Modify Tools	NA	NA
Discovery	T1046 - Network Service Discovery	FGT1046 - Network Service Discovery	MOT1046 - Network Service Scanning
Collection	T1040 - Network Sniffing	FGT1040 - Network Sniffing	MÖT1040 -Network Sniffing
Command and Control & Exfiltration	T1048.001 - Exfiltration Over Symmetric Encrypted Non-C2Protocol	FGT1048 - Exfiltration Over Alternative Protocol	NA

3. Impact Analysis

3.1 Threat Severity

Liminal Panda's operations are highly specialized, targeting global telecom providers to conduct signals intelligence (SIGINT) activities, with a primary focus on data disclosure. While the group's primary objective is limited to this type of activity, the following additional threats are feasible on compromised networks:

- Subscriber Data Disclosure
- Fraud
- Subscriber DoS
- Traffic Interception
- Infrastructure DoS
- Infrastructure Disclosure

3.2 Likelihood of Occurrence

Given the high-value nature of telecom networks and the group's demonstrated expertise, the likelihood of future attacks remains significant.

4. Mitigation

Liminal Panda primarily exploits trust relationships between telecom providers and leverages less-monitored telecom protocols to evade detection. The following measures are recommended to protect against the group's activities:

4.1 Immediate Steps

- Configure firewalls at GRX/IPX network edges to allow GTP interconnect traffic only to and from IP ranges of authorized roaming partners.
- Configure firewalls at GRX/IPX network edges to allow only GTP-C, GTP-U, and DNS protocols over GTP interconnects. Block access to internal OAM network services, such as SSH.
- Enforce a strong password policy for SSH authentication or switch to secure SSH key-based authentication.

4.2 Long-term Recommendations

- Conduct regular security audits to ensure that non-essential services for international roaming are not exposed on the GRX/IPX network.
- Deploy continuous signaling security monitoring to detect unauthorized core network activities (e.g., GTP/SIGTRAN traffic from eDNS servers) and anomalies in signaling protocols like SIGTRAN and GTP to prevent tunneling of C2 traffic.
- Implement endpoint security monitoring for IT network elements that support the core telecom network, such as eDNS servers.
- Use out-of-band management channels with dedicated network interfaces for managing infrastructure nodes.
- Implement network segmentation to isolate critical systems and apply strict access controls to prevent unauthorized lateral movement.

References

(1) CrowdStrike. 'Unveiling LIMINAL PANDA'.
Available at: https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

(2) CrowdStrike. 'An Analysis of LightBasin Telecommunications Attacks'.
Available at: https://dev.crowdstrike.com/en-us/blog/an-analysis-of-lightbasin-telecommunications-attacks/

About SecurityGen

SecurityGen is a global company focused on telecom cyber security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

Email: **contact@secgen.com**
Website: **www.secgen.com**
/company/securitygen/

UK | Italy | Czech Republic | Brazil | Mexico | India | Malaysia | UAE | Egypt | Lebanon