ADVISORY FOR ICM SECTORS

Liminal Panda leverage telecom-specific protocols for espionage operations

Original report published on: 19 November 2024[1]

Executive Summary

Researchers at CrowdStrike published a report on LIMINAL PANDA, a China-nexus APT group targeting the global telecommunication sector since at least 2020. The group demonstrates advanced capabilities in exploiting telecom systems, employing custom tools like PingPong, CordScan, and SIGTRANslator, alongside publicly available proxy tools, to achieve covert access, lateral movement, and data exfiltration. The group's activities focus on gathering sensitive subscriber metadata and leveraging trusted relationships between telecom providers to propagate intrusions. Tied to signals intelligence (SIGINT) collection, LIMINAL PANDA uses telecom-specific protocols (e.g. GSM and GTP) for reconnaissance and command and control (C2) operations.

Background

LIMINAL PANDA is a sophisticated APT group leveraging advanced capabilities to infiltrate telecommunication networks. The group often gains initial access by exploiting external DNS (eDNS) servers of other compromised telecoms' GPRS networks to connect directly to additional victim's eDNS servers via SSH. They frequently conduct password dictionary attacks targeting the root user account of these servers. Once access is established, LIMINAL PANDA moves laterally across interconnected telecom networks by exploiting trust relationships and gaps in security configurations. To facilitate this lateral movement, the group employs tools such as ProxyChains, Microsocks Proxy, and Fast Reverse Proxy. Their reconnaissance activities include the use of CordScan, a tool capable of scanning via TCP and ICMP as well as telecom-specific protocols like GTP and SCTP. CordScan can also perform Packet Data Protocol (PDP) context scans against Serving GPRS Support Nodes (SGSN), enabling the extraction of subscriber metadata and International Mobile Subscriber Identity (IMSI) numbers.

LIMINAL PANDA employs several custom malware families to maintain access and execute their objectives. Notable examples include PingPong, a Linux backdoor that uses ICMP to listen for specific secret value within ICMP packets, allowing it to establish reverse shell connections stealthily. The group also uses SIGTRANslator, a custom tool designed to proxy telecommunication-specific network protocols and monitor retransmitted sensitive metadata, such as phone numbers and call records, obfuscating communications with an XOR key. To maintain persistence, LIMINAL PANDA deploys tools like TinyShell, a lightweight backdoor, alongside modified versions of exploits like BlueKeep (CVE-2019-0708) for lateral movement in Windows-based systems. Furthermore, they were observed to have added iptables rules to the eDNS servers, ensuring that other compromised telecommunications servers maintained SSH access to the host, demonstrating their emphasis on redundancy and long-term access.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Deploy endpoint detection and response (EDR) across the network environment, including servers considered inaccessible from the public Internet.
- Implement complex password strategies (avoiding default or generic options) for SSH authentication and enable multi-factor authentication.
- Log SSH connections between internal servers and monitor them for anomalous activity.
- Verify iptables rules implemented on servers, checking for the presence of abnormal entries that enable inbound access from unknown external IP addresses.
- Monitor `sbin` directory for modification of binaries such as `iptables` on critical systems.

MITRE ATT&CK Tactics and Techniques

Tactics	**Technique ID**	**Technique Name**
Reconnaissance	T1589	Gather Victim Identity Information
	T1595	Active Scanning
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server
	T1584.004	Compromise Infrastructure: Server
	T1587.001	Develop Capabilities: Malware
	T1588.002	Obtain Capabilities: Tool
Initial Access	T1078	Valid Accounts
	T1199	Trusted Relationship
Persistence	T1133	External Remote Services
Defense Evasion	T1564	Hide Artifacts
	T1574	Hijack Execution Flow
Lateral Movement	T1021.004	Remote Services: SSH
Collection	T1213	Data from Information Repositories
Command and Control	T1090	Proxy
Exfiltration	T1048	Exfiltration Over Alternative Protocol

References

1. **^** “Unveiling LIMINAL PANDA – Threats to Telecom Sector”