OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

China-Linked APT CL-STA-0969 Targets Southeast Asian Telecoms with Custom Malware and Stealth Tactics

Informational TLP:CLEAR Alert ID : a98753b9 Aug 04, 2025, 06:33 PM

Key Highlights

A state-sponsored threat actor, CL-STA-0969—linked to the China-based group Liminal Panda—conducted a prolonged cyber espionage campaign against Southeast Asian telecommunications providers from February to November 2024. The group targeted critical infrastructure using a blend of custom malware, public tools, and exploits for known vulnerabilities, including CVE-2016-5195, CVE-2021-4034, and CVE-2021-3156. Their operations demonstrated deep knowledge of telecom protocols and a strong emphasis on stealth and persistence.

Recent Activity

CL-STA-0969 gained initial access through SSH brute-force attacks, leveraging a well-tuned account dictionary list that included built-in accounts specific to telecommunications equipment. The group established long-term access and attempted to collect mobile device location data using tools like Cordscan. Although no confirmed data exfiltration was observed, the attackers set up resilient remote access likely for future espionage operations.

Spread and Exploitation

The group exploited telecom-specific protocols such as SSH, ICMP, DNS, and GTP for covert command-and-control (C2) operations. They used a combination of custom tools—AuthDoor, GTPDoor, ChronosRAT, and NoDepDNS—and public utilities like Microsocks, FRP, FScan, and Responder. To maintain stealth, CL-STA-0969 employed advanced

OPSEC techniques including disguising process names, clearing logs, disabling SELinux, and routing traffic through compromised telecom nodes.

Malware Behavior

CL-STA-0969 deployed a suite of specialized malware tailored for telecom environments:

1. **AuthDoor**: A PAM backdoor that captures credentials, supports hardcoded access, and executes files from a specific directory for persistence.
2. **Cordscan**: Scans telecom networks to extract IMSI and operator data by crafting GTP packets, logging results in `.pcap` files.
3. **GTPDoor**: A Linux implant using GTP-C signaling over UDP port 2123 to tunnel C2 traffic, supporting beaconing and remote code execution.
4. **EchoBackdoor**: A passive ICMP-based backdoor that executes encrypted commands received via echo request packets.
5. **SGSN Emulator**: Uses the OsmoGGSN project to emulate SGSN nodes, creating tunnels to mobile operators and setting up a SOCKS proxy for data exfiltration.
6. **ChronosRAT**: A modular Linux RAT with AES-encrypted TCP C2, dynamic RSA key updates, and modules for remote shell, keylogging, screenshots, and SOCKS proxy.
7. **NoDepDNS**: A Go-based backdoor using DNS tunneling over port 53, decoding XOR-encrypted commands embedded in DNS response IPs.

Mitigation

Organizations should implement the following measures to mitigate threats from CL-STA-0969:

1. Enforce strong authentication policies and monitor for brute-force attempts, especially on SSH services.
2. Patch known vulnerabilities such as CVE-2016-5195, CVE-2021-4034, and CVE-2021-3156.
3. Monitor for unusual DNS, ICMP, and GTP traffic patterns indicative of covert C2 channels.
4. Audit PAM modules and SELinux configurations for unauthorized changes.
5. Deploy endpoint detection and response (EDR) tools capable of identifying stealthy malware and backdoors.

Reference

securityaffairs

Tags

NoDepDNS, AuthDoor, ChronosRAT, Telecom Protocols, PAM Backdoor, GTPDoor, CL-STA-0969, Telecom Infrastructure, CordScan, LIMINAL PANDA, DNS Tunneling, Cyber Espionage, SSH brute force, Unit 42, cybersecurity, Palo Alto Networks, Southeast Asia

---

distributed without restriction.