## Pakistan Telecom Authority Headquarters, Islamabad

**PTA Cyber Security Advisory No. 239** **05-03-2024**

**Name:** GTPDOOR Linux Malware Targets Telecoms via GPRS Roaming Networks

**Threat Classification:** Linux Malware / Network Threat

**Affected Software / Services:**

- Telecom Networks, Linux Systems in GPRS Roaming Exchanges (GRX)

**Summary:**

GTPDOOR, a newly discovered Linux malware, specifically targets telecom networks, particularly those adjacent to GPRS roaming exchanges (GRX). What sets this malware apart is its utilization of the GPRS Tunneling Protocol (GTP) for command-and-control (C2) communications. GPRS roaming enables users to access GPRS services beyond their home mobile network through GRX, which transports roaming traffic between visited and home Public Land Mobile Networks (PLMN).

Upon execution, GTPDOOR undergoes process-name stomping, disguising itself as '[syslog],' and opens a raw socket for receiving UDP messages via network interfaces. This allows threat actors, with established persistence on the roaming exchange network, to send GTP-C Echo Request messages carrying malicious payloads. These messages serve as a covert conduit for issuing commands to compromised hosts and receiving results.

| | |
|---|---|
| **Severity** | **High** |
| **Attack Vector** | GTP Exploitation |

**Recommendations:**

- Implement robust network monitoring to detect unusual GTP-C Echo Request messages.
- Regularly update and patch Linux systems in GPRS roaming exchanges to mitigate vulnerabilities.
- Employ intrusion detection and prevention systems capable of identifying GTPDOOR-related activities.
- Conduct security awareness training to educate telecom network personnel about potential threats and phishing attempts.
- Utilize firewalls and access controls to restrict external access to critical network components.
- Follow GSMA standards for enhanced security measures.
- Collaborate with relevant cybersecurity agencies and share threat intelligence to enhance collective defense against threats like GTPDOOR.
- Monitor network traffic for any unusual TCP packets, especially those targeting specific port numbers.
- Consider implementing network segmentation to isolate critical components from potentially compromised hosts.
- In case of any incident, please report to this office, through PTA CERT Portal and email.