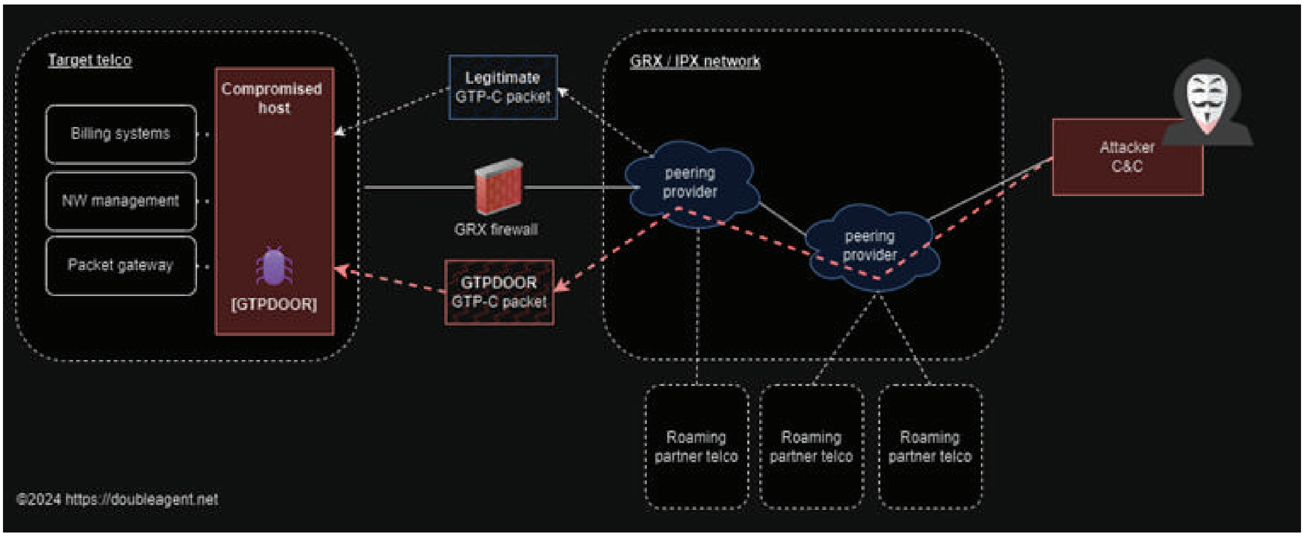
SecurityGen
Telecom Security. Transcending Generations.

GTPDOOR – The Tactic, the Technique, and the Protection

In the cybersecurity domain, new threats like **GTPDOOR,** a sophisticated Linux backdoor uncovered by security researcher HaxRob, pose substantial risks to digital infrastructure, especially in the telecommunications sector. GTPDOOR revolves around its ability to exploit the **GPRS Roaming exchange (GRX).** The GRX acts as a pivotal hub for interconnecting network operators, streamlining data roaming for subscribers and thus becoming a prime target for unauthorized access by malicious actors.

The Anatomy of Attack

It leverages the GTP-C protocol as a conduit for communication, establishing a covert channel between the attacker's **command and control (C&C) server** and the pre-installed software implant via the GRX network.
This reliance on GTP-C protocol allows GTPDOOR to fly under the radar, bypassing traditional security measures such as firewalls. By embedding itself within routine network traffic, GTPDOOR maintains persistent, undetected access to the compromised network components, enabling threat actor to have persistence in mobile operator in highly stealth mode.



©2024 https://doubleagent.net

The Technique

The attackers cleverly use **GTP Echo requests** to send commands. These requests are like **ICMP Echo (Ping)** but work in a different way in the GTP layer of the network. Unlike ICMP pings, GTP Echo requests can't be easily stopped because they're crucial for keeping connections alive between different parts of the GTP network.

If a GTP Echo request doesn't reach its destination, it forces a reset of all connections between peering nodes. These GTP Echo requests are sent every **0.5 to 3 minutes** to make sure everything stays connected. Furthermore, these are often overlooked in monitoring processes, because they are seen as unimportant background noise in network traffic.

Exploiting this oversight, GTPDOOR embeds additional instructions within these requests, evading detection while maintaining covert communication with the compromised infrastructure.

The Implications and the Call for Action

The discovery of GTPDOOR sheds light on the evolving threat landscape within the telecommunications sector. Incidents like the LightBasin attack and the GTPDOOR, underscore the vulnerabilities within GRX network and how these are exploited by malefactors, who have developed deep understanding of the telecom infrastructure. **The ability of GTPDOOR to bypass traditional security mechanisms (firewalls)and maintain unauthorized access poses significant risks to both operational integrity and subscriber privacy within the telecommunications ecosystem.**
From interception and manipulation of data to disruption of service and financial fraud, the potential impacts of GTPDOOR are far-reaching and multifaceted. Moreover, the exploitation of the GTP-C protocol highlights a critical vulnerability within the telecom sector, necessitating urgent attention and proactive measures to mitigate the risk posed.

In the short-terms following measures can be deployed :

- **Mitigating the Threat:** Addressing the threat posed by GTPDOOR requires a concerted effort encompassing proactive detection, and collaborative initiatives within the telecommunications community. Key strategies for mitigating the risk of GTPDOOR in the short-term includes:

- **Enhanced Monitoring:** Implementing robust intrusion detection systems (IDS) and monitoring solutions to pinpoint malicious transmissions indicative of GTPDOOR activity.

- **Thorough Investigation:** Conducting thorough examinations of software binaries, open sockets, and system processes to identify and isolate compromised nodes.

- **Indicators of Compromise (IOC):** Identifying specific indicators such as the presence of mutex /var/run/daemon.pid; unauthorized configuration files **system.conf** ; disguised processes that do not follow the typical kernel thread pattern, as indicated by an atypical parent process ID (PPID).

- **In the event** that any of these indicators are found, isolate the compromised node immediately and take the necessary steps to eradicate the malware.

- **Continuous Vigilance:** Continuously monitoring network traffic for any anomalous behavior or suspicious activity that may signal a compromise.

Long-term Recommendations:

To protect telecommunications infrastructure from GTPDOOR and similar threats in the long run, a strategy that includes improved detection capabilities, strict security protocols, and constant attention is essential.

- Implementing a strong security monitoring for GTP across all network nodes to ensure thorough monitoring for suspicious activities.

- Regularly updating and fine-tuning detection signatures and rules with the latest threat intelligence to match the changing tactics of malware.

- Carrying out regular security checks on network infrastructure to find and fix possible vulnerabilities that attackers could exploit.

- Providing continuous training for cybersecurity teams on the newest threat vectors and mitigation techniques, highlighting the need for quick action when warning signs appear.

- Increasing cooperation with other operators and security organizations to exchange intelligence and best practices for fighting against cyber threats targeting telecommunications.

- Adhering to **GSMA guidelines, including the FS.31 GSMA Baseline Security Controls and IR.77** Inter-Operator IP Backbone Security Requirements, for Service Providers and Inter operator IP backbone Providers. These guidelines set the foundation for securing telecommunications infrastructure and should be incorporated into the security strategy.

For a detailed discussion and deep dive with our telecom expert:
contact@secgen.com

Reference:
https://doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR