ADVISORY FOR ICM SECTORS

Compromised GRX Networks Delivers GTPDOOR Linux Malware

Original report published on: Feb 27, 2024[1]
Updated on: Mar 17, 2024

Executive Summary

Security researcher “HaxRob” discovered a new Linux-based malware named “GTPDOOR”. The threat actor is believed to target systems adjacent to the GRX (GPRS Roaming eXchange Network), such as Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), and Packet Data Network Gateway (P-GW). These components are crucial for roaming and data services that can provide direct access to the core of telecommunications networks.

Background

The GRX is a component of mobile telecommunications that is responsible for data roaming services across different geographical areas and networks. While SGSN, GGSN, and P-GW (for 4G LTE) are components within a mobile operator’s network infrastructure, each serves different roles in mobile communications.

The SGSN, GGSN and P-GW networks are exposed to the public for partner roaming operators and to facilitate routing needs, interoperability, and network troubleshooting. Although these publicly routable IP addresses are exposed, they will typically be assigned dynamically but the researcher believed they would still be targeted for gaining initial access into a mobile operator’s network.

The researcher explained that GTPDoor is likely a tool, belonging to the ‘LightBasin’ threat group (UNC1945), that is deployed for intelligence-collection operations targeting telecommunications company globally. The threat actor can exploit this malware to gain access to a carrier’s core network, facilitating the ability to steal sensitive data or disrupt communication services. The malware could change its process name to mimic legitimate system processes.

Due to the complexity of the attack vector execution, the roaming partner environment, or mobile carrier network must be first compromised as a pre-requisite to deploy and operationalise into the environment.

Detection and Mitigation

IMDA recommends organisations in the infcomm and media sectors to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE FiGHT (Fifth-Generation (5G) Hierarchy of Threats) techniques identified in this advisory:

- Using the YARA rule (refer to Annex) provided by the Security Researcher (“HaxRob”) to detect and prevent presence of GTPDOOR via security solutions such as Intrusion Detection/Prevention Systems (“ID/PS”) and Endpoint Detection and Response (“EDR”).
- Utilise network traffic monitoring tools to identify unusual activity, particularly communication consists of GTP-U packets.
- Monitor for unusual raw socket activities, unexpected process names, and specific malware indicators such as duplicate syslog processes not typical for your system.
- Implement GTP capable firewalls in compliance with GSMA security guidelines[2], to detect and deny malicious packets/connections. Probe TCP packets with RST/ACK flag set could be dropped on the GRX firewall.

The table below describe the Tactics, Techniques, and Procedures (“TTPs”) of GTPDOOR.

Notable MITRE FiGHT Techniques

Tactic	Technique	ID
Initial Access	Protocol Tunneling	FGT1572[3]
Discovery	Discover TEID	FGT5031[4]
Defence Evasion	Network Boundary Bridging: GTP-U Abuse	FGT1599.505[5]
Collection, Credential Access	Adversary-in-the-Middle: Roaming and Interconnection	FGT1557.502[6]

Annex

```
rule Linux_Malware_GTPDOOR_v1v2
{
        meta:
                description = "Detects GTPDOOR"
                author = "@haxrob"
                data = "28/02/2024"
                reference =
"https://doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-
TELCO-BACKDOOR"
                hash1 =
"827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161"
                hash2 =
"5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4"
        strings:
```

```
        $s1 = "excute result is" ascii fullword
        $s2 = "idkey not correct" ascii fullword
        $s3 = "send ret message" ascii fullword
    condition:
        uint16(0) == 0x457f and
        2 of them and
        filesize < 20KB
}
```

References

1. ^ "GTPDOOR – A novel backdoor tailored for covert access over the roaming exchange"
2. ^ "GSMA Baseline Security Controls"
3. ^ "MITRE FiGHT Technique (FGT1572) - Protocol Tunneling"
4. ^ "MITRE FiGHT Technique (FGT5031) - Discover TEID"
5. ^ "MITRE FiGHT Technique (FGT1599.505) - Network Boundary Bridging: GTP-U Abuse"
6. ^ "MITRE FiGHT Technique (FGT1557.502) - Adversary-in-the-Middle: Roaming and Interconnection"