SecurityGen
Telecom Security. Transcending Generations.

# LightBasin: A Synchronised, Sophisticated APT attack across a cluster of MNOs

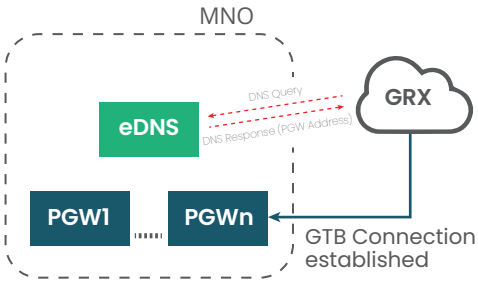
This week has brought to light, yet another stealth attack focused on the Telecom sector. This time it is a notorious hacking group - the LightBasin. As per a detailed investigation report by cybersecurity firm CrowdStrike this group has been infiltrating telecommunications companies worldwide in a campaign targeted at intelligence gathering and cyber espionage.

Active since 2016, this group deployed advanced persistent threat (APT) techniques to gain access and covertly monitor telecommunications networks around the world. This group of sophisticated threat actors targeted telcos by establishing implants across Linux and Solaris systems, which run a critical infrastructure for the sector. They sagaciously used custom tools and "in-depth knowledge" of telecommunication network architecture to compromise network and harvest data.

## Initial attack vector & tools: to breach and gain access

As per the industry report, LightBasin activity was detected in a recent CrowdStrike Services investigation exercise. The adversaries had used a combination of techniques to gain access and compromise telecom data. Ranging from simple methods like logging into systems using the standard credentials of equipment vendors to more complex external DNS compromises were used.

**Example of eDNS usage on 4G Roaming**

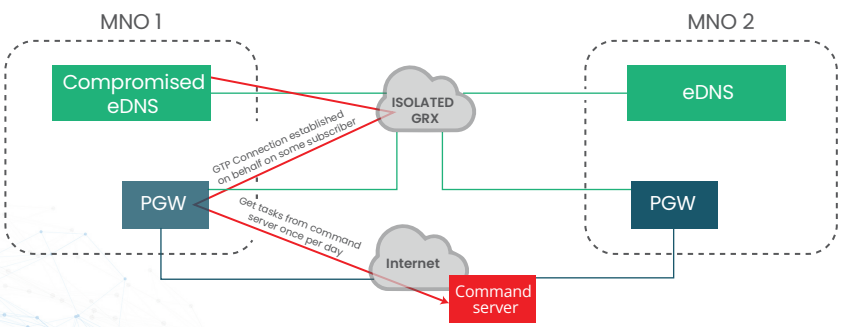



External DNS, or eDNS for short, are crucia to the roaming service and since that must be exposed to the roaming interfaces (GRX).

The hackers got initial network access via the DNS servers, which are part of the GPRS (General Packet Radio Service) network. The attackers used very weak and default passwords as part of the initial compromise. Then via compromised external DNS servers of a telco, the hackers covertly connected to other compromised telcos through their General Packet Radio Service (GPRS) networks. Upon establishing their malware on a system – the hackers concealed their traffic within GPRS connections via SSH. This technique helped the group operate stealthily and spread laterally without being detected by the security monitoring tools.

**THE IDEA OF ATTACK STEP 1**

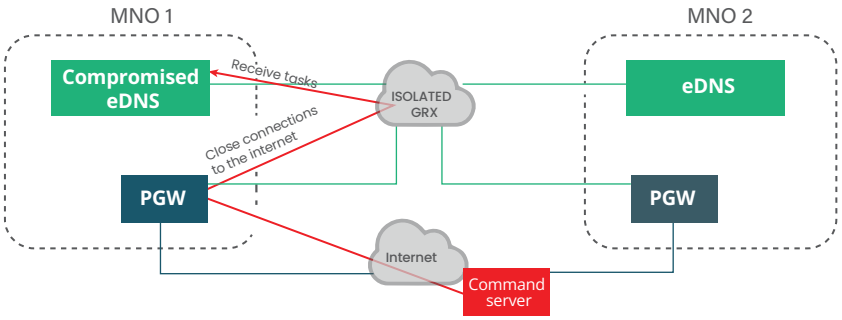
**Connect to the internet via GTP**



Attacker get access to some eDNS server in isolated GRX network. Deploys implant with backdoor functionality. This backdoor connects to the internet on behalf of mobile subscriber using GTP protocol via PGW, then connects to command server and set up reverse shell for 30 min per day.

### THE IDEA OF ATTACK STEP 2

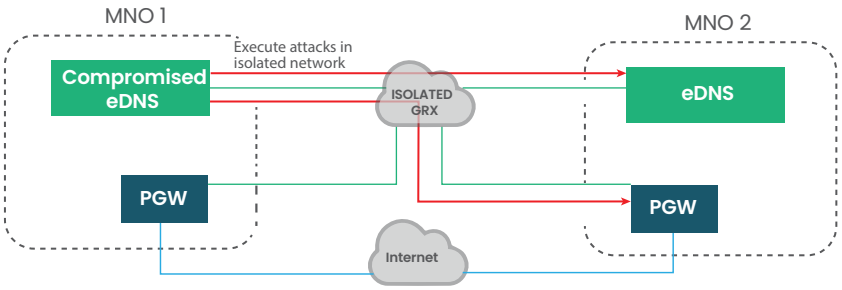
Get tasks, download malicious software, etc




Using this time window, malefactor can upload additional malic ious software and set up schedule for attacks.

### THE IDEA OF ATTACK STEP 3

Execute attack in isolated telecom network - GRX




Compromised eDNS can attack any node in GRX network, even while not being connected to the internet

## Security: A crucial enabler for telecom operations

A few days back, Symantec had reported a previously unseen advanced persistent threat (APT) group dubbed "Harvester," which was linked to an information-stealing campaign aimed at telecommunications, government, and information technology sectors within South Asia. Here the hackers which were active since June 2021 had used a custom implant called "Graphon" And now, the LightBasin attack. These series of compromises and stealth attacks demonstrate how the telecom sector has become a preferred target of malicious actors. In the coming times, with the adoption of 5G technologies and the ensuing complex and interconnected ecosystems MNOs will become even more vulnerable to security breaches. A Security-by-design framework needs to be established to protect the core network and the connected systems of MNOs.

## Security practices to protect the MNO environment

1. Implement Host/Function security (because not using default password is a fundamental security requirement)– use firm password policy

2. Protect GRX network using edge FW and setting up adequate rules:

• No other protocols than required (GTP, DNS) should be allowed in any direction

• DNS servers shouldn't be a source of GTP data

• IP Whitelisting would be also recommended

3. Make an inventory of equipment accessible from the GRX network. Sometimes some interfaces and even entire network segments are accessible from the GRX network, which shouldn't be there

4. With inventory in place, make sure those assets are on the vulnerability management program, have change control and routine integrity check procedures and, if available, externalize management interventions to a SIEM

.

5. Implement GTP IDS (to have full visibility of your network and prevent attacks through the GRX layer)

6. Consider GRX as a border, rather than a friendly interface between MNOs, and proceed with securing also SS7 and Diameter

SecurityGen provides a set of Security Assessments to assure your network is protected from GRX attacks. These security services range from Interconnection Security to the NFVi that hosts most of interconnection services nowadays. We also provide Next Generation Firewalls and IDS for Signaling protocols SS7, Diameter and GTP.