Anatomy of Telecom Malware

Speaker:
Akib Sayyed,
Founder Matrix Shell
Telco Sec Company & NESAS Lab

Agenda

- Why Care?
- Threat Landscape & Trends
- Malware Taxonomy
- Anatomy Deep Dive (Kill Chain)
- Case Studies
- Detection & Response
- Future Outlook
- Q&A

Why Care?

- High-value target: subscriber data, network control, espionage
- Revenue impact: fraud, service disruption, brand damage
- Regulatory penalties & compliance (3GPP, GDPR, NCCS)

Telecom Attack Surface

- Radio Access Network (RAN)
  - Connect User Devices to Telecom Core
- Why RAN Matters
  - Its Entry Point
  - Vulnerable to Jamming ,Fuzz, Abuse
  - Misconfig
  - Real World Threat : Firmware Mod for BTS
- Transport & Backhaul
  - Connect RAN and Core Via Fibre
- Why Transport & Backhaul Matters
  - Often Overlooked
  - Misconfig/Routing causes Lateral Movement
  - Malware
  - Real world Threat : Data Exfiltration

Telecom Attack Surface

Core Network (EPC/5GC)

- Its a Brain that handles mobility,sessions,billing info

- Why Core Network Matters
  - Favorite Target for Malware
  - Subscriber Info Holders
  - Roaming Abuse
  - Billing Abuse
  - Real World Threat : Light Basin

- OSS/BSS & Management
  - Provisioning,Monitoring,Configurations

- Why OSS/BSS & Management Matters
  - Single Compromise can give serious trouble
  - Real World Threat : Malicious Package Deployment via Upgrade Scripts

Telecom Attack Surface

Supply Chain (SIM, devices, firmware)

- External Components that are used by Network and Subscribers

Why Supply Chain (SIM, devices, firmware) Matters

- SIM/USIM malware
- Malicious IOT Firmware
- Real World Threat : Unknowingly deploy backdoor-ed code device management firmware

Threat Landscape 2022–2025

- LightBasin/UNC1945 – multi-MNO intrusion
  - “Global APT campaign targeting telecom core networks across 13+ MNOs.”
- Soft Cell – persistent APT in operator core
  - “APT threat actors maintained presence in operator core networks for month s.”
- Signaling exploits on SS7, Diameter, GTP
  - “Legacy and modern signaling protocols remain widely abused for location tr acking and session hijacking.”
- Rogue gNodeB implants & ORAN vulnerabilities
  - “Open RAN and 5G disaggregation introduce new attack surfaces.”

Trends Shaping Malware

- Virtualized & cloud-native 5G cores
  - “5G Core functions are now microservices running on cloud infrastructure.”
    - Traditional telecom security tools often don’t detect cloud-native threats.
- Open RAN components and xApps
  - “Open interfaces and 3rd-party RAN apps increase flexibility—also risk.”
    - This creates opportunities for subtle, low-level manipulation of user traffic.
- Post-Quantum Cryptography transition
  - “The upcoming PQC shift creates both opportunity—and temporary weakness.”
    - Hybrid implementations (PQ + classic) introduce complexity and compatibility gaps.
- AI-driven signaling analysis (both attacker & defender)
  - “AI is being used to both exploit and detect telecom anomalies.”
    - But attackers also use AI

Malware Taxonomy Overview

- Network-resident implants
  - Malware embedded in core network functions (e.g., MME, HSS, UPF).
    - Example :
      - Modified Packet Gateway Binary
- Signaling-plane malware
  - Exploits SS7, Diameter, or GTP to hijack sessions or impersonate users
    - Example :
      - LightBasin campaign used GTP tunneling
- Endpoint & RAN-focused malware
  - Targets user devices, SIMs, or rogue base stations (eNodeB/gNodeB).
    - Malicious eNodeB setup captured all IMSIs in vicinity + pushed spyware to specific devices
- Supply-chain backdoors
  - Malware embedded via third-party vendors, firmware, SIMs, or OSS software.
    - OSS upgrade package came with hidden shell access

Network-Resident Implants

- Core service (MME/AMF, HSS/UDM, PGW/UPF) implants
  - Malware is inserted into the logic of core functions
  - Malware on Host OS/Firewall/Transport Switches& Routers
- SIGTRAN/Diameter sniffers & injectors
  - Tools implanted to intercept or modify control-plane signaling inside the core
  - Signalling Router Logs Stealers
- Manipulation of subscriber databases
  - Direct edits to HSS/UDM/HLR entries for impersonation, cloning, or fraud.
  - DB Edits/Steal

Signaling-Plane Malware

- SS7 route hijacking & location tracking
  - Exploits MAP messages to track, intercept, or manipulate subscribers remotely.
- Diameter edge proxy exploitation
  - Attacks on unfiltered Diameter peers to hijack sessions or manipulate charging rules.
- GTP tunnel abuse for data exfiltration
  - Malicious use of GTP-C/U tunnels to reroute or siphon subscriber traffic.
  - GTPDoor

Endpoint & RAN Malware

- Rogue eNodeB/gNodeB firmware
  - Malicious or modified firmware in base stations used for interception or protocol abuse.
  - Misuse of Local Breakout
- IMSI catchers & over-the-air SIM updates
  - Devices forced to reveal identity or accept malicious SIM toolkit commands over the air.
  - SK Telecom
- Mobile OS trojans targeting baseband APIs
  - Malware on smartphones abusing low-level modem interfaces for covert control.
    - Amat Cama (The Baseband Hacking : A walk with Shannon)

Supply-Chain Backdoors

- Compromised SIM/USIM applets
  - SIMs can carry malicious Java applets—triggered silently via OTA or STK
  - S@TBrowser hacks
  - Possible outcome of Latest Telecom hack related to SIMCard
- Malicious OAM/OSS software updates
  - Backdoored/Weak management scripts for software updates
- Third-party vendor libraries in VNFs
  - VNFs often depend on opaque libraries or containers—any one of which may be compromised.
  - Open5GS has over 12 critical CVEs affecting versions up to v2.7.3,

Telecom Kill Chain

[Reconnaissance]
|
[Initial Access]
|
[Privilege & Signaling Abuse]
|
[Payload Execution]
|
[Persistence & Evasion]

Telecom Kill Chain

Reconnaissance

TTPs: IMSI/IMEI lookups, SS7/HLR probing, network fingerprinting

Goal: Identify subscriber targets and weak network entry points.

Initial Access

TTPs: Compromised VPN, test node abuse, unsecured Diameter peer

Goal: Establish control over a signaling or management plane entry point.

Privilege & Signaling Abuse

TTPs: GTP tunnel injection, Diameter spoofing, PCRF rule tampering

Goal: Escalate access, impersonate subscribers, manipulate traffic.

Payload Execution

TTPs: Call/SMS interception, CDR theft, data exfiltration

Goal: Achieve espionage, fraud, or disruption objectives.

Persistence & Evasion

TTPs: VNF implants, stealth signaling, tampered logs

Goal: Maintain long-term access and evade detection.

Case Study: LightBasin

- Targeted multiple MNOs via signaling links
  - Exploited SS7/Diameter trust to move laterally between telecom networks.
- Installed custom GTP tunneling tools
  - Deployed malware to control and exfiltrate user-plane traffic over GTP.
- Stole roaming subscriber data over months
  - Exfiltrated CDRs, IMSI logs, and subscriber profiles undetected for extended periods.

Case Study: PGW Implant

- Modified CXXXX Packet Gateway binary
  - Implant was injected into core PGW binary to gain direct control over data-plane flows.
- Survived firmware upgrades via init script
  - Persistence achieved using a tampered init script reloading the implant post-upgrade.
- Enabled covert call redirection
  - Allowed selective hijacking of data or voice sessions without affecting billing or logs.

Detection Pipeline

- Collect core & signaling telemetry (SS7, Diameter, GTP)
  - Ensure telemetry coverage across control and user planes for full network visibility.
- Anomaly detection on KPIs & traffic baselines
  - Use behavioral baselining to spot signaling abuse and malware implants.
- Decoy subscribers & canary IMSIs
  - Deploy deception techniques to detect unauthorized signaling or data access.

Response Playbook

- Isolate compromised network functions
  - Quarantine affected VNFs, routers, or signaling peers to stop malware propagation.
- Purge unauthorized subscriber profiles
  - Remove rogue IMSIs, cloned SIMs, or modified subscriber entitlements.
- Coordinate with LEAs & CERTs
  - Engage regulators, CERTs, and law enforcement early to contain legal and reputational impact.
- Post-incident red-team validation
  - Use internal or external red teams to validate containment and resilience.

Defense in Depth

- 3GPP TS 33-series security controls
  - Standards-based security architecture covering core, access, and signaling layers.
- NESAS & ISO/IEC 17025 accredited testing
  - Independent, repeatable lab validation of network function and protocol security.
- Regulatory Steps
  - Define Testing Specs
    - Define Mandatory Testing Specs
    - Accredited Testing Lab for Testing Telco Security
    - Need FCC, GSMA, ENISA and regulatory to take step
- Continuous security assessments & fuzzing
  - Ongoing validation of telecom infrastructure against evolving threats

Future Threats & Research

- Network slicing lateral movement
  - Attackers may pivot across slices if isolation is weak or misconfigured.
- ORAN xApp supply-chain risks
  - 3rd-party xApps introduce code execution and logic manipulation risks into the RAN.
- Quantum-safe signaling protocols
  - Need for PQC adoption in SIM authentication, OTA updates, and interconnects.
- AI-generated social engineering
  - Deepfake voice, SMS phishing, and impersonation attacks against operators and subscribers.

Key Takeaways

- Telecom networks are high-value targets
  - Malware campaigns are increasingly aimed at telecom infrastructure for espionage, fraud, and surveillance—not just disruption.
- Malware spans signaling, core, and RAN
  - Malware isn’t isolated to endpoints or internet-facing systems—it can live inside PGWs, SIM cards, OSS scripts, and even signaling messages.
- Traditional security tools fall short in telecom
  - Generic EDRs or firewalls often miss GTP tunnels, SS7/Diameter abuse, or signaling-based privilege escalation.
- Defense requires layered controls & red-teaming
  - Full signaling telemetry (SS7, Diameter, GTP),
  - Canary subscribers and anomaly models,
  - Implementation of 3GPP TS 33-series, NCCS, and continuous fuzz testing.
- Stay ahead with continuous research & testing
  - Slice-level lateral movement in 5G,
  - xApp supply chain abuse in ORAN,
  - Quantum-safe signaling pitfalls, and
  - AI-driven social engineering.

Q&A

- Thank you!
- Contact: akibsayyed@matrixshell.com
- LinkedIn: https://www.linkedin.com/in/akibsayyed/