

THREAT HUNTING IN THE TELECOMMUNICATION SECTOR USING MITRE ATT&CK

Project Overview

This project focuses on proactive threat hunting within the telecommunication industry, leveraging the MITRE ATT&CK framework to identify and analyze Advanced Persistent Threat (APT) groups

targeting the sector.

The objective was to:

- Identify telecommunication -targeted APTs.
- Analyze their Tactics, Techniques, and Procedures (TTPs)
- Visualize the threat landscape using MITRE Navigator.
- Compare APTs to find common attack vectors.

Objectives

1. Understand the MITRE ATT&CK framework and its application to real-world threat

hunting.

2. Research APTs targeting the healthcare sector using SOCRadar Labs.

3. Map identified APTs to relevant TTPs in MITRE ATT&CK Navigator.

4. Perform a comparative analysis to highlight overlapping attack patterns.

Tools & Resources

- SOCRadar Labs – For retrieving healthcare -specific APT threat intelligence.
- MITRE ATT&CK Navigator – For mapping APT TTPs.
- MITRE ATT&CK Framework – For structured adversary behavior taxonomy.

Project Steps

1. Understanding the MITRE ATT&CK Framework

- Studied the MITRE ATT&CK framework structure:
 - Tactics – The *why* of an attack (e.g., Initial Access, Persistence, Defense Evasion).
 - Techniques – The *how* of an attack (e.g., phishing, credential dumping).
 - Procedures – Real -world implementations of techniques.

2. Research APTs Peculiar to the Sector

- Used SOCRadar Labs to identify APT groups targeting Telecommunication. Found the following:
 - APT29 - [APT29](#) is threat group that has been attributed to Russia's Foreign Intelligence Service. They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks.
 - APT31- APT31, also known as Zirconium, is a Chinese state-sponsored threat actor known for conducting cyber espionage activities targeting various sectors globally including the telecommunication sector
 - AjaxTM- Also known as the Ajax Security Team, is an Iranian state-aligned threat group active since at least 2010. The group initially engaged in website defacement but transitioned into cyber

espionage and credential theft campaigns around 2013–2014, focusing on both internal dissidents and foreign defense and telecom targets

3. Highlight of the TTPs

- For each APT, identified their key TTPs from MITRE:

- o Example (APT29):

- T1190 – Exploit Public Facing Application
- T1115 – Credentials from Password Stores
- T1087 – Account Discovery

4. Map APTs to TTPs using MITRE Navigator

- Created individual layers in MITRE Navigator for each APT.

Color -coded:

- Red
- Orange
- Green

5. Compare the APTs

- Imported all three APT layers into a combined Navigator view. Noted common techniques across multiple APTs, such as:

- o T1105 - Ingress tool transfer

- o T1665 - Hide Infrastructure

- o T1068- Exploitation for Privilege escalation

FINDINGS

- To gain initial access, they may exploit public facing application or use external remote services
- They may implement boot or logon initialization script to stay in the system
- They could steal password through web session cookie or even through application access token

To better understand each column of the phase of attack, I've briefly explained each column meanings for better understanding:

1. **Resource Development** - Attackers prepare tools, infrastructure, and accounts (e.g., buy domains, create malware, set up C2 servers, obtain exploits).
2. **Reconnaissance** - Attackers gather info about targets (open ports, employee emails, technologies used, public cloud resources) to plan an attack.
3. **Initial Access** – How the attacker first gets in (e.g. phishing, exploiting a public-facing app)
4. **Execution** – How malicious code is run (e.g. PowerShell, command line)
5. **Persistence** – How the attacker stays in the system (e.g. scheduled tasks, registry changes)
6. **Privilege Escalation** – How they gain more power/admin rights
7. **Defense Evasion** – How they avoid antivirus, logs, detection
8. **Credential Access** – How they steal passwords
9. **Discovery** – How they explore the network and systems

10. **Lateral Movement** – How they move to other computers
11. **Collection** – What data they gather
12. **Command & Control (C2)** – How they communicate with their server
13. **Exfiltration** – How data is stolen out
14. **Impact** – What damage they do (data deletion, ransomware, etc)