Threat Hunting in the Energy & Utilities Sector using MITRE ATT&CK

Project Overview

This project focuses on proactive threat hunting in the Energy and Utilities sector, using the MITRE ATT&CK framework to identify and analyze Advanced Persistent Threat (APT) groups targeting critical infrastructure.

The Objective was to:

- Identify healthcare-targeted APTs.
- Analyze their Tactics, Techniques, and Procedures (TTPs).
- Visualize the threat landscape using MITRE Navigator.
- Compare the APT groups to identify common attack vectors and overlapping patterns.
- Utilize SOCRadar Labs to gather threat intelligence on healthcare-focused APTs.

Tools & Resources

- **SOCRadar Labs** – For retrieving healthcare-specific APT threat intelligence.
- **MITRE ATT&CK Navigator** – Used to map and visualize TTPs.
- **MITRE ATT&CK Framework** – Provides the standardized taxonomy of attacker behaviors.
- **OSINT Research** – Used to validate and expand on APT reports from open sources.

Project Steps

1. Understanding the MITRE ATT&CK Framework.

Reviewed the structure of the framework:

- **Tactics:** The purpose behind attacker activities (e.g., Initial Access, Persistence, Impact).
- **Techniques:** The methods used to achieve each tactic (e.g., lateral movement, credential access).
- **Procedures:** Real-world attacker behavior implementing those techniques.

2. Research APTs Peculiar to the Sector

- Used SOCRadar Labs to identify APT groups targeting healthcare.

Found the following:

- **APT28** – Ukraine-related organizations by exploiting CVE-2022-38028, using living-off-the-land techniques, and gaining access through nearby Wi-Fi networks by pivoting through compromised neighboring systems.
- **APT29** – linked to Russia's Foreign Intelligence Service (SVR), has operated since at least 2008, targeting government networks, NATO countries, research institutes, and think tanks. They are also known for compromising the Democratic National Committee in 2015.
- **APT10 –** This is a threat group with members linked to China's Ministry of State Security (MSS), specifically the Tianjin State Security Bureau, and associated with the Huaying Haitai Science and Technology Development Company.
- **BITTER –** This is a suspected South Asian cyber espionage group that targets government, energy, and engineering organizations in Pakistan, China, Bangladesh, and Saudi Arabia.

3. **Highlight of the TTPs**
    - For each APT, identified their key TTPs from MITRE:

      Examples (APT29):

        - **T1548 -** Bypass User Account Control
        - **T1595** - Vulnerability Scanning
        - **T110** - Password Guessing

4. **Map APTs to TTPs using MITRE Navigator**
    - Created individual layers in MITRE Navigator for each APT.
    - **Color - Coded:**

      Red – APT28
      Orange – APT29
      Yellow – APT10
      Green – BITTER

5. **Compare the APTs**

   Imported all four APT layers into a combined Navigator view.

   Noted common techniques across multiple APTs, such as:

   T1586 – Compromising Accounts

   T1606– Forge Web Credentials

   T1059 – Command and Scripting Interpreter