Report on Cyber Threat Analysis

This report addresses the following components as per the rubric:

- **Malware Sample Analysis**
- **Phishing Template Creation**
- **APT Campaign Mapping to MITRE ATT&CK**

1. Malware Sample Analysis

The document includes an analysis of a malware sample using VirusTotal.

- **Platform Used:** VirusTotal

- **Sample Hash:** d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

- **Detection Results:** The document shows various activities and modifications the malware sample performed on a Windows system. This implies the sample was detected as malicious by VirusTotal's analysis.
- **Behavioral Indicators:** The analysis reveals several behavioral indicators:
  - Processes Terminated: The malware terminated processes like `DiagTrackRunner.exe`, `slui.exe`, `taskhost.exe`, `sc.exe`, `schtasks.exe`, and others.

  - Services Opened: It opened services like `VaultSvc` and `WSCSvc`.

  - Registry Keys Modified: The malware set and deleted various registry keys, indicating an attempt to modify system settings and potentially establish persistence.

  - Files Dropped: The malware dropped several files, including DLLs (`AudioCapture.dll`, `HTCTL32.DLL`, `KBDTAM99.DLL`) and configuration files.

  - Files Written/Deleted: The malware wrote and deleted files in the `C:\ProgramData\Microsoft\Windows\WER\` directory, likely related to Windows Error Reporting.

- **Potential Impact:** Based on the observed behavior, the potential impact of this malware includes:
  - System Instability: Terminating critical processes can lead to system instability.
  - Privilege Escalation: Modifying registry keys can be a technique for privilege escalation.
  - Data Theft: The dropped DLLs could be used for malicious activities like capturing audio or keystrokes, leading to data theft.
  - Persistence: Modifying registry settings helps the malware to persist across system reboots.

2. Phishing Template Creation

The document demonstrates the use of the Social Engineering Toolkit (SET) to create a phishing template.

- **Tool Used:** Social Engineering Toolkit (SET)

- **Platform:** Parrot OS/Kali Linux (The document shows Parrot OS terminal)

- **Attack Type:** Credential Harvester Attack

- **Template Cloning:** The tool was used to clone the website "http://www.google.com".

- **Functionality:** The Credential Harvester captures POST requests, meaning it is designed to steal login credentials from web forms.

- **Additional SET Capabilities:** The document also mentions other web attack vectors available in SET, including:
  - Java Applet Attack Method
  - Metasploit Browser Exploit Method
  - Tabnabbing Attack Method
  - Web Jacking Attack Method
  - Multi-Attack Web Method (combining multiple attacks)
  - HTA Attack Method (for PowerShell injection)

3. APT Campaign Mapping to MITRE ATT&CK

The document mentions the APT group "Earth Lusca" and its associated techniques. To map this to the MITRE ATT&CK framework, we need to research Earth Lusca and their tactics.

- **APT Group:** Earth Lusca (also known as TAG-22, Charcoal Typhoon, CHROMIUM, ControlX)

Based on external research (which the document allows), Earth Lusca is known for targeting government, education, and non-governmental organizations. Some of their tactics, mapped to MITRE ATT&CK, include:

- **Tactic: Initial Access**
  - Technique: Spearphishing (T1566) - Earth Lusca uses spearphishing to deliver malicious payloads or links.

- **Tactic: Execution**
  - Technique: Exploitation of Remote Services (T1021) - They exploit vulnerabilities in web servers and other services.
  - Technique: Scripting (T1064) - They use scripting languages to automate tasks and execute malicious code.
- **Tactic: Persistence**
  - Technique: Scheduled Tasks/Jobs (T1053) - They create scheduled tasks to maintain persistence.
- **Tactic: Command and Control**
  - Technique: Web Protocols (T1071) - They use web protocols (HTTP, HTTPS) for command and control.

Summary

The document provides a foundation for understanding cyber threats by demonstrating malware analysis, phishing template creation, and APT group identification. The malware analysis reveals potentially harmful behavior, the SET examples illustrate phishing techniques, and the Earth Lusca reference allows for mapping real-world threats to the MITRE ATT&CK framework.