Detecting and Analyzing the Zeus Banking Trojan

Objective

This project focuses on detecting and analyzing the Zeus Banking Trojan using various tools and techniques. The analysis includes malware simulation, network monitoring, memory analysis, and signature-based detection.

Prerequisites

- **Virtual Machine**: Install and set up a VM (e.g., VirtualBox or VMware) with an isolated network environment.
- **Operating System**: Ensure the VM uses an operating system compatible with the Zeus Trojan binary (e.g., Windows).
- **Tools Required**:
    - Suricata
    - Splunk
    - Volatility Framework
    - YARA
    - theZoo repository: Zeus Banking Trojan Binary

Note: Ensure strict isolation for the malware environment to avoid unintentional infections.

Steps to Implement

1. Simulate Malware Execution

- Set up a VM and download the Zeus Banking Trojan from theZoo repository.
- Execute the malware in a controlled environment.

2. Configure Suricata for Network Monitoring

- Install Suricata on the host machine or within the VM.
- Monitor network traffic using Suricata's default rules to detect common threats.
- Write custom Suricata rules for Zeus-specific patterns (e.g., Command and Control (C2) communication).
- Forward Suricata alerts to Splunk for centralized log analysis.

3. Integrate with Splunk

- Ingest logs from Suricata and the VM system logs into Splunk.
- Create correlation rules in Splunk to:
    - Detect abnormal outbound traffic.
    - Link network anomalies with system activities, such as file system changes or process creation.
- Build visual dashboards in Splunk to monitor malicious activities.

4. Analyze Memory with Volatility

- Capture a memory dump from the infected VM.
- Use Volatility Framework to:
    - Identify active and injected processes related to Zeus.
    - Analyze Zeus-specific network connections.

5. Detect Zeus with YARA Signatures

- Write custom YARA rules to detect Zeus-related patterns in binaries, configuration files, and memory dumps.
- Scan the infected system and memory dumps using YARA to identify Zeus artifacts.

Important Notes

- **Malware Safety**: Execute the Zeus Trojan only within a controlled and isolated environment. Ensure it does not affect the host system or other networked devices.
- **Legal Compliance**: Ensure compliance with all applicable laws and regulations regarding malware analysis and usage.

Detailed Setup Instructions for Tools

1. YARA Installation on Windows

Prerequisites:

- Ensure Python 3.x is installed on your system.

Installation Steps:

1. **Download YARA**:
    - Visit the YARA releases page and download the latest precompiled binary for Windows.
    - Alternatively, you can build YARA from source using the following commands.
2. **Install YARA Using Python (optional)**:

3. pip install yara-python
4. **Verify Installation**:
    - Open a Command Prompt and type:
    - yara --version
    - If installed correctly, it will display the YARA version.
5. **Create and Test Rules**:
    - Create a .yar file with your custom rules.
    - Run YARA against a file or directory:
    - yara <rule_file> <target_file_or_directory>

---

2. Volatility Installation on Windows

Prerequisites:

- Ensure Python 3.x is installed.
- Install necessary dependencies.

Installation Steps:

1. **Download Volatility**:
    - Visit the Volatility GitHub page and download the source code.
2. **Install Volatility**:
    - Open Command Prompt and navigate to the downloaded folder.
    - Install the required dependencies:
    - pip install -r requirements.txt
3. **Set Environment Variables (optional)**:
    - Add the path of the Volatility folder to your system's environment variables for easier access.
4. **Test Installation**:
    - Run the following command to verify:
    - python vol.py -h
5. **Analyze Memory Dumps**:
    - Capture a memory dump using tools like FTK Imager or DumpIt.
    - Analyze the dump:
    - python vol.py -f <memory_dump> --profile=<profile_name> <plugin>

---

3. Splunk Installation

Prerequisites:

- Minimum 8 GB RAM and 20 GB storage available.

Installation Steps:

1. **Download Splunk**:
    - Go to the Splunk Downloads page and download the free trial for Splunk Enterprise.
2. **Install Splunk**:
    - Run the downloaded installer and follow the on-screen instructions.
    - Set up an admin username and password during the installation.
3. **Start Splunk**:
    - Open the Splunk web interface by navigating to:
    - http://localhost:8000
    - Log in using your credentials.
4. **Ingest Data**:
    - Add Suricata logs and other logs to Splunk:
        - Go to **Settings > Add Data > Upload Files**.
        - Configure the data source and indexing.
5. **Create Dashboards**:
    - Use the data to create custom dashboards and correlation rules for monitoring malicious activities.

---

4. Suricata Installation

Prerequisites:

- Windows 10 or 11 (64-bit).
- WinPcap or npcap (network packet capture libraries).

Installation Steps:

1. **Download Suricata**:
    - Visit the Suricata Downloads page and download the Windows installer.
2. **Install Suricata**:
    - Run the installer and follow the prompts.
    - During installation, ensure you enable the option to install WinPcap/npcap.

3. **Configure Suricata**:
    - Navigate to the Suricata installation directory.
    - Edit the suricata.yaml configuration file to:
        - Specify the network interface to monitor.
        - Enable logging options (e.g., JSON logging for integration with Splunk).
4. **Start Suricata**:
    - Run Suricata in IDS mode using Command Prompt:
    - suricata -c suricata.yaml -i <network_interface>
5. **Write Custom Rules**:
    - Add Zeus-specific rules in the rules directory:
    - alert http any any -> any any (msg:"Zeus C2 traffic detected"; content:"zeus"; sid:100001;)
6. **Test Configuration**:
    - Run Suricata in test mode to validate the setup:
    - suricata -T -c suricata.yaml
