KYGnus

Loa - AMD

Android Malware Detection Tool

Loa - AMD is a cutting-edge Android malware detection tool designed to safeguard your device from harmful threats. Developed as part of the LoA Project (Linux on Android), KYGnus AMD offers a comprehensive suite of scanning engines and techniques, ensuring robust protection against various types of malware.

Overview of LoA Project

The LoA Project (Linux on Android) is an innovative initiative aimed at enhancing Android security by bringing the reliability and security of Linux to the Android ecosystem. This project leverages the strengths of Linux's security features and integrates them seamlessly with the Android platform.

The LoA Project addresses a crucial gap in Android security by providing a robust platform for detecting and mitigating malware threats. It aims to create a secure and trustworthy environment for Android users, ensuring their devices are protected from malicious software.

ClamAV Engine

KYGNUS AMD incorporates the widely recognized ClamAV engine, a powerful and efficient open-source antivirus solution. This engine plays a pivotal role in detecting and removing malware from your device.

ClamAV's extensive database of malware signatures and its constant updates ensure it can identify even the latest and most sophisticated malware threats. KYGNUS AMD leverages ClamAV's capabilities to provide comprehensive protection against known and emerging malware.

Abnormal File Detection

Beyond the power of ClamAV, KYGNUS AMD utilizes a sophisticated abnormal file detection mechanism. This layer of defense goes beyond signature-based detection and identifies suspicious files based on their behavior and characteristics.

The abnormal file detection system analyzes files for unusual patterns, potentially malicious code, and unauthorized access attempts. This approach helps KYGNUS AMD detect and neutralize even zero-day threats, which may not yet have a signature in traditional antivirus databases.

YARA Rule Scanning

KYGNUS AMD integrates YARA rule scanning, a powerful technique for detecting malware based on predefined patterns and characteristics. YARA rules, written in a specialized language, define specific criteria that identify malicious software.

YARA rules allow KYGNUS AMD to detect malware that may not be recognized by traditional signature-based methods. These rules can target specific types of malware, exploit techniques, or even suspicious code structures, providing an additional layer of protection.

Hash Database Checks

KYGNUS AMD leverages a comprehensive hash database to detect known malware based on their unique digital fingerprints. Each file has a unique hash value, like a digital ID, that can be used for identification.

KYGNUS AMD's hash database contains millions of known malware hashes. When a new file is scanned, its hash is compared against the database. If a match is found, KYGNUS AMD can immediately identify the file as malicious and take appropriate action, preventing it from infecting your device.

Androguard APK Analysis

KYGNUS AMD goes beyond traditional scanning techniques by incorporating advanced APK analysis using Androguard. This powerful tool provides a deep dive into the structure and behavior of Android applications (APK files).

Androguard analyzes the APK's code, permissions, and other metadata to identify potentially malicious activities. This analysis helps KYGNUS AMD detect malware that may be attempting to hide its true intentions or evade traditional antivirus solutions. It provides a comprehensive understanding of the application's behavior, allowing for more accurate and proactive threat detection.

Comprehensive Malware Protection

KYGNUS AMD offers a comprehensive solution for Android malware protection, combining multiple layers of defense to safeguard your device. The combination of ClamAV, abnormal file detection, YARA rules, hash database checks, and Androguard APK analysis provides a robust and multifaceted approach to malware detection and prevention.

This approach ensures that KYGNUS AMD can identify a wide range of malware threats, from traditional viruses and Trojans to more sophisticated, emerging threats. It provides a proactive and intelligent solution to keep your Android device safe and secure.

Installation

1. **Download the Script**

1 - First Install termux on Andriod Device From PlayStore or Fdroid

Note1 : First Install wget

Note2 : If you download and use this software from sanctioned countries, be sure to change your IP address before starting the installation process.

2 - Then Install Basic Tools

```
pkg update && pkg upgrade
```

```
pkg install wget -y
```

3 - Then Install Loa

```
wget https://kooshayeganeh.github.io/Files/loa.tar.gz && tar xvf loa.tar.gz && cd loa && ./install
```

Run the Script

Execute the script with the desired option:

./loa [OPTION]

Options

- `--help`: Show the help message.
- `--scan`: Perform a full scan using all available engines.
- `--clamav`: Scan using the ClamAV engine only.
- `--amd`: Perform AMD-specific scans (abnormal files, hash check, file signature check, APK analysis).
- `--yara`: Perform a scan using YARA rules only.
- `--update`: Update the system, including ClamAV database and installed packages.
- `--apk`: Scan APK files using Androguard.

Example Commands

- **Full Scan:** `./loa --scan`
- **ClamAV Scan:** `./loa --clamav`
- **AMD-specific Scans:** `./loa --amd`
- **YARA Scan:** `./loa --yara`
- **System Update:** `./loa --update`
- **APK Analysis:** ```sh ./loa

Ansible

to Automate Task Run

```
ansible-playbook loa_playbook.yml --extra-vars "task=update"
```

```
ansible-playbook loa_playbook.yml --extra-vars "task=clamav"
```

```
ansible-playbook loa_playbook.yml --extra-vars "task=all"
```

Scan Results

Scan results are stored in the file `scan_results.txt` located in the same directory as the script. A summary of the results is displayed after each scan.

Troubleshooting

- Ensure you have granted storage permissions to Termux.
- Make sure the required directories are set up properly.
- If you encounter issues with ClamAV database updates, try using a VPN if you're in a restricted region.

Resources

- https://www.virussamples.com/
- https://github.com/MalwareSamples/Android-Malware-Samples
- https://www.kaggle.com/datasets/shashwatwork/android-malware-dataset-for-machine-learning?resource=download
- https://www.unb.ca/cic/datasets/dns-2021.html
- https://www.malwarefox.com/android-virus-list/\
- https://www.researchgate.net/figure/List-of-Android-malware-families-detected-on-the-Google-Play-Store-23-113-114_tbl1_371543033?__cf_chl_tk=04E1P2x3JLP3zXqUhSLBs7Dp1Ws4KqYLtc3ABa7vjZc-1720886392-0.0.1.1-4842
  http://ahlashkari.com/Datasets-Android-Malware-Static-Analysis.asp