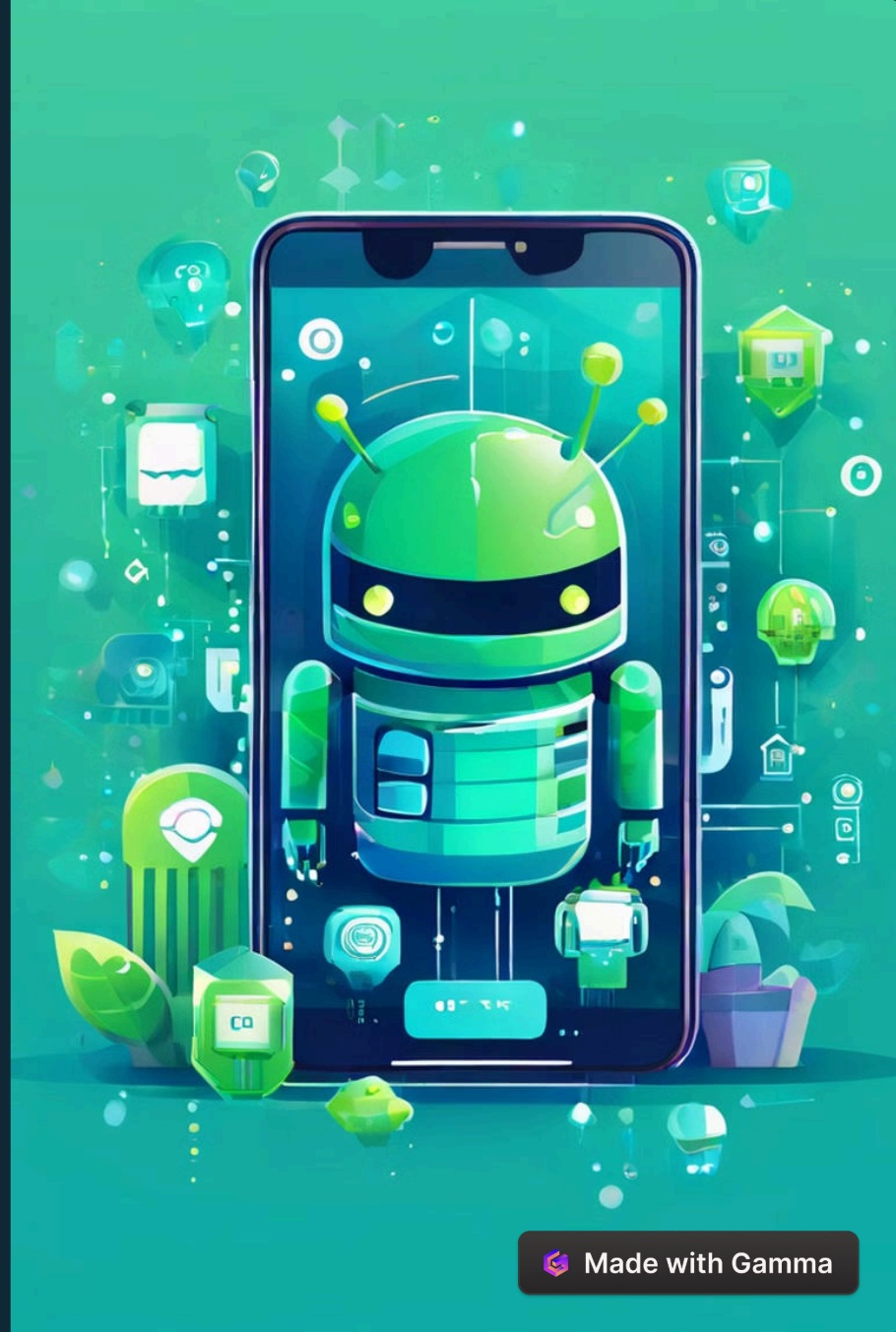
KYGNUS AMD

Android Malware Detection Tool

KYGnus AMD is a powerful tool for Android malware detection. It provides comprehensive scanning capabilities to ensure the security of your devices.

by koosha yeganeh



Overview of the LoA Project

1

Linux on Android

The LoA project aims to bring the power and flexibility of Linux to Android devices.

2

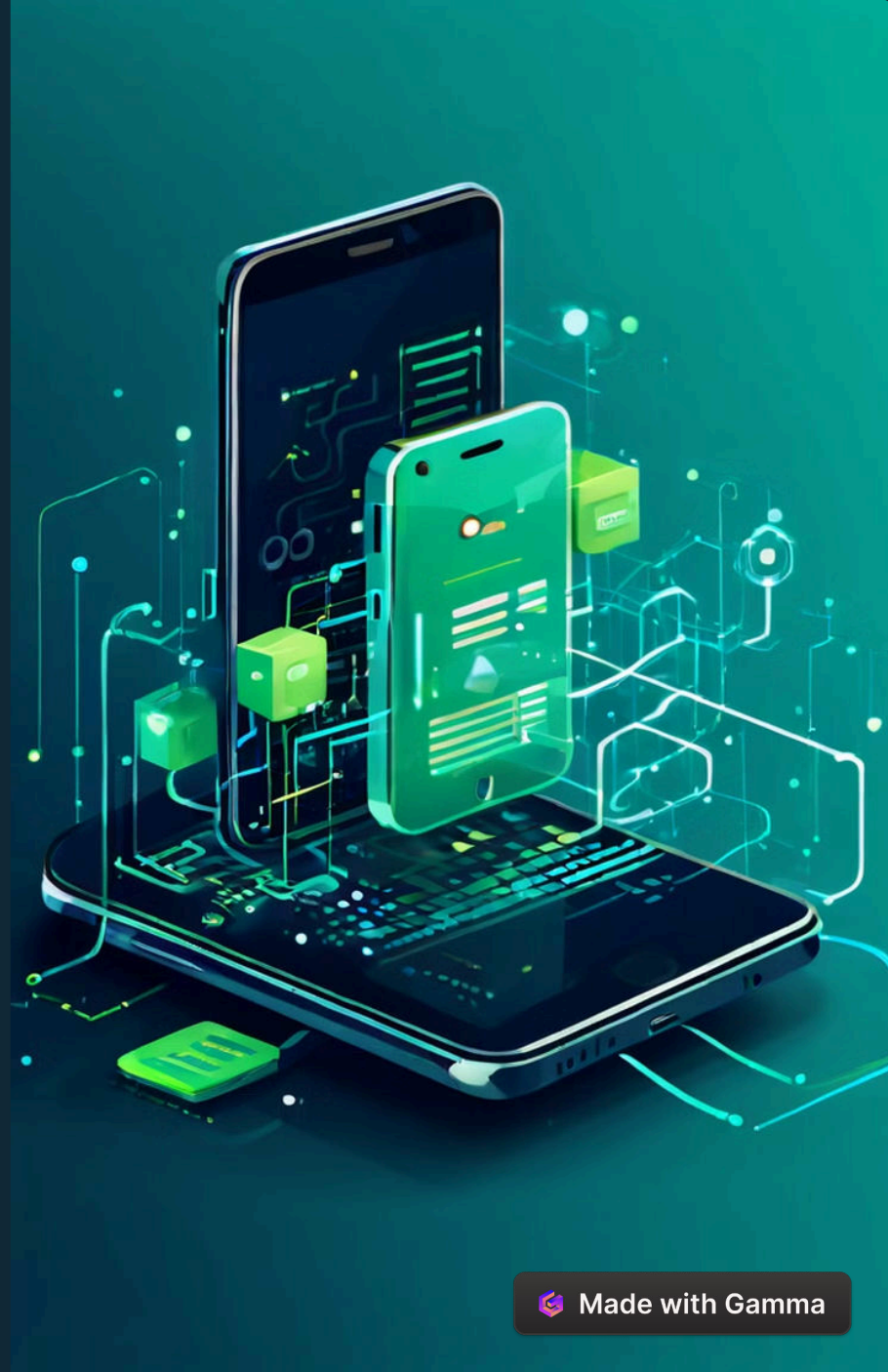
Enhanced Security

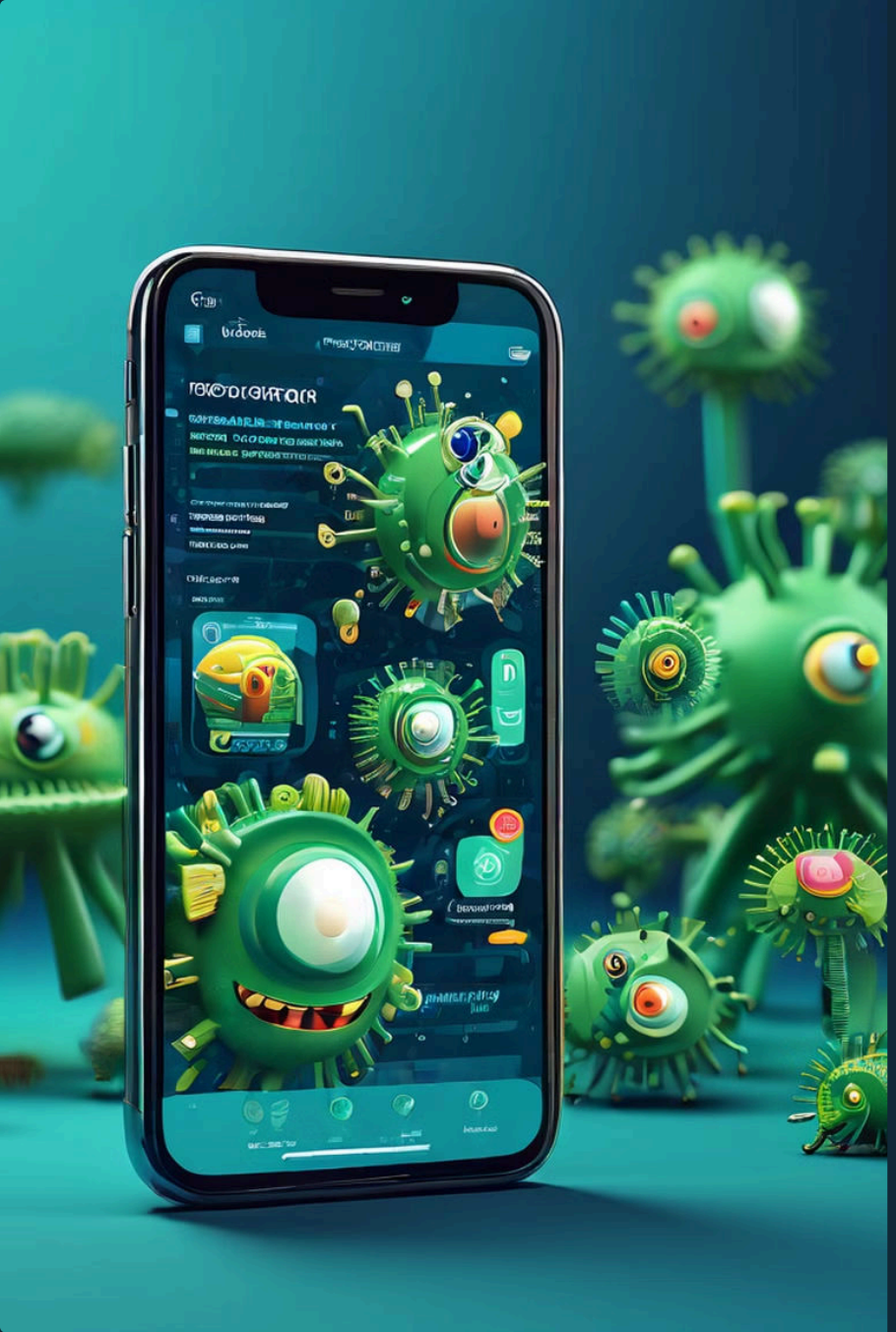
By integrating Linux components, LoA improves the security posture of Android devices.

3

Malware Detection

KYGNUS AMD is a key component of LoA, providing robust malware detection and removal capabilities.





Malware Detection Capabilities

1 Static Analysis

KYGNUS AMD analyzes the structure and behavior of suspicious files without executing them.

2 Heuristic Detection

KYGNUS AMD identifies malware based on patterns and characteristics, even if they are not explicitly known.

3 Signature-Based Detection

It uses a database of known malware signatures to identify and remove threats.

ClamAV Engine

Open Source

ClamAV is a widely used open-source antivirus engine.

Signature Database

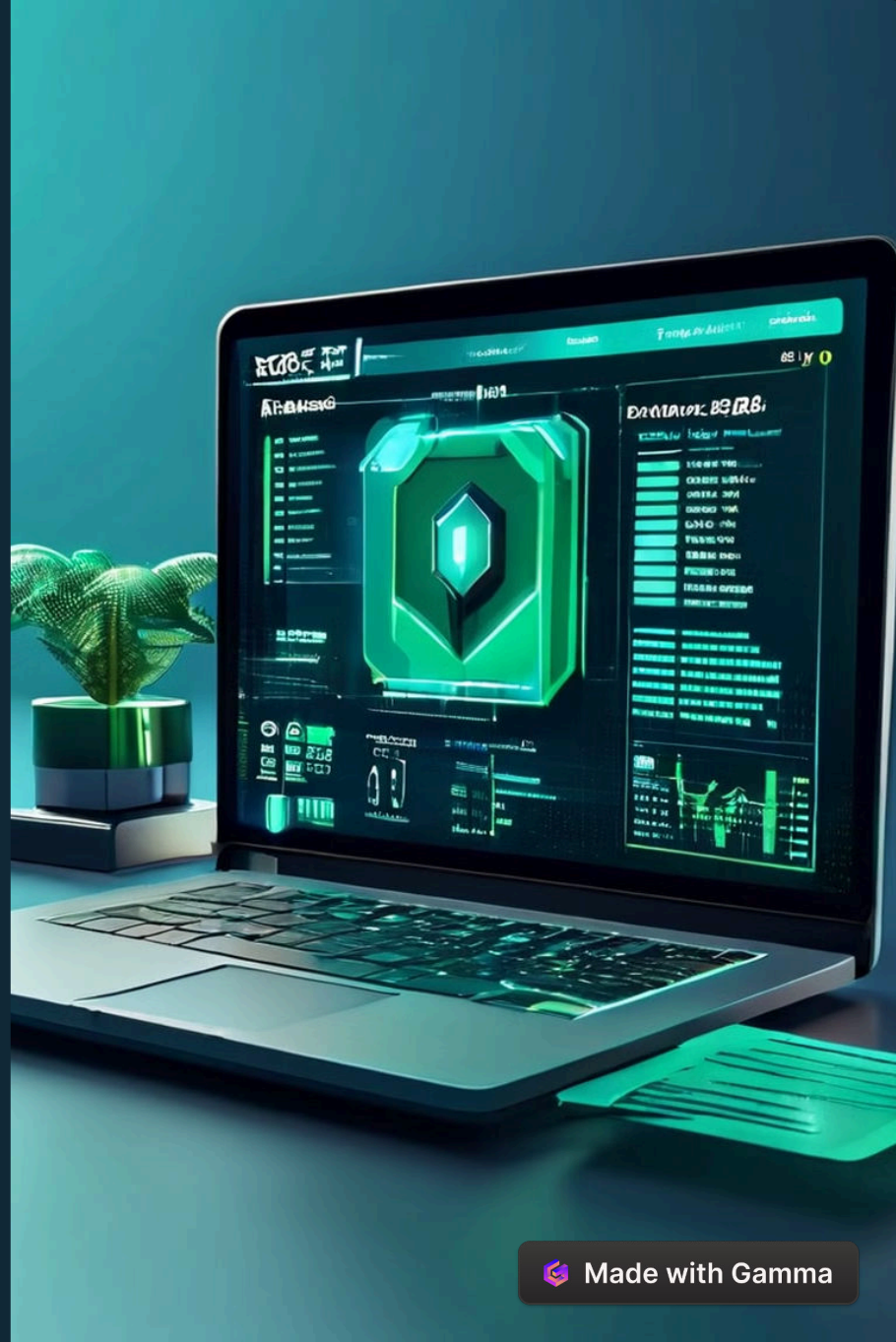
It relies on a comprehensive database of known malware signatures.

Real-Time Scanning

ClamAV provides real-time scanning for incoming files and applications.

Malware Removal

It can remove detected malware from your device.



Abnormal File Detection

Suspicious Executables

KYGNUS AMD identifies and isolates executable files that exhibit unusual behavior.

Sensitive File Access

It detects files attempting to access sensitive data or system components.

YARA Rules and Hash Databases

YARA Rules

YARA rules define patterns and characteristics of known malware.

Hash Databases

KYGNUS AMD utilizes a database of known malware hashes to identify threats.

Hash Matching

It compares the hashes of files to the database to detect known malware.

Androguard APK Analysis

1

APK Decompilation

Androguard decompiles the APK file to reveal its underlying code structure.

2

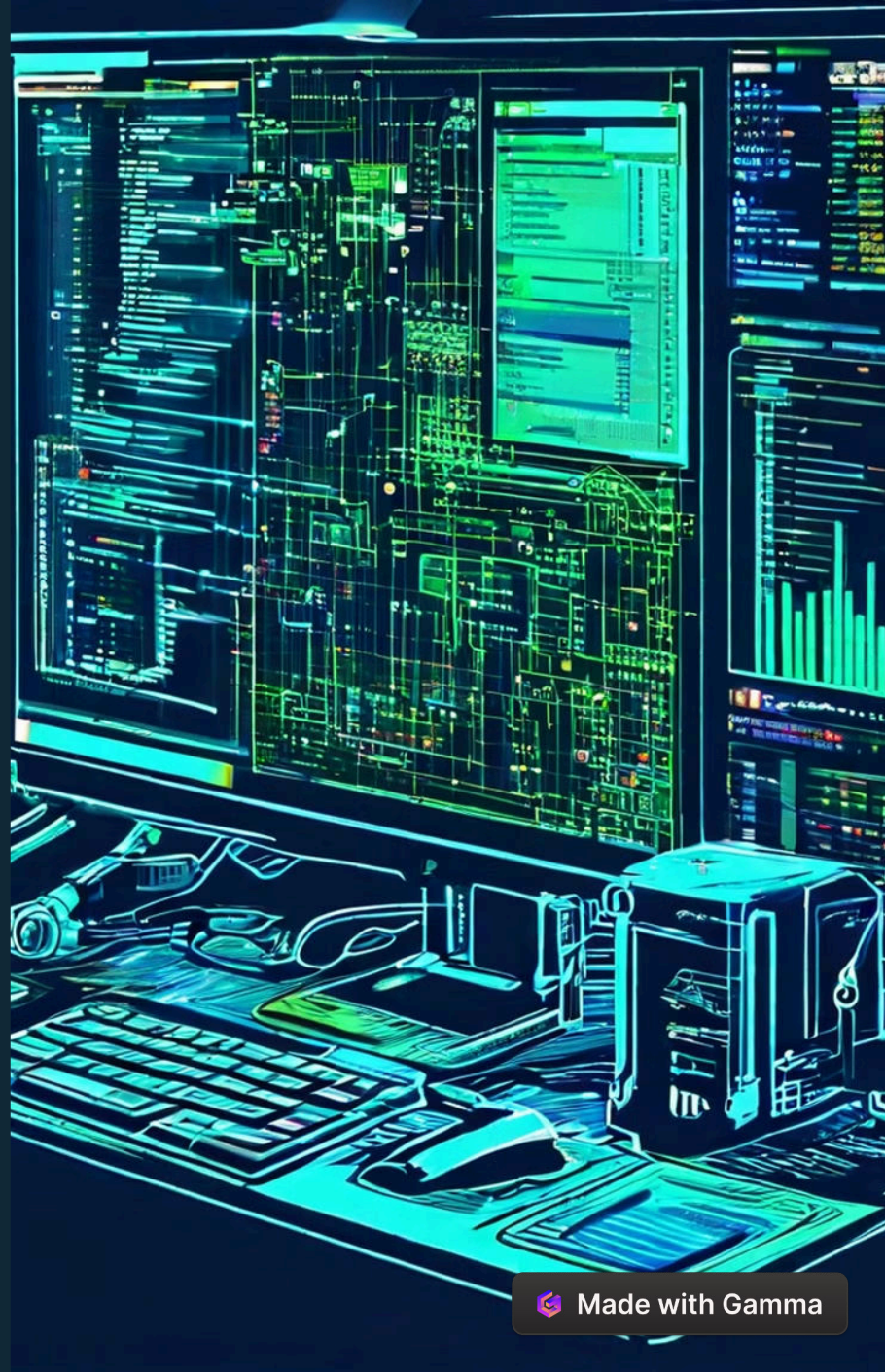
Code Analysis

It analyzes the decompiled code to identify potential malicious behavior.

3

Permission Analysis

Androguard examines the permissions requested by the APK to detect suspicious access.

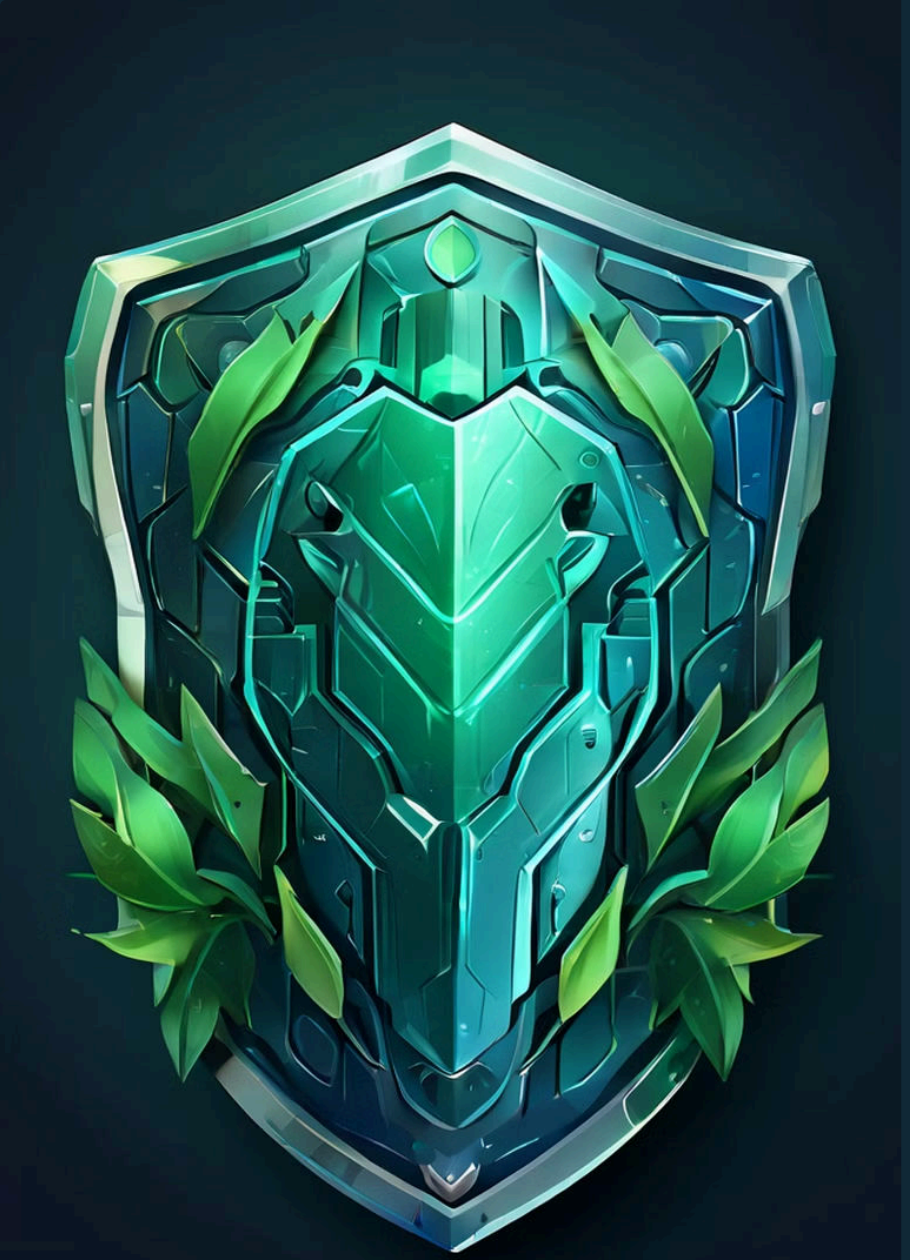


Simultaneous Scanning

With the KYGnus AMD solution, you can perform a comprehensive scan of all devices authorized to access your system with a single command. This feature saves valuable time and provides enhanced protection for your entire infrastructure.

Concurrent scanning ensures comprehensive coverage and increased responsiveness to security risks.

This feature is particularly useful in environments with many devices, such as corporate networks or large IT estates.



Conclusion and Key Takeaways

KYGNUS AMD is a powerful tool for Android malware detection. It combines multiple scanning engines and techniques to provide comprehensive protection.

About

- website : kooshayeganeh.github.io
- Github : github.com/KooshaYeganeh
- Gitlab : gitlab.com/KooshaYeganeh
- Gmail : koosahkooshadv@gmai.com