KYGnus

LoA

لینوکس در اندروید

AMD

شناسایی بدافزار اندروید

مقدمه کوتاه

این پروژه بخشی از پروژه LoA می باشد. پروژه LoA مبتنی بر شبیه سازی و کار با لینوکس گنو بر روی پوسته اندروید است که در آن سعی شده است ابزارها و روش هایی برای ارائه یک سیستم توسعه برای توسعه دهندگان دسکتاپ و همچنین اطلاع رسانی عادی باشد. کاربران در مورد سیستم و ابزار اندروید و کارهایی که می توان به روش معمول انجام داد آغاز شده است.

در این راستا سعی داریم از ابزارهایی برای بهینه سازی و بهبود عملکرد و عملکرد سیستم و فایل های شما در اندروید استفاده کنیم.

مرحله اول پروژه **AMD** است که وظیفه آن شناسایی فایل های خراب در سیستم ذخیره سازی شما با استفاده از ابزارهای قدرتمند لینوکس است.

بیانیه هایی که برای اسکن سیستم شما ایجاد شده یا در Android پست شده اند عبارتند از:

clamAV - 1

یک نرم افزار آنتی ویروس رایگان و منبع باز و یک جعبه ابزار آنتی ویروس چند پلتفرمی است. هدف اصلی آن شناسایی انواع مختلف نرم افزارهای مخرب مانند ویروس ها، کرم ها، تروجان ها، روت کیت ها و بسیاری از اشکال دیگر تهدیدات احتمالی برای سیستم شما است.

آنتی ویروس ClamAV یک رابط خط فرمان برای اسکن سیستم فایل شما (فایل ها و دایرکتوری ها) ارائه می دهد و همچنین شامل ابزارهای متعددی برای فیلتر کردن ایمیل، به روز رسانی خودکار امضا و سایر عملکردها است. بسیاری از برنامه‌ها از ClamAV، عمدتاً دروازه‌های اینترنتی و سرورهای ایمیل، به عنوان یک اقدام ایمنی برای اسکن ارتباطات ورودی و توقف توزیع بدافزار استفاده می‌کنند.

YARA – 2

قوانین YARA الگوهای شناسایی بدافزار هستند که برای شناسایی حملات هدفمند و تهدیدات امنیتی خاص محیط شما کاملاً قابل تنظیم هستند.

برای اطلاعات بیشتر : https://github.com/Yara-Rules/rules

AMD – 3

ADB-Android Debug bridge با KYGnus AMD

اتصال، اشکال زدایی و اسکن دستگاه های Android برای فعالیت های مخرب

برای اطلاعات بیشتر : https://github.com/KooshaYeganeh/AMD

این سیستم امنیتی از 3 موتور مجزا برای اسکن فایل های شما استفاده می کند. موتور اول clamAV است که یکی از قوی ترین آنتی ویروس های موجود است و به طور گسترده روی سرورهای لینوکس نصب می شود.
موتور دوم یارا است که متخصصان امنیتی از آن برای بررسی و دسته بندی ویروس ها استفاده می کنند.
موتور سوم موتور توسعه یافته توسط KYGnus است که مشابه موتور اسکن لینوکس است و فایل ها و فعالیت های غیرعادی سیستم شما را به دقت بررسی می کند.
برای نصب این اسکن به هیچ مهارت خاصی نیاز ندارید.

نصب

کافیست Termux را روی دستگاه اندرویدی خود نصب کنید و سپس این دستور را کپی کرده و در ترماکس اجرا کنید.
هشدار : برای شروع فرآیند نصب باید Licence را وارد نمایید.

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

```
pkg install wget -y
```

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

Manual

Help:

```
./loa --help
```

Full Scan with all Tools :

```
./loa --scan
```

Scan with clamAV :

```
./loa --clamav
```

Scan with Yara :

```
./loa --yara
```

Scan with amd Engine :

```
./loa --amd
```

Update :

```
./loa --update
```

مهمترین مزایای استفاده برای کاربران

1- آنتی ویروس سازمانی روی موبایل خود دارید.
2- با توجه به استفاده از سیستم های منبع باز، باگ های آنتی ویروس همیشه در سریع ترین زمان ممکن برطرف می شوند.
3- این آنتی ویروس قابلیت شخصی سازی را دارد. در صورت نیاز میتوان نرم افزار را بر اساس نیاز سازمان یا فرد شخصی سازی کرد.
4- سه موتور بودن آنتی ویروس به کاربران اطمینان می دهد که توانایی تامین حداکثر امنیت داده ها را دارد.
5- در موتور توسعه یافته سوم، نرم افزار از چند روش برای بررسی فایل ها استفاده می کند.
6- در این آنتی ویروس برای هر شخص یا سازمانی این امکان وجود دارد که پایگاه داده خود را توسعه دهد و یا پایگاه داده موجود را بر اساس فایل های خود تغییر دهد.
به عنوان مثال، شما فایلی به نام App.apk نمی خواهید. در دستگاه شما کافی است فایل های sha256sum یا md5sum را محاسبه کرده و در دیتابیس قرار دهید. از این پس این فایل برای سیستم شما مخرب خواهد بود.