

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИТМО»**

Факультет безопасности информационных технологий

Дисциплина:

«Обеспечение информационной безопасности мобильных устройств»

ОТЧЕТ ПО ЛАБАРАТОРНОЙ РАБОТЕ №4

«Особенности антивирусного ПО для мобильных платформ»

Выполнил:

Гаврилова В. В., студент группы N33471


(подпись)

Проверил:

Федоров Иван Романович

24.03.2022

(отметка о выполнении)

(подпись)

Санкт-Петербург

2022г.

Содержание

1. Цель работы

2. Основная часть

3. Выводы

1. Цель работы

Ознакомиться с особенностями антивирусного ПО для мобильных устройств.

2. Основная часть

2.1 Описание выбранных средств реализации и обоснования выбора

Для проверки файлов apk было выбрано приложение VirusTotal.

2.2 Основная часть

1) Загрузка APK из Лабораторной работы 2

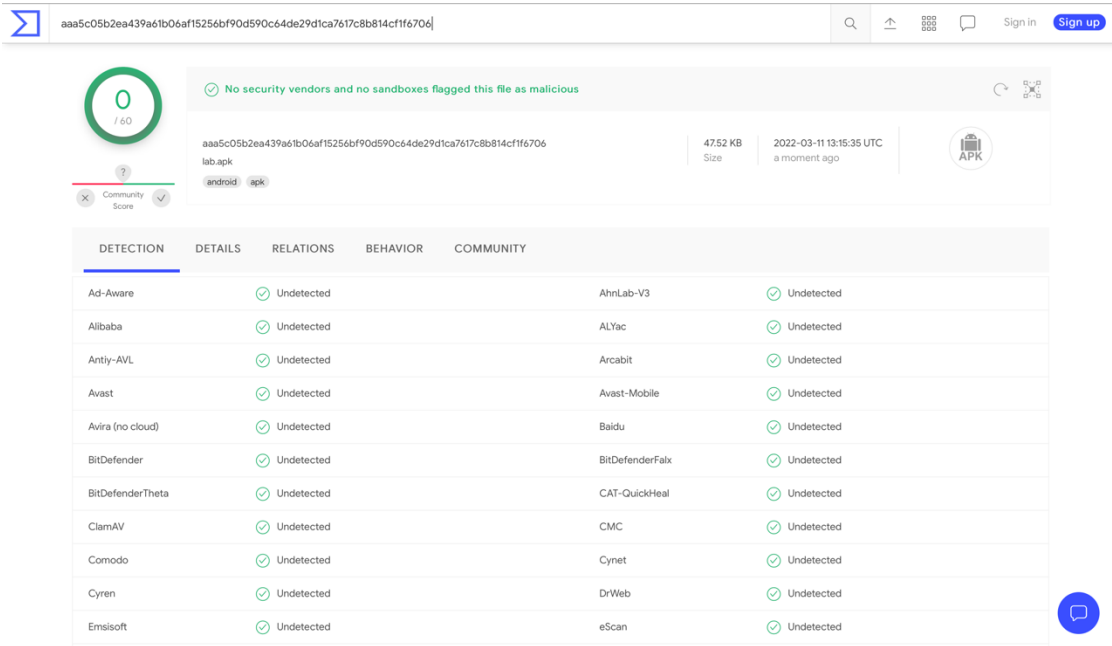


Рисунок 1 – APK из ЛР2

Сканирование ничего не выявило так как приложение никак не взаимодействует с сервером, не запрашивает доступ в интернет исходный код остался без изменений.

2) Сканирование TikTok

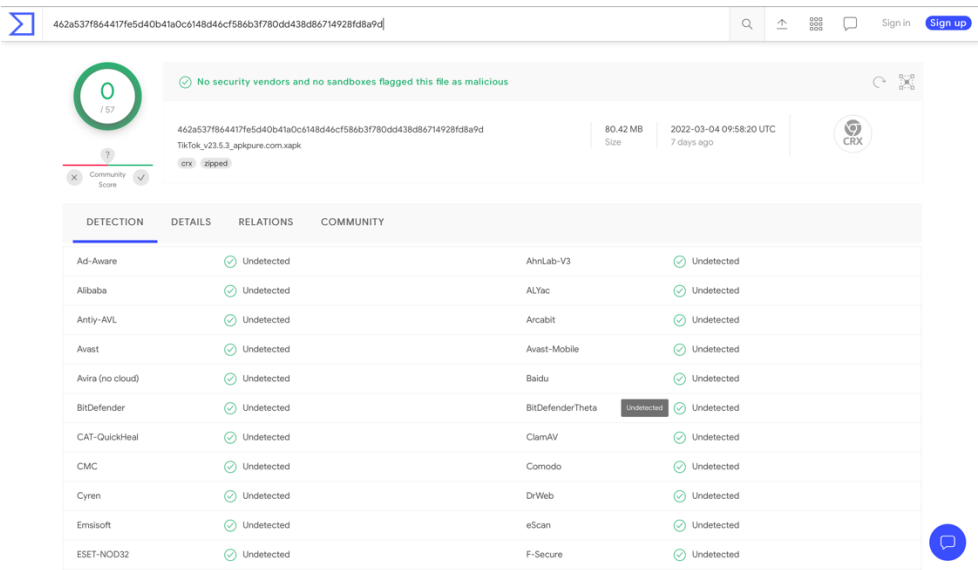


Рисунок 2 – TikTok

Сканирование показало, что файл не заражен и не поврежден.

3) Проверка malware Rubilyn

https://github.com/ytisf/theZoo/blob/master/malware/Source/Original/Rubilyn/Rubilyn.zip

200 Status text/html; charset=utf-8 Content Type 2022-03-11 13:19:30 UTC a moment ago

DETECTION	DETAILS	LINKS	COMMUNITY
Dr.Web	Malicious	Kaspersky	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean
Artists Against 419	Clean	Avira	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
benkow.cc	Clean	Bfore.AI PreCrime	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean

Рисунок 3 - Rubilyn

Только Dr.Web и Kaspersky смогли распознать вредоносный код.

4) Проверка malware Candy Corn

be0df39d6e334908c685e4c77b89efc49cc9bddc528a7c2434576b5a8b740f88

163.00 KB Size 2021-12-15 21:19:08 UTC 2 months ago

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Adware.GenericKD.36125842	AhnLab-V3	Spyware/Android.BgService.634995	
Alibaba	Trojan.Spy.Android.Hijoff.14298c7f	Antiy-AVL	Trojan.Generic.ASMalwAD.542	
Arcabit	Adware.Generic.D2273C92	Avast	Android.Agent-GZH [Trj]	
Avast-Mobile	Android.Agent-GZH [Trj]	AVG	Android.Agent-GZH [Trj]	
Avira (no cloud)	ANDROID.Spy.Agent.FHZW.Gen	BitDefender	Adware.GenericKD.36125842	
BitDefenderFalx	Android.Trojan.Spy.Agent.A	CAT-QuickHeal	Android.Hijoff.A	
ClamAV	Legacy.Trojan.Agent-1388638	Comodo	Malware@#7dqu7cm2y9ex	
Cyren	Malicious (score: 99)	Cyren	AndroidOS/PowerOffHijack.A.gen/Eldora...	
Dr.Web	Android.Spy.161.origin	Emsisoft	Adware.GenericKD.36125842 (B)	
eScan	Adware.GenericKD.36125842	ESET-NOD32	Android/Spy.Agent.JJ	
Fortinet	Android.Agent.NBtr.spy	GData	Adware.GenericKD.36125842	

Рисунок 4 - Candy Corn

В данном случае было обнаружено множество уязвимостей всеми представленными антивирусами.

3. Вывод

В результате выполнения работы я ознакомилась с особенностями антивирусного ПО для мобильных устройств.

