
# SAHTE BİR E-DEVLET UYGULAMASININ DERİNLEMESİNE ANALİZİ

EMRE ÇAKAR

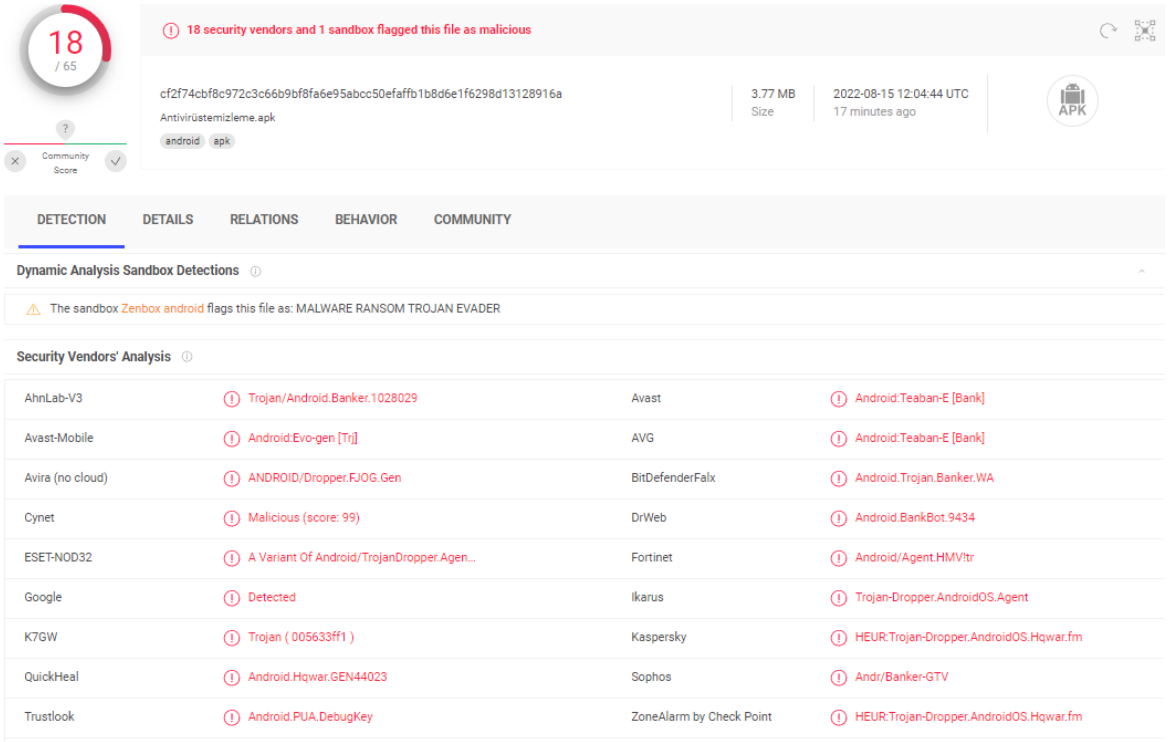
# 1. Uygulama Bilgileri

## 1.1 Cerberus nedir?

**Cerberus**, hacker forumlarında kiralanabilen bir **Android bankacılık Truva atıdır**. 2019'da oluşturulduğu tahmin ediliyor ve hassas, gizli bilgileri çalmak için kullanılıyor. Kullanıcıların cihazlarına **komut göndermek** ve tehlikeli eylemler gerçekleştirmek için de kullanılabilir.

Tipik olarak, Cerberus gibi bankacılık Truva atlarının arkasındaki siber suçlular, gelir elde etmek için kötüye kullanılabilecek bilgilere erişmeye çalışır.

| | |
|---|---|
| MD5 | 55aa2b8f540873a63b39b828bae6c9a8 |
| SHA-1 | 65d38e5b34db9deb22ff774fb988cb911126c231 |
| SHA-256 | cf2f74cbf8c972c3c66b9bf8fa6e95abcc50efaffb1b8d6e1f6298d13128916a |
| Vhash | 206dfe08de86858192965c10ee0ea65e |
| SSDEEP | 98304:NmcrjygLsrQ7tisyjoS/5TT4sKxnZfU/nXg8yLTRoWSbAc7:TrhYrQ7tiuy5Xws/hYwbV |
| TLSH | T1310633F1FBA0C455E71785316602E2D28322457672DCEBAF0B145C84BF92AC1E637DBA |
| File type | Android |
| Magic | Zip archive data, at least v2.0 to extract |
| TrID | Android Package (43.5%) |
| TrID | Opera Widget (15.8%) |
| TrID | Java Archive (15.2%) |
| TrID | Sweet Home 3D design (generic) (11.8%) |
| TrID | Mozilla Archive Format (gen) (7.9%) |
| File size | 3.77 MB (3956990 bytes) |




Yukarıda virustotal verilerine göre 18 antivirüs yazılımı tarafından zararlı bir yazılım olduğu tespit edilmiştir.

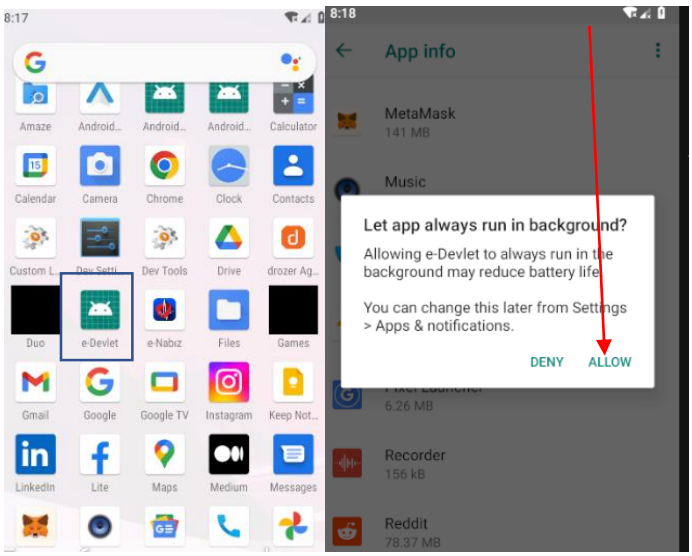
**Paket adı**: evidence.census.trophy

**Main Activity** :decide.industry.grape.quxoolxd

**key**: KLJasduiJWNDUIIAd

**c2**:http://anavatan353saf.]digital,,http://exzpzipleste.]digital,
http://istanbulsokaklari1453.]digital

**tür**: cerberus android banking malware



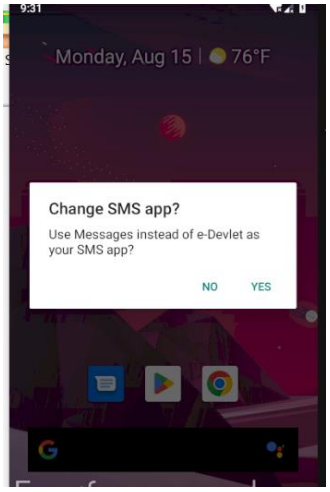

Uygulama kurulduktan hemen sonra yine diğer Truva atları gibi ikonunu gizleyip kendini arka olana atıyor. Bu esnada admin yetkileri, etkinlik izin yetkilerini de eline alıyor.

```
<meta-data android:name="android.app.device_admin" android:resource="@xml/sbxtyvomokeqomk" />
<intent-filter android:priority="136">
    <action android:name="android.app.action.DEVICE_ADMIN_DISABLED" />
    <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLE_REQUESTED" />
    <action android:name="android.app.action.DEVICE_ADMIN_ENABLED" />
</intent-filter>
```

**AndroidManifest.xml** dosyası incelendiği zaman ;

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_NOTIFICATION_POLICY" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.NFC" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.ACCESS_NOTIFICATION_POLICY" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES" />
```

Birçok hassas bilgiye erişmek için gerekli izinleri yukarıdaki gibi alıyor.




Bir süre sonra da kendini sms uygulaması olarak kullanılması için ekrana sürekli uyarı veriyor.

### 1.2 INTENTS

```
0×fb0 intent-filter
0×20cc intent.action.SEND
0×2104 intent.action.SENDTO
0×2154 intent.category.DEFAULT
0×2196 intent.category.BROWSABLE
0×25fa intent.action.RESPOND_VIA_MESSAGE
0×3016 intent.category.LAUNCHER
0×3086 intent.action.MAIN
0×31c2 intent.action.BOOT_COMPLETED
0×320e intent.action.QUICKBOOT_POWERON
0×32b2 intent.action.QUICKBOOT_POWERON
0×3304 intent.action.USER_PRESENT
0×334c intent.action.PACKAGE_ADDED
0×3396 intent.action.PACKAGE_REMOVED
```

**0x20cc:** verileri diğer uygulamalara gönderme eylemi(yani kendisine)
**0x2104:** Veriler tarafından belirtilen birine bir mesaj gönderme
**0x334c:** Cihaza yeni bir uygulama paketi yükleme

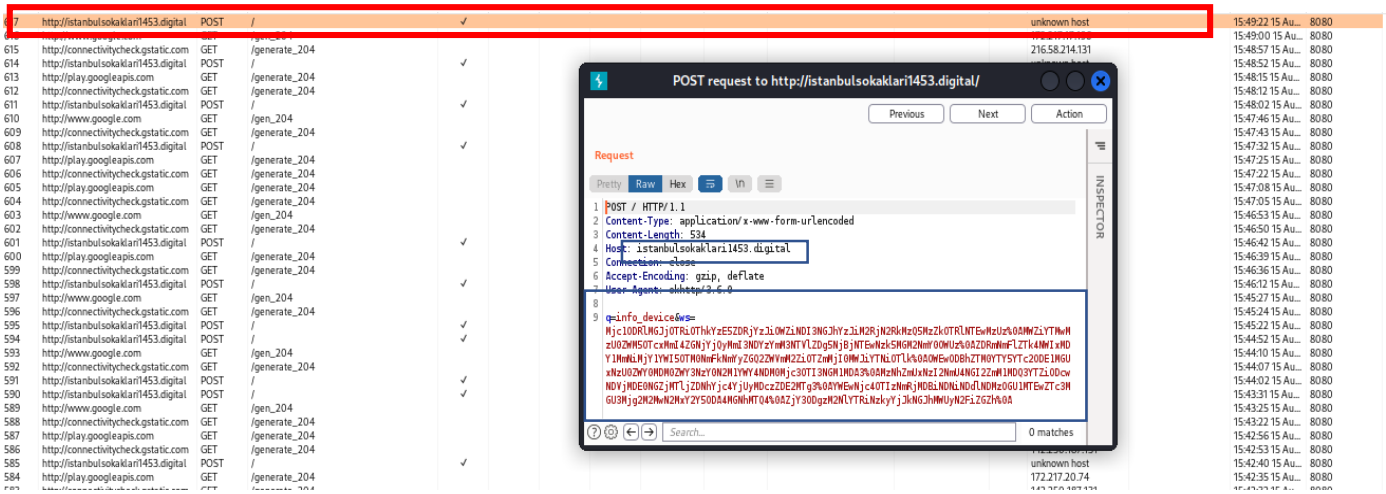
### 1.3 BROADCAST RECEIVERS

```
dz> run app.broadcast.info -a evidence.census.trophy
Package: evidence.census.trophy
  decide.industry.grape.txzpyhegdf
    Permission: android.permission.BROADCAST_WAP_PUSH
  decide.industry.grape.lvhujkizoxqmombt
    Permission: android.permission.BIND_DEVICE_ADMIN
  decide.industry.grape.umnsrhes
    Permission: android.permission.BROADCAST_SMS
```

**android.permission.BROADCAST_WAP_PUSH**: Kötü amaçlı uygulamalar bunu, MMS mesajı alımını taklit etmek veya herhangi bir web sayfasının içeriğini kötü niyetli varyantlarla sessizce değiştirmek için kullanabilir.

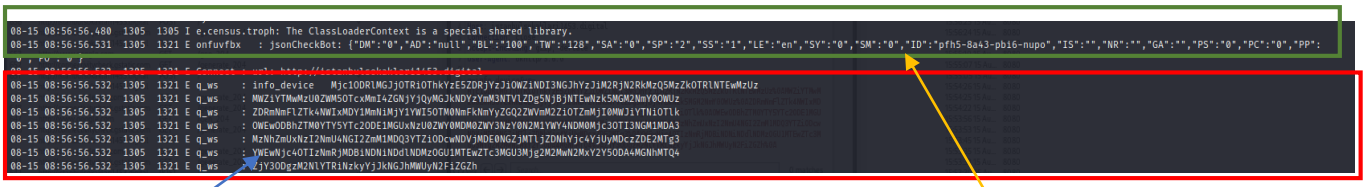
**android.permission.BROADCAST_SMS:** Uygulamaya, bir SMS mesajının alındığına dair bir bildirim yayınlama izni verir. Kötü amaçlı uygulamalar, gelen SMS mesajlarını taklit etmek için bunu kullanabilir.

# 2.Giden Trafiğin İncelemesi ve Verinin Çözümlenmesi



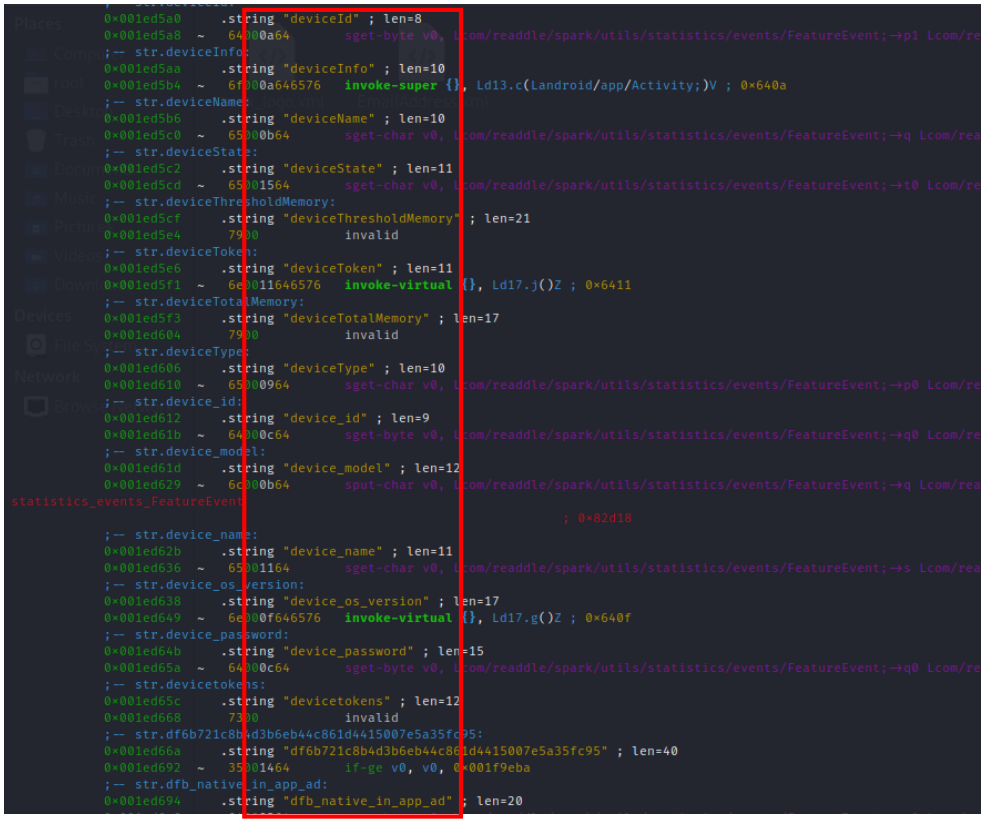

Yukarıda **burpsuite** ile uygulamanın trafiği incelendiğinde **istanbulsokaklari1453[.]digital** adresine şifreli veri gönderdiği tespit edilmiştir.

**ADB** ile Cihazın anlık **logu** incelendiğinde giden şifreli verinin çözülmüş haline ulaşılacaktır.



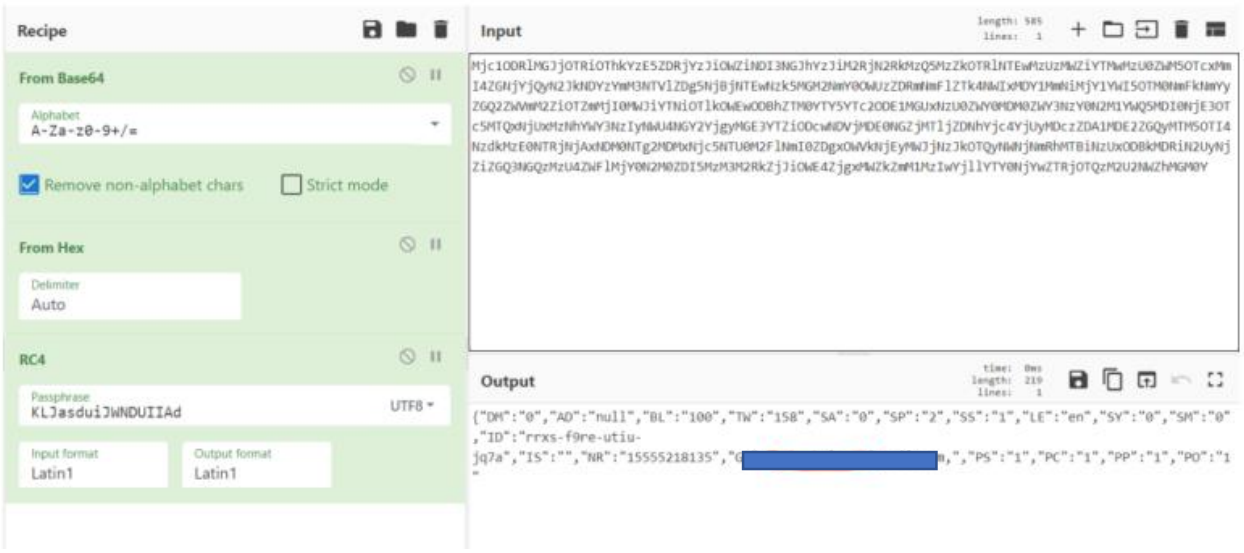

Şifreli veri

karşı tarafa gitmek üzere olan çözülmüş veri




veriler telefonun anlık durum bilgisidir. (yukarıdaki kodda da görüldüğü gibi telefon id numarası, telefon bilgisi, telefon tipi modeli gibi bilgiler)

Not:**data/data/evidence.census.trophy/shared_prefs** dizininde **ring0.xml** dosyasının içinde bulunan key kullanılarak da şifre çözülebilir.

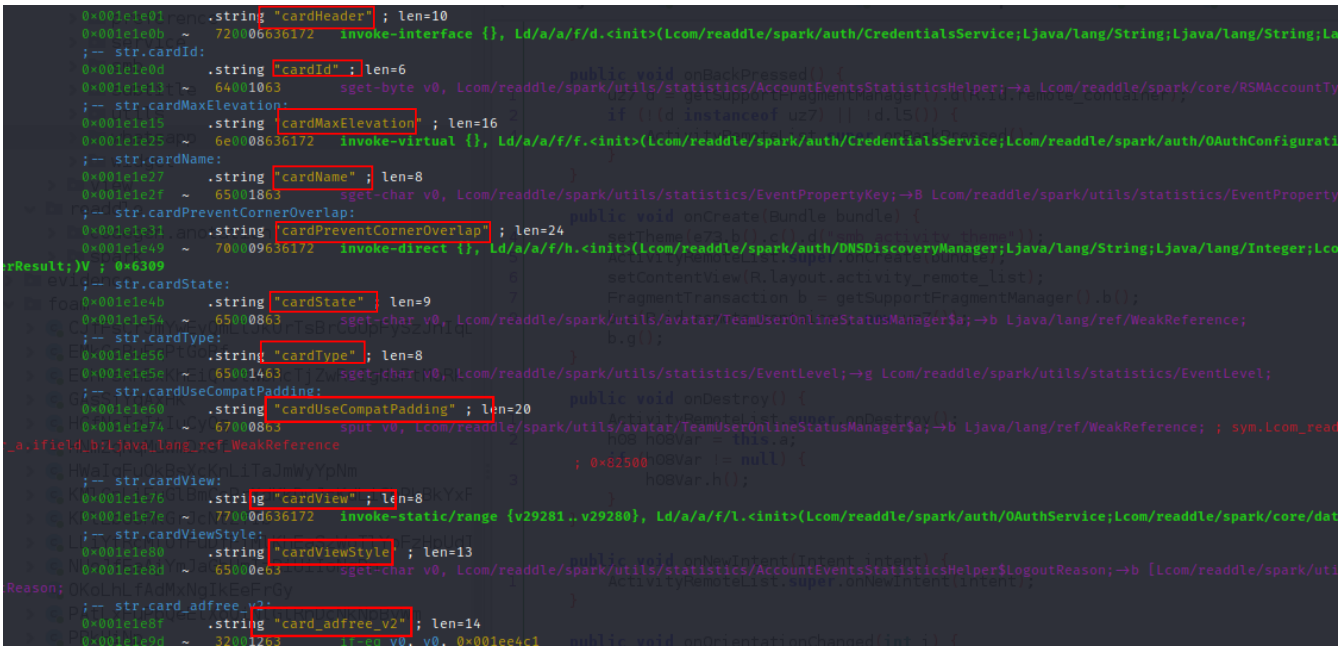


# 3.KOD ANALİZİ

**Radare2** aracı ile diassembiling işlemi yapılmıştır(.dex)

Radare2, fareyi kullanmanıza ve yalnızca statik bir komut isteminden daha etkileşimli bir görünüm elde etmenize olanak tanıyan bir görsel mod (V komutu) ve web kullanıcı arabirimi (=H komutu aracılığıyla) sağlar.

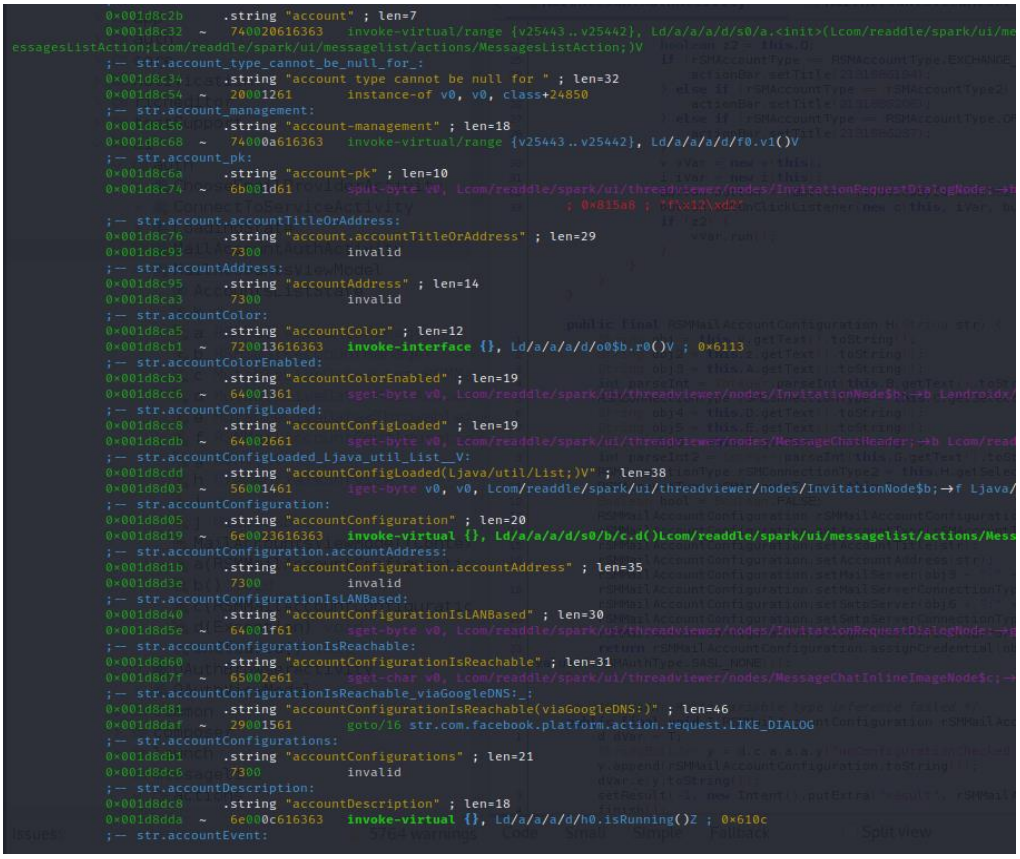
### 3.1 KART BİLGİLERİNİN TOPLANMASI




Hedef kullanıcıdan kart bilgilerini almak için çeşitli parametreler kullanıldığı belirlenmiştir.Bu parametreler ile hedef kartı ayıklanıp karşı tarafa string olarak gidiyor.


**Resim: bank.xml içinde kart tiplerine uygun banka bilgileri**

## 3.2 HESAP BİLGİLERİNİN ELE GEÇİRİLMESİ



Yukarıdaki kodda hedef için yapılan hesap konfigüre işlemleri, hesap adresleri, hesap yönetimi gibi bilgileri çağırmak için çeşitli parametreler kullanıldığı görülmüştür.

Uygulama geliştiricisinin yukarıdaki kodda da görüldüğü gibi [https://twitter[.]com/Neat.Bytes](https://twitter[.]com/Neat.Bytes) , [https://www.facebook[.]com/pages/NeatBytes/1516789311908389](https://www.facebook[.]com/pages/NeatBytes/1516789311908389) bağlantılı olduğu tespit edilmiştir

```
public String toString() {
    StringBuilder y = a.y("RSMMailAccountConfiguration{pk=");
    y.append(this.pk);
    y.append(", accountType=");
    y.append(this.accountType);
    y.append(", accountTitle='");
    a.P(y, this.accountTitle, '\'', ", orderNumber=");
    y.append(this.orderNumber);
    y.append(", pictureURL=");
    y.append(this.pictureURL);
    y.append(", ownerFullName='");
    a.P(y, this.ownerFullName, '\'', ", accountAddress='");
    a.P(y, this.accountAddress, '\'', ", mailServer='");
    a.P(y, this.mailServer, '\'', ", mailServerAuthenticationKCKey='");
    a.P(y, this.mailServerAuthenticationKCKey, '\'', ", mailServerConnectionType=");
    y.append(this.mailServerConnectionType);
    y.append(", smtpServer='");
    a.P(y, this.smtpServer, '\'', ", smtpServerAuthenticationKCKey='");
    a.P(y, this.smtpServerAuthenticationKCKey, '\'', ", smtpServerConnectionType=");
    y.append(this.smtpServerConnectionType);
    y.append(", mailServerCapabilitiesVersion=");
    y.append(this.mailServerCapabilitiesVersion);
    y.append(", ignoreCertificateError=");
    y.append(this.ignoreCertificateError);
    y.append(", emailAliases='");
    a.P(y, this.emailAliases, '\'', ", mailAccountStatus=");
    y.append(this.mailAccountStatus);
    y.append(", flags=");
    y.append(this.flags);
    y.append('}');
    return y.toString();
```

**Jadx** ile uygulamanın kaynak kodları incelendiğinde yukarıdaki kodda da görüldüğü gibi uygulama ile haberleşen saldırgan istediği bilgileri mail server (smtp) ile verileri kendine çekebiliyor.

```
public static void l(OAuthBrowserActivity oAuthBrowserActivity) {
    Objects.requireNonNull(oAuthBrowserActivity);
    fO fOVar = new fO(oAuthBrowserActivity);
    ArrayList arrayList = new ArrayList(Arrays.asList("Email", "login-username", "iO116", "profileIdentifier", "identifierId"));
    if (oAuthBrowserActivity.b.equals(OAuthModule.HOTMAIL_REDIRECT)) {
        arrayList.add("displayName");
        z.H(oAuthBrowserActivity.h, arrayList, Arrays.asList("value", "title"), fOVar);
        return;
    }
    z.H(oAuthBrowserActivity.h, arrayList, Collections.singletonList("value"), fOVar);
}

public final void m(Uri uri) {
    String str = uri.getScheme() + "://";
    SpannableString spannableString = new SpannableString(d.c.a.a.a.q(str, uri.getHost()));
    int i = 0;
    spannableString.setSpan(new ForegroundColorSpan(getResources().getColor(2131100055)), 0, str.length(), 33);
    spannableString.setSpan(new ForegroundColorSpan(getResources().getColor(2131100054)), str.length(), spannableString.length(),
    this.j.setText(spannableString);
    ImageView imageView = this.l;
    if (!str.equals("https://")) {
        i = 8;
```