



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.

MD555aa2b8f540873a63b39b828bae6c9a8

SHA-165d38e5b34db9deb22ff774fb988cb911126c231

SHA-256cf2f74cbf8c972c3c66b9bf8fa6e95abcc50efaffb1b8d6e1f6298d13128916a

Vhash206dfe08de86858192965c10ee0ea65e

SSDEEP98304:NmcryjgLsrQ7tisyjoS/5TT4sKxnZfU/nXg8yLTRoWSbAc7:TrhYrQ7tiuy5Xws/hYwbV

TLSHT1310633F1FBA0C455E71785316602E2D28322457672DCEBAF0B145C84BF92AC1E637DBA

File typeAndroid

MagicZip archive data, at least v2.0 to extract

TrIDAndroid Package (43.5%)

TrIDOpera Widget (15.8%)

TrIDJava Archive (15.2%)

TrIDSweet Home 3D design (generic) (11.8%)

TrIDMozilla Archive Format (gen) (7.9%)

File size3.77 MB (3956990 bytes)

18/65

18 security vendors and 1 sandbox flagged this file as malicious

cf2f74cbf8c972c3c66b9bf8fa6e95abcc50efaffb1b8d6e1f6298d13128916a

Antivirustemizleme.apk

androidapk

3.77 MBSize

2022-08-15 12:04:44 UTC17 minutes ago

APK

Community Score

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY

Dynamic Analysis Sandbox Detections

The sandbox Zenbox android flags this file as: MALWARE RANSOM TROJAN EVADER

Security Vendors' Analysis

AhnLab-V3	Trojan.Android.Banker.1028029	Avast	Android:Teaban-E [Bank]
Avast-Mobile	Android:Evo-gen [Trj]	AVG	Android:Teaban-E [Bank]
Avira (no cloud)	ANDROID/Dropper.FJOG.Gen	BitDefenderFalx	Android.Trojan.Banker.WA
Cynet	Malicious (score: 99)	DrWeb	Android.BankBot.9434
ESET-NOD32	A Variant Of Android/TrojanDropper.Agen...	Fortinet	Android/Agent.HMVtr
Google	Detected	Ikarus	Trojan-Dropper.AndroidOS.Agent
K7GW	Trojan (005633ff1)	Kaspersky	HEUR:Trojan-Dropper.AndroidOS.Hqwar.fm
QuickHeal	Android.Hqwar.GEN44023	Sophos	Andr/Banker-GTV
Trustlook	Android.PUA.DebugKey	ZoneAlarm by Check Point	HEUR:Trojan-Dropper.AndroidOS.Hqwar.fm

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

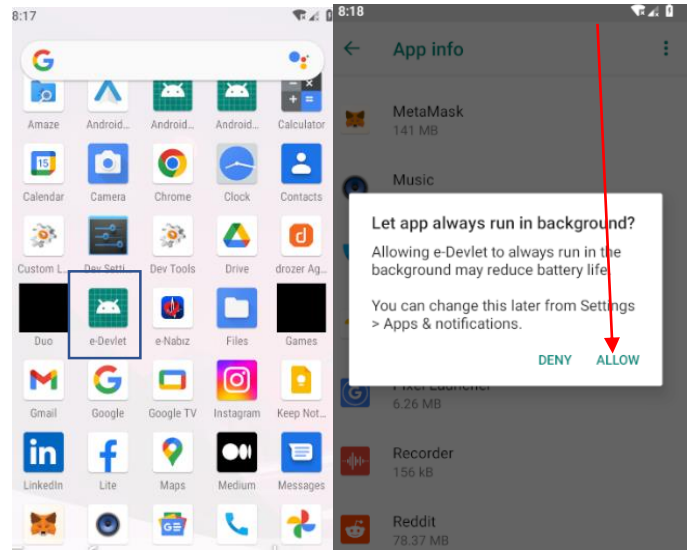
Paket adı: evidence.census.trophy

Main Activity :decide.industry.grape.quxoolxd

key: KLJasduiJWNDUIIAd

c2:[http://anavatan353saf.\].digital,](http://anavatan353saf.].digital,)
[http://exzpzipleste.\].digital,](http://exzpzipleste.].digital,)
[http://istanbulsokaklari1453.\].digital](http://istanbulsokaklari1453.].digital)

tür: cerberus android banking malware



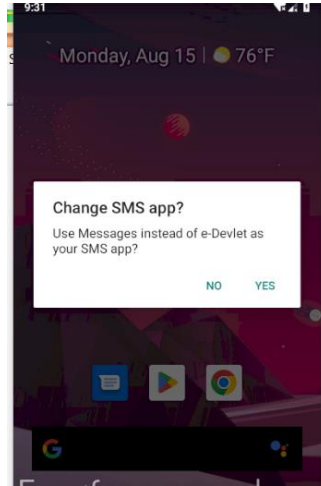
Uygulama kurulduktan hemen sonra yine diğer Truva atları gibi ikonunu gizleyip kendini arka olana atıyor. Bu esnada admin yetkileri, etkinlik izin yetkilerini de eline alıyor.

```
<meta-data android:name="android.app.device_admin" android:resource="@xml/sbxyvomoqeomk" />
<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

```
0xfb0 intent-filter
0x20cc intent.action.SEND
0x2104 intent.action.SENDTO
0x2154 intent.category.DEFAULT
0x2196 intent.category.BROWSABLE
0x25fa intent.action.RESPOND_VIA_MESSAGE
0x3016 intent.category.LAUNCHER
0x3086 intent.action.MAIN
0x31c2 intent.action.BOOT_COMPLETED
0x320e intent.action.QUICKBOOT_POWERON
0x32b2 intent.action.QUICKBOOT_POWERON
0x3304 intent.action.USER_PRESENT
0x334c intent.action.PACKAGE_ADDED
0x3396 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 Çözülmesi

The screenshot displays a network traffic analysis tool interface. On the left, a list of outgoing traffic is shown, including various GET and POST requests to different domains. A red box highlights a specific POST request to `http://istanbulsokaklari1453.digital/`. On the right, a detailed view of this POST request is shown, including the raw data and the decoded content. The decoded content is a JSON object with a key `q=info_device` and a value that is a long string of characters, likely a device identifier or a token. The tool also shows the request's headers, including `Content-Type: application/x-www-form-urlencoded` and `Accept-Encoding: gzip, deflate`.

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

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

The screenshot shows an Android logcat output. It displays a series of log messages, including a warning from `e.census.troph` and a log message from `onufvfbx` showing a JSON object. The JSON object has a key `q` and a value that is a long string of characters, likely a device identifier or a token. A red box highlights the JSON object, and a yellow arrow points to the value of `q`. A blue arrow points to the log message from `onufvfbx`.

Şifreli veri

karşı tarafa gitmek üzere olan çözülmüş veri

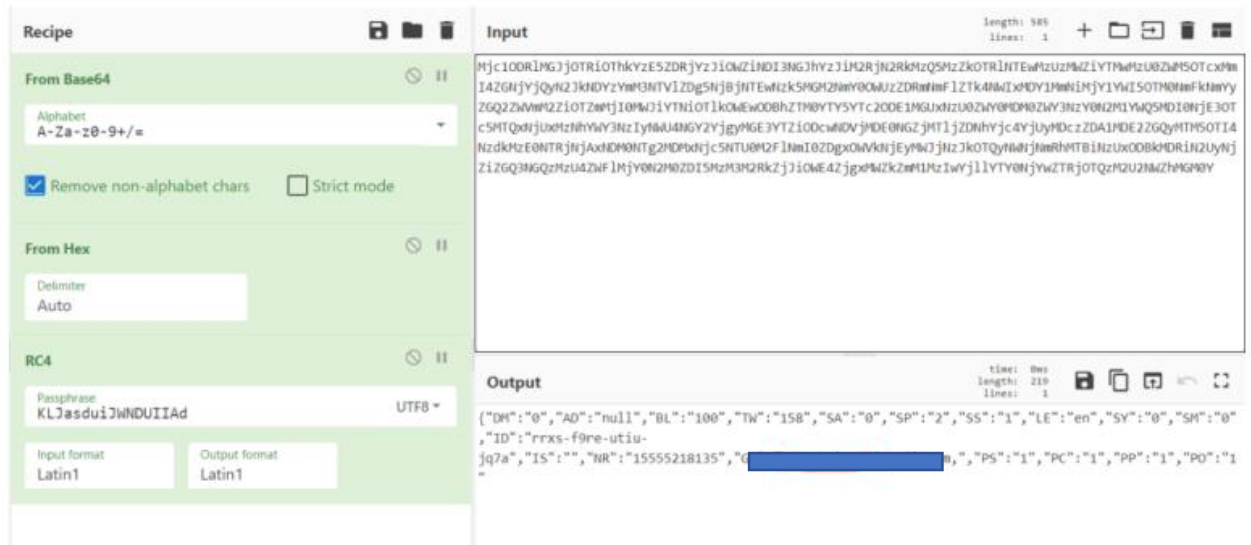
```

Places: 0x001ed5a0 .string "deviceId" ; len=8
        0x001ed5a8 ~ 64 00a64 sget-byte v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→p1 lcom/re
;-- str.deviceInfo:
        0x001ed5aa .string "deviceInfo" ; len=10
        0x001ed5b4 ~ 6f 00a646576 invoke-super {}, Ld13.c(Landroid/app/Activity;);V ; 0x640a
;-- str.deviceName:
        0x001ed5b6 .string "deviceName" ; len=10
        0x001ed5c0 ~ 65 00b64 sget-char v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→q lcom/re
;-- str.deviceState:
        0x001ed5c2 .string "deviceState" ; len=11
        0x001ed5cd ~ 65 011564 sget-char v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→t0 lcom/re
;-- str.deviceThresholdMemory:
        0x001ed5cf .string "deviceThresholdMemory" ; len=21
        0x001ed5e4 ~ 79 00 invalid
;-- str.deviceToken:
        0x001ed5e6 .string "deviceToken" ; len=11
        0x001ed5f1 ~ 6c 011646576 invoke-virtual {}, Ld17.j()Z ; 0x6411
;-- str.deviceTotalMemory:
        0x001ed5f3 .string "deviceTotalMemory" ; len=17
        0x001ed604 ~ 79 00 invalid
;-- str.deviceType:
        0x001ed606 .string "deviceType" ; len=10
        0x001ed610 ~ 65 00964 sget-char v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→p0 lcom/re
;-- str.device_id:
        0x001ed612 .string "device_id" ; len=9
        0x001ed61b ~ 64 00c64 sget-byte v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→q0 lcom/re
;-- str.device_model:
        0x001ed61d .string "device_model" ; len=12
        0x001ed629 ~ 6c 00b64 sput-char v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→q lcom/re
statistics_events_FeatureEvent
;-- str.device_name:
        0x001ed62b .string "device_name" ; len=11
        0x001ed636 ~ 65 01164 sget-char v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→s lcom/re
;-- str.device_os_version:
        0x001ed638 .string "device_os_version" ; len=17
        0x001ed649 ~ 6c 00f646576 invoke-virtual {}, Ld17.g()Z ; 0x640f
;-- str.device_password:
        0x001ed64b .string "device_password" ; len=15
        0x001ed65a ~ 64 00c64 sget-byte v0, lcom/readdle/spark/utils/statistics/events/FeatureEvent;→q0 lcom/re
;-- str.device_tokens:
        0x001ed65c .string "device_tokens" ; len=12
        0x001ed668 ~ 79 00 invalid
;-- str.dfb6721c8b4d3b6eb44c861d4415007e5a35fc95:
        0x001ed66a .string "dfb6721c8b4d3b6eb44c861d4415007e5a35fc95" ; len=40
        0x001ed692 ~ 35 01464 if-gc v0, v0, 0x001f9eba
;-- str.dfb_native_in_app_ad:
        0x001ed694 .string "dfb_native_in_app_ad" ; len=20

```

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 diassembling 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

```
0x001e01 rom .string "cardHeader"; len=10
0x001e0b ~ 720006636172 invoke-interface {}, Ld/a/a/f/d.<init>(Lcom/readdle/spark/auth/CredentialsService;Ljava/lang/String;Ljava/lang/String;L
;- str.cardId:
0x001e0d ~ 64001063 sget-byte v0, Lcom/readdle/spark/utlils/statistics/AccountEventsStatisticsHelper;→a Lcom/readdle/spark/core/RSMAccountTy
0x001e13 ~ 64001063 sget-byte v0, Lcom/readdle/spark/utlils/statistics/AccountEventsStatisticsHelper;→a Lcom/readdle/spark/core/RSMAccountTy
;- str.cardMaxElevation:
0x001e15 ~ 64001063 sget-byte v0, Lcom/readdle/spark/utlils/statistics/AccountEventsStatisticsHelper;→a Lcom/readdle/spark/core/RSMAccountTy
0x001e15 ~ 64001063 sget-byte v0, Lcom/readdle/spark/utlils/statistics/AccountEventsStatisticsHelper;→a Lcom/readdle/spark/core/RSMAccountTy
;- str.cardName:
0x001e27 ~ 65001863 sget-char v0, Lcom/readdle/spark/utlils/statistics/EventPropertyKey;→B Lcom/readdle/spark/utlils/statistics/EventProperty
;- str.cardPreventCornerOverlap:
0x001e31 ~ 700009636172 invoke-virtual {}, Ld/a/a/f/h.<init>(Lcom/readdle/spark/auth/CredentialsService;Lcom/readdle/spark/auth/OAuthConfigurati
0x001e49 ~ 700009636172 invoke-direct {}, Ld/a/a/f/h.<init>(Lcom/readdle/spark/auth/CredentialsService;Lcom/readdle/spark/auth/OAuthConfigurati
;- str.cardState:
0x001e4b ~ 65001863 sget-char v0, Lcom/readdle/spark/utlils/statistics/EventPropertyKey;→B Lcom/readdle/spark/utlils/statistics/EventProperty
;- str.cardType:
0x001e56 ~ 65001463 sget-char v0, Lcom/readdle/spark/utlils/statistics/EventLevel;→g Lcom/readdle/spark/utlils/statistics/EventLevel;
;- str.cardUseCompatPadding:
0x001e74 ~ 67000863 sput v0, Lcom/readdle/spark/utlils/avatar/TeamUserOnlineStatusManager$a;→b Ljava/lang/ref/WeakReference; ; sym.Lcom_rea
_a.iffield_b:Ljava/lang/ref/WeakReference
;- str.cardView:
0x001e76 ~ 770006636172 invoke-static/range {v29281..v29280}, Ld/a/a/f/l.<init>(Lcom/readdle/spark/auth/OAuthService;Lcom/readdle/spark/core/dat
;- str.cardViewStyle:
0x001e80 ~ 65001063 sget-char v0, Lcom/readdle/spark/utlils/statistics/AccountEventsStatisticsHelper$LogoutReason;→b [Lcom/readdle/spark/utl
Reason; OKoLHLfAdMaNoKKEeRjy
;- str.card_adfree_v2:
0x001e8f ~ 32001763 sput v0, v0, 0x001e6c1
```

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

```
1 { "bank_urls_list" :
2
3
4
5     "bank_desc": "NBB", "bank_type": "NBCB_CREDIT" },
6
7     "bank_desc": "CMB", "bank_type": "CMB_DEBIT" },
8
9
10    "bank_desc": "ABC", "bank_type": "ABC_DEBIT"
11
12
13    "bank_desc": "BOC", "bank_type": "BOC_DEBIT"
14
15    "bank_desc": "GDB", "bank_type": "CGB_DEBIT"
16
17    "bank_desc": "GDB", "bank_type": "CGB_CREDIT"
18
19    "bank_desc": "CITIC", "bank_type": "ECITIC_CREDIT"
20
21
22    "bank_desc": "CITIC", "bank_type": "ECITIC_DEBIT"
23
24
25    "bank_desc": "VISA", "bank_type": "VISA_CREDIT"
26
27
28    "bank_desc": "MASTERCARD", "bank_type": "MASTERCARD_CREDIT"
29
30
31    "bank_desc": "JCB", "bank_type": "JCB_CREDIT"
32
33
34 }
35 }
```

Resim: bank.xml içinde kart tiplerine uygun banka bilgileri

3.2 HESAP BİLGİLERİNİN ELE GEÇİRİLMESİ

```
0x001d8c2b .string "account" ; len=7
0x001d8c32 ~ 740020616363 invoke-virtual/range {v25443..v25442}, Ld/a/a/a/d/s0/a.<init>()Lcom/readdle/spark/ui/mess
essagesListAction;Lcom/readdle/spark/ui/messagelist/actions/MessageListAction;)V
;- str.account_type: cannot be null for ; len=32
0x001d8c34 ~ 20001261 instance-of v0, v0, class+24850
;- str.account_management:
0x001d8c56 ~ 74000a616363 invoke-virtual/range {v25443..v25442}, Ld/a/a/a/d/f0.v1()V
0x001d8c68 ~ 66001d61 sput-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/InvitationRequestDialogNode;→a
;- str.account_pk:
0x001d8c6a ~ 7300 invalid
0x001d8c74 ~ 7300 invalid
;- str.account_titleOrAddress:
0x001d8c76 ~ 7300 invalid
0x001d8c93 ~ 7300 invalid
;- str.accountAddress:
0x001d8c95 ~ 7300 invalid
0x001d8ca3 ~ 7300 invalid
;- str.accountColor:
0x001d8ca5 ~ 720013616363 invoke-interface {}, Ld/a/a/a/d/o0$b.re0()V ; 0x6113
0x001d8cb1 ~ 64001f61 sget-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/MessageChatHeader;→b Lcom/read
;- str.accountColorEnabled:
0x001d8cb3 ~ 64001361 sget-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/InvitationNode$b;→b Landroidx
0x001d8ccb ~ 64001361 sget-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/MessageChatHeader;→b Lcom/read
;- str.accountConfigLoaded:
0x001d8ccb ~ 64001361 sget-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/MessageChatHeader;→b Lcom/read
0x001d8cdd ~ 56001461 sget-byte v0, v0, Lcom/readdle/spark/ui/threadviewer/nodes/InvitationNode$b;→f Ljava/
;- str.accountConfiguration:
0x001d8e05 ~ 6e0023616363 invoke-virtual {}, Ld/a/a/a/d/s0/b/c.d()Lcom/readdle/spark/ui/messagelist/actions/Mess
0x001d8e19 ~ 6e0023616363 invoke-virtual {}, Ld/a/a/a/d/s0/b/c.d()Lcom/readdle/spark/ui/messagelist/actions/Mess
;- str.accountConfiguration.accountAddress:
0x001d8e1b ~ 7300 invalid
0x001d8e3e ~ 7300 invalid
;- str.accountConfigurationIsLANBased:
0x001d8e40 ~ 64001f61 sget-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/InvitationRequestDialogNode;→a
0x001d8e5e ~ 64001f61 sget-byte v0, Lcom/readdle/spark/ui/threadviewer/nodes/InvitationRequestDialogNode;→a
;- str.accountConfigurationIsReachable:
0x001d8e60 ~ 65002e61 sget-char v0, Lcom/readdle/spark/ui/threadviewer/nodes/MessageChatInlineImageNode$c;→
0x001d8e7f ~ 65002e61 sget-char v0, Lcom/readdle/spark/ui/threadviewer/nodes/MessageChatInlineImageNode$c;→
;- str.accountConfigurationIsReachable_viaGoogleDNS:
0x001d8e81 ~ 29001561 goto/16 str.com.facebook.platform.action.request.LIKE_DIALOG Configuration.r32MailAc
0x001d8e8f ~ 29001561 goto/16 str.com.facebook.platform.action.request.LIKE_DIALOG Configuration.r32MailAc
;- str.accountConfigurations:
0x001d8e91 ~ 7300 invalid
0x001d8e93 ~ 7300 invalid
;- str.accountDescription:
0x001d8e95 ~ 6e000c616363 invoke-virtual {}, Ld/a/a/a/d/h0.isRunning()Z ; 0x610c
0x001d8e9d ~ 6e000c616363 invoke-virtual {}, Ld/a/a/a/d/h0.isRunning()Z ; 0x610c
;- str.accountEvent:
0x001d8e9f ~ 6e000c616363 invoke-virtual {}, Ld/a/a/a/d/h0.isRunning()Z ; 0x610c
```

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

```
;- str.https://twitter.com.Neat.Bytes:
0x00202f0f .string "https://twitter.com/Neat.Bytes" ; len=30
0x00202f2d ~ 7300 invalid
;- str.https://www.facebook.com/adnw.logging:
0x00202f2f .string "https://www.facebook.com/adnw.logging/" ; len=38
0x00202f55 ~ 2f003968 cml-double v0, v57, v104
;- str.https://www.facebook.com/pages/NeatBytes/1516789311908389:
0x00202f57 .string "https://www.facebook.com/pages/NeatBytes/1516789311908389" ; len=57
0x00202f90 ~ 39002868 if-nez v0, 0x0020ffe0
;- str.https://www.googleapis.com/auth/calendar:
0x00202f92 .string "https://www.googleapis.com/auth/calendar" ; len=40
0x00202fba ~ 72002e687474 invoke-interface {}, Levidence/census/seminar/IXuYpQpFpJeSeDzKd.b(Landroid/content/Cont
;- str.https://www.googleapis.com/auth/userinfo.email:
0x00202fbc .string "https://www.googleapis.com/auth/userinfo.email" ; len=46
0x00202fea ~ 6c003068 sput-char v0, Levidence/census/process/WReToPyNrNrYhHaIlSxPfKhUeAiAtJwKgBfXlXkSkPuMuHnS
;- str.https://www.googleapis.com/auth/userinfo.profile:
0x00202fec .string "https://www.googleapis.com/auth/userinfo.profile" ; len=48
0x0020301c ~ 65002a68 sget-char v0, Levidence/census/process/WReToPyNrNrYhHaIlSxPfKhUeAiAtJwKgBfXlXkSkPuMuHnS
;- str.https://www.googleapis.com/oauth2/v4/token:
0x0020301e .string "https://www.googleapis.com/oauth2/v4/token" ; len=42
0x00203048 ~ 6e0017687474 invoke-virtual {}, Levidence/census/seminar/FAwBjNpHnSm.e(Ljava/lang/String;Ljava/lang/
;- str.https://www.mxplayer.in:
0x0020304a .string "https://www.mxplayer.in" ; len=23
0x00203061 ~ 6e0022687474 invoke-virtual {}, Levidence/census/seminar/FAwBjNpHnSm.newFile(Ljava/lang/String;IJJ)L
;- str.https://www.reddit.com_r_NeatBytes:
0x00203063 .string "https://www.reddit.com/r/NeatBytes" ; len=34
```

Uygulama geliştiricisinin yukarıdaki koda da görüldüğü gibi

<https://twitter.com/Neat.Bytes> ,
<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 f0Var = new fo(oAuthBrowserActivity);
    ArrayList arrayList = new ArrayList(Arrays.asList("Email", "login-username", "i0116", "profileIdentifier", "identifierId"));
    if (oAuthBrowserActivity.b.equals(OAuthModule.HOTMAIL_REDIRECT)) {
        arrayList.add("displayName");
        z.H(oAuthBrowserActivity.h, arrayList, Arrays.asList("value", "title"), f0Var);
        return;
    }
    z.H(oAuthBrowserActivity.h, arrayList, Collections.singletonList("value"), f0Var);
}

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(), 33);
    this.j.setText(spannableString);
    ImageView imageView = this.l;
    if (!str.equals("https://")) {
        i = 8;
    }
}

```