

# Cerberus Analizi

written by Mert SARICA | 1 December 2020

If you are looking for an English version of this article, please visit [here](#).

2020 yılının Şubat ayında cep telefonuma beni oldukça şüphelendiren bir SMS geldi. Mesajda yer alan [https://ko\[.\]tc/hediyekazani](https://ko[.]tc/hediyekazani) web adresini ziyaret ettiğimde [http://www-bedavainternethediyeuygulama\[.\]com](http://www-bedavainternethediyeuygulama[.]com) web adresine yönlendirildiğimi farkettim. SMS'in gelmesinden kısa bir süre sonra web sitesini tekrar ziyaret ettiğimde bu defa da sitedeki görsellerin değişmiş olduğunu gördüm. "Şüphe, siber güvenlik araştırmacısının kamçısıdır" diyerek bu durum ile yakından ilgilenmeye karar verdim.

18:07

70%



+90 212 985 05 78



14:41

SN; ██████████ SARICA Tüm operatorlerde  
gecerli 1000 DK, 5 GB INTERNET 3 Ay  
bedava! Hemen uygulamayı indir, kur ve  
kazan; <https://ko.tc/hediyekazani>  
B187

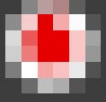
|





thediyeliuygulama.com

16



## 5G Uygulaması 5GB İnternet Veriyor



1)5G Uygulaması İnternet  
Kazandırıyor 5GB İnternet  
Kazanmak İçin Hemen  
İndir

İndir



Bu türden dosyalar cihazınıza zarar  
verebilir. Yine de 5GBeta.apk adlı  
dosyayı saklamak istiyor musunuz?



İptal

Tamam





## Tüm Operatörler

5GB İNTERNET VE 5GB KONUŞMA



## 5G Beta Test

5G Uygulamasını İndirip  
Yükleyen Tüm Operatör  
Müşterilerine 5GB İnternet  
Hediye Sizde Hemen İndirin  
Yükleyin 5GB İnterneti  
Hemen Kazanın

Uygulamayı  
Yükle



Web sitesinden sunulan 5GBeta.apk dosyasını indirip, mobil zararlı yazılım analizi amacıyla kullanılan o meşhur Koodous web uygulamasına yüklediğimde analiz başarısızlıkla sonuçlandı. Ardından bu uygulamayı VirusTotal web uygulamasına yüklediğimde her ne kadar bunun bir bankacılık zararlı uygulaması olduğuna dair bir ipucu (Cerberus) ile karşılaşsam da davranışsal analiz çıktısında komuta kontrol merkezinin adresini göremedim. Aklıma takılan sorulara yanıt bulamadığım için iş başa düştü ve 5GBeta.apk uygulamasını Genymotion Android öykünücüsü (emulator) ile hızlıca dinamik olarak analiz etmeye karar verdim.

Zararlı uygulamayı Android'e yükler yüklemesiz kötü emellerini gerçekleştirmek için ilk iş olarak izinleri teker teker istemeye başladı. İzinleri aldıktan ve yükleme işlemi başarıyla tamamlandıktan sonra simgesini gizleyip, arka planda çalışmaya ve komuta kontrol merkezi ile olan kryll[.]ug (8[.]208.19.185) web adresi ile haberleşmeye başladı. 8[.]208.19.185 ip adresini VirusTotal üzerinden arattığımda pasif DNS bilgilerinden hiç de masum olmadığı net olarak görülüyordu.

### Accessibility

Accessibility shortcut  
No service selected

#### Downloaded services

 5G\_   
OFF

 ClockBack  
OFF

 Magnification  
OFF

 QueryBack  
OFF


#### Screen readers

Text-to-speech output

#### Display

Font size  
Default

Display size  
Default

 Magnification  
Off

Large mouse pointer

Enable 5G\_Turkcell

#### Interaction controls

Click after pointer stops moving



5G\_

Off

No description provided.

**Use 5G\_ ?**

5G\_ needs to:

- **Observe your actions**  
Receive notifications when you're interacting with an app.
- **Retrieve window content**  
Inspect the content of a window you're interacting with.

CANCEL OK



### Accessibility

Accessibility shortcut  
No service selected

#### Downloaded services

5G\_   
OFF

ClockBack   
OFF

Magnification   
OFF

QueryBack   
OFF

#### Screen readers

Text-to-speech output

#### Display

Font size  
Default

Display size  
Default

Magnification   
Off

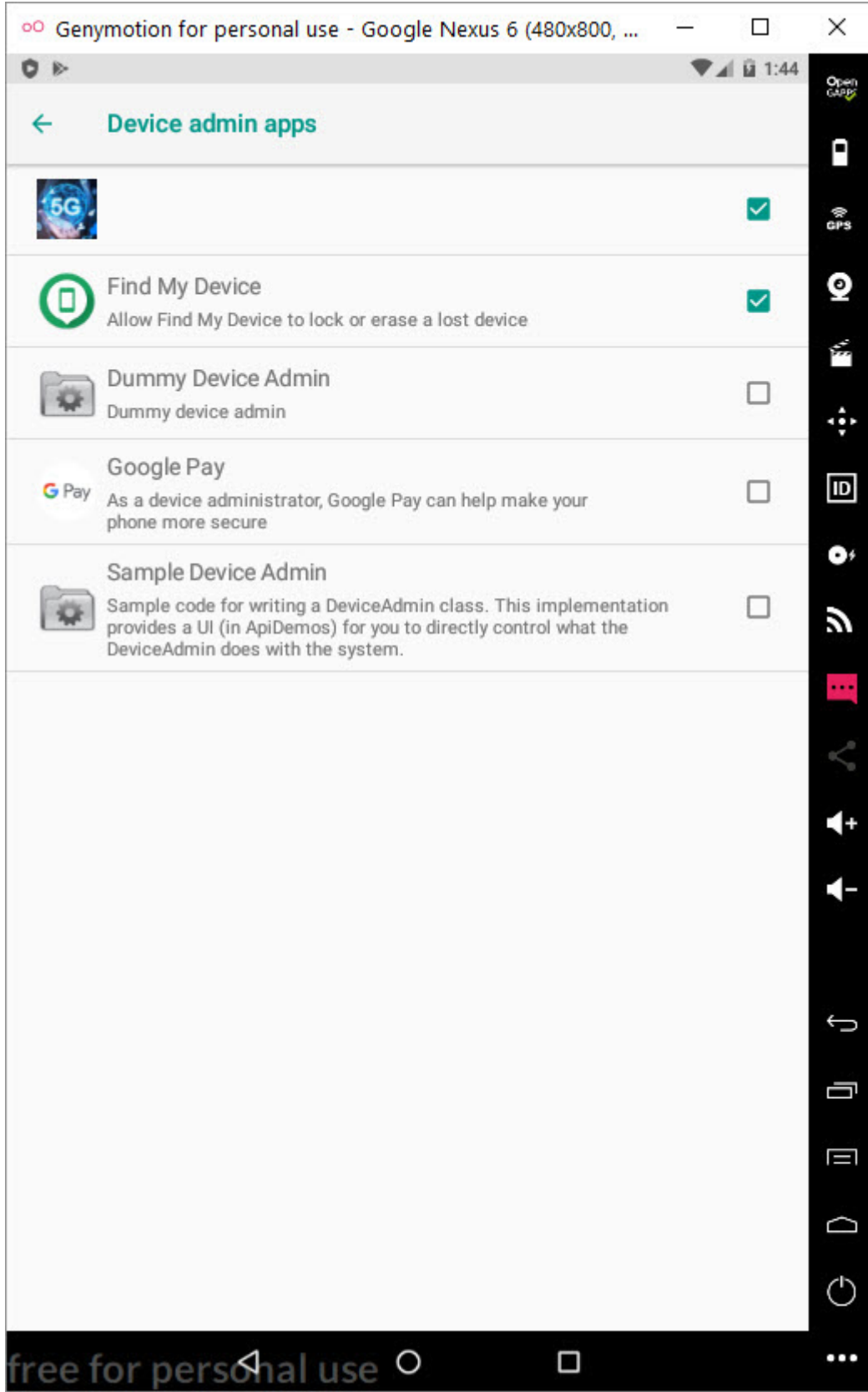
Large mouse pointer

Enable 5G\_

#### Interaction controls

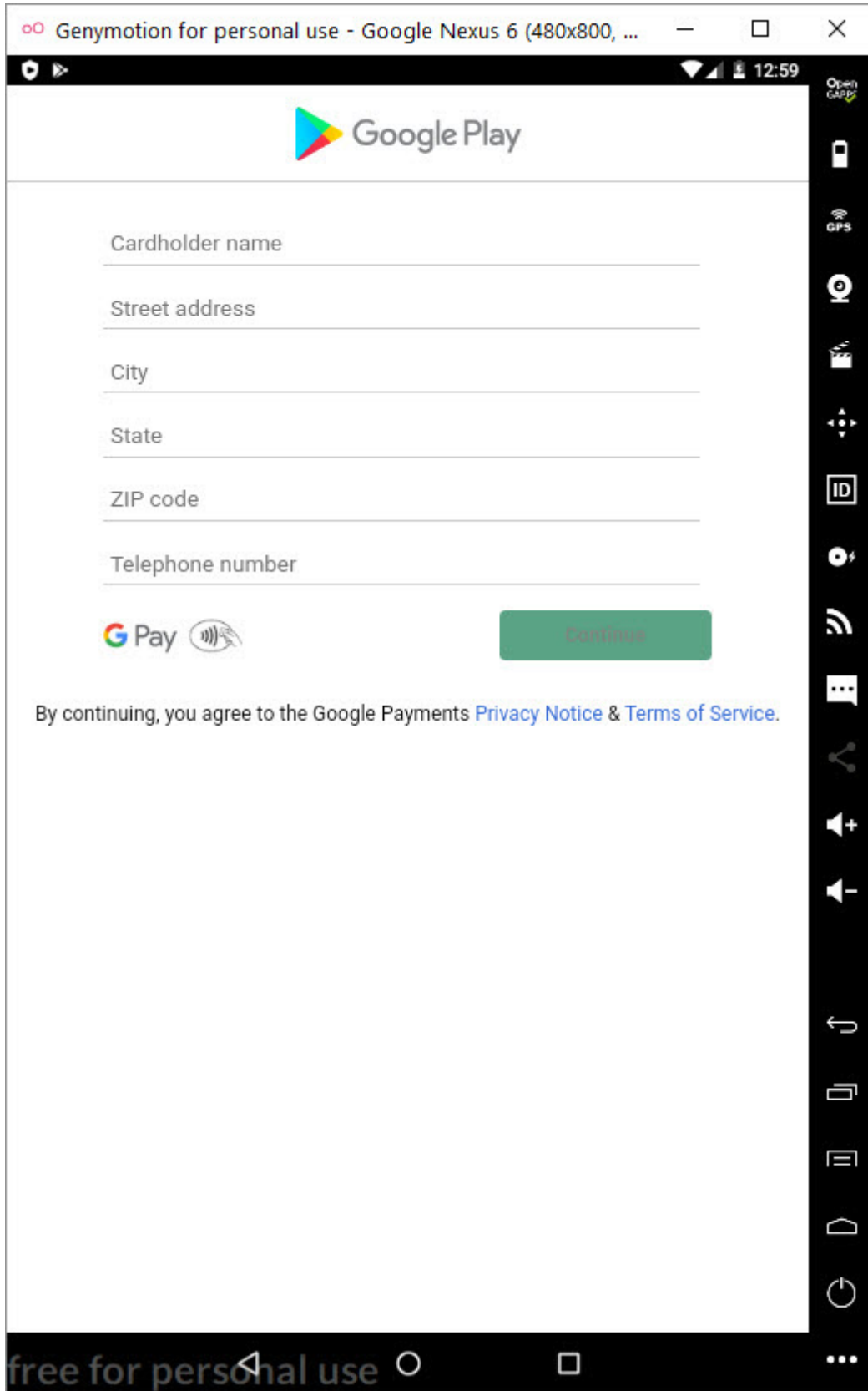
Click after pointer stops moving





Sanal Android işletim sistemimde herhangi bir bankacılık uygulaması yüklü olmadığı için karşıma kredi kartı bilgimi çalmak üzere oluşturulmuş Google Play ekranı çıktı. Test için oluşturulan 16 haneli bir kredi kartı numarası girdiğimde kaydetme butonunun (SAVE) etkinleşmediğini gördüm. Kredi kartı hanesini 19 yaptığımda SAVE butonu aktif hale geldi. Muhtemelen art niyetli kişi, 3 haneli CVV2 numarasının kontrolünü kredi kartı numarasının girildiği

forma yönelik yapmış ve böyle bir hata ortaya çıkmıştı. Girdiğim tüm bilgilerin komuta kontrol merkezine şifreli olarak gittiğini gördükten sonra şifreleme anahtarının da peşine düşmeye karar verdim.





Osman|

Turkey

Istanbul

Kadikoy

34878


+902163534466



Continue

By continuing, you agree to the Google Payments [Privacy Notice](#) & [Terms of Service](#).



 [Test Generator / Validator](#)

Who do not carry at least one credit card (CC) in their wallet nowadays? Few. Especially with the boom of online shopping, a credit card is a must buying anything online. One of the most popular CC brands is from a company called VISA. Almost every bank and small-mom shop out there try to issue a VISA card to their customers; whether it's a credit, debit, prepaid, or just a charge card.

### Valid VISA Credit Card Generator that Work

<b>Generator:</b>	Test VISA Credit Cards
<b>Issuing network:</b>	Visa
<b>Card number:</b>	4510 9658 3456 0735
<b>Pin:</b>	1537
<b>Name:</b>	Josh Lunar
<b>Address:</b>	9007 Mountaintrail Way
<b>Country:</b>	France
<b>CVV:</b>	938
<b>Expiration date:</b>	11 / 2022

[Generate VISA Credit Card](#)



Take a look at the legendary [VISA company](#) if you don't know who they are duh.

People hesitate to share their VISA CC details for an online purchase. Those working as developers or quality assurance engineers for software companies may need to have thousands of credit card numbers to feed through their applications. They need a tool to generate these kinds of valid VISA card numbers in bulk. They should use a [VISA Credit Card Generator 2020](#) for getting these test numbers regularly.





VISA

4510 9658 3456 0735 333|

Invalid card number

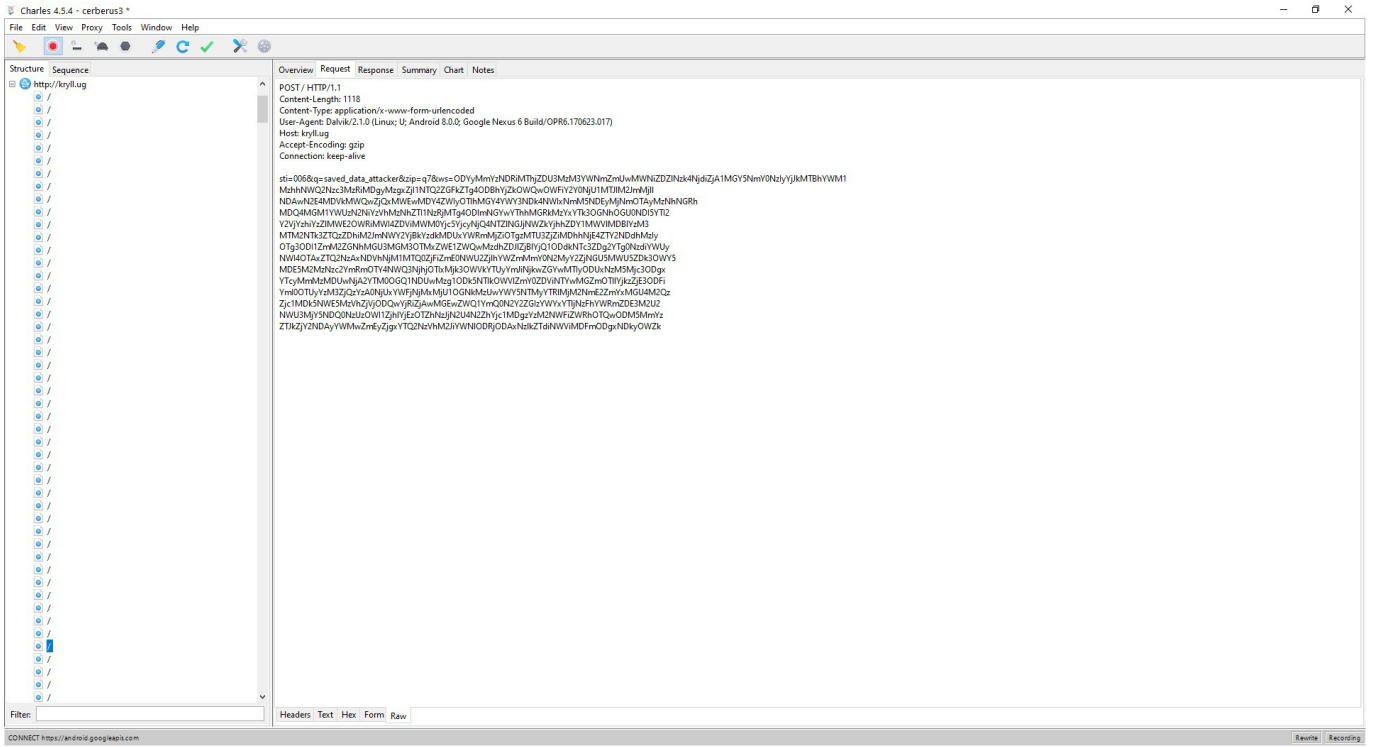
11 / 22



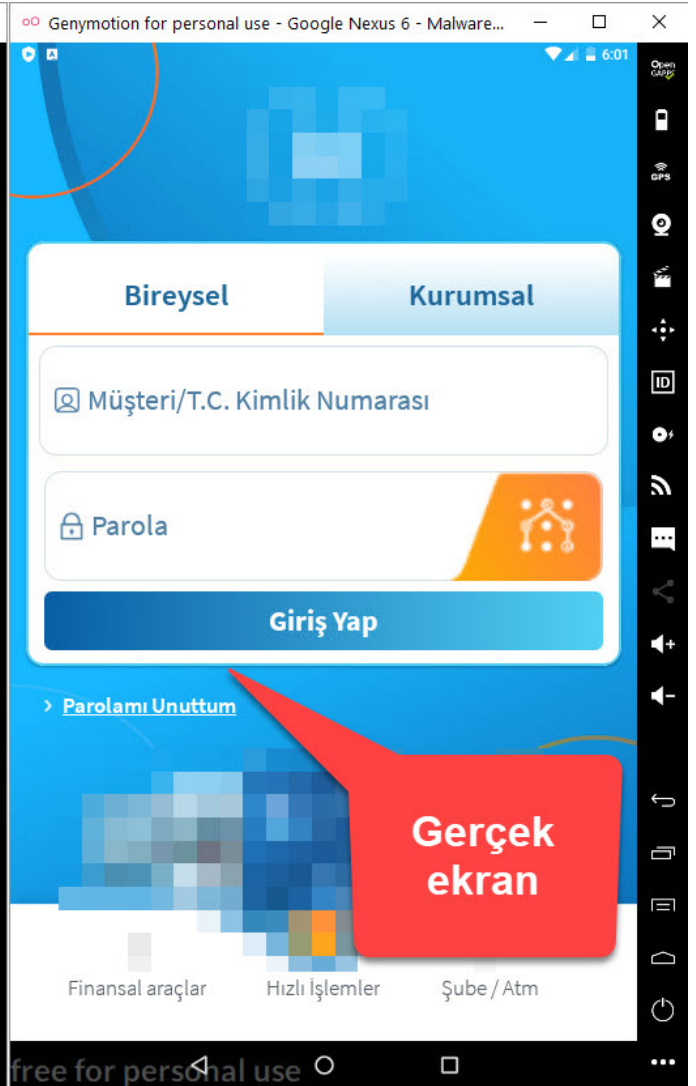
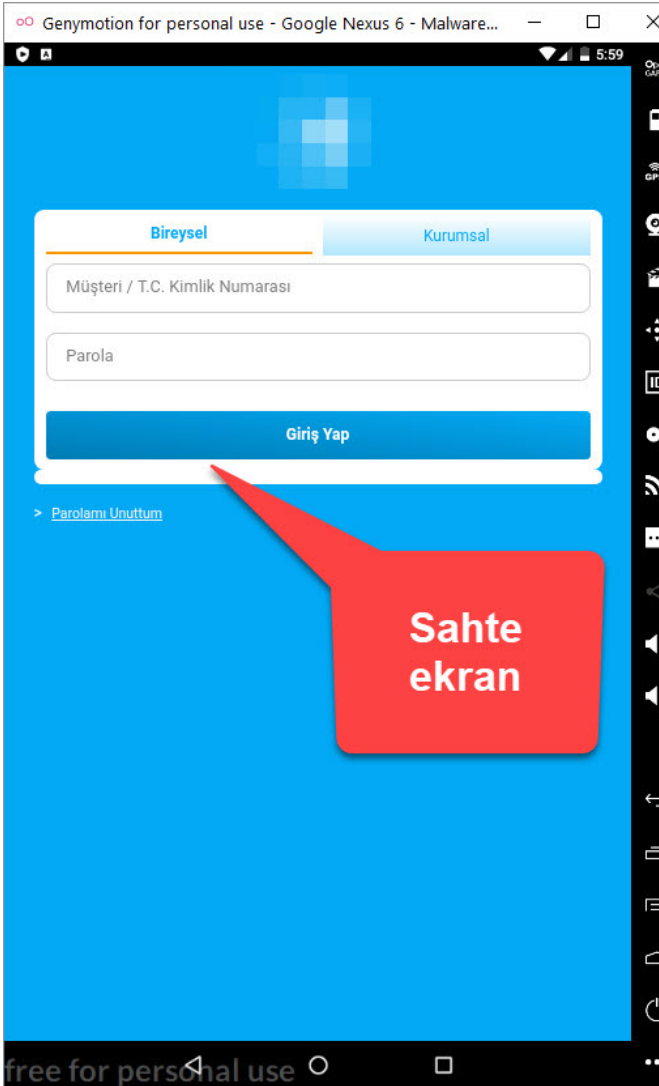
Save

By continuing, you agree to the Google Payments [Privacy Notice](#) & [Terms of Service](#).





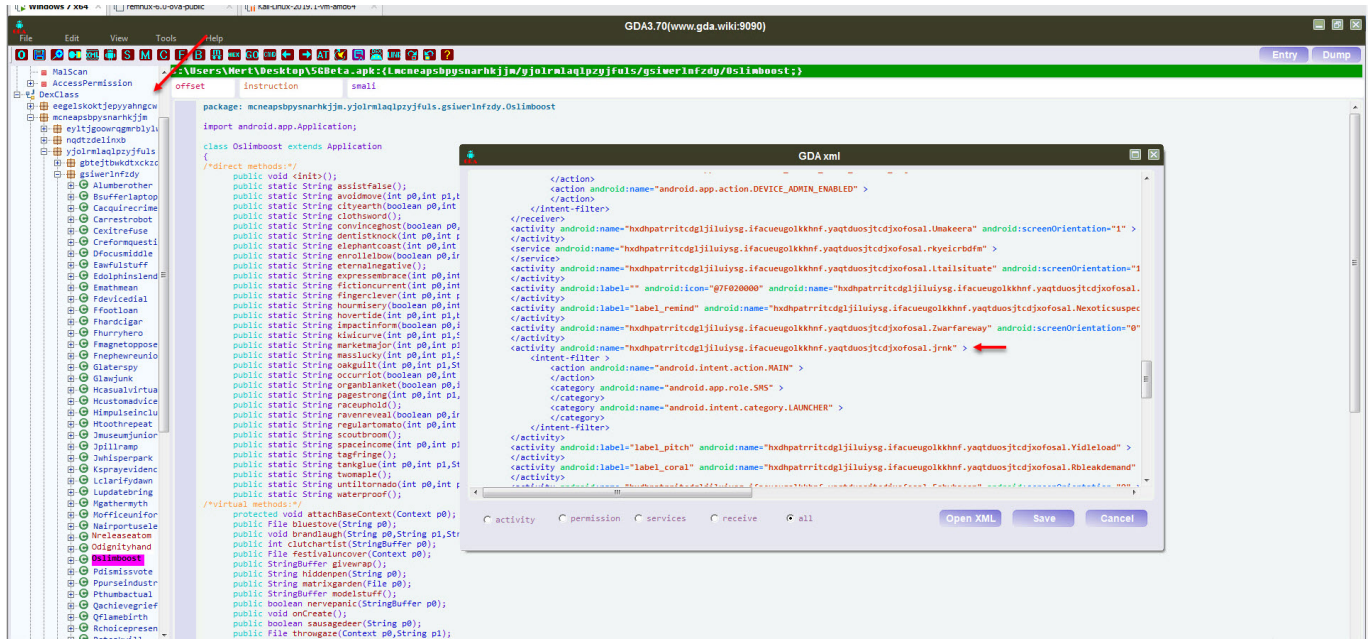
Şifreleme anahtarından önce zararlı uygulamanın bankacılık bilgilerini çalıp çalmadığını teyit etmek için sanal sistemim üzerine 10 tane bankanın mobil uygulamasını yükledim ve teker teker çalıştırmaya başladım. Yaptığım testler sonucunda zararlı uygulama, hedef aldığı mobil bankacılık uygulaması çalıştığı anda bankacılık uygulamasının giriş ekranının üzerine sahte bir ekran açarak kullanıcı tarafından ekrana girilen tüm bilgileri çalabiliyordu.



```
2066 02-10 17:59:36.538 384 384 D gps_vh0e84: gps navigation has stopped
2067 02-10 17:59:36.538 464 495 I GmsLocationProvider: WakeLock released by handleMessage(SET_REQUEST, 0, com.android.server.location.GmsLocationProvider@8a9e889c)
2068 02-10 17:59:36.547 1207 1303 E EGL_emulation: tid 1303: eglSurfaceAttrib(1210): error 0x3009 (EGL_BAD_MATCH)
2069 02-10 17:59:36.547 1207 1303 W OpenGLRenderer: failed to set EGL_RENDER_BUFFER on surface 0x2a722050, error=EGL_BAD_MATCH
2070 02-10 17:59:36.722 368 368 E EGL_emulation: tid 368: eglCreateSyncNR(1881): error 0x3004 (EGL_BAD_ATTRIBUTE)
2071 02-10 17:59:37.050 1207 1303 W OpenGLRenderer: Incorrectly called buildLayer on View: ShortcutAndWidgetContainer, destroying layer...
2072 02-10 17:59:37.050 1207 1303 W OpenGLRenderer: Incorrectly called buildLayer on View: ShortcutAndWidgetContainer, destroying layer...
2073 02-10 17:59:37.356 464 474 I syzote : Background concurrent copying GC freed 71099(NB) AllocSpace objects, 10(26KB) LOS objects, 424 free, 11MB/20MB, paused 1.031ms total 726.501ms
2074 02-10 17:59:42.183 4341 4360 W syzote : Skipping duplicate class check due to unrecognized classloader
2075 02-10 17:59:42.237 4341 5476 W ResourceType: For resource 0x7f060007, entry index(7) is beyond type entryCount(2)
2076 02-10 17:59:42.237 4341 5476 W ResourceType: Failure getting entry for 0x7f060007 (e=5 e=7) (error -75)
2077 02-10 17:59:42.237 4341 5476 E GooglePlayServicesDsl: The Google Play services resources were not found. Check your project configuration to ensure that the resources are included.
2078 02-10 17:59:44.693 464 495 E memtrack: Couldn't load memtrack module
2079 02-10 17:59:44.693 464 495 W android.os.Debug: failed to get memory consumption info: -1
2080 02-10 17:59:44.693 464 497 W AlarmManager: Suspiciously short interval 12000 millis: expanding to 60 seconds
2081 02-10 17:59:44.694 4341 4352 I syzote : Background concurrent copying GC freed 83597(NB) AllocSpace objects, 11(220KB) LOS objects, 509 free, 9MB/19MB, paused 156us total 152.944ms
2082 02-10 17:59:44.693 4341 5477 W syzote : Skipping duplicate class check due to unrecognized classloader
2083 02-10 17:59:44.693 5332 5347 W syzote : Checksum mismatch for dex base.apk
2084 02-10 17:59:49.454 464 1205 I ActivityManager: START u0 (act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=com.bank/.../ui.beforelogin.nonbanking.NonBankingActivity bnds=[395,244][473,374] from uid 10015)
2085 02-10 17:59:50.054 4341 5480 W ResourceType: Skipping duplicate class check due to unrecognized classloader
2086 02-10 17:59:50.054 4341 5480 W ResourceType: For resource 0x7f060007, entry index(7) is beyond type entryCount(2)
2087 02-10 17:59:50.054 4341 5480 W ResourceType: Failure getting entry for 0x7f060007 (e=5 e=7) (error -75)
2088 02-10 17:59:50.054 4341 5480 E GooglePlayServicesDsl: The Google Play services resources were not found. Check your project configuration to ensure that the resources are included.
2089 02-10 17:59:50.241 1207 1207 I Choreographer: Skipped 47 frames! The application may be doing too much work on its main thread.
2090 02-10 17:59:50.284 313 313 I main : type=1400 audit(0.0:35154): avc: denied { read } for path="/dev/socket/syzote" scontext=u:r:syzote:s0 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
2091 02-10 17:59:50.284 313 313 I main : type=1400 audit(0.0:35155): avc: denied { getattr } for path="/dev/socket/[14125]" dev="socket" ino=14125 scontext=u:r:syzote:s0 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
2092 02-10 17:59:50.300 313 313 I main : type=1400 audit(0.0:35156): avc: denied { write } for path="/dev/socket/syzote" scontext=u:r:syzote:s0 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
2093 02-10 17:59:50.305 464 1196 I ActivityManager: Start proc 5481:com.bank/.../ui.beforelogin.nonbanking.NonBankingActivity
2094 02-10 17:59:50.313 464 495 E memtrack: Couldn't load memtrack module
2095 02-10 17:59:50.313 464 495 W android.os.Debug: failed to get memory consumption info: -1
2096 02-10 17:59:50.323 5481 5481 W syzote : Unexpected CPU variant for X86 using defaults: x86
2097 02-10 17:59:50.856 400 400 I HlsMpegDumper: Loaded [com.android.vending:libdexopt:10091]
2098 02-10 17:59:50.856 400 400 I Healthd : type=1400 audit(0.0:35157): avc: denied { read } for name="capacity" dev="fuse" ino=8 scontext=u:r:healthd:s0 tcontext=u:object_r:fuse:s0 tclass=file permissive=1
2099 02-10 17:59:50.856 400 400 I Healthd : type=1400 audit(0.0:35158): avc: denied { open } for path="/dev/pipe/battery/BAT0/capacity" dev="fuse" ino=8 scontext=u:r:healthd:s0 tcontext=u:object_r:fuse:s0 tclass=file permissive=1
2100 02-10 17:59:50.856 400 400 I Healthd : type=1400 audit(0.0:35159): avc: denied { getattr } for path="/dev/pipe/battery/BAT0/capacity" dev="fuse" ino=8 scontext=u:r:healthd:s0 tcontext=u:object_r:fuse:s0 tclass=file permissive=1
2101 02-10 17:59:50.946 5481 5496 I vndksupport: sgal namespace is not configured for this process. Loading /system/lib/egl/libEGL_emulation.so from the current namespace instead.
2102 02-10 17:59:50.946 5481 5496 I vndksupport: sgal namespace is not configured for this process. Loading /system/lib/egl/libEGL_emulation.so from the current namespace instead.
2103 02-10 17:59:51.028 5481 5481 I MultiDex: VM with version 2.1.0 has multidex support
2104 02-10 17:59:51.028 5481 5481 I MultiDex: Installing application
2105 02-10 17:59:51.028 5481 5481 I MultiDex: VM has multidex support. MultiDex support library is disabled.
2106 02-10 17:59:51.116 5481 5481 D FirebaseApp: com.google.firebase.auth.FirebaseAuth is not linked. Skipping initialization.
2107 02-10 17:59:51.147 5481 5496 I vndksupport: sgal namespace is not configured for this process. Loading /system/lib/egl/libGLESv1_CM_emulation.so from the current namespace instead.
2108 02-10 17:59:51.209 5481 5481 D FirebaseApp: com.google.firebase.crash.FirebaseCrash is not linked. Skipping initialization.
2109 02-10 17:59:51.240 5481 5481 I FA : App measurement is starting up, version: 11020
2110 02-10 17:59:51.240 5481 5481 I FA : To enable debug logging run: adb shell setprop log.tag.FA VERBOSE
2111 02-10 17:59:51.258 5481 5481 I FA : To enable faster debug mode event logging run:
2112 02-10 17:59:51.258 5481 5481 I FA : adb shell setprop debug.firebase.analytics.*
2113 02-10 17:59:51.273 5481 5481 I FirebaseInitProvider: FirebaseApp initialization successful
2114 02-10 17:59:51.289 464 1182 I ActivityManager: START u0 (flg=0x10000000 cmp=com.bank/.../ui.beforelogin.nonbanking.NonBankingActivity bnds=[395,244][473,374] from uid 10015)
2115 02-10 17:59:51.492 312 312 I main : type=1400 audit(0.0:35160): avc: denied { getprop } for path="/dev/socket/fmarkd" scontext=u:r:netd:s0 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
2116 02-10 17:59:51.492 312 312 I main : type=1400 audit(0.0:35161): avc: denied { read } for path="/dev/socket/fmarkd" scontext=u:r:netd:s0 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
2117 02-10 17:59:51.492 312 312 I main : type=1400 audit(0.0:35162): avc: denied { write } for path="/dev/socket/[71172]" dev="socket" ino=17172 scontext=u:r:netd:s0 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
2118 02-10 17:59:51.496 5481 5501 D NetworkSecurityConfig: No Network Security Config specified, using platform default.
2119 02-10 17:59:51.698 5481 5481 I CrashlyticsCore: Initializing Crashlytics 2.3.17.dev
```

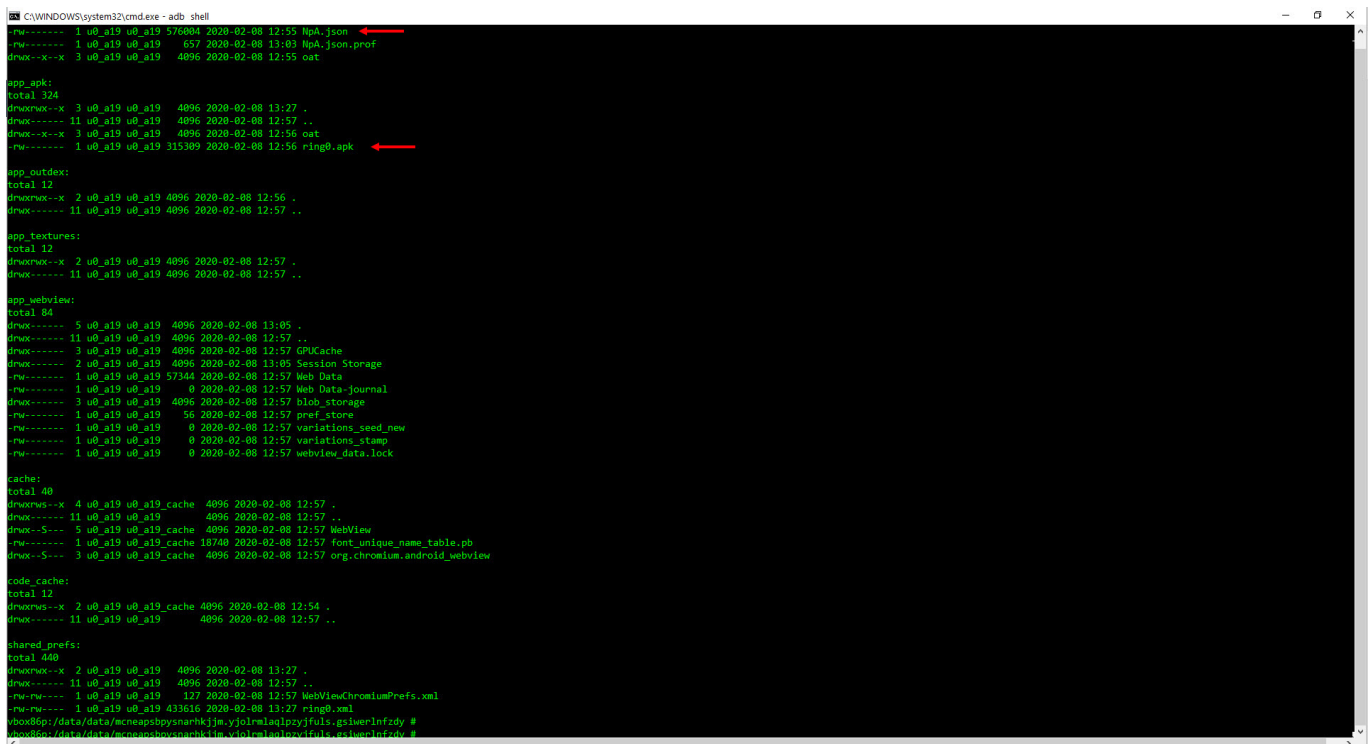
Şifreleme anahtarını bulmak için GDA aracı ile 5GBeta.apk uygulamasını kaynak kodunu çevirip uygulama ile ilgili temel bilgilerin yer aldığı AndroidManifest.xml dosyasına baktığımda, zararlı uygulama başlatıldığında ilk çalışacak olan MainActivity sınıfı ile kaynak kodu arasındaki sınıfların

farklı olduğunu gördüm. Bu da zararlı kod bloğunun dinamik olarak çalışma esnasında yüklendiğine işaret ediyordu.



Zararlı uygulamanın yüklü olduğu

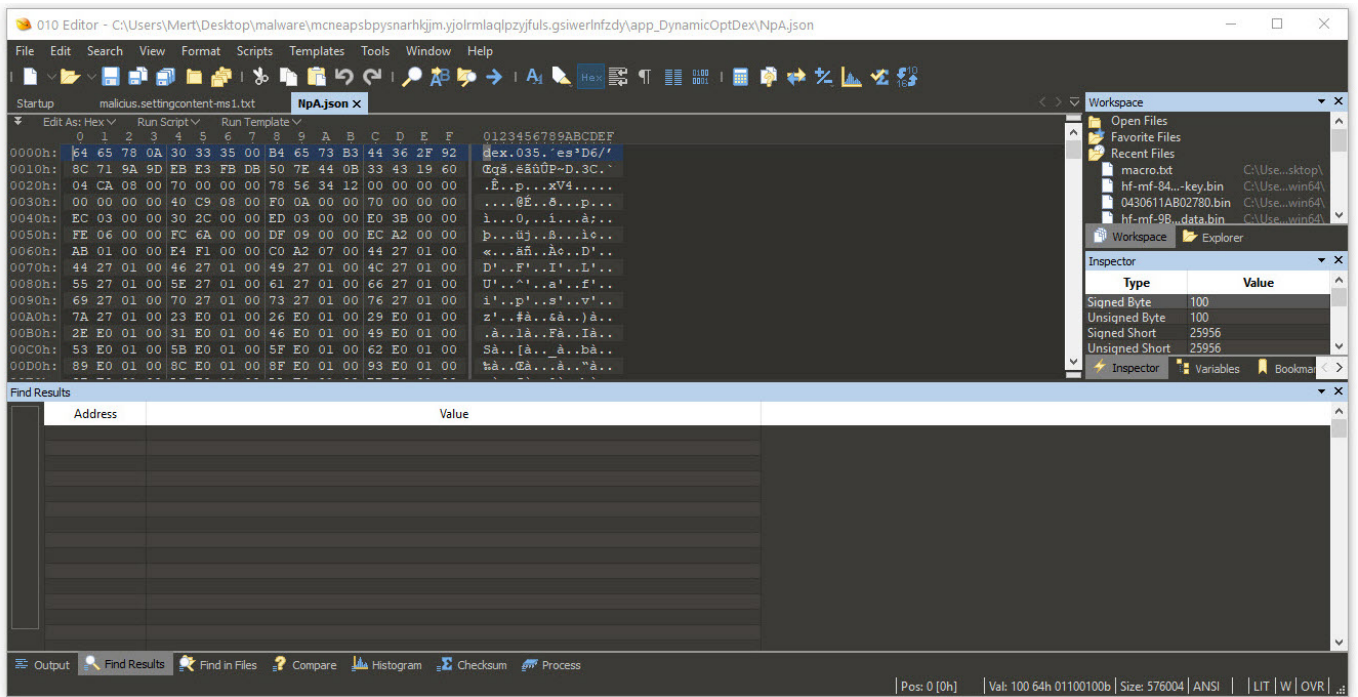
/data/data/mcneapsbypsnsarhkjkm.yjolrmlaqlpzyjfuls.gsiwerlnfzdy klasörüne baktığımda boyutu büyük olan ring0.apk ve NpA.json dosyaları dikkatimi çekti. NpA.json dosyasının aslında bir DEX dosyası olduğunu öğrenip jadx aracı ile kaynak koduna çevirdiğim de AndroidManifest.xml dosyasında yer alan MainActivity sınıfı ile karşılaşmış oldum.





Şifrelenmiş karakter dizilerini incelediğimde f sınıfının şifreleri çözmekten sorumlu olduğunu öğrendim. Bunu yapmak için şifreli karakter dizisinin RC4 anahtarı olan ilk 12 karakterini alıp, BASE64 ile çözülen geri kalan karakterlerin şifresini bu anahtar sayesinde çözüyordu. (Örnek şifreli karakter dizisi

mjwpnqfxpgweNDNiYjQ2M2JiNzMxNzE30WM50DRjZmI1ZWfKyzYxMjY4NDE4YTY3MDVhNTZlZGZlMGhNmQ1ZDVLmzU2MTE5NWU5YjYyNw== ise RC4 şifreleme anahtarı mjwpnqfxpgwe değeri oluyor. Bu anahtar ile geri kalan şifreleri karakterleri (NDNiYjQ2M2JiNzMxNzE30WM50DRjZmI1ZWfKyzYxMjY4NDE4YTY3MDVhNTZlZGZlMGhNmQ1ZDVLmzU2MTE5NWU5YjYyNw==) BASE64 ile çözdükten sonra şifreleme anahtarı sayesinde çözüyor) Ben de tüm şifreleri karakter dizilerini çözmek için f sınıfında yer alan Java kodlarını compilejava.net sitesinden kolaylıkla faydalanarak çözebildim.









```
Online Java IDE (javac 1.8.0_201) x +
compilejava.net
Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mertsarica...
Other bookmarks

41 public final byte[] b(byte[] barr) {
42     byte[] barr2 = new byte[barr.length];
43     for (int i = 0; i < barr.length; i++) {
44         this.b = (this.b + 1) % 256;
45         int i3 = this.c;
46         int[] iarr = this.a;
47         this.c = (i2 + iarr[i3]) % 256;
48         a[i3, this.c, iarr];
49         int[] iarr2 = this.a;
50         barr2[i] = (byte) (iarr2[(iarr2[this.b] + iarr2[this.c]) % 256] ^ barr[i]);
51     }
52     return barr2;
53 }
54 }
55 }
56 // one class needs to have a main() method
57 public class HelloWorld {
58 {
59     public static String a(String str) {
60         try {
61             // return new String(new f(str.substring(0, 12).getBytes()), a(b(new String(Base64.getDecoder().decode(str.substring(12), 0), "UTF-8"))));
62             return new String(new f(str.substring(0, 12).getBytes()), a(b(new String(Base64.getDecoder().decode(str.substring(12))))));
63         } catch (Exception unused) {
64             return "";
65         }
66     }
67 }
68 }
69 private static byte[] b(String str) {
70     int length = str.length();
71     byte[] barr = new byte[(length / 2)];
72     for (int i2 = 0; i2 < length; i2 += 2) {
73         barr[i2 / 2] = (byte) ((Character.digit(str.charAt(i2), 16) << 4) + Character.digit(str.charAt(i2 + 1), 16));
74     }
75     return barr;
76 }
77 }
78 public static void main(String[] args) {
79     // System.out.println("cccxdsjycolv4j1j1k5NDVhT11N4hY0DcxYyZy7hZm1z2Y4Nz3z2Dv1MD0Mh1kYwI3H2FN0YxZJUS2uRHHwIh5d1HTHzvA");
80 }
81 System.out.println(a("stxubcehoobwM2h2#Shz15h1Y2Y12N1I4Y3Q3ZDkyYyYUu3NGUxWg2H5Y1N2U3N7hWjEZYUzN1LVFkZTThOD1wVw=="));
82 System.out.println(a("p0ep1um100h7m2h4m3WbYzawW131Y8wZ1h4j1h1g003k0H0220z2Dv1zVz5w4WbW1h1z131ng5S00R1ngWw=="));
83 System.out.println(a("t0h3jknf0f4y2qW1T2KvY21NDU10MkVxZyZ1B1h1E5R1zgxvz0ZDc500kz2hEwVwR1zJwM1Q5YThJNwH2T11y1hdZjz1"));
84 }
85 }
86 }
87 }
88 }
89 }
90 }
91 }
92 }
93 }
94 }
95 }

(command line arguments) COMPILER & EXECUTE PASTE SOURCE DOWNLOAD ZIP default
Successfully compiled /tmp/java_xBFGST/f.java
Successfully compiled /tmp/java_xBFGST/HelloWorld.java -- main method
stl=0058q=1; attacker&zip=q&us=
stl=0048i=1; info_device&zip=q&us=
stl=0058q=new_device&zip=q&us=
```

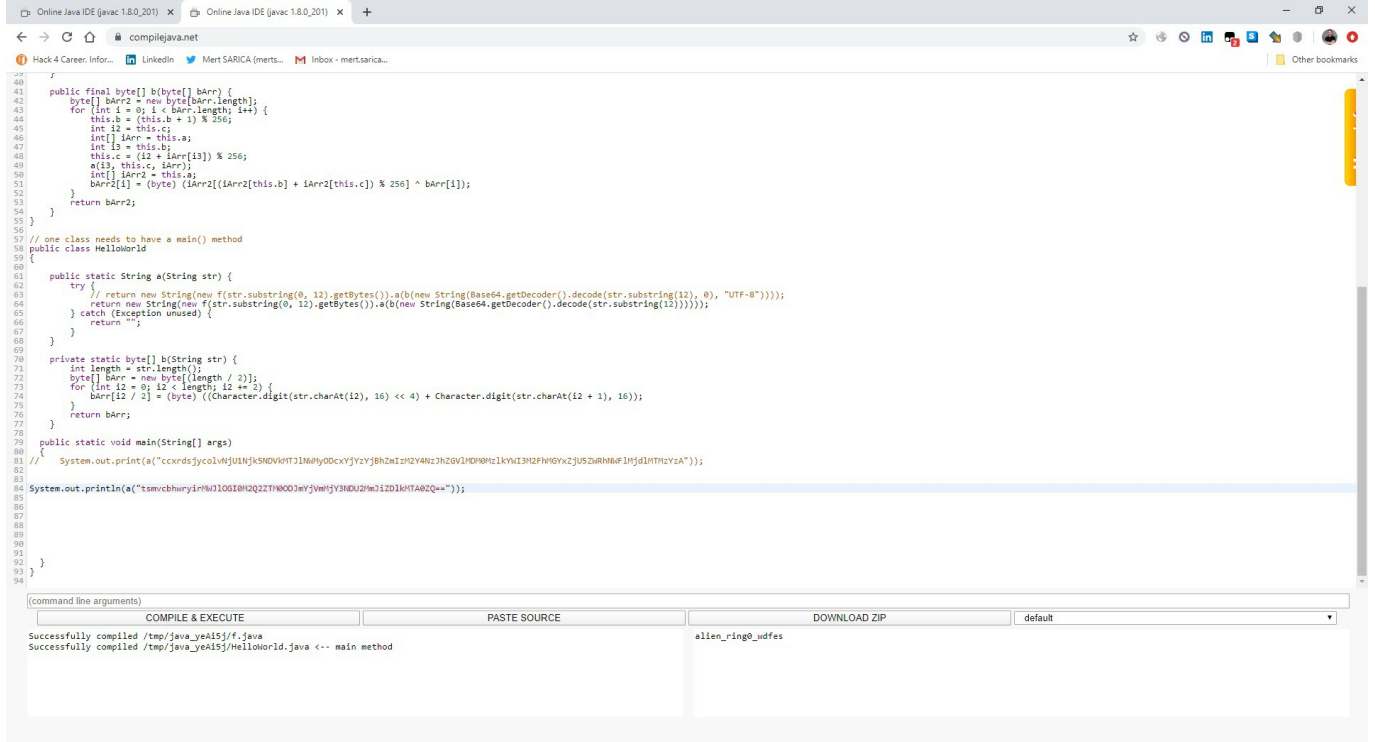
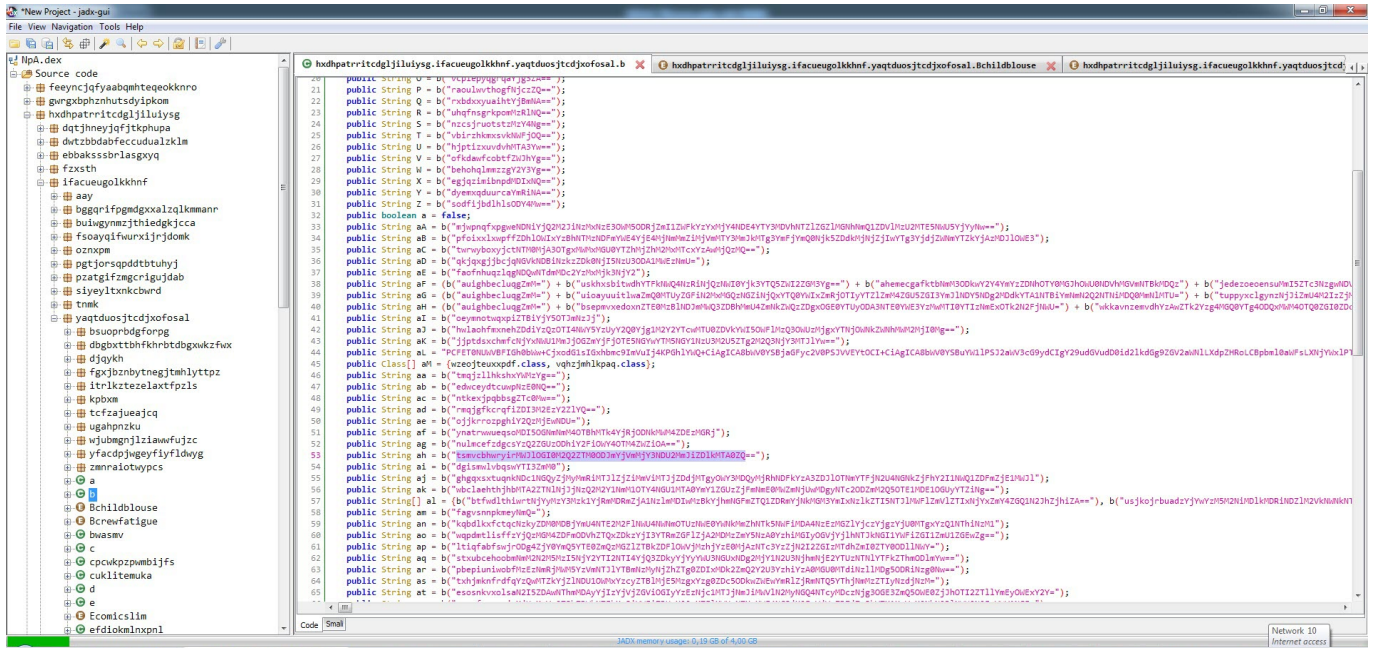
```
*New Project - jadx-gui
File View Navigation Tools Help

Source code
NPA.dex
  feqncjfyabqbshtgeokknro
  gprgpxhznhtsdypkpm
  hxdhptrritcdgjljiluyg
  dqtjhneyqfjtkphupa
  dwtzbbdbafecduualzklm
  ebbakssbrlasyqy
  fxxsth
  ifacuegolkhnf
  aay
  bggrifpmdgxalqkmmannr
  bulngymzjthiedgkjcca
  fs0ayq1fwrux1jrjdomk
  oznxpm
  pctjorsapddbtuhuj
  psatg1fzngcrigujdab
  siyeyltxknbcubnd
  tnmk
  yaqtduosjtdcjoxofosal
  bsuoprbdgforpg
  d0g0ctt0nKhrtdbgwzcfwx
  dgykh
  fgxjzbnbynegjthlytptz
  itr1ktezelxtfpzls
  kpbxm
  tcfzajueajcq
  ugahpnzku
  xjubegnjl1awufujzc
  yfacdpjygyfyfldhyg
  zmnratwypcs
  a
  b
  Bch1dlouse
  Brepfatigue
  bwasev
  c
  cpwkpzpbmbiifs
  cuklitemuka
  d
  E
  Ecomicslim
  efdiokmlnxpnl

427 public final void c(Context context) {
428     if (e(context, this.a.X).equals("true")) {
429         context.startService(new Intent(context, kivrzh1mmhesd.class));
430     }
431 }
432 }
433 }
434 public final String d() {
435     try {
436         return new JSONObject(this.a.aG).getString(Locale.getDefault().getLanguage());
437     } catch (Exception unused) {
438         return this.a.aJ;
439     }
440 }
441 }
442 public final String d(Context context, String str) {
443     String e = e(context, this.a.d);
444     new StringBuilder().append(e);
445     a aVar = new a();
446     return aVar.a(e + this.a.am, str);
447 }
448 }
449 public final String e() {
450     try {
451         return new JSONObject(this.a.aH).getString(Locale.getDefault().getLanguage());
452     } catch (Exception unused) {
453         return this.a.aK;
454     }
455 }
456 }
457 public final String e(Context context, String str) {
458     if (c == null) {
459         SharedPreferences sharedPreferences = context.getSharedPreferences(this.a.ad, 0);
460         c = sharedPreferences;
461         d = sharedPreferences.edit();
462     }
463     return c.getString(str, (String) null);
464 }
465 }
466 public final String f(String str) {
467     return a(str, this.a.ah);
468 }
469 }
470 public final String g(String str) {
471     return b(str, this.a.ah);
472 }
473 }

Code Small
JADX memory usage: 0,35 GB of 4,00 GB
Bluetooth Devices
```





Sıra alien\_ring0\_wdfes şifreleme anahtarı ile daha önce elde ettiğim şifreli verileri çözmeye, şifreleme anahtarının doğruluğunu teyit etmeye geldiğinde yazının başında belirtmiş olduğum sahte ekranların (html) komuta kontrol merkezinden geldiğini de öğrenmiş oldum.



```
Online Java IDE (javac 1.8.0_201) x +
compilejava.net
Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mertsarica... Other bookmarks

41 public final byte[] b(byte[] barr) {
42     byte[] barr2 = new byte[barr.length];
43     for (int i = 0; i < barr.length; i++) {
44         this.b = (this.b + 1) % 256;
45         int i2 = this.c;
46         int[] iArr = this.a;
47         this.c = (i2 + iArr[i3]) % 256;
48         a(i3, this.c, iArr);
49         int[] iArr2 = this.a;
50         barr2[i1] = (byte) (iArr2[(iArr2[this.b] + iArr2[this.c]) % 256] ^ barr[i]);
51     }
52     return barr2;
53 }
54 }
55 }
56 // one class needs to have a main() method
57 public class HelloWorld {
58 {
59     public static String a(String str) {
60         String key = "alienring_w0ffes";
61         try {
62             return new String(new f(str.substring(0, 12).getBytes()).a(b(new String(Base64.getDecoder().decode(str.substring(12), 0), "UTF-8"))));
63         } catch (Exception unused) {
64             return new String(new f(key.getBytes()).a(b(new String(Base64.getDecoder().decode(str))));
65         }
66     }
67     private static byte[] b(String str) {
68         int length = str.length();
69         byte[] barr = new byte[(length / 2)];
70         for (int i2 = 0; i2 < length; i2 += 2) {
71             barr[i2 / 2] = (byte) ((Character.digit(str.charAt(i2), 16) << 4) + Character.digit(str.charAt(i2 + 1), 16));
72         }
73     }
74     public static void main(String[] args) {
75         System.out.println("000YmYzNDRIHThJZDU3Hh3VhWwZuWwNHzDZ1Hzk4Njd1ZJAl1GyVStw0Hz1yYj3HtBhYh1HhzhNwQznc3HzR1H0gyHtZgZj11HTQZ2GFkZTg40DBhVj2Kw0QwUf1Y2Y0HjU1HTj1H23Hj11NDuW2E4HDVhWQuz3Qx8hEwHD4ZwZyOT1hWYvYyY3DKk4NtIxfWt5NDeyHfjWOTAYtzhNwGRhDQ4HG1YhUz);
76     }
77 }
78 }
79 }
80 }
81 }
82 }
83 }
84 }
85 }
86 }
87 }
88 }
89 }
90 }
91 }
92 }
93 }
94 }

(command line arguments) COMPILER & EXECUTE PASTE SOURCE DOWNLOAD ZIP default
Successfully compiled /tmp/java_t9fsAU/f.java
Successfully compiled /tmp/java_t9fsAU/HelloWorld.java -- main method
{"@": "
{"holder_name": "Osman", "address": "Turkey", "city": "Istanbul", "state": "Kadikoy", "zip": "34878", "phone": "902163534466", "number_card": "4510 9650 3456 0735
333", "exp_mm": "11", "exp_yy": "22", "cvv": "311", "type_injects": "credit_cards", "closed": "close_activity_injec
ts", "top": "1520 gcc1-7gcc-r1v8", "app": "com.android.vending", "it": "11aghyx3f4r6ohj1ij"}
}
```

Sonuç itibariyle son yıllarda adından özellikleri ile sıklıkla söz ettiren Cerberus mobil bankacılık zararlı yazılımının vatandaşlarımızı adı ve soyadını içeren SMS yolu ile hedef almaya başladığını öğrenmek beni oldukça şaşırttı ve endişelendirdi. Her zaman olduğu gibi Android kullanıcılarının bilmedikleri kaynaklardan uygulama yüklemekten kaçınmaları gerektiğinin altını tekrar ve tekrar önemle çizerek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

**Not:**

1. Bu güvenlik araştırmasını yaptığımda (2020 Şubat) herkes tarafından Cerberus olarak bilinen bu zararlı yazılımın daha sonra Cerberus v1 sürümünden çatallanan Alien isimli bir zararlı yazılım olduğu ortaya çıkmıştır. (Eylül 2020)
2. Bu yazı ayrıca Pi Hediyem Var #18 oyununun çözüm yolunu da içermektedir.