

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

VoLTE LTE 70%



+90 212 985 05 78



14:41

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

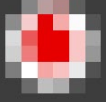
|





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





5G Beta Test

5G Uygulamasini 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

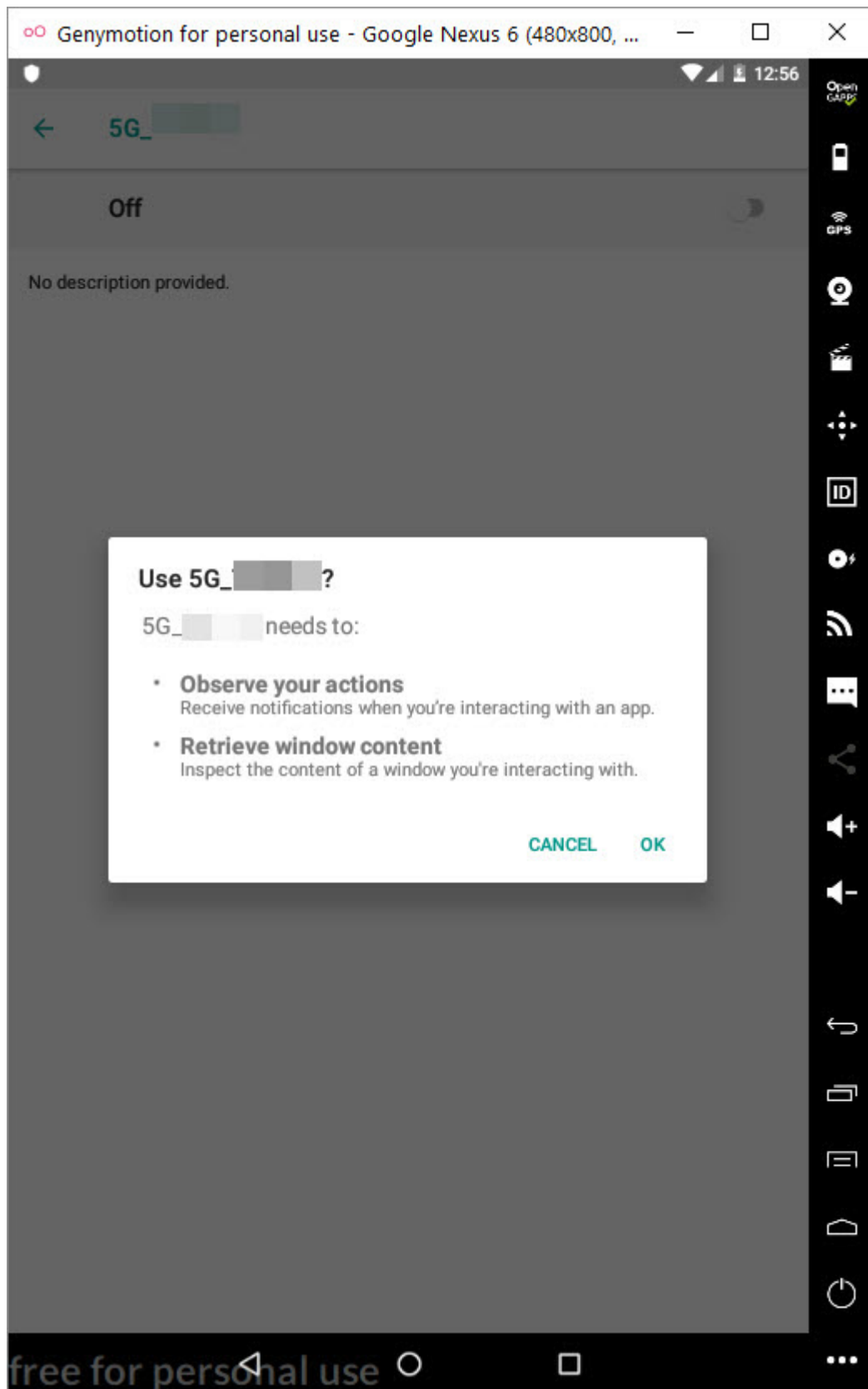


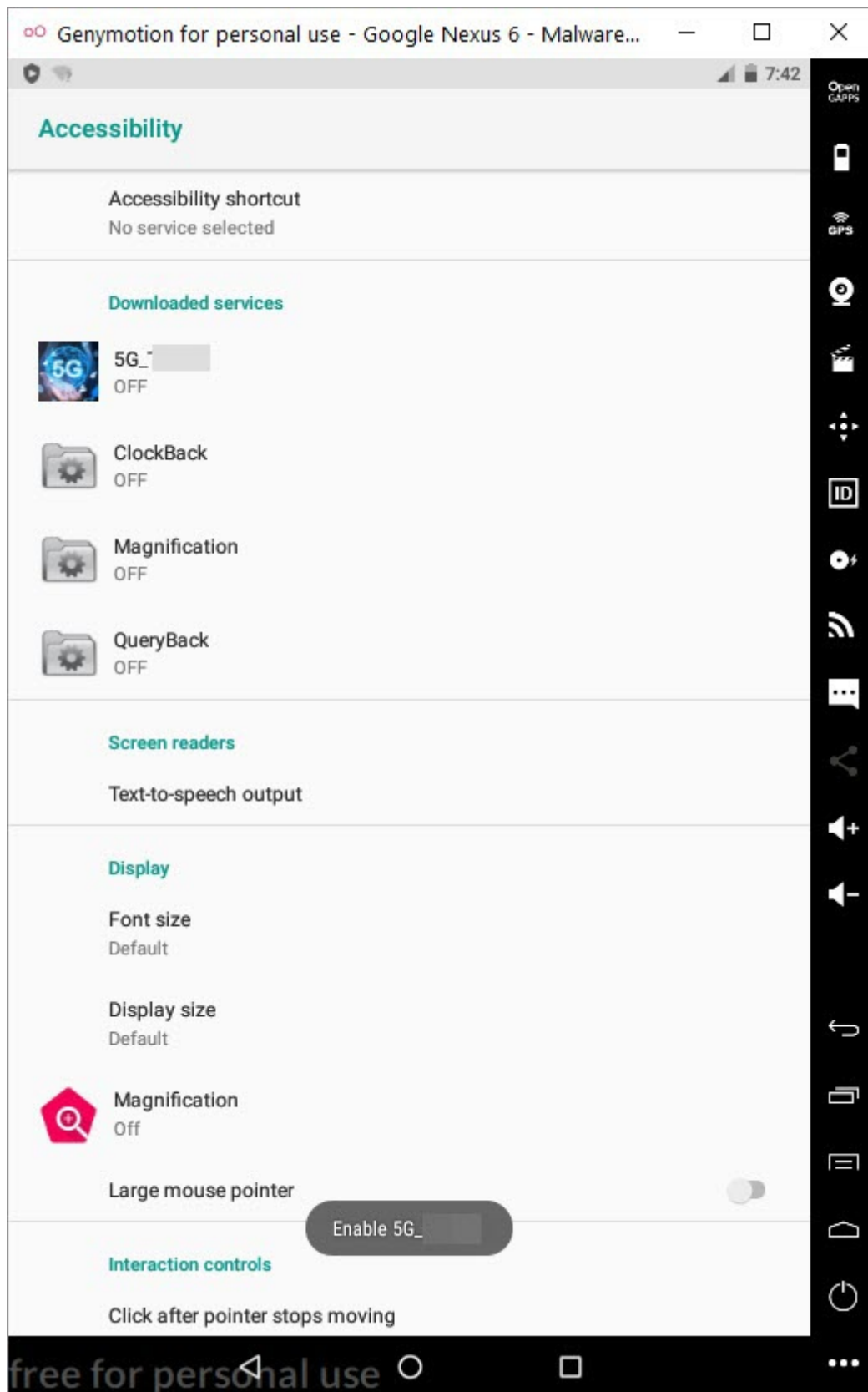
Enable 5G_Turkcell

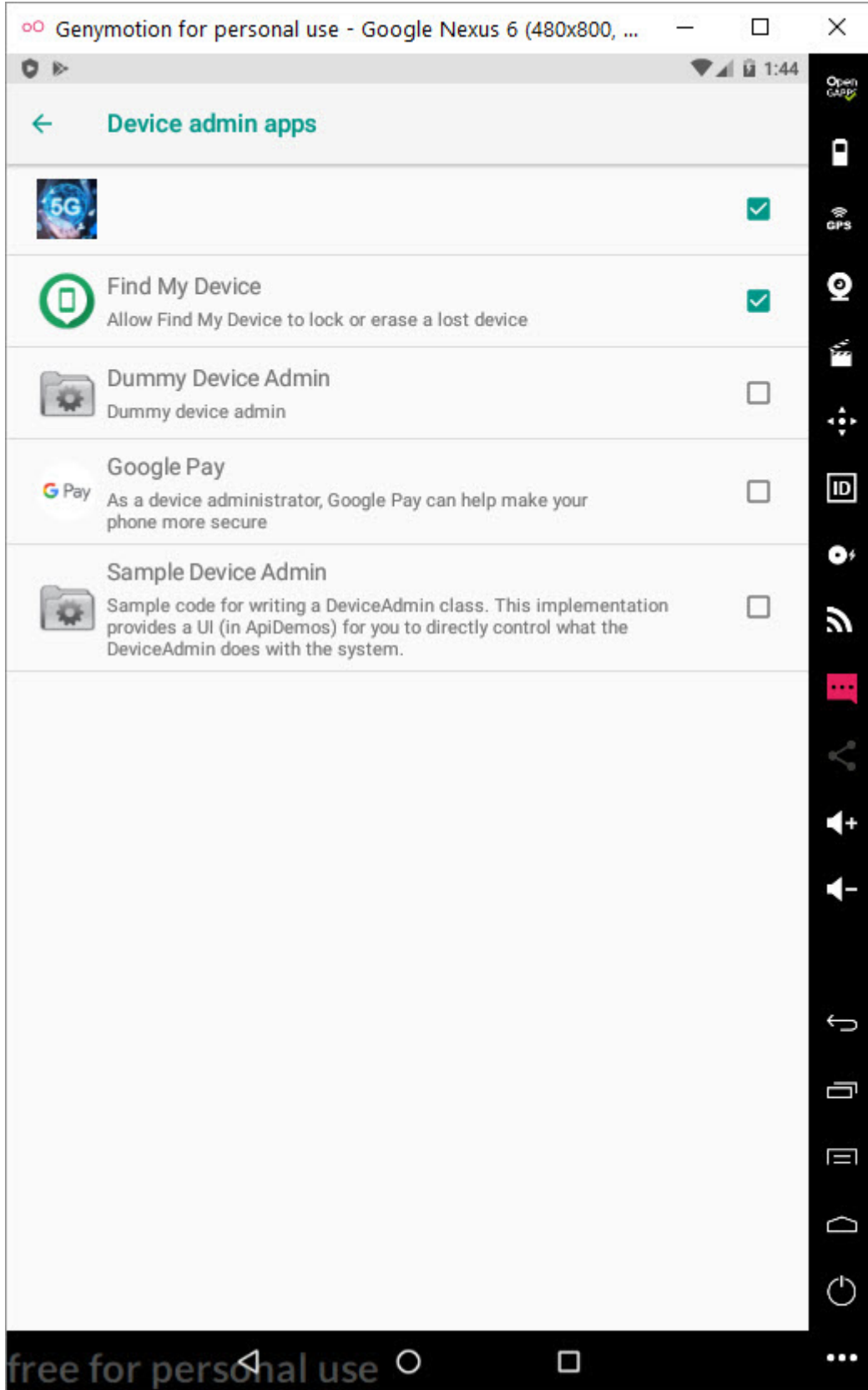
Interaction controls

Click after pointer stops moving









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.

Genymotion for personal use - Google Nexus 6 (480x800, ...)

12:59

Google Play

Cardholder name

Street address

City

State

ZIP code

Telephone number

G Pay 

Continue

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

free for personal use



Osman|

Turkey

Istanbul

Kadikoy

34878

+902163534466



Continue

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



VISA Credit Card Generator, 100% x

creditcardgenerator.com/visa-credit-card-generator/

Other bookmarks



Search

 [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

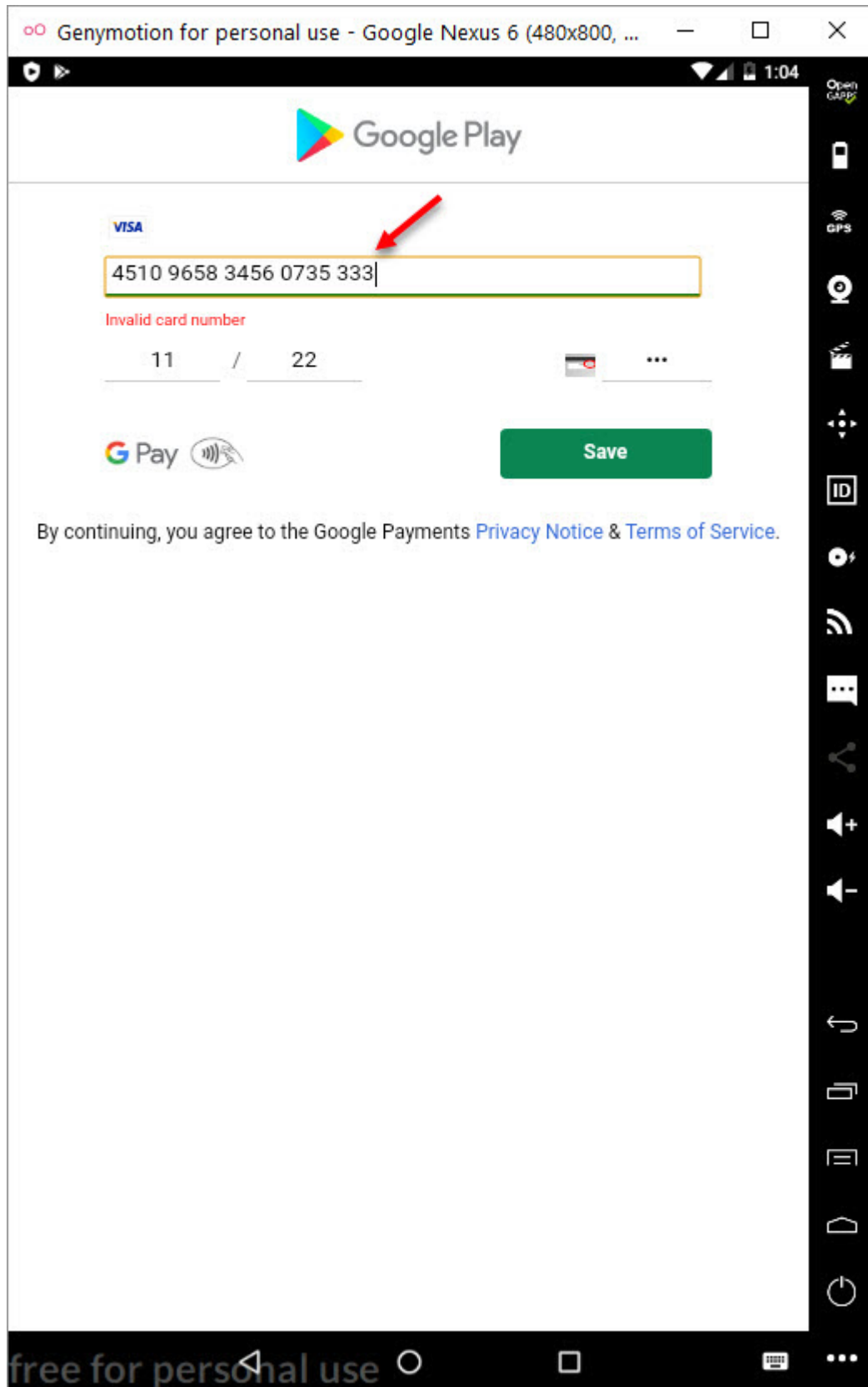
Generator:	Test VISA Credit Cards
Issuing network:	Visa
Card number:	4510 9658 3456 0735
Pin:	1537
Name:	Josh Lunar
Address:	9007 Mountaintrail Way
Country:	France
CVV:	938
Expiration date:	11 / 2022

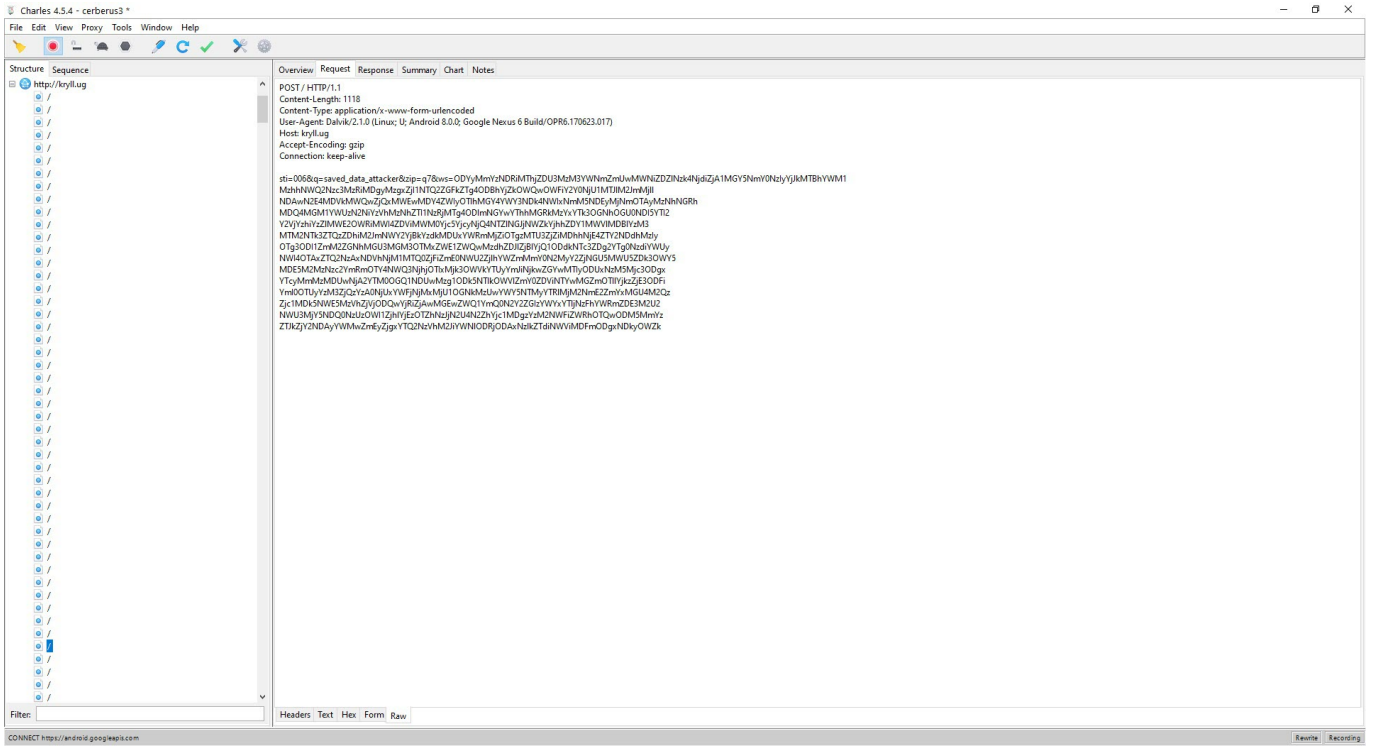
Generate VISA Credit Card



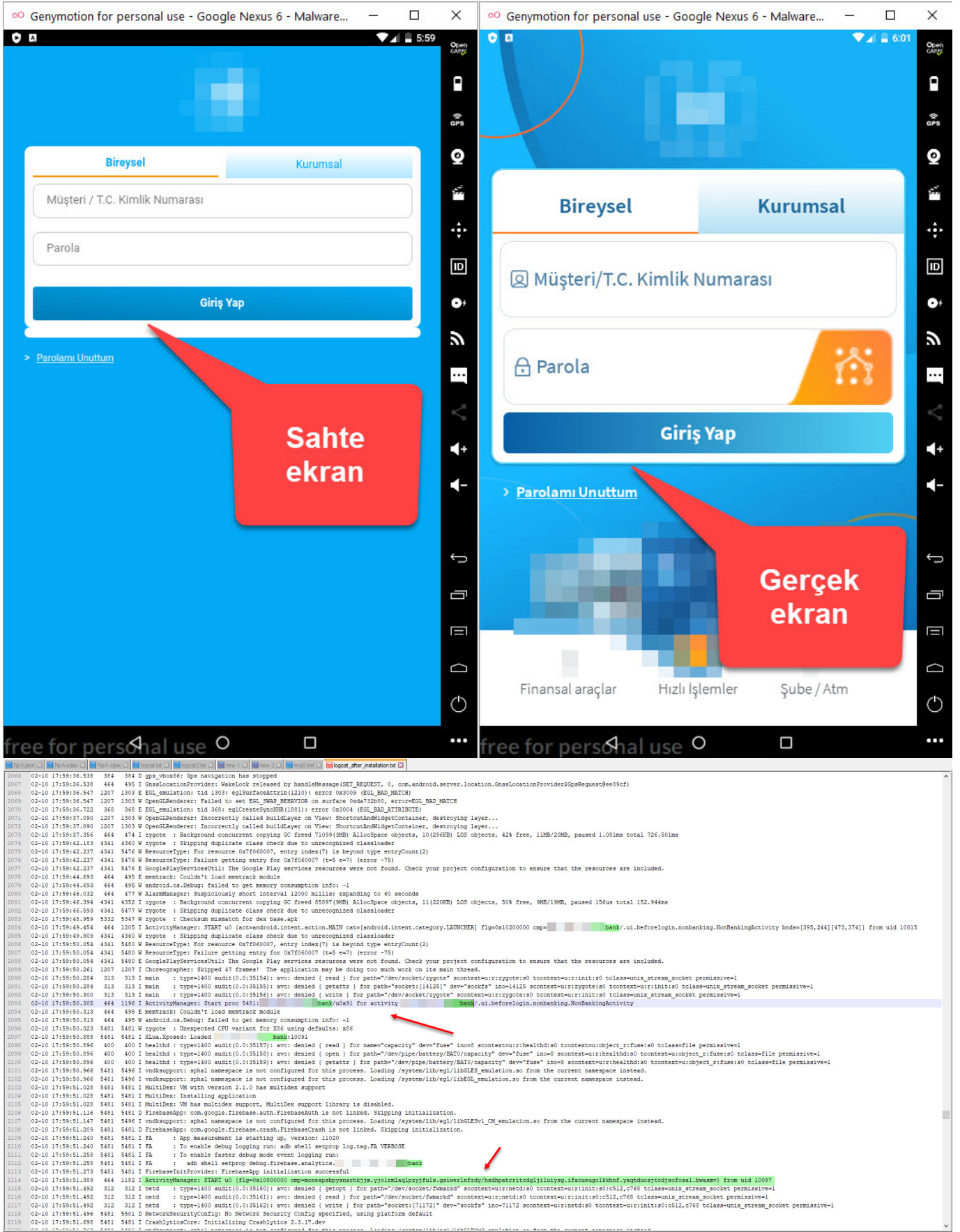
Take a look at the legendary [VISA company](#) if you don't know who they are duh.

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.





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.



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

The screenshot shows the GDA XML tool interface. The left pane lists the components of the AndroidManifest.xml file, including permissions, activities, services, and receivers. The main pane displays the XML code with annotations. A red arrow points to the 'android.permission.READ_EXTERNAL_STORAGE' permission in the list of detected permissions.

/data/data/mcneapsbpysnarhkjjm.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 çevirdiğimde AndroidManifest.xml dosyasında yer alan MainActivity sınıfı ile karşılaşmış oldum.

```
C:\WINDOWS\system32\cmd.exe - adb shell
rw----- 1 u0_a19 u0_a19 576044 2020-02-08 12:55 Ndk.json
rw----- 1 u0_a19 u0_a19 657 2020-02-08 13:03 Ndk.json.prof
drwx--x--x 3 u0_a19 u0_a19 4096 2020-02-08 12:55 oat

app_apk:
total 324
drwxrwx--x 3 u0_a19 u0_a19 4096 2020-02-08 13:27 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..
drwx--x--x 3 u0_a19 u0_a19 4096 2020-02-08 12:56 oat
-rw----- 1 u0_a19 u0_a19 315309 2020-02-08 12:56 ring0.apk

app_outdex:
total 12
drwxrwx--x 2 u0_a19 u0_a19 4096 2020-02-08 12:56 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..

app_textures:
total 12
drwxrwx--x 2 u0_a19 u0_a19 4096 2020-02-08 12:57 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..

app_webview:
total 84
drwx----- 5 u0_a19 u0_a19 4096 2020-02-08 13:05 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..
drwx----- 3 u0_a19 u0_a19 4096 2020-02-08 12:57 GPUCache
drwx----- 2 u0_a19 u0_a19 4096 2020-02-08 13:05 Session Storage
-rw----- 1 u0_a19 u0_a19 57344 2020-02-08 12:57 Web Data
-rw----- 1 u0_a19 u0_a19 0 2020-02-08 12:57 Web Data-Journal
drwx----- 3 u0_a19 u0_a19 4096 2020-02-08 12:57 lib.storage
-rw----- 1 u0_a19 u0_a19 56 2020-02-08 12:57 pref_store
-rw----- 1 u0_a19 u0_a19 0 2020-02-08 12:57 variations_seed_new
-rw----- 1 u0_a19 u0_a19 0 2020-02-08 12:57 variations_stamp
-rw----- 1 u0_a19 u0_a19 0 2020-02-08 12:57 webview_data.lock

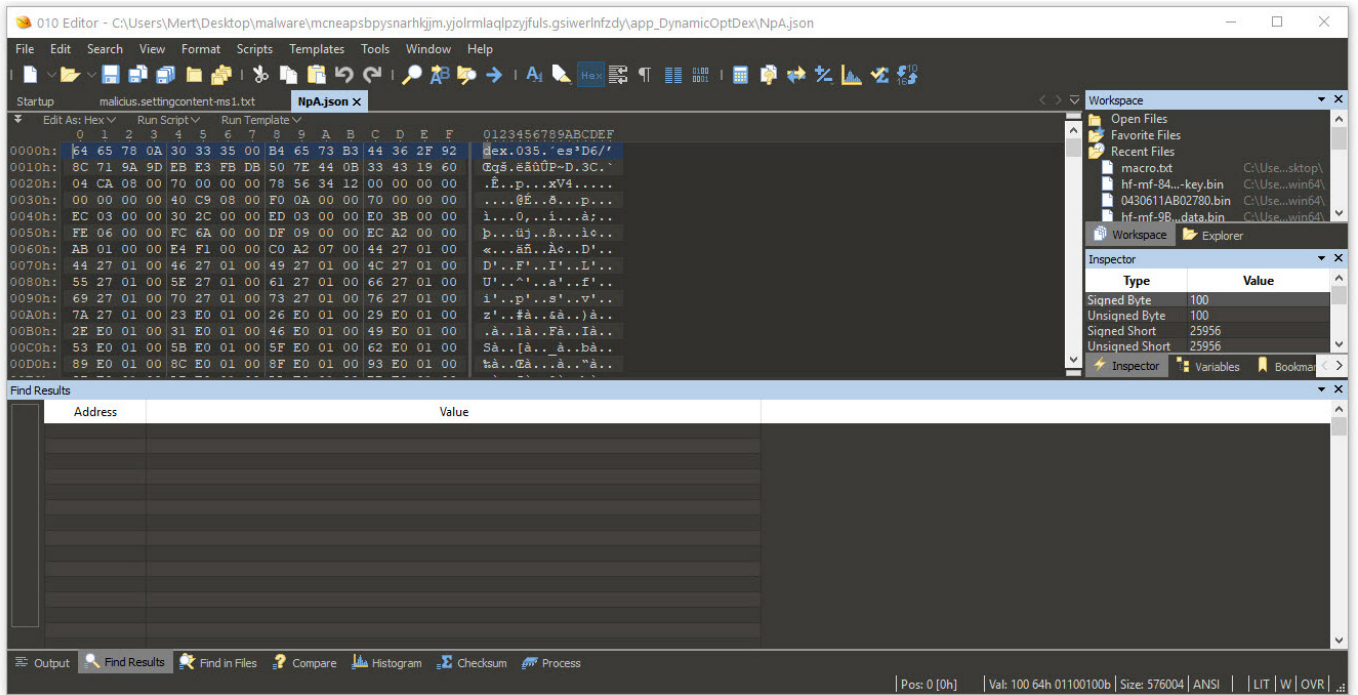
cache:
total 40
drwxrwx--x 4 u0_a19 u0_a19_cache 4096 2020-02-08 12:57 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..
drwx----- 5 u0_a19 u0_a19_cache 4096 2020-02-08 12:57 WebView
-rw----- 1 u0_a19 u0_a19_cache 16740 2020-02-08 12:57 font_unique_name_table.pb
drwx----- 3 u0_a19 u0_a19_cache 4096 2020-02-08 12:57 org.chromium.android_webview

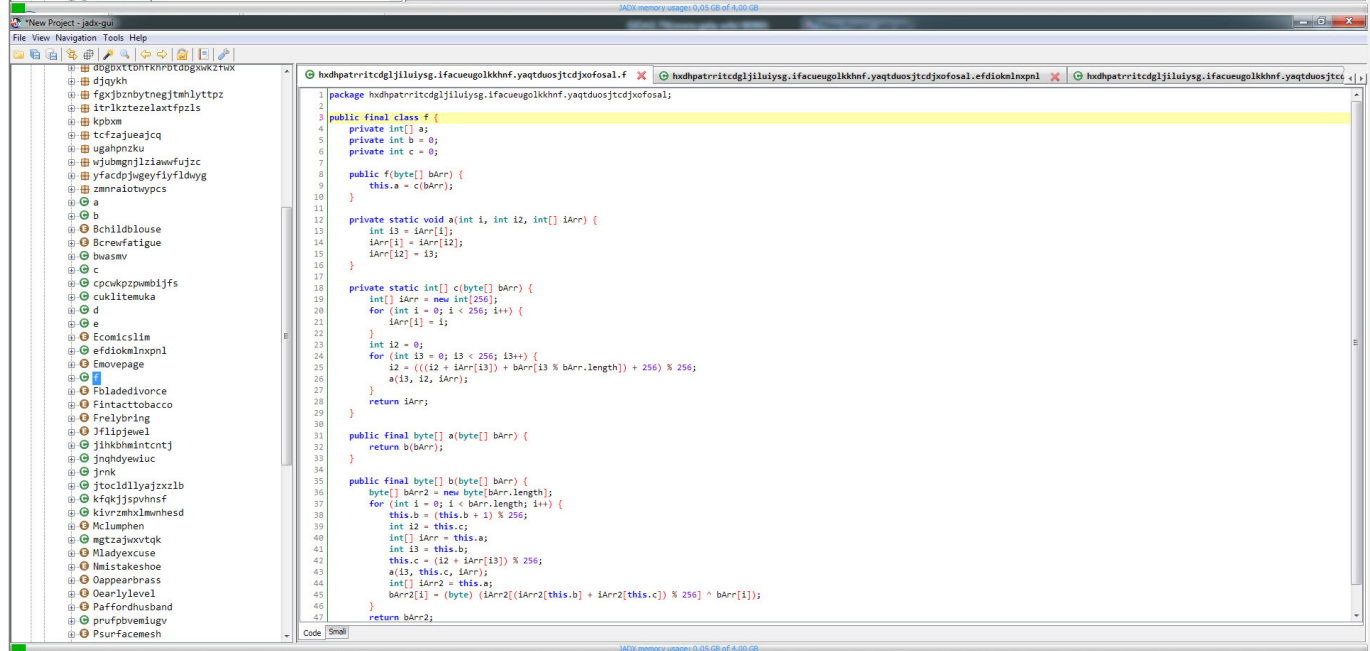
code_cache:
total 12
drwxrwx--x 2 u0_a19 u0_a19_cache 4096 2020-02-08 12:54 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..

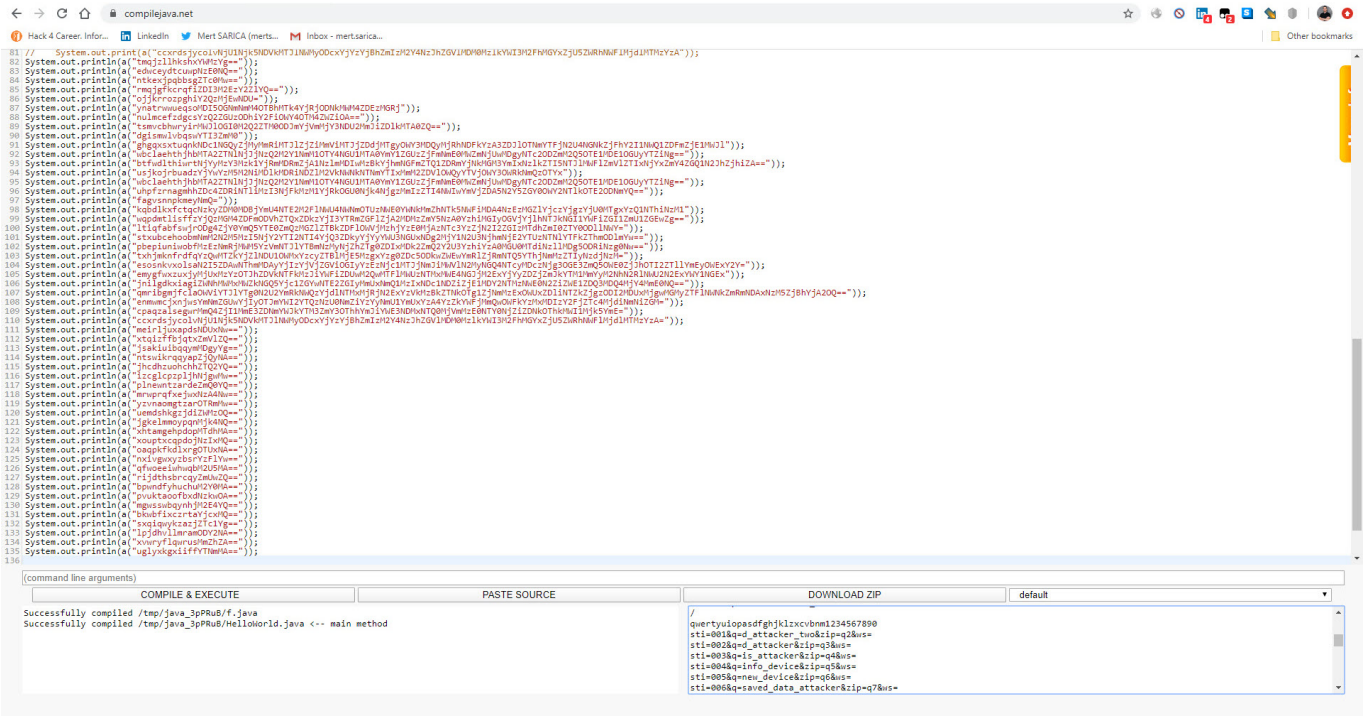
shared_prefs:
total 440
drwxrwx--x 2 u0_a19 u0_a19 4096 2020-02-08 13:27 .
drwx----- 11 u0_a19 u0_a19 4096 2020-02-08 12:57 ..
-rw-rw-rw- 1 u0_a19 u0_a19 127 2020-02-08 12:57 WebViewChromiumPrefs.xml
-rw-rw-rw- 1 u0_a19 u0_a19 433616 2020-02-08 13:27 ring0.xml
-rwxr-xr-x 1 u0_a19 u0_a19 0 2020-02-08 12:57 variations_seed_new
-rwxr-xr-x 1 u0_a19 u0_a19 0 2020-02-08 12:57 variations_stamp
-rwxr-xr-x 1 u0_a19 u0_a19 0 2020-02-08 12:57 webview_data.lock
```

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

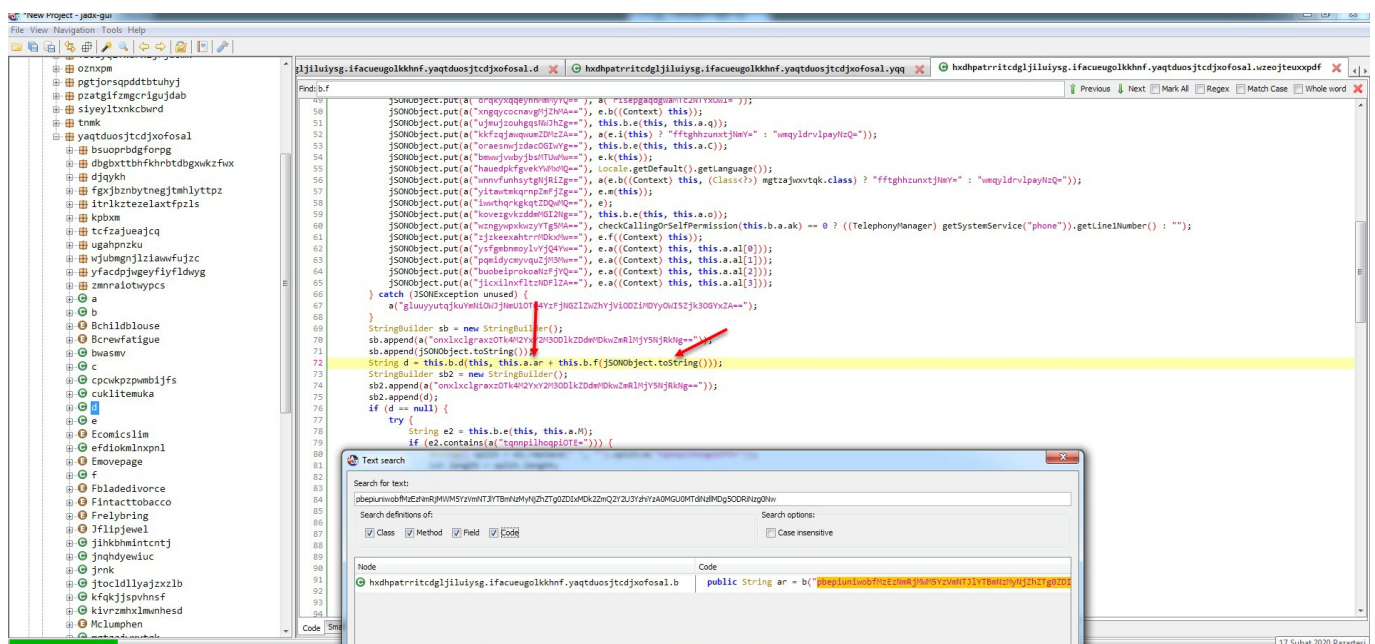
mjwpnqfxpgweNDNiYjQ2M2JiNzMXNzE3OWM5ODRjZmI1ZWFKYzYxMjY4NDE4YTY3MDVhNTZlZGZlMGhNmQ1ZDVlMzU2MTE5NWU5YjYyNw== ise RC4 şifreleme anahtarı mjwpnqfxpgwe değeri oluyor. Bu anahtar ile geri kalan şifreleri karakterleri (NDNiYjQ2M2JiNzMXNzE3OWM5ODRjZmI1ZWFKYzYxMjY4NDE4YTY3MDVhNTZlZGZlMGhNmQ1ZDVlMzU2MTE5NWU5YjYyNw==) 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.

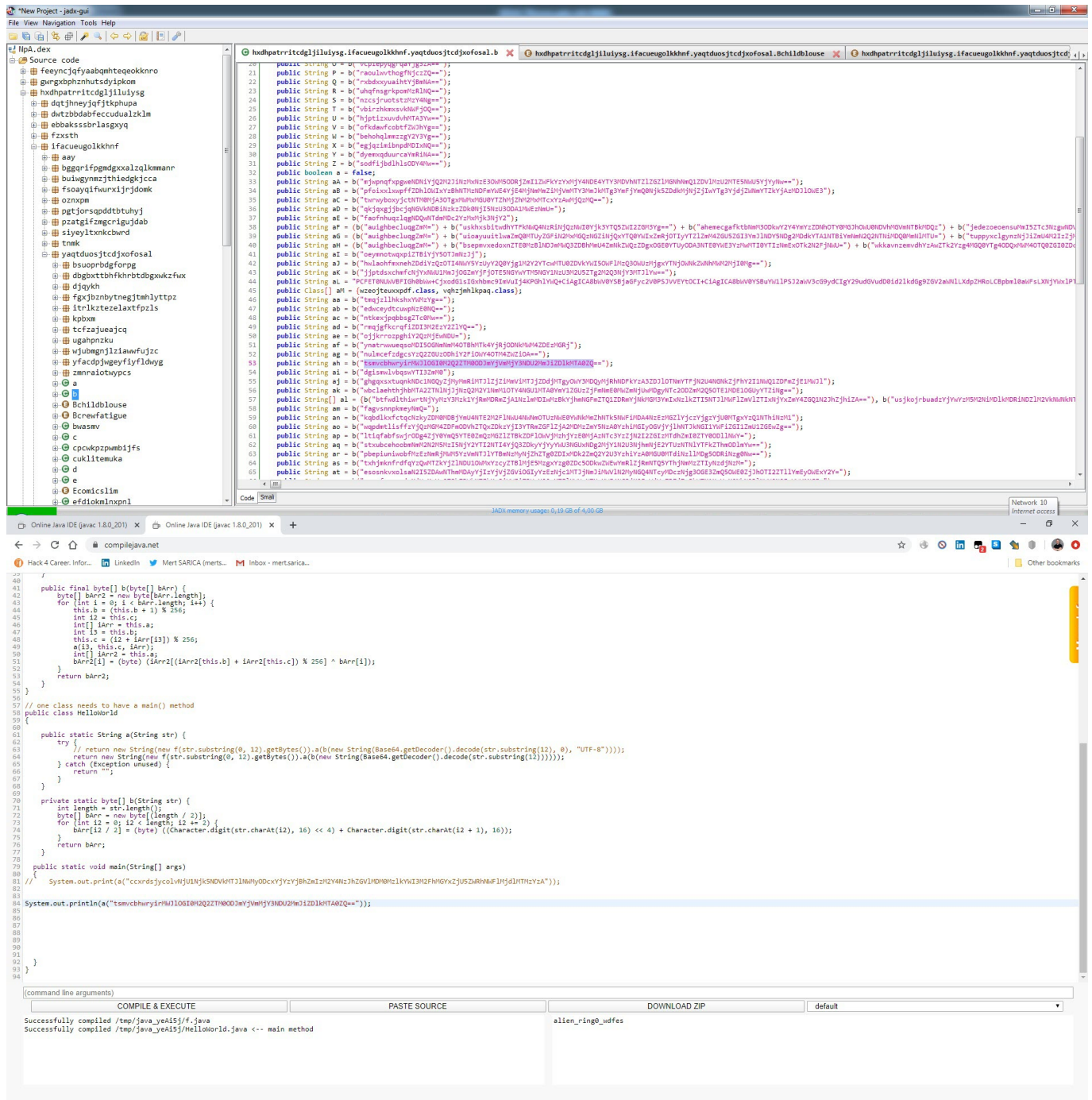




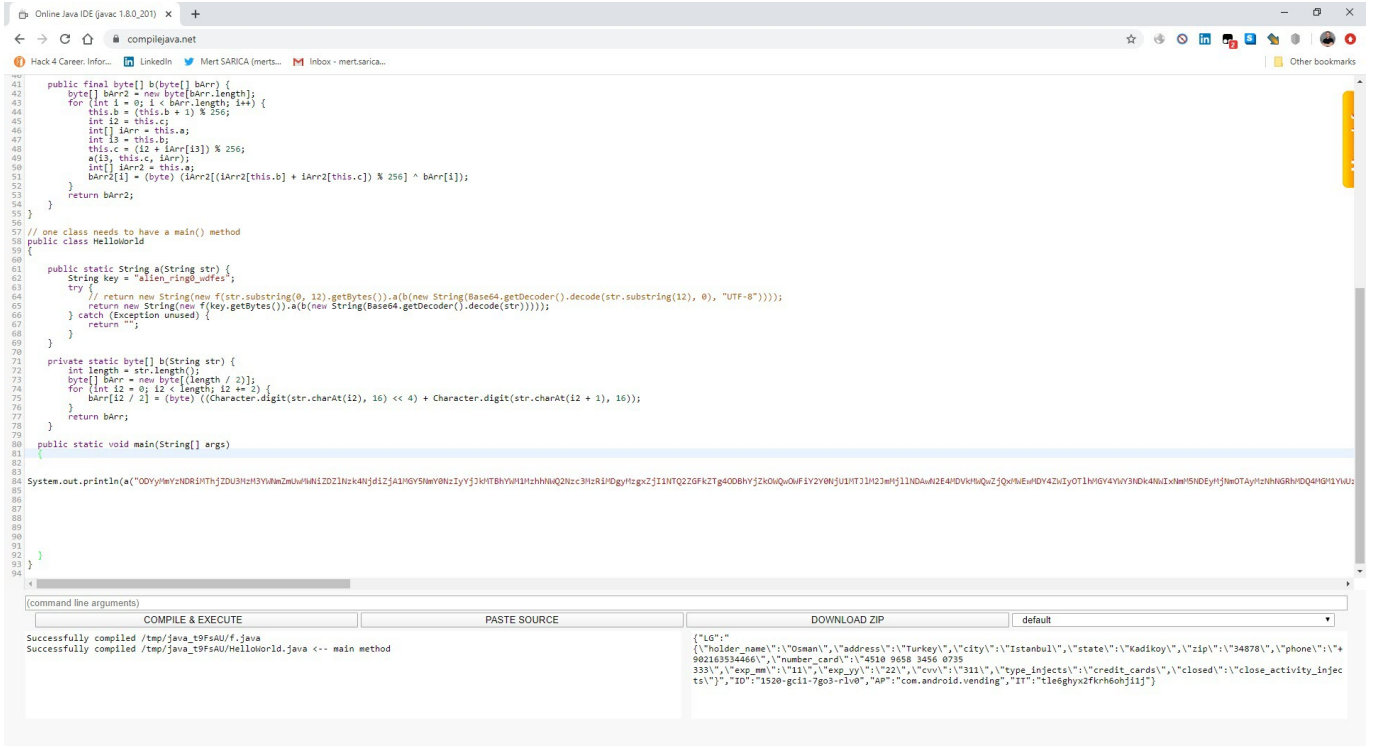


Komuta kontrol merkezine gönderilen şifreli verilerin şifreleme anahtarını bulmak için şifresi çözülmüş karakter dizilerinde JSON geçtiğini gördüğüm için koda bu sınıfın kullanıldığı noktalara odaklandım. Zararlı uygulama çalıştıktan sonra komuta kontrol merkezine belli periyotlarda sti=004&q=info_device parametresini ardından da ws= şifreli parametresini gönderdiğini bildiğim için bu iki değer birbire eklendiği kod bloğunu buldum. Bu kod bloğunu analiz ettiğimde ise ws parametresinin alien_ring0_wdfes RC4 anahtarı ile şifrelendiğini tespit ettim.





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.



```
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 // one class needs to have a main() method
56 public class HelloWorld
57 {
58     public static String a(String str) {
59         String key = "alien_@ng_@ffes";
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(key.getBytes()).a(b(new String(Base64.getDecoder().decode(str))));
63         } catch (Exception unused) {
64             return "";
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         return barr;
74     }
75     public static void main(String[] args)
76     {
77         System.out.println(a("00YrWYzNDRIH7J2DU3H2H3YVWwZuWwNINZDZ1HzK4Njd1ZJA1NGY5WwY0HzIyY7jXHTBHYW1H7zhNHWQ2Hzc3HzR1HDgyfzgxZj1THTQ2ZGFkZTg4ODBiYyJ2K0uQwJfIY2Y0HJ1HTJ1H23eHj11NDuW1ZE4HDVWbQuZj3Qw8uWHDY4ZwZyOT1HNGY4YVY3HDk4NUIxWwY5NDEyHj7WOTAYtHzhNNGRNfDQ4HGI1YUuZ
78     }
79 }
80 }
81 }
82 }
83 }
84 }
85 }
86 }
87 }
88 }
89 }
90 }
91 }
92 }
93 }
94 }
```

Successfully compiled /tmp/java_t9fsAU/f.java
Successfully compiled /tmp/java_t9fsAU/HelloWorld.java <- main method

COMPILER & EXECUTE PASTE SOURCE DOWNLOAD ZIP default

```
{
  "holder_name": "Osman",
  "address": "Turkey",
  "city": "Istanbul",
  "state": "Kadikoy",
  "zip": "34878",
  "phone": "902163534466",
  "number_card": "4510 9658 3456 0735",
  "exp_mm": "11",
  "exp_yy": "22",
  "cvv": "311",
  "type_injects": [
    "credit_cards",
    "close_activity_inject",
    "id": "1520-gc11-gn3-r1v8",
    "api": "com.android.vending",
    "it": "11e8ghy3fkn6ohj1ij"
  ]
}
```

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.