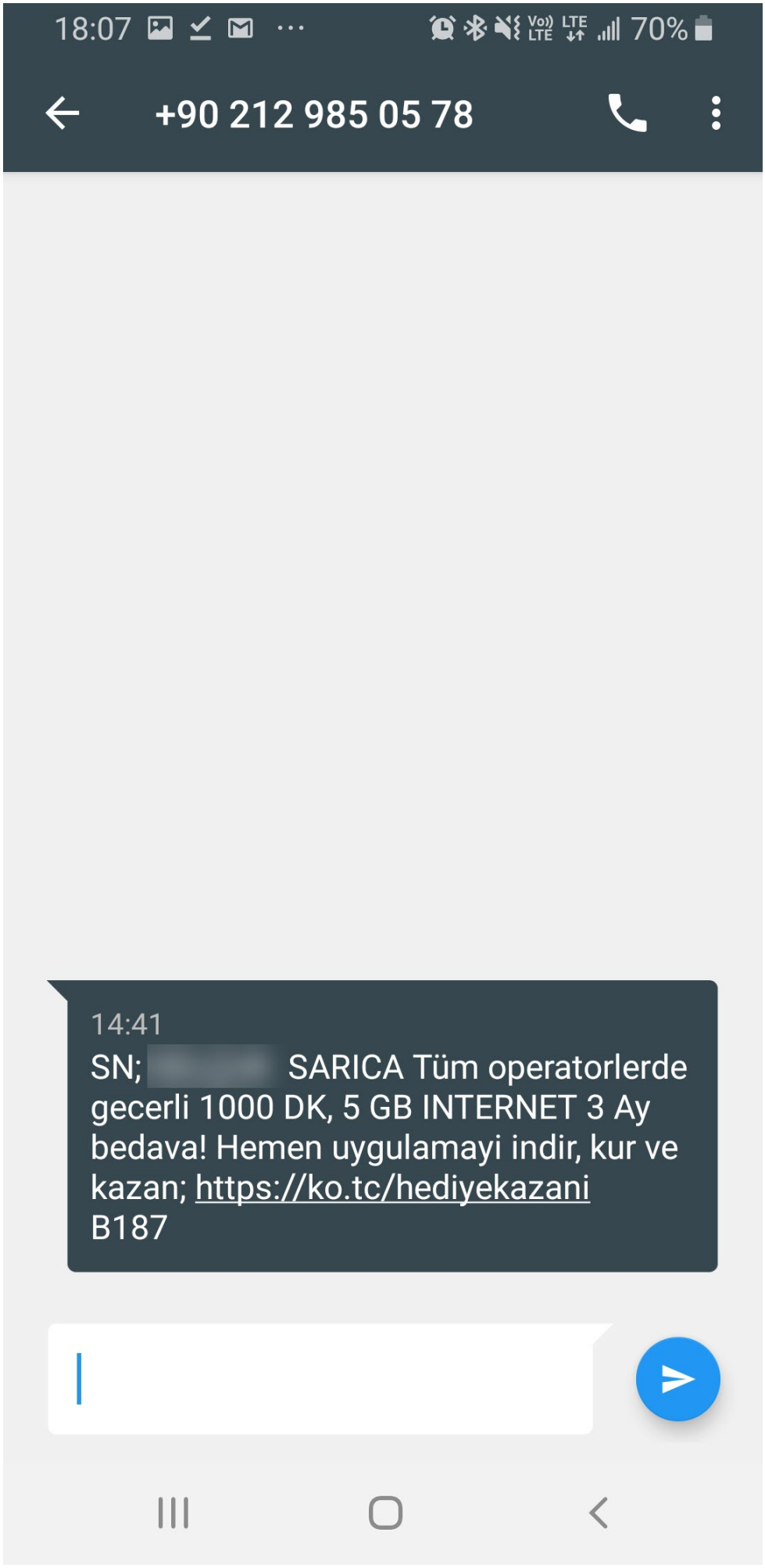
Cerberus Analizi

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 web adresini ziyaret ettiğimde 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 uygulamayi indir, kur ve kazan; https://ko.tc/hediyekazani
B187


18:04
71%
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

18:20 68%

thediyeliuygulama.com

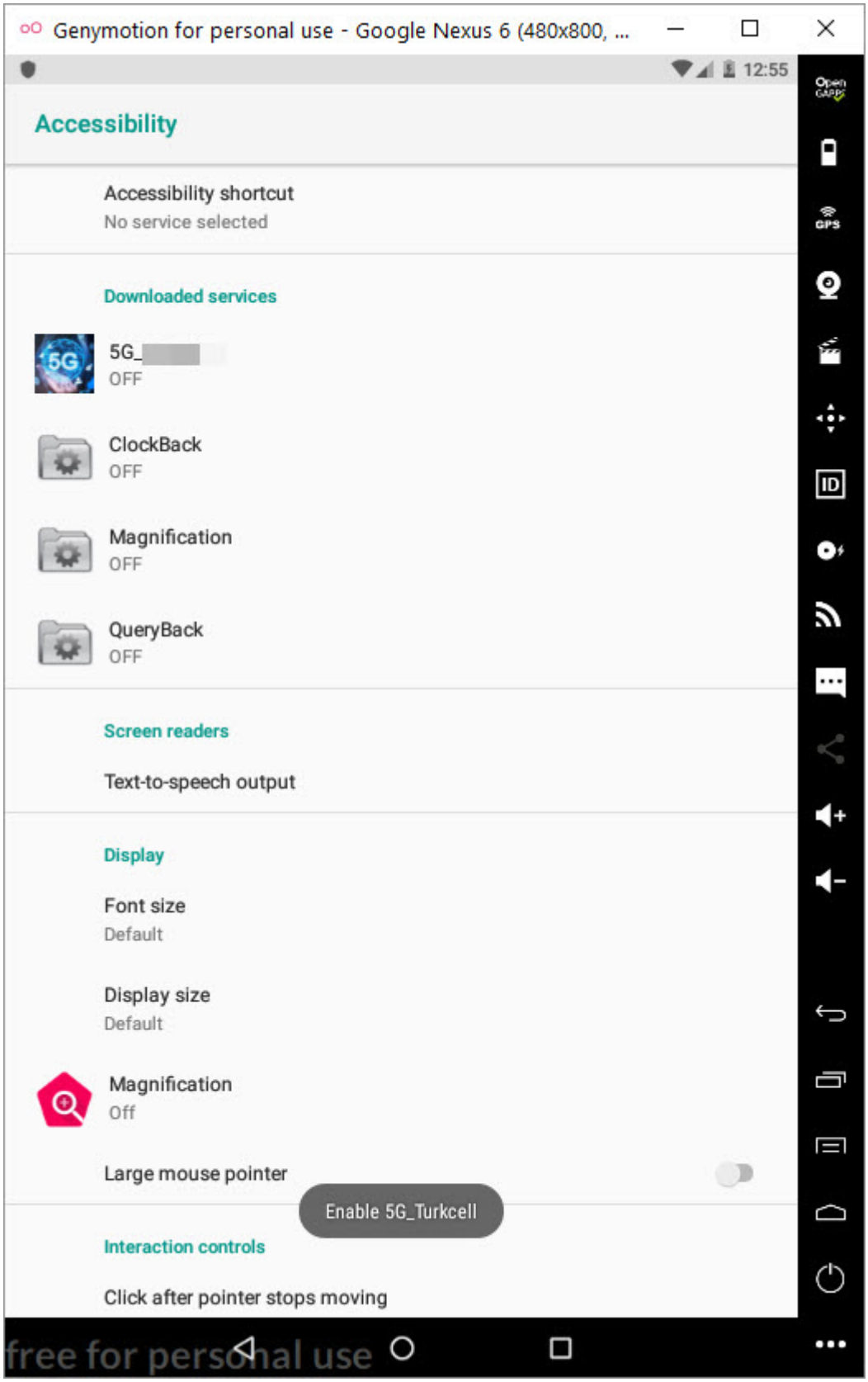
5G Beta Test

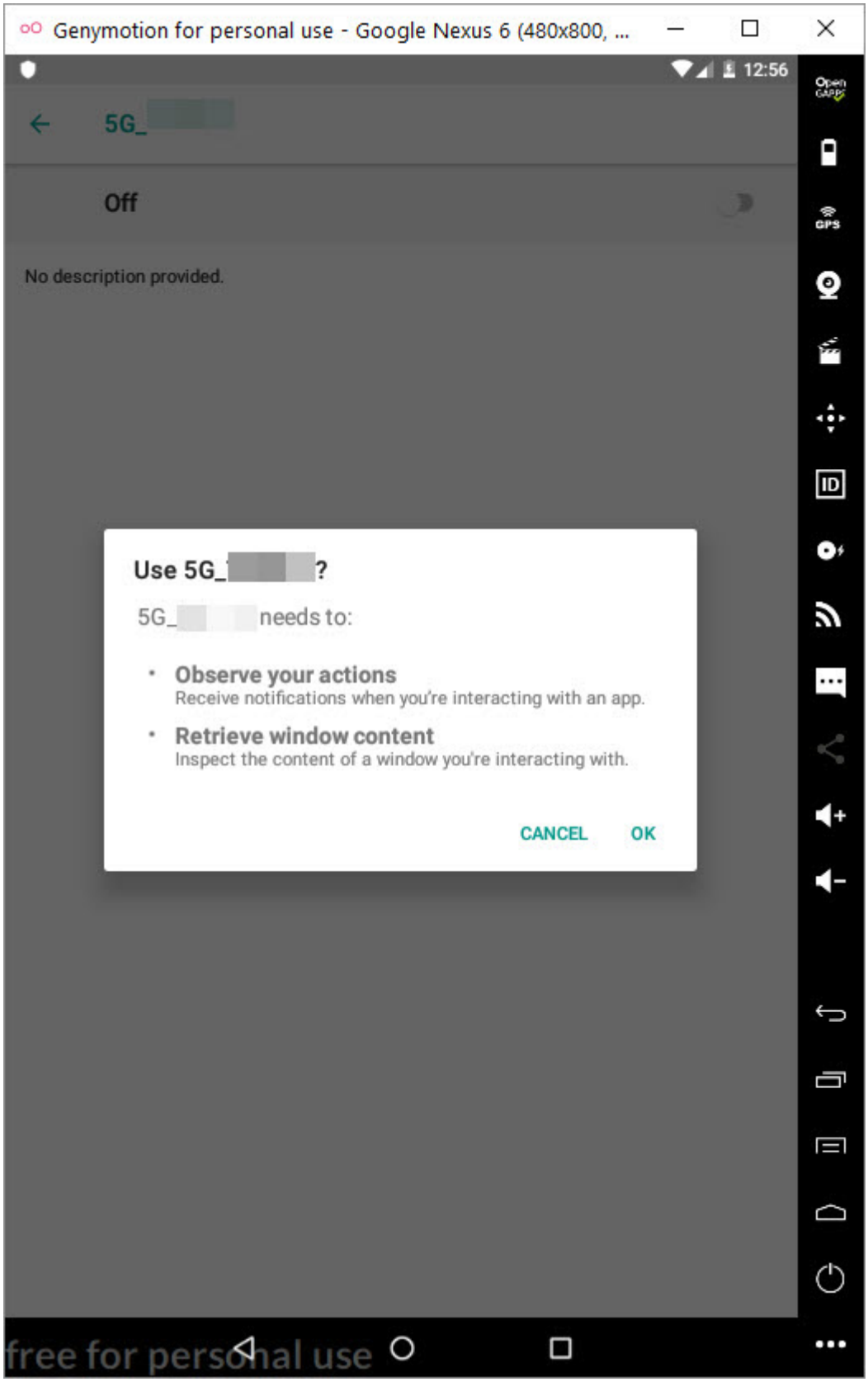
5G Uygulamasini İndirip Yükleyen Tüm Operatör Müşterilerine 5GB İnternet Hediye Sizde Hemen İndirin Yükleyin 5GB İnterneti Hemen Kazanın

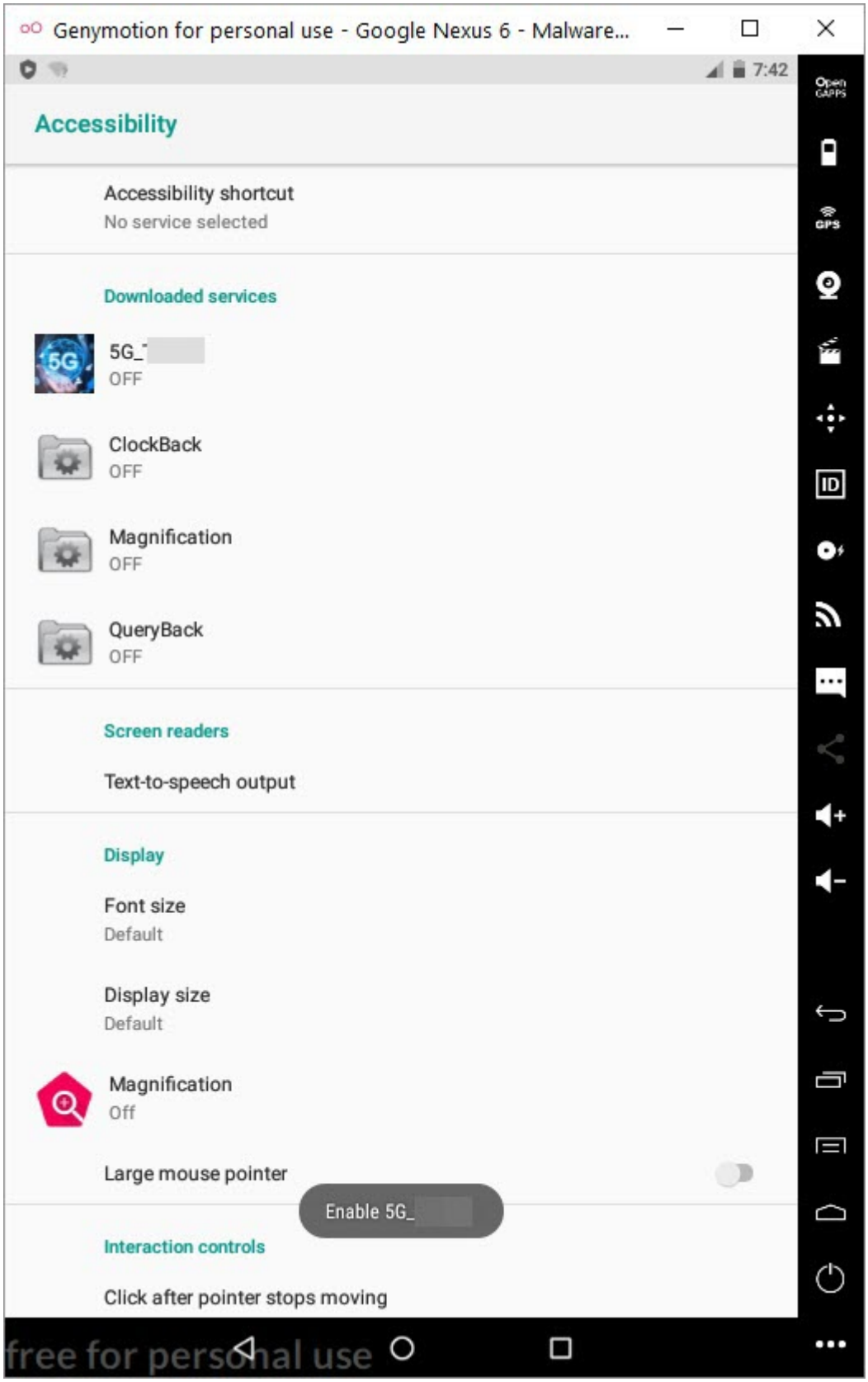
Uygulamayı Yükle

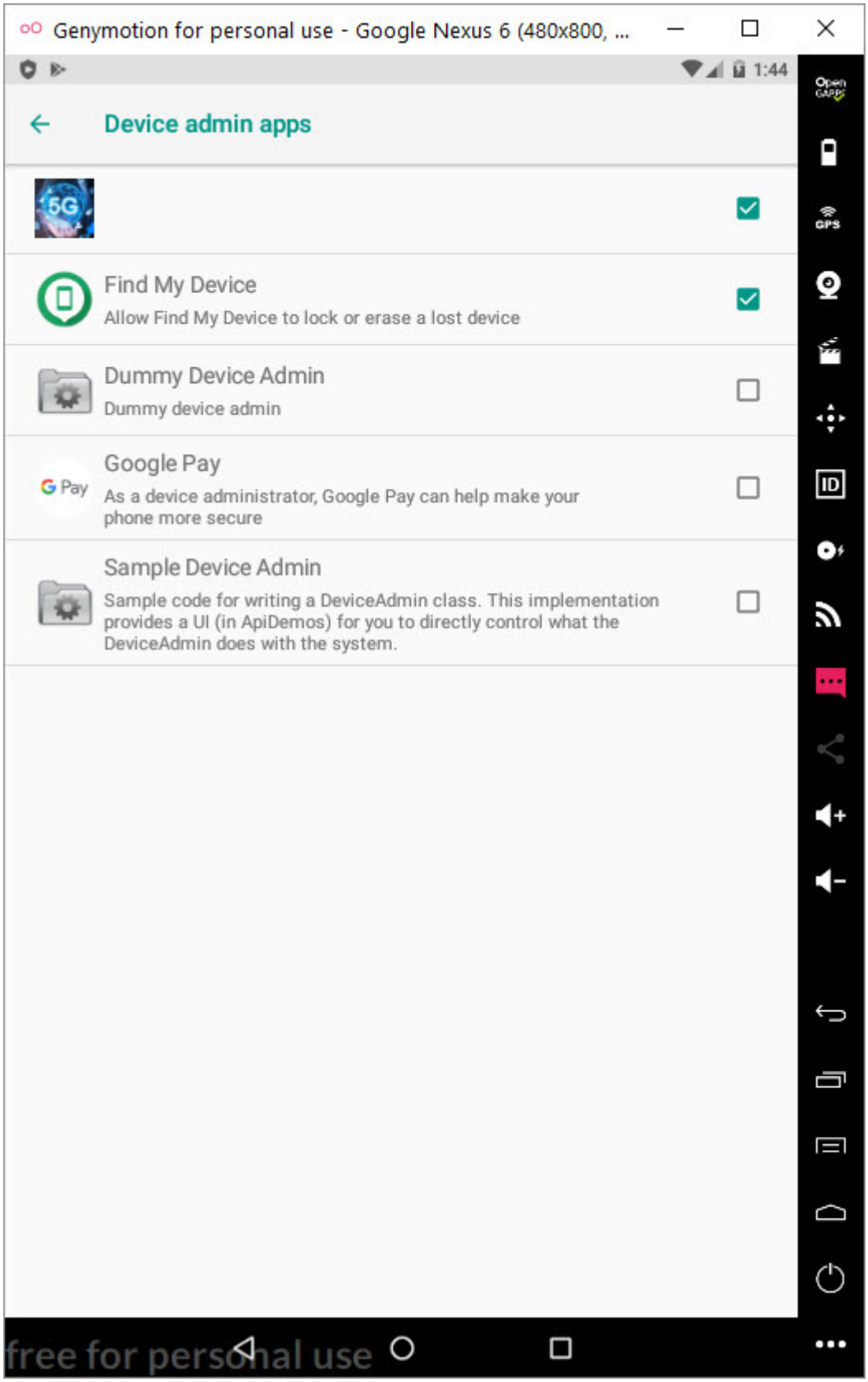
Web sitesinden sunulan 5GBeta.apk dosyasını indirip, mobil zararlı yazılım analizi amacıyla kullanılan o meşhur Koodous web uygulamasına yüklediğimde analiz başarısızlıkla sonuçlandı. Ardından bu uygulamayı VirusTotal web uygulamasına yüklediğimde her ne kadar bunun bir bankacılık zararlı uygulaması 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 yüklemez 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.


Genymotion for personal use - Google Nexus 6 (480x800, ...
12:55
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
free for personal use

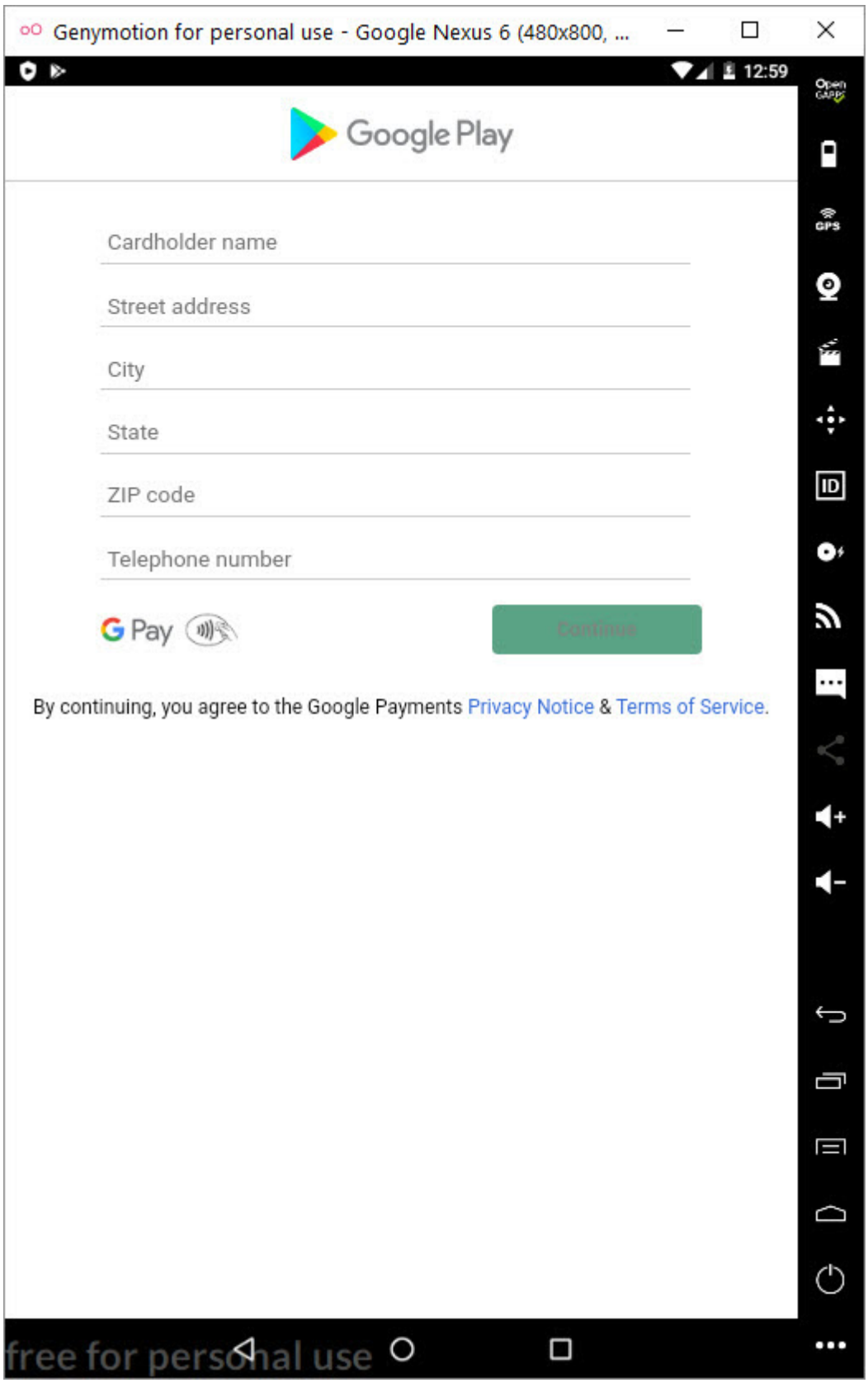

Genymotion for personal use - Google Nexus 6 (480x800, ...
12:56
5G_
Off
No description provided.
Use 5G_ ?
5G_ needs to:
Observe your actions
Receive notifications when you're interacting with an app.
Retrieve window content
Inspect the content of a window you're interacting with.
CANCEL
OK
free for personal use

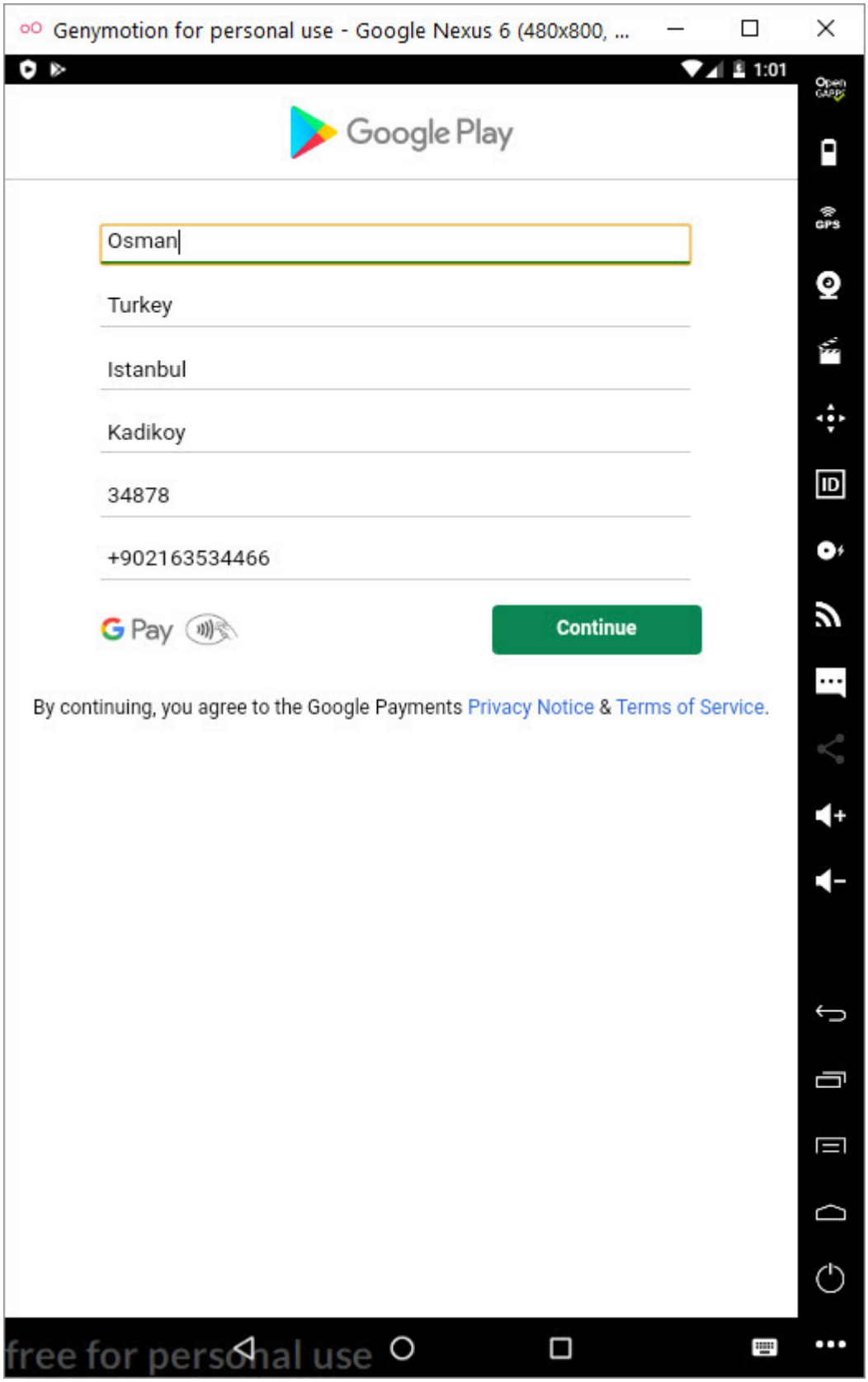

Genymotion for personal use - Google Nexus 6 - Malware...
7:42
Accessibility
Accessibility shortcut
No service selected
Downloaded services
5G_
OFF
ClockBack
OFF
Magnification
OFF
QueryBack
OFF
Screen readers
Text-to-speech output
Display
Font size
Default
Display size
Default
Magnification
Off
Large mouse pointer
Enable 5G_
Interaction controls
Click after pointer stops moving
free for personal use

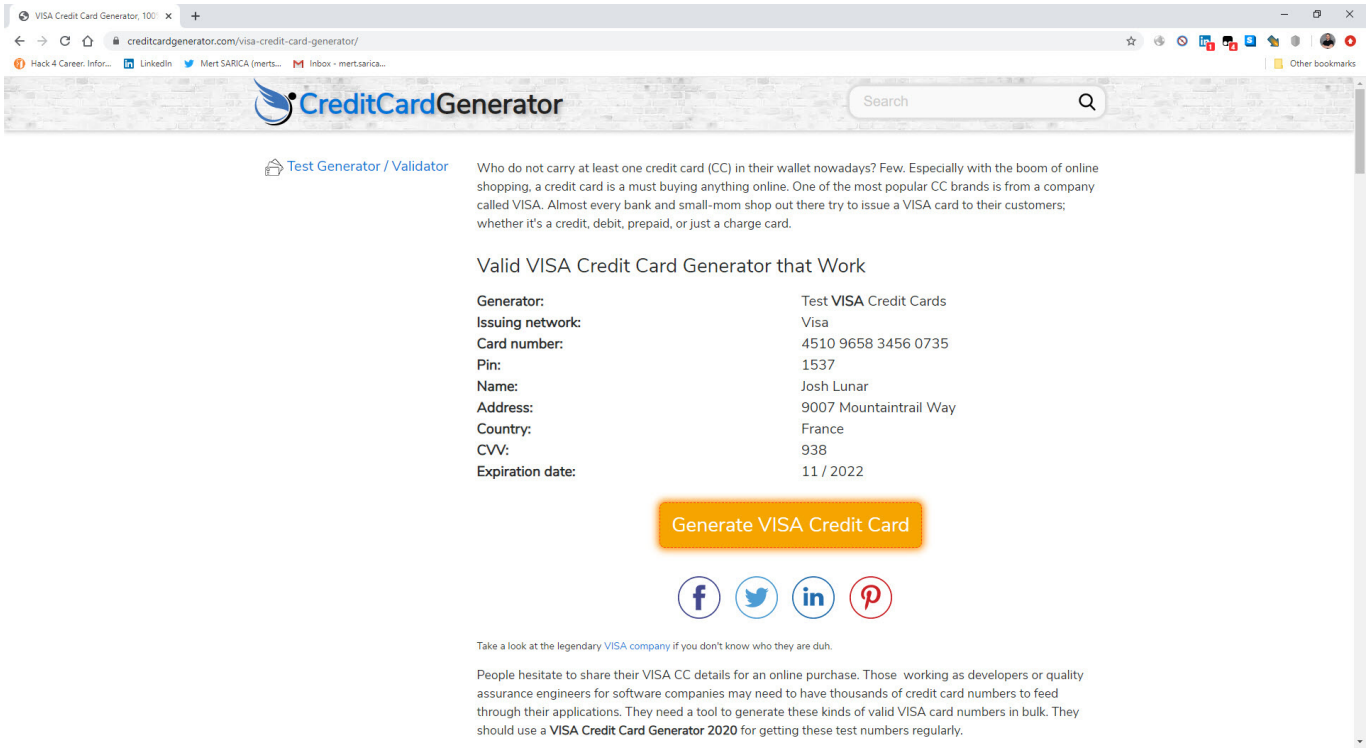


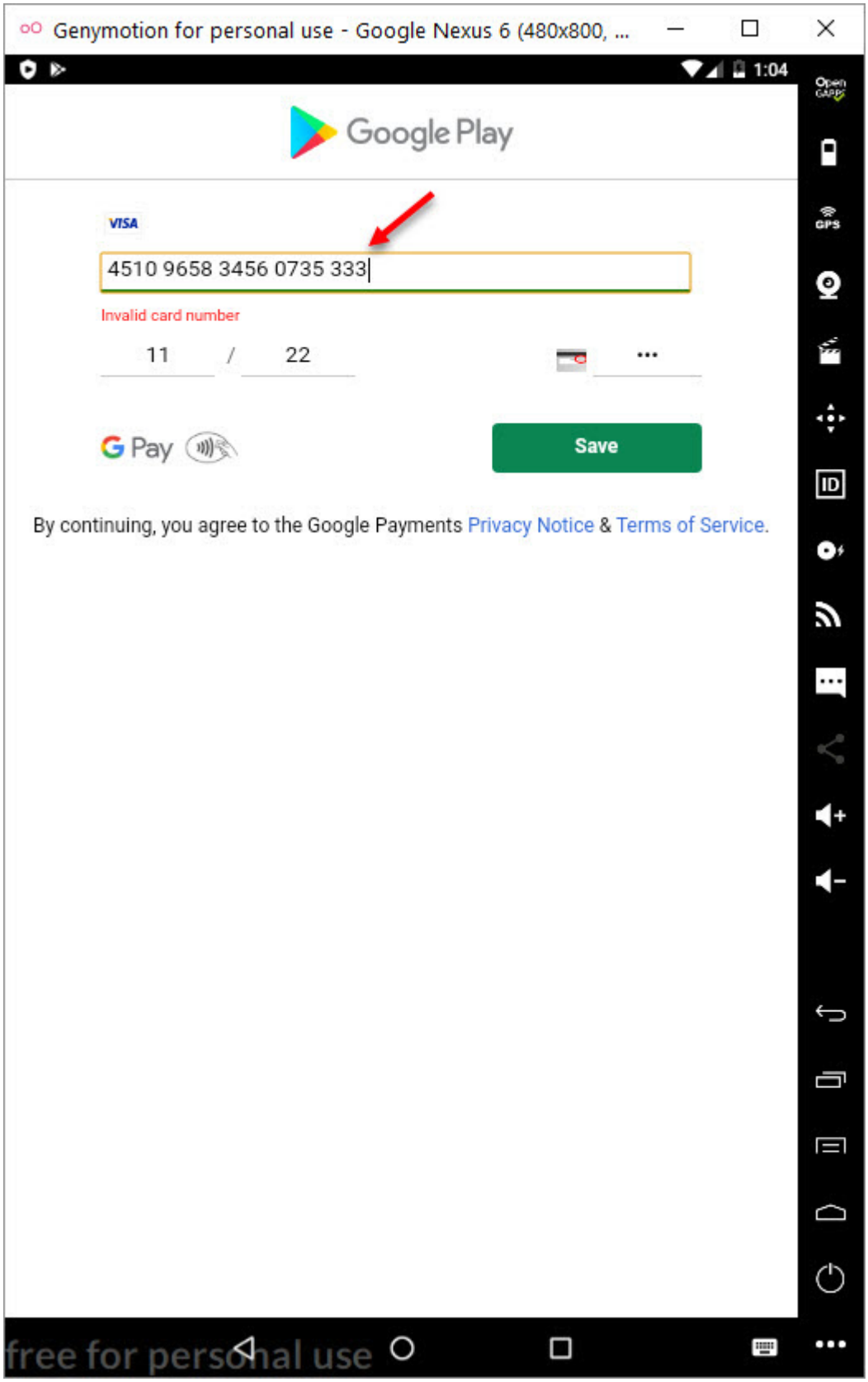
Sanal Android işletim sistemimde herhangi bir bankacılık uygulaması yüklü olmadığı için karşıma kredi kartı bilgimi çalmak üzere oluşturulmuş Google Play ekranı çıktı. Test için oluşturulan 16 haneli bir kredi kartı numarası girdiğimde kaydetme butonunun (SAVE) etkinleşmediğini gördüm. Kredi kartı hanesini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

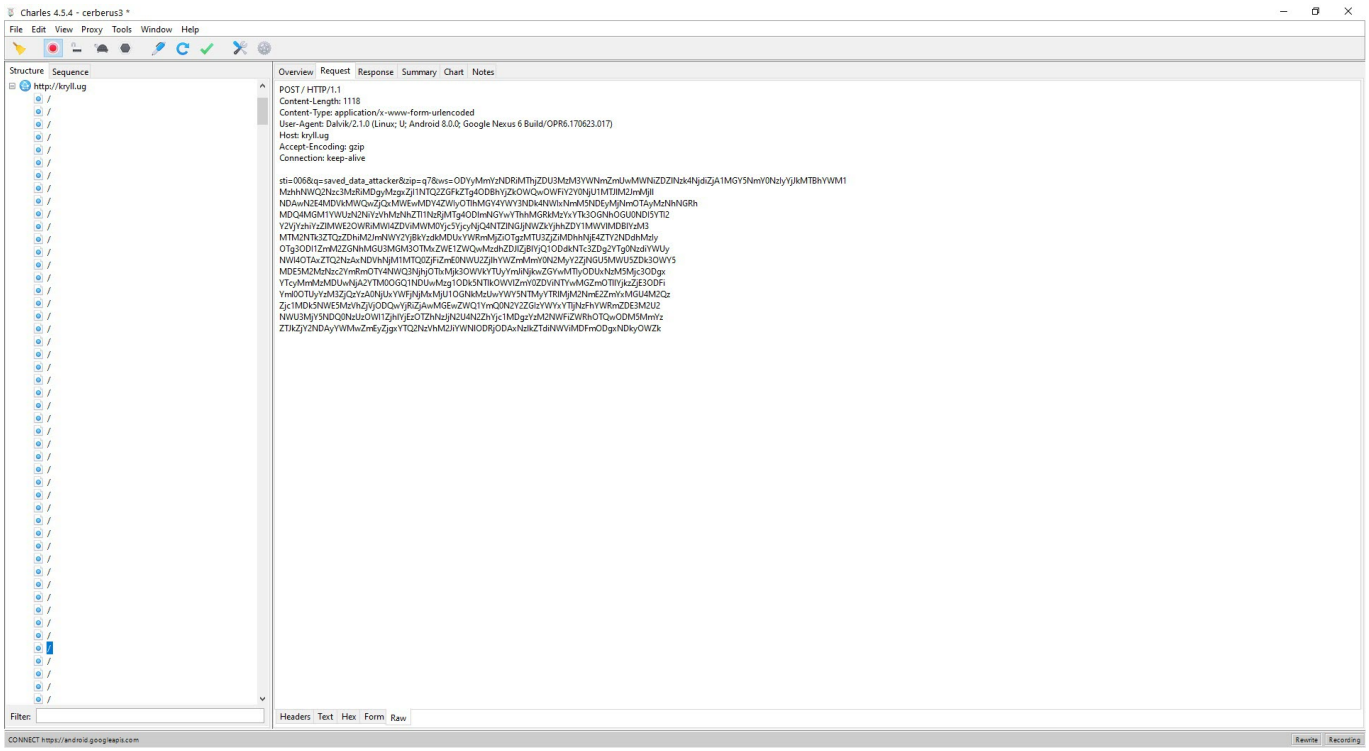
forma yönelik yapmış ve böyle bir hata ortaya çıkmıştı. Girdiğim tüm bilgilerin komuta kontrol merkezine şifreli olarak gittiğini gördükten sonra şifreleme anahtarının da peşine düşmeye karar verdim.



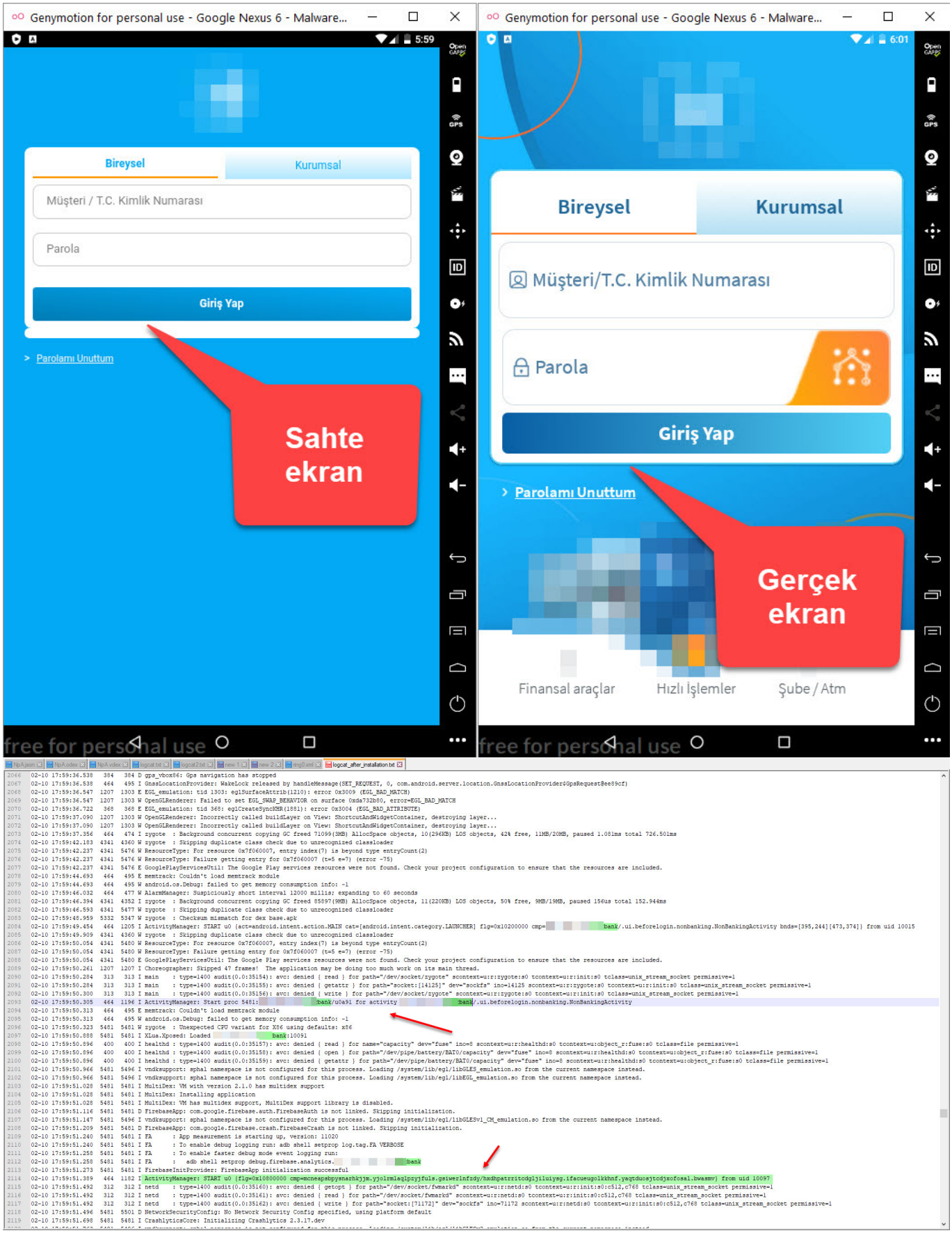

Genymotion for personal use - Google Nexus 6 (480x800, ...
1:01
Google Play
Osman
Turkey
Istanbul
Kadikoy
34878
+902163534466
G Pay
Continue
By continuing, you agree to the Google Payments Privacy Notice & Terms of Service.
free for personal use


VISA Credit Card Generator, 100
creditcardgenerator.com/visa-credit-card-generator/
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Other bookmarks
CreditCardGenerator
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.


Genymotion for personal use - Google Nexus 6 (480x800, ...
1:04
Google Play
VISA
4510 9658 3456 0735 333
Invalid card number
11
/
22
G Pay
Save
By continuing, you agree to the Google Payments Privacy Notice & Terms of Service.
free for personal use

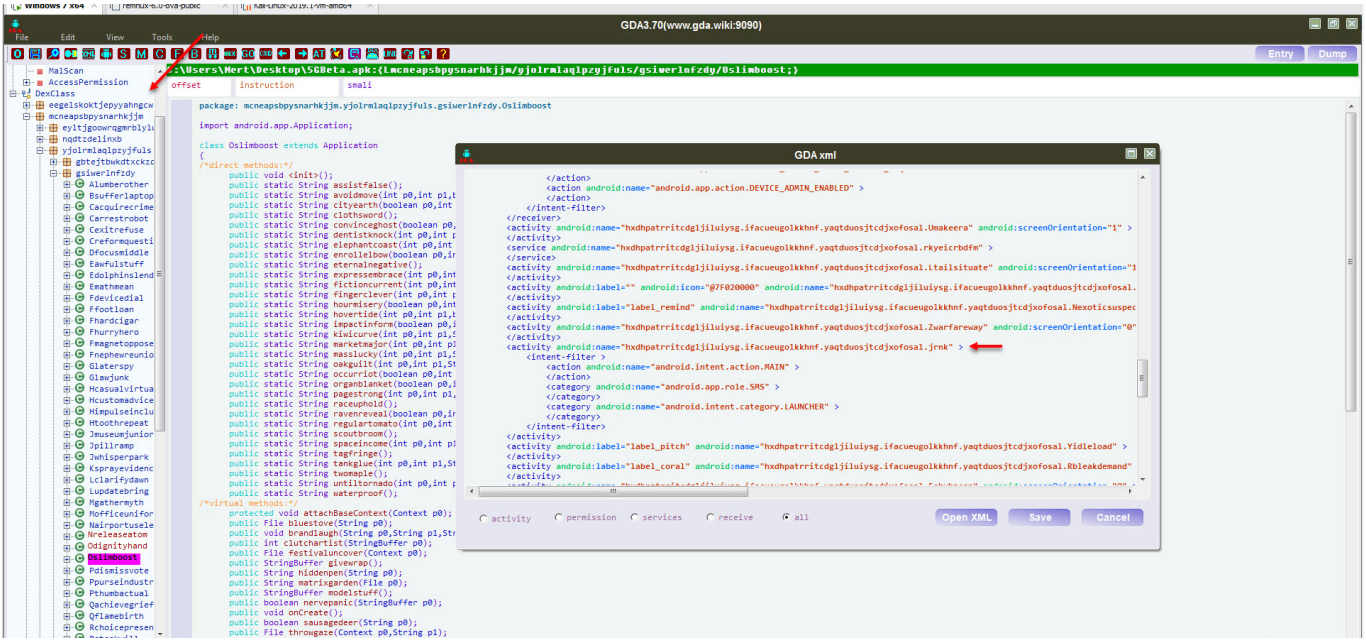


Şifreleme anahtarından önce zararlı uygulamanın bankacılık bilgilerini çalıp çalmadığını teyit etmek için sanal sistemim üzerine 10 tane bankanın mobil uygulamasını yükledim ve teker teker çalıştırmaya başladım. Yaptığım testler sonucunda zararlı uygulama, hedef aldığı mobil bankacılık uygulaması çalıştığı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

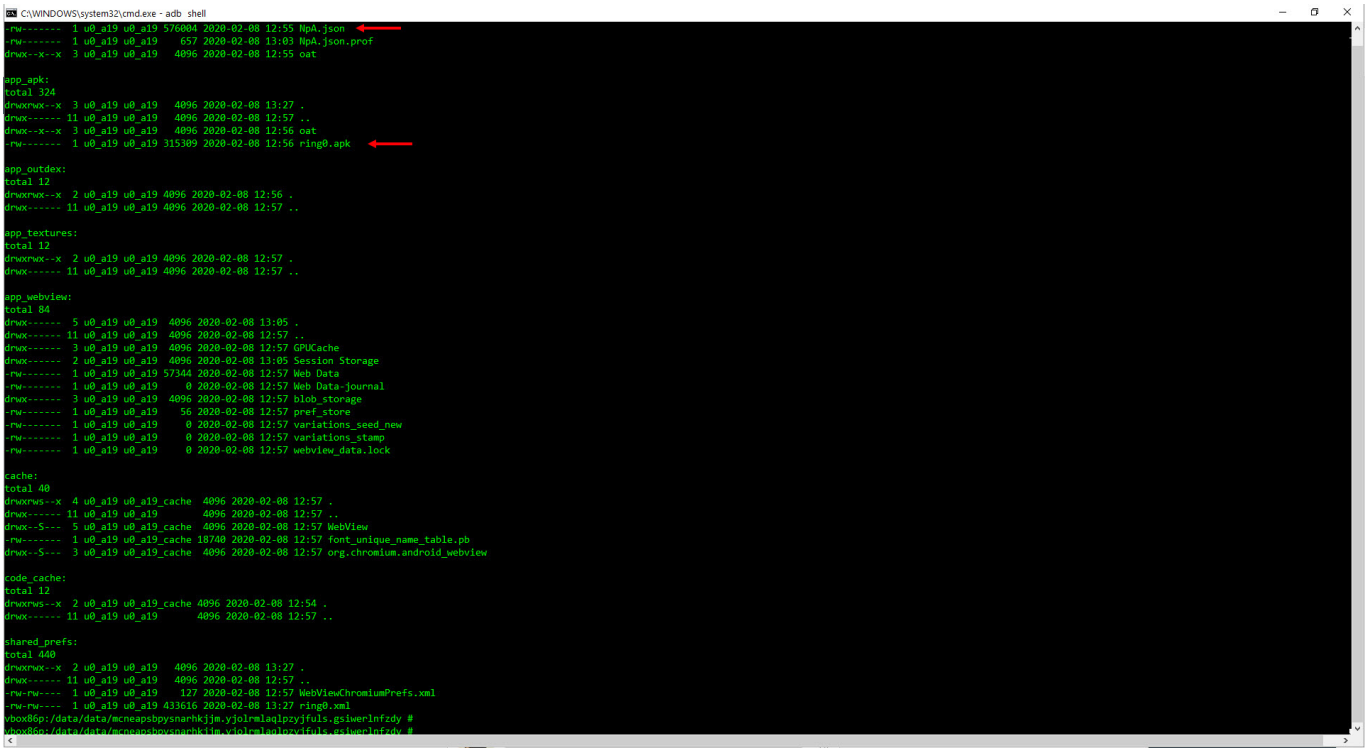


Şifreleme anahtarını bulmak için GDA aracı ile 5GBeta.apk uygulamasını kaynak kodunu çevirip uygulama ile ilgili temel bilgilerin yer aldığı AndroidManifest.xml dosyasına baktığımda, zararlı uygulama başlatıldığında ilk çalışacak olan MainActivity sınıfı ile kaynak kodu arasındaki sınıfların

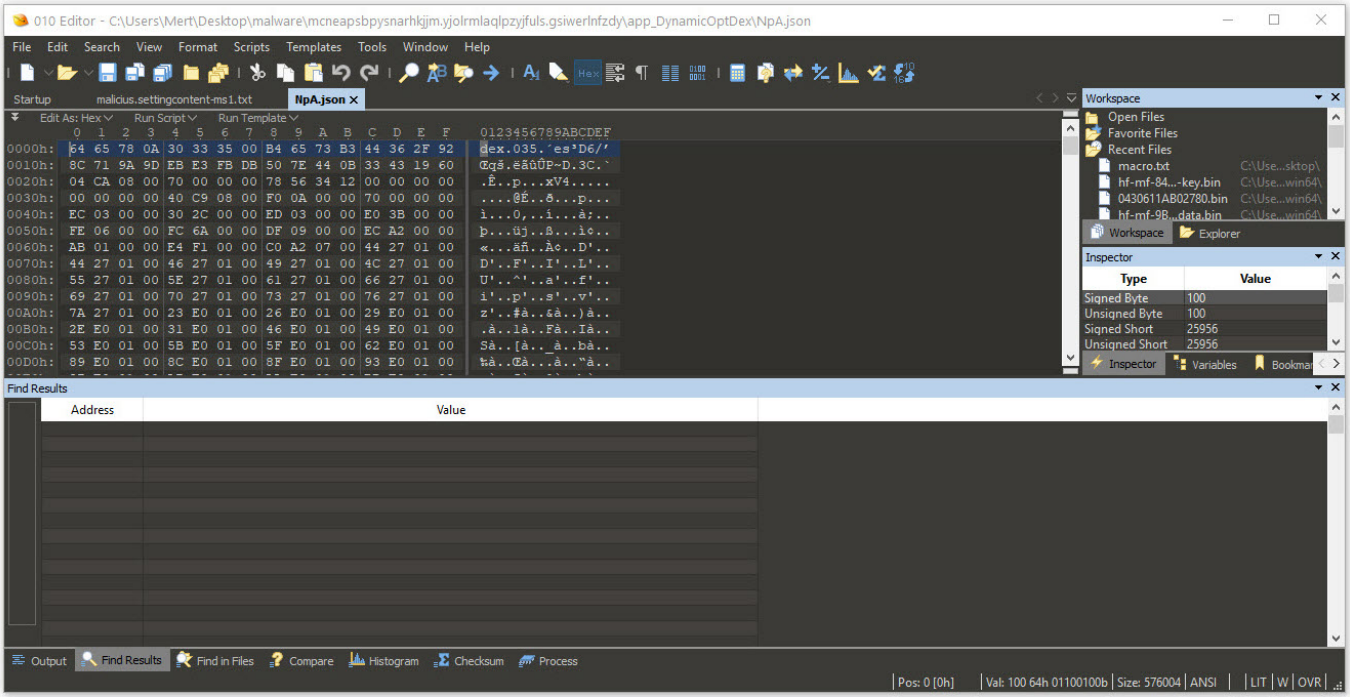
farklı olduğunu gördüm. Bu da zararlı kod bloğunun dinamik olarak çalışma esnasında yüklendiğine işaret ediyordu.

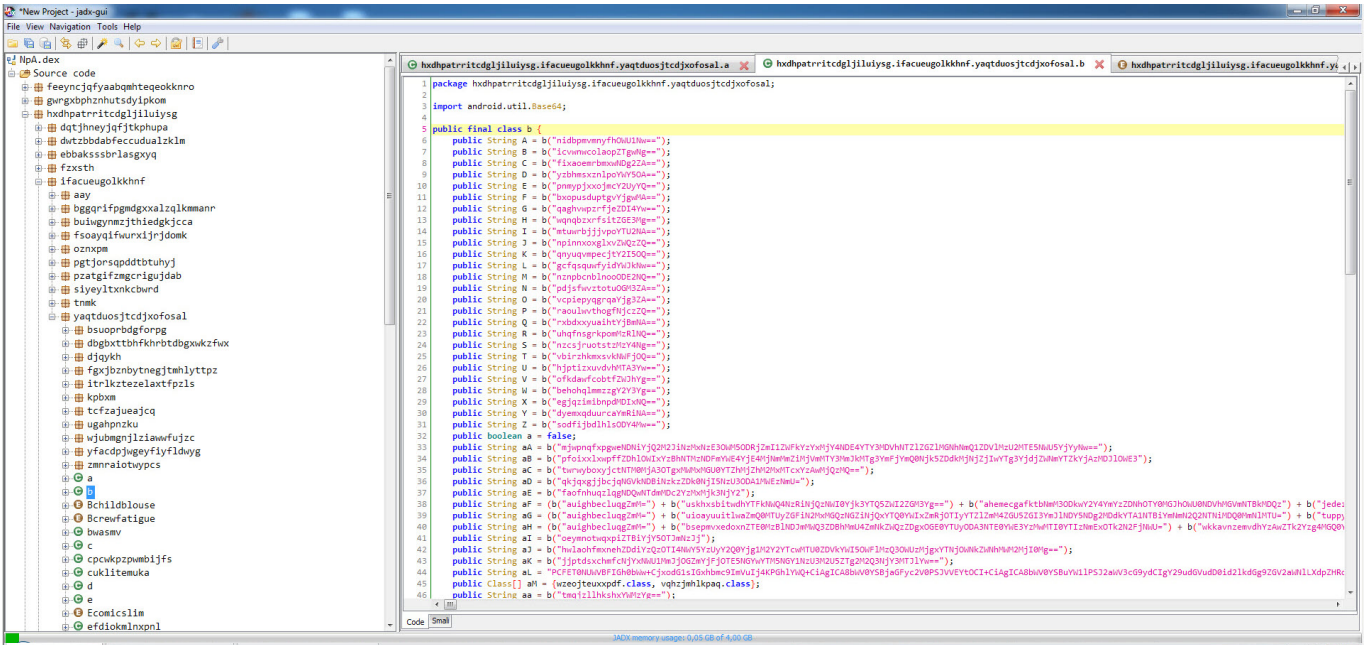


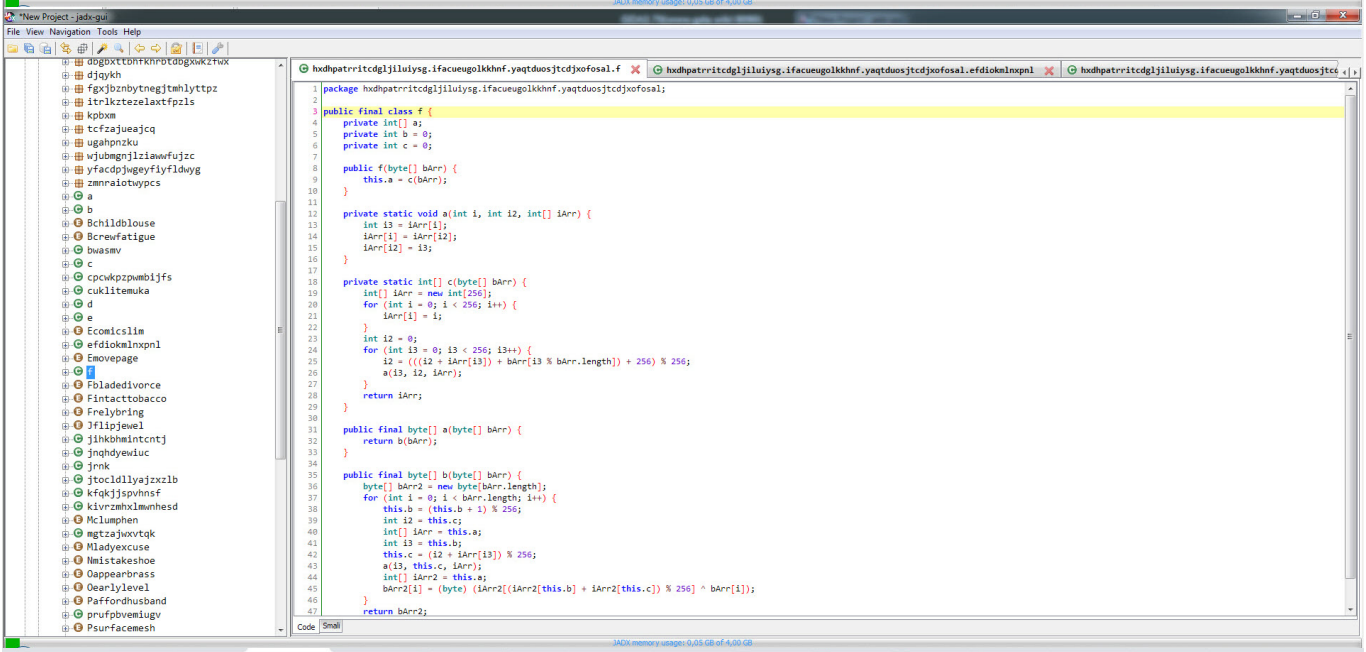
Zararlı uygulamanın yüklü olduğu /data/data/mcneapsbpysnarhkjjm.yjolrmlaqlpzyjfuls.gsiwerlnfzdy klasörüne baktığımda boyutu büyük olan ring0.apk ve NpA.json dosyaları dikkatimi çekti. NpA.json dosyasının aslında bir DEX dosyası olduğunu öğrenip jadx aracı ile kaynak koduna çevirdiğimde AndroidManifest.xml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

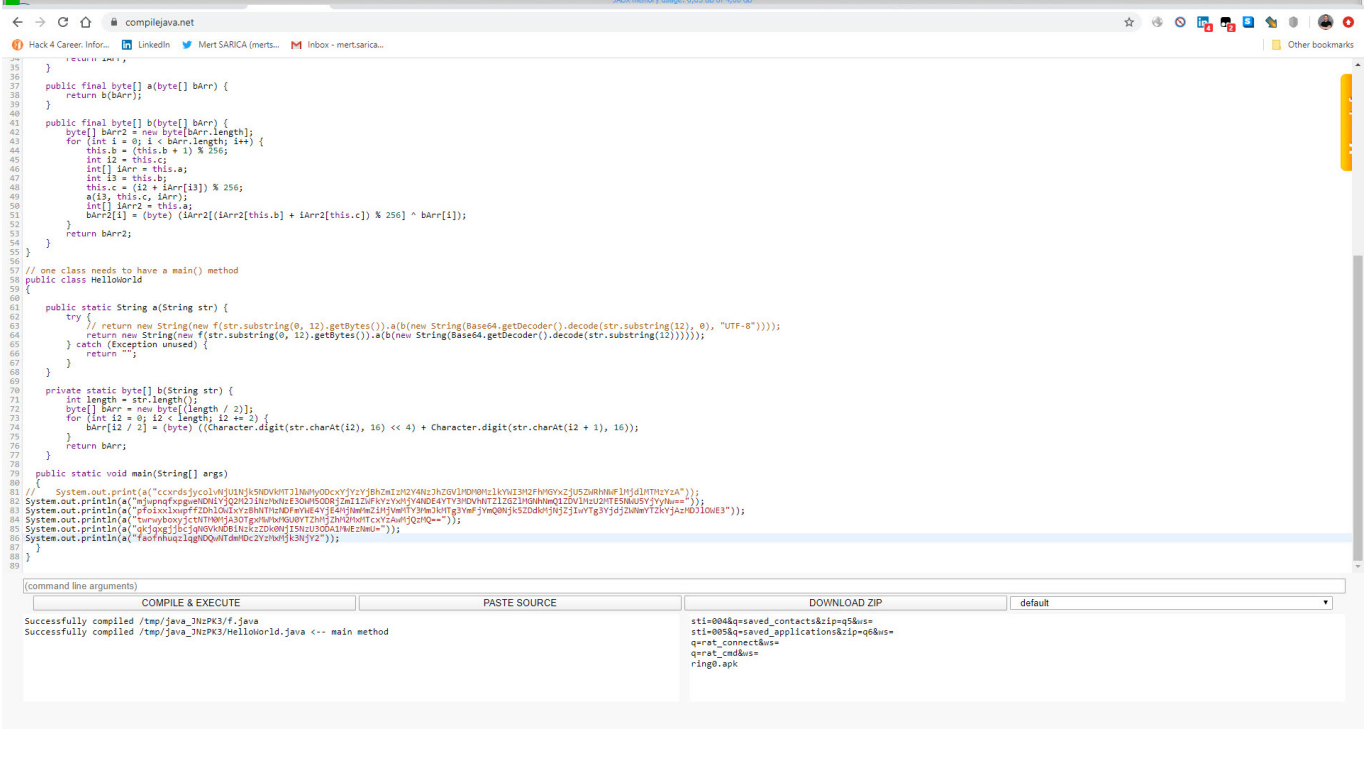


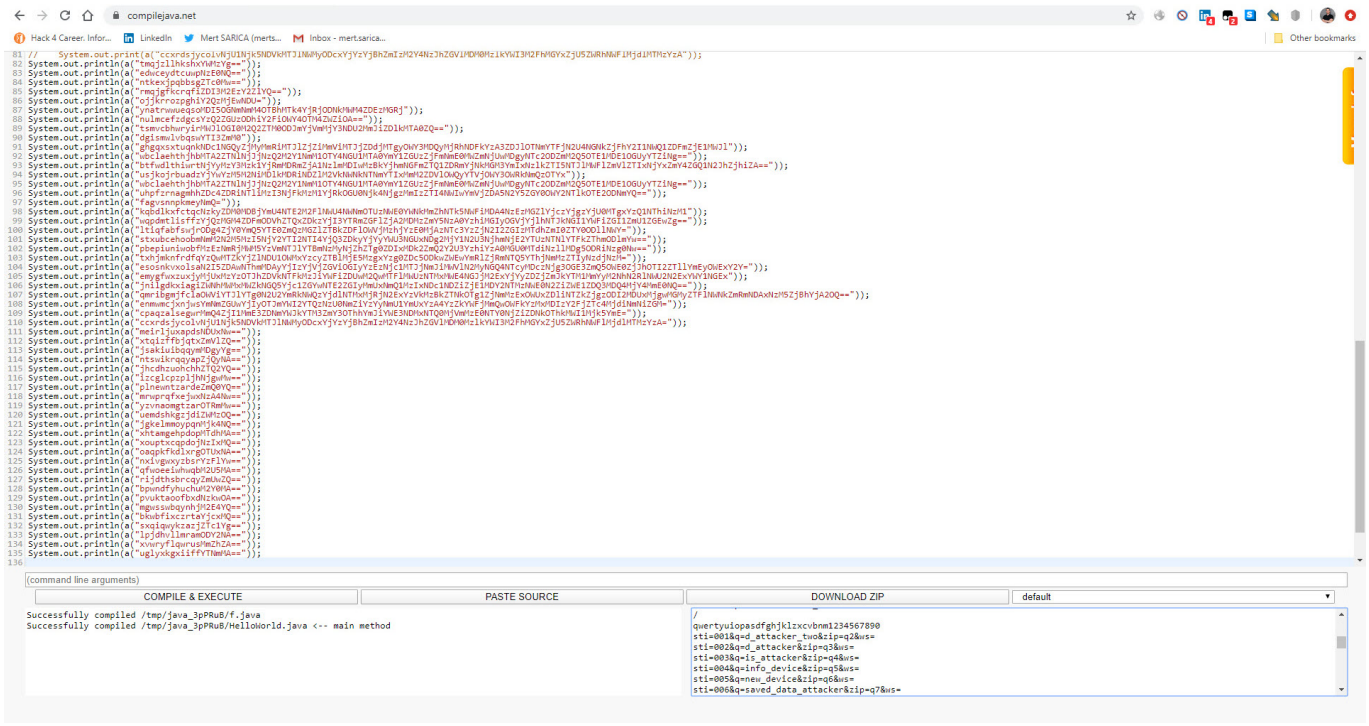
Şifrelenmiş karakter dizilerini incelediğimde f sınıfının şifreleri çözmekten sorumlu olduğunu öğrendim. Bunu yapmak için şifreli karakter dizisinin RC4 anahtarı olan ilk 12 karakterini alıp, BASE64 ile çözülen geri kalan karakterlerin şifresini bu anahtar sayesinde çözüyordu. (Örnek şifreli karakter dizisi mjwpnqfxpgweNDNiYjQ2M2JiNzMxNzE3OWM5ODRjZmI1ZWFkYzYxMjY4NDE4YTY3MDVhNTZlZGZlMGNhNmQ1ZDVlMzU2MTE5NWU5YjYyNw== ise RC4 şifreleme anahtarı mjwpnqfxpgwe değeri oluyor. Bu anahtar ile geri kalan şifreleri karakterleri (NDNiYjQ2M2JiNzMxNzE3OWM5ODRjZmI1ZWFkYzYxMjY4NDE4YTY3MDVhNTZlZGZlMGNhNmQ1ZDVlMzU2MTE5NWU5YjYyNw==) 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.



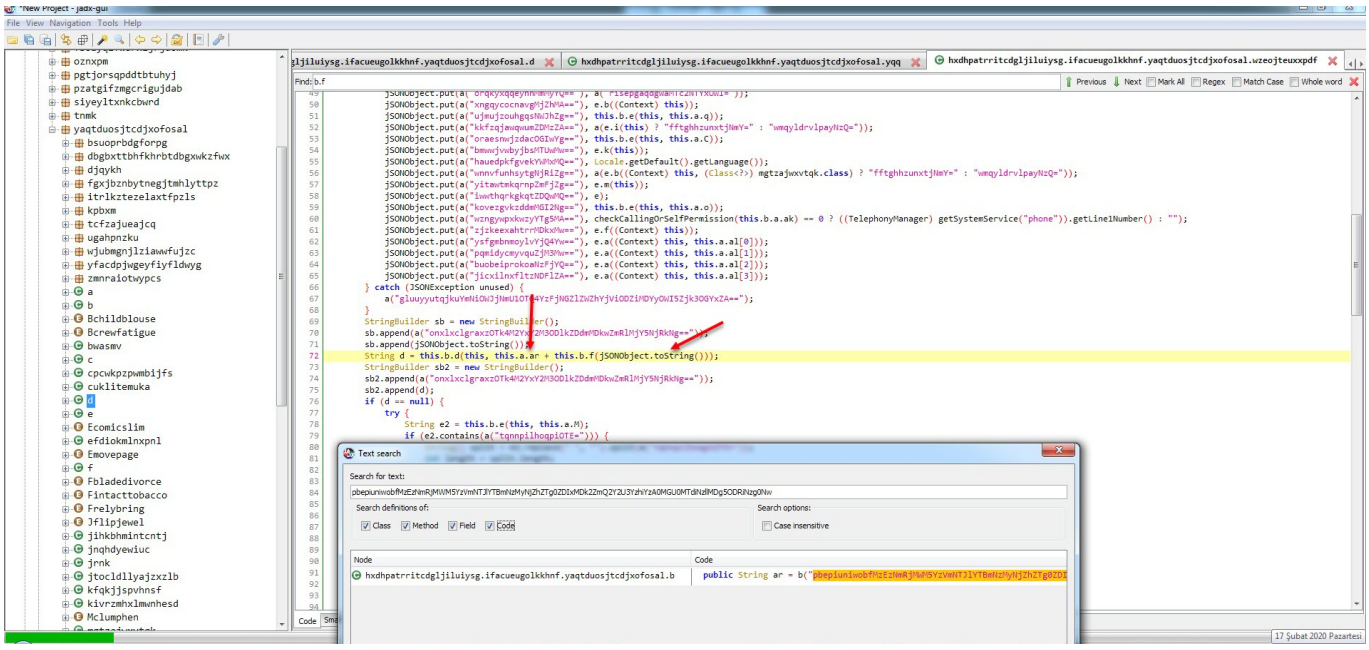

*New Project - jadx-gui
File View Navigation Tools Help
NpA.dex
Source code
hxdhpatrritcdgljliuiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal.a
hxdhpatrritcdgljliuiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal.b
package hxdhpatrritcdgljliuiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal;
import android.util.Base64;
public final class b {
Code
Smal
JADX memory usage: 0,05 GB of 4,00 GB

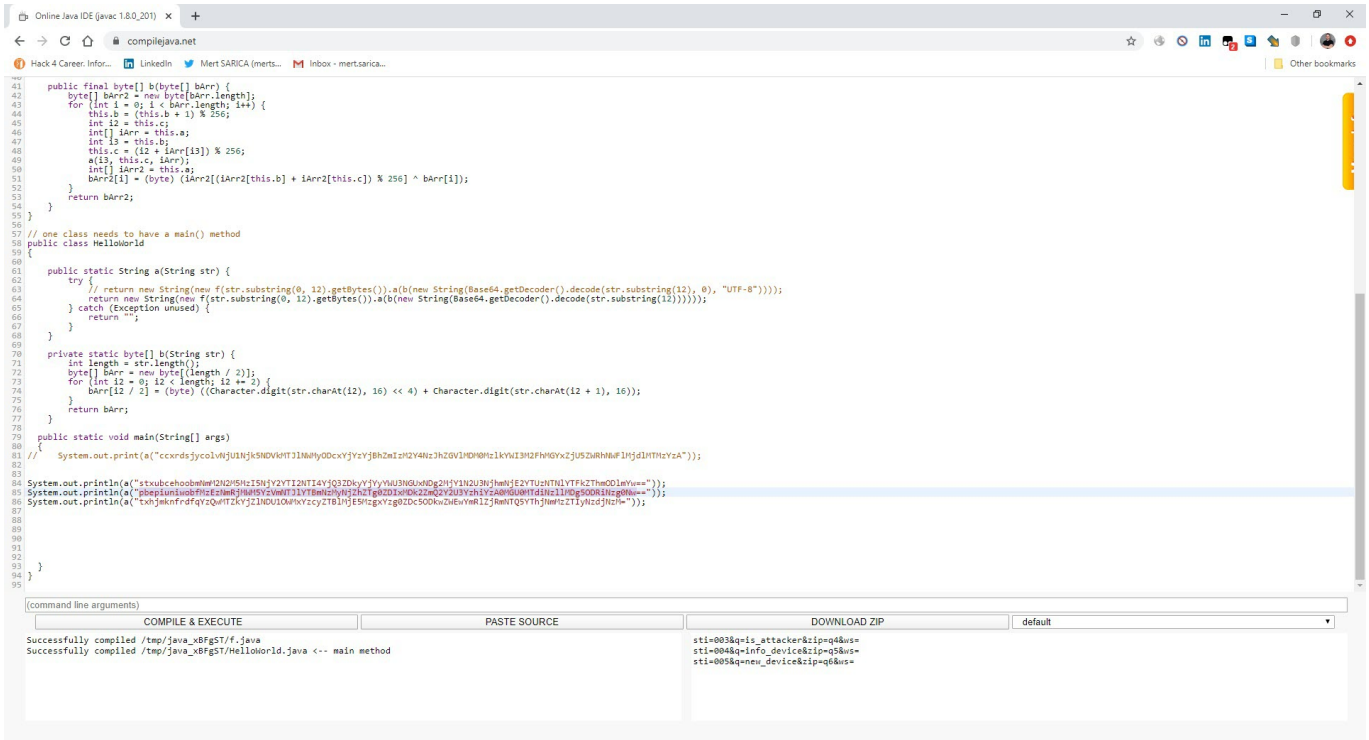

*New Project - jadx-gui
File View Navigation Tools Help
hxdhpatrritcdgljliuiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal.f
hxdhpatrritcdgljliuiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal.efdiokmlnxpnl
package hxdhpatrritcdgljliuiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal;
public final class f {
Code
Smal
JADX memory usage: 0,05 GB of 4,00 GB

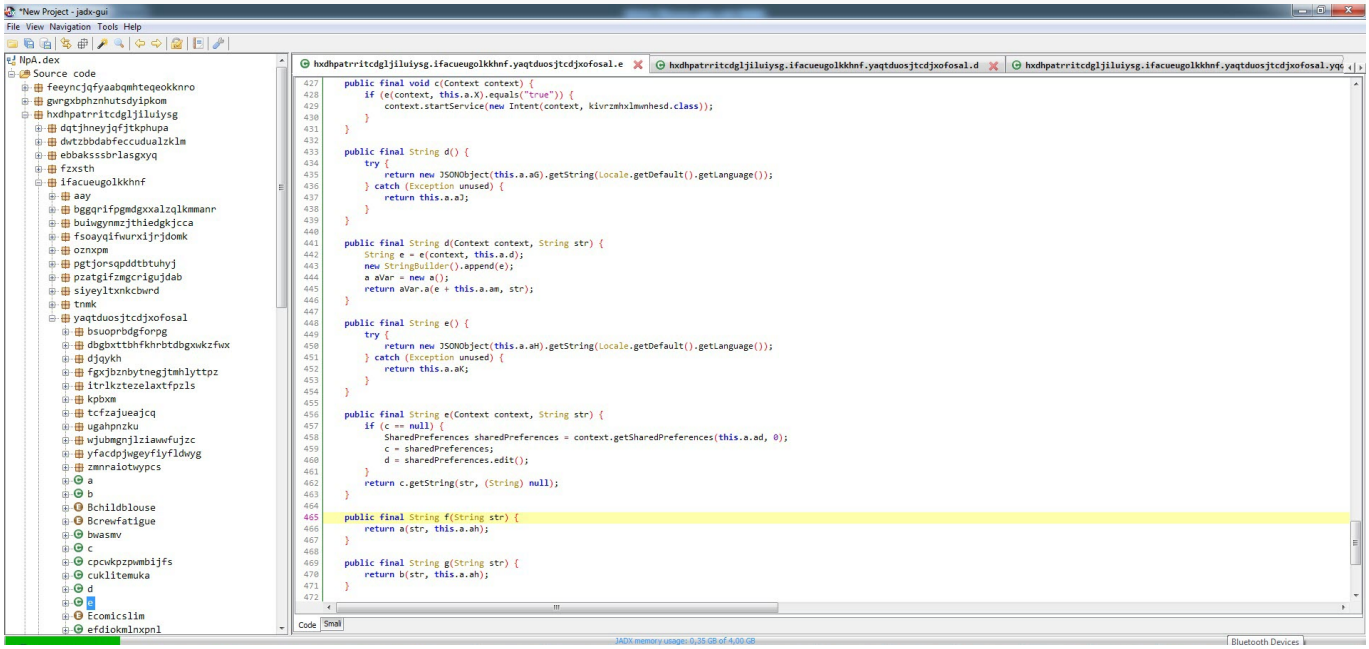

compilejava.net
(command line arguments)
COMPILE & EXECUTE
PASTE SOURCE
DOWNLOAD ZIP
default
Successfully compiled /tmp/java_JNzPK3/f.java
Successfully compiled /tmp/java_JNzPK3/HelloWorld.java <-- main method

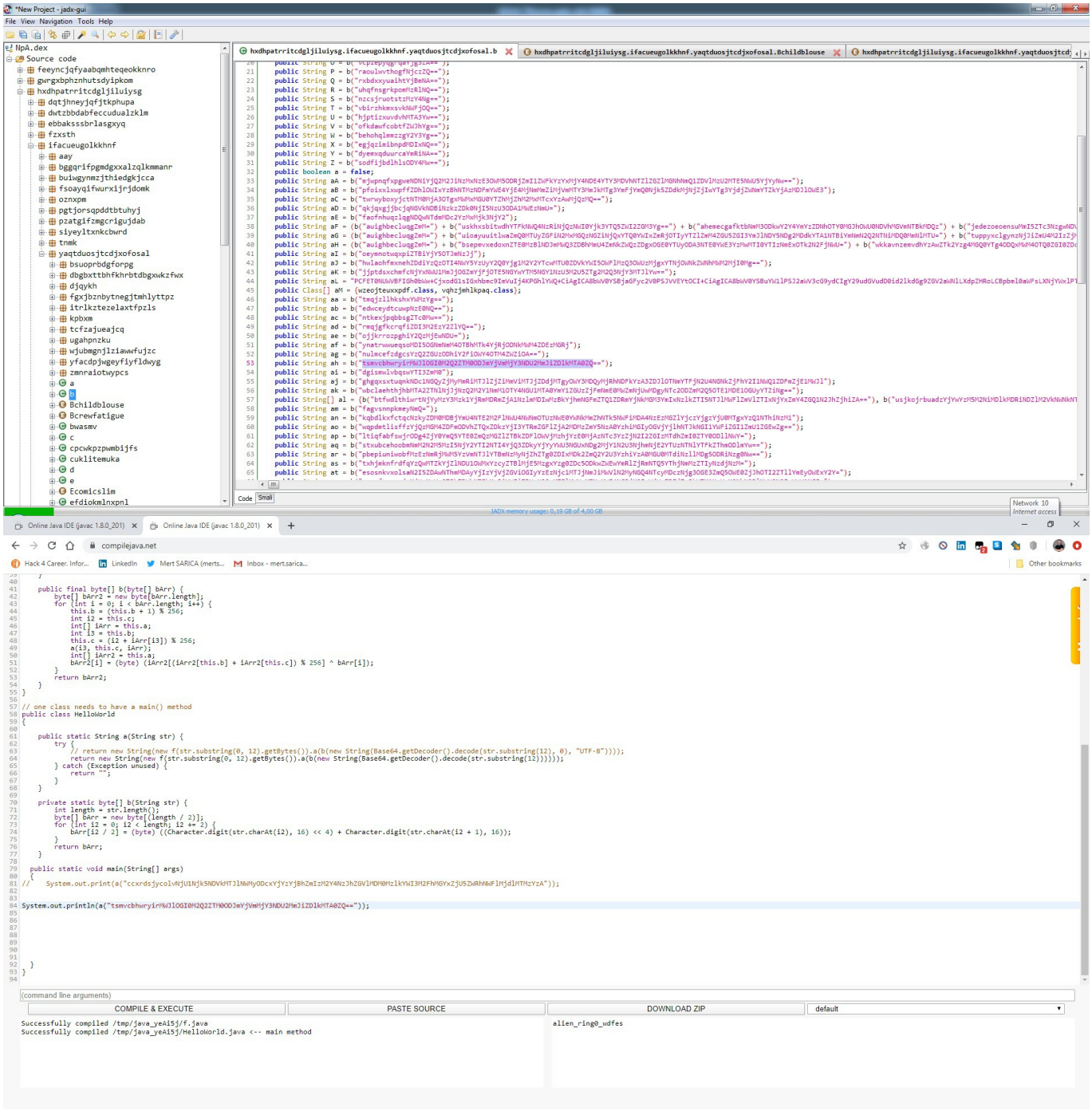


Komuta kontrol merkezine gönderilen şifreli verilerin şifreleme anahtarını bulmak için şifresi çözülmüş karakter dizilerinde JSON geçtiğini gördüğüm için kodda bu sınıfın kullanıldığı noktalara odaklandım. Zararlı uygulama çalıştıktan sonra komuta kontrol merkezine belli periyotlarda sti=004&q=info_device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

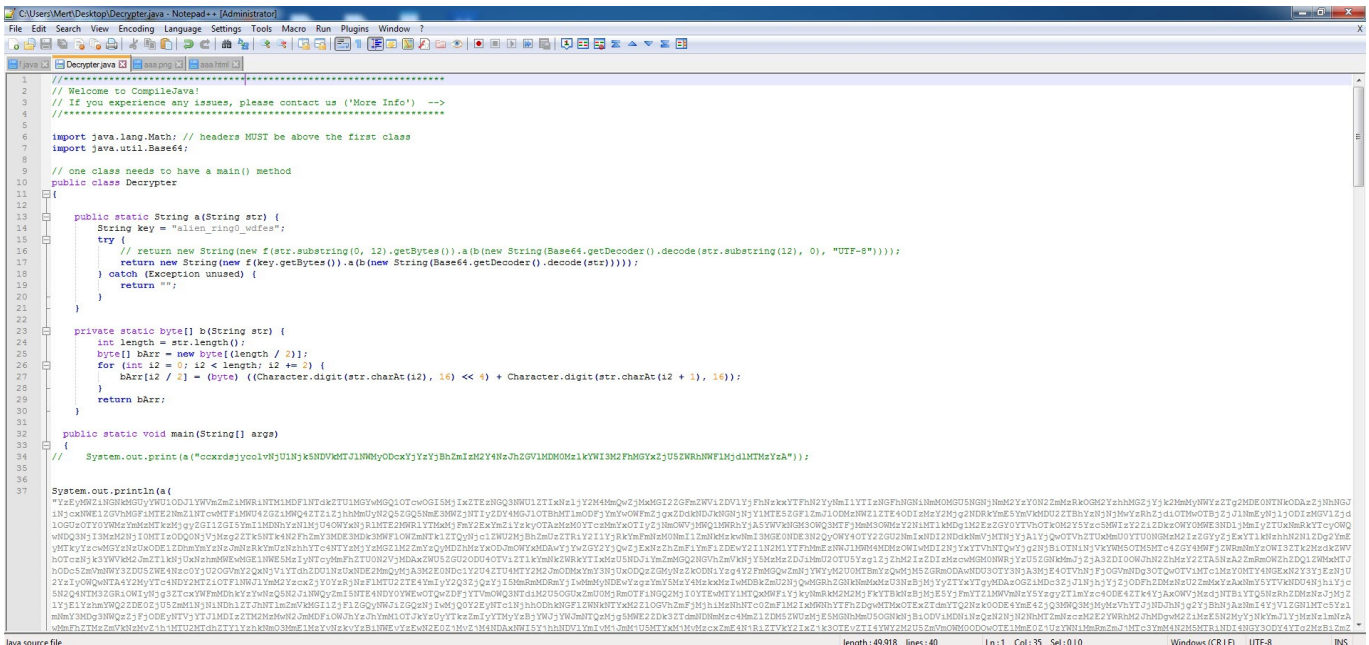


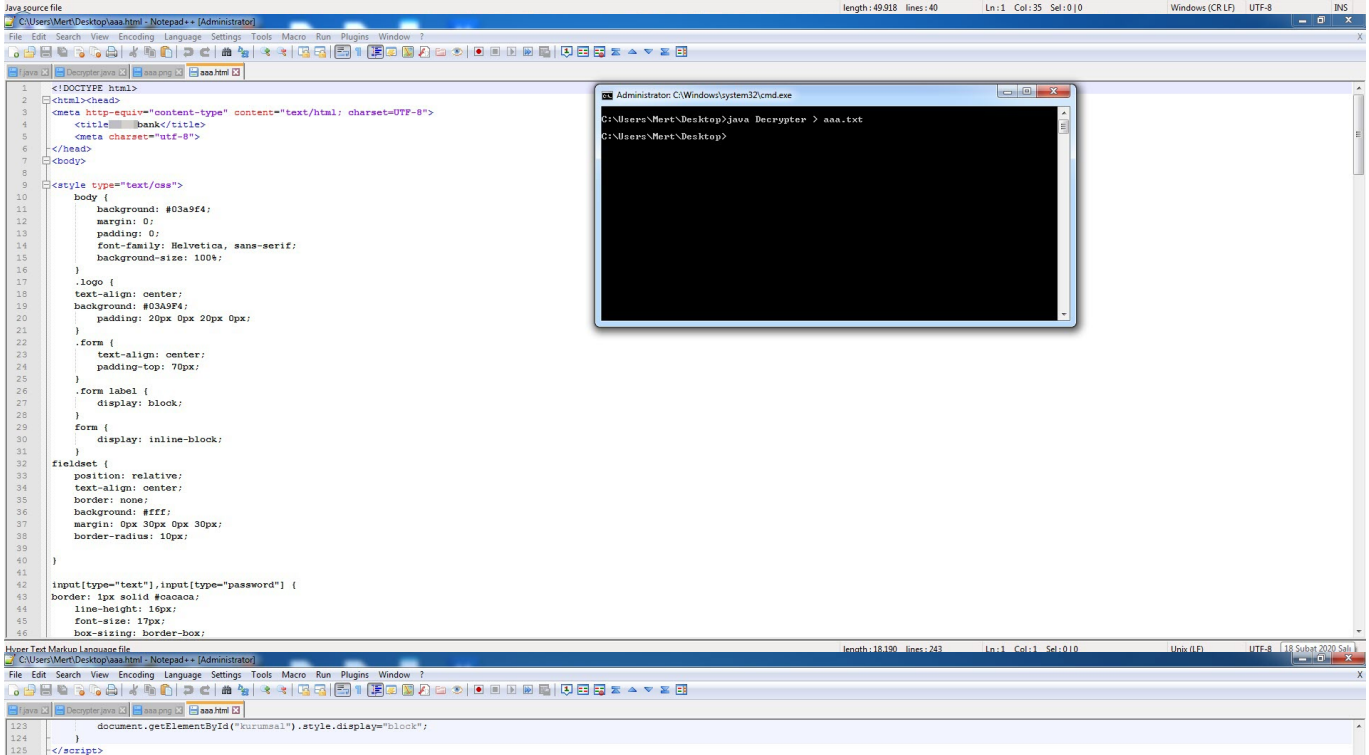

Online Java IDE (javac 1.8.0_201)
compilejava.net
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Other bookmarks
(command line arguments)
COMPILE & EXECUTE
PASTE SOURCE
DOWNLOAD ZIP
default
Successfully compiled /tmp/java_xBFgST/f.java
Successfully compiled /tmp/java_xBFgST/HelloWorld.java <-- main method
sti=003&q=is_attacker&zip=q4&ws=
sti=004&q=info_device&zip=q5&ws=
sti=005&q=new_device&zip=q6&ws=

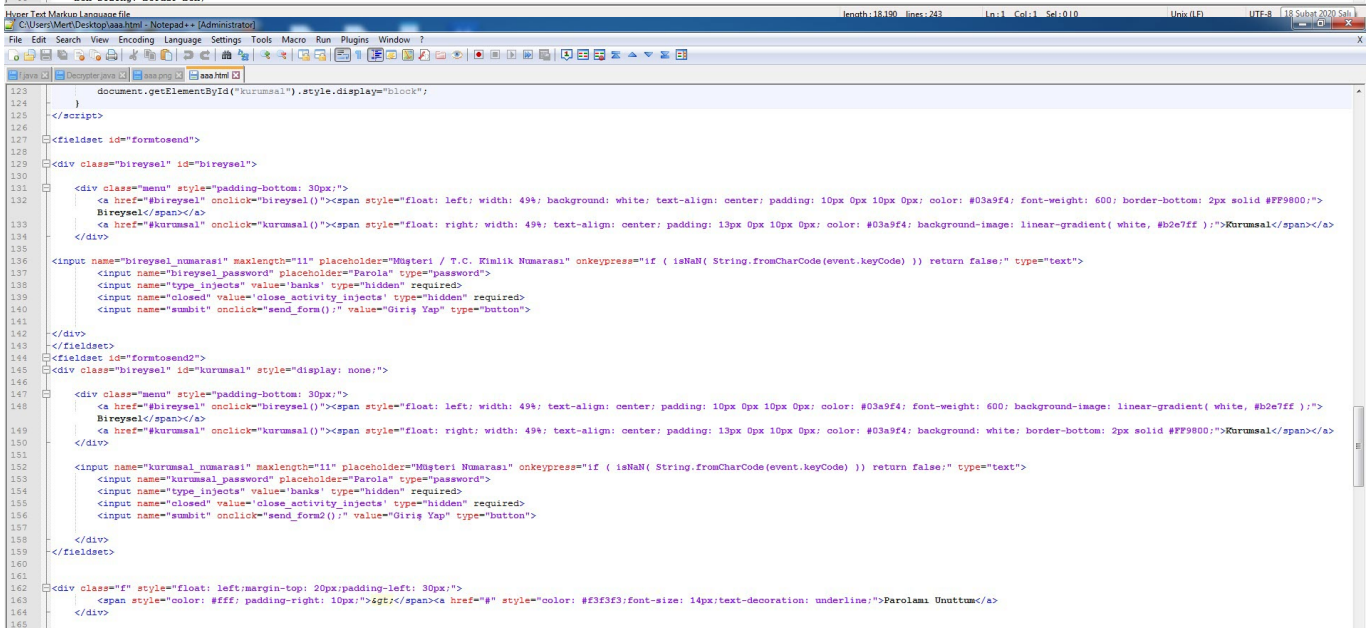

*New Project - jadx-gui
File View Navigation Tools Help
NpA.dex
Source code
hxdhpatrritcdgljiluiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal.e
hxdhpatrritcdgljiluiysg.ifacueugolkkhnf.yaqtduosjtcdjxofosal.d
Code
Smali
Bluetooth Devices



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.


C:\Users\Mert\Desktop\Decrypter.java - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Decrypter.java
aaa.png
aaa.html
//**********
// Welcome to CompileJava!
// If you experience any issues, please contact us ('More Info') -->
//**********
import java.lang.Math; // headers MUST be above the first class
import java.util.Base64;
// one class needs to have a main() method
public class Decrypter
{
public static String a(String str) {
String key = "alien_ring0_wdfes";
try {
// return new String(new f(str.substring(0, 12).getBytes()).a(b(new String(Base64.getDecoder().decode(str.substring(12), 0), "UTF-8"))));
return new String(new f(key.getBytes()).a(b(new String(Base64.getDecoder().decode(str))))); } catch (Exception unused) {
return "";
}
}
private static byte[] b(String str) {
int length = str.length();
byte[] bArr = new byte[(length / 2)];
for (int i2 = 0; i2 < length; i2 += 2) {
bArr[i2 / 2] = (byte) ((Character.digit(str.charAt(i2), 16) << 4) + Character.digit(str.charAt(i2 + 1), 16));
}
return bArr;
}
public static void main(String[] args)
{
//   System.out.print(a("ccxrdsjycolvNjUiNjk5NDVkMTJlNWMyODcxYjYzYjBhZmIzM2Y4NzJhZGVlMDM0Mzlk YWI3M2FhMGYxZjU5ZWRhNWFlMjdlMTMzYzA"));
System.out.println(a(
Java source file
length : 49,918 lines : 40
Ln : 1 Col : 35 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS


C:\Users\Mert\Desktop\aaa.html - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
aaa.html
<!DOCTYPE html>
<html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<title bank</title>
<meta charset="utf-8">
</head>
<body>
<style type="text/css">
body {
background: #03a9f4;
margin: 0;
padding: 0;
font-family: Helvetica, sans-serif;
background-size: 100%;
}
.logo {
text-align: center;
background: #03A9F4;
padding: 20px 0px 20px 0px;
}
.form {
text-align: center;
padding-top: 70px;
}
.form label {
display: block;
}
form {
display: inline-block;
}
fieldset {
position: relative;
text-align: center;
border: none;
background: #fff;
margin: 0px 30px 0px 30px;
border-radius: 10px;
}
input[type="text"],input[type="password"] {
border: 1px solid #cacaca;
line-height: 16px;
font-size: 17px;
box-sizing: border-box;
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop>java Decrypter > aaa.txt
C:\Users\Mert\Desktop>
Hyper Text Markup Language file
length : 18,190 lines : 243
Ln : 1 Col : 1 Sel : 0 | 0
Unix (LF)
UTF-8
18 Subat 2020 Sal


C:\Users\Mert\Desktop\aaa.html - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
aaa.html
document.getElementById("kurumsal").style.display="block";
}
</script>
<fieldset id="formtosend">

Bireysel
Kurumsal

<input name="bireysel_numarasi" maxlength="11" placeholder="Müşteri / T.C. Kimlik Numarası" onkeypress="if (isNaN(String.fromCharCode(event.keyCode))) return false;" type="text">
<input name="bireysel_password" placeholder="Parola" type="password">
<input name="type_injects" value='banks' type="hidden" required>
<input name="closed" value='close_activity_injects' type="hidden" required>
<input name="sumbit" onclick="send_form();" value="Giriş Yap" type="button">

</fieldset>
<fieldset id="formtosend2">

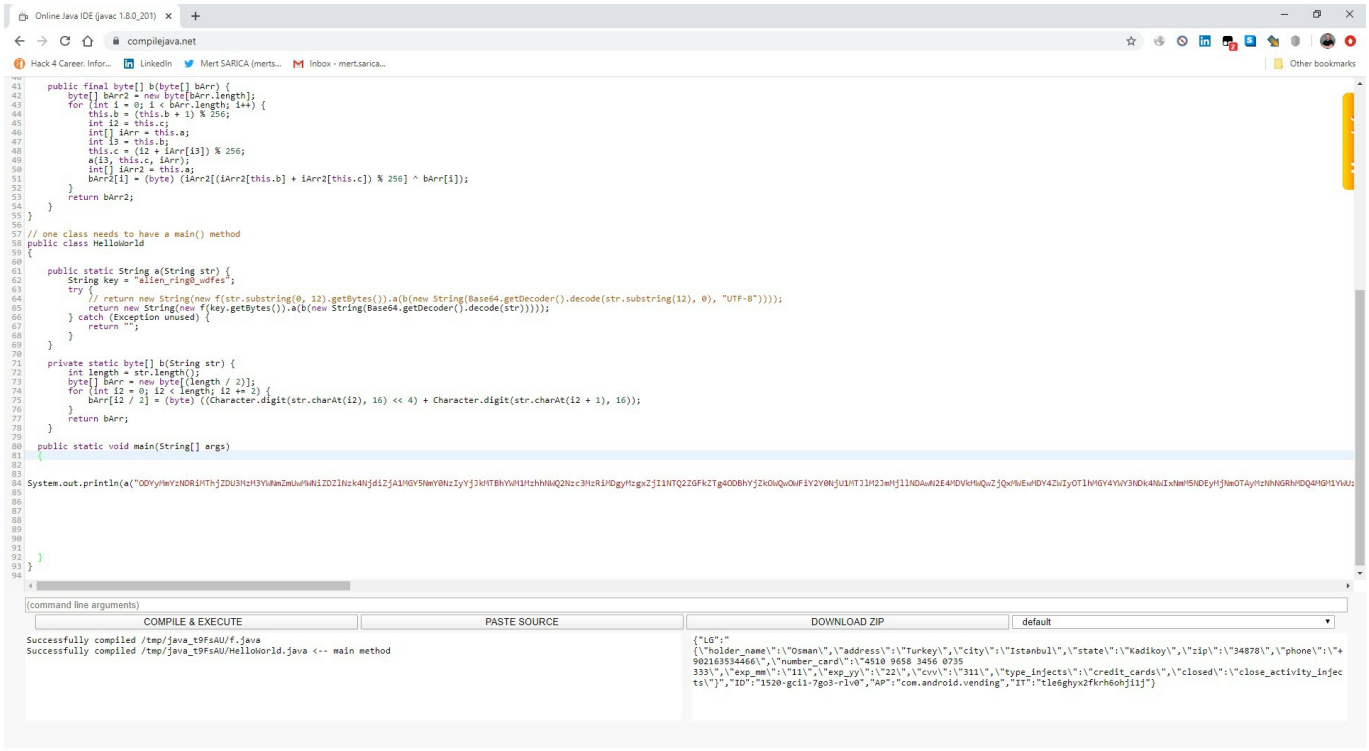
Bireysel
Kurumsal

<input name="kurumsal_numarasi" maxlength="11" placeholder="Müşteri Numarası" onkeypress="if (isNaN(String.fromCharCode(event.keyCode))) return false;" type="text">
<input name="kurumsal_password" placeholder="Parola" type="password">
<input name="type_injects" value='banks' type="hidden" required>
<input name="closed" value='close_activity_injects' type="hidden" required>
<input name="sumbit" onclick="send_form2();" value="Giriş Yap" type="button">

</fieldset>

>Parolamı Unuttum

<script>
Solve PC issues: 2 important messages



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.