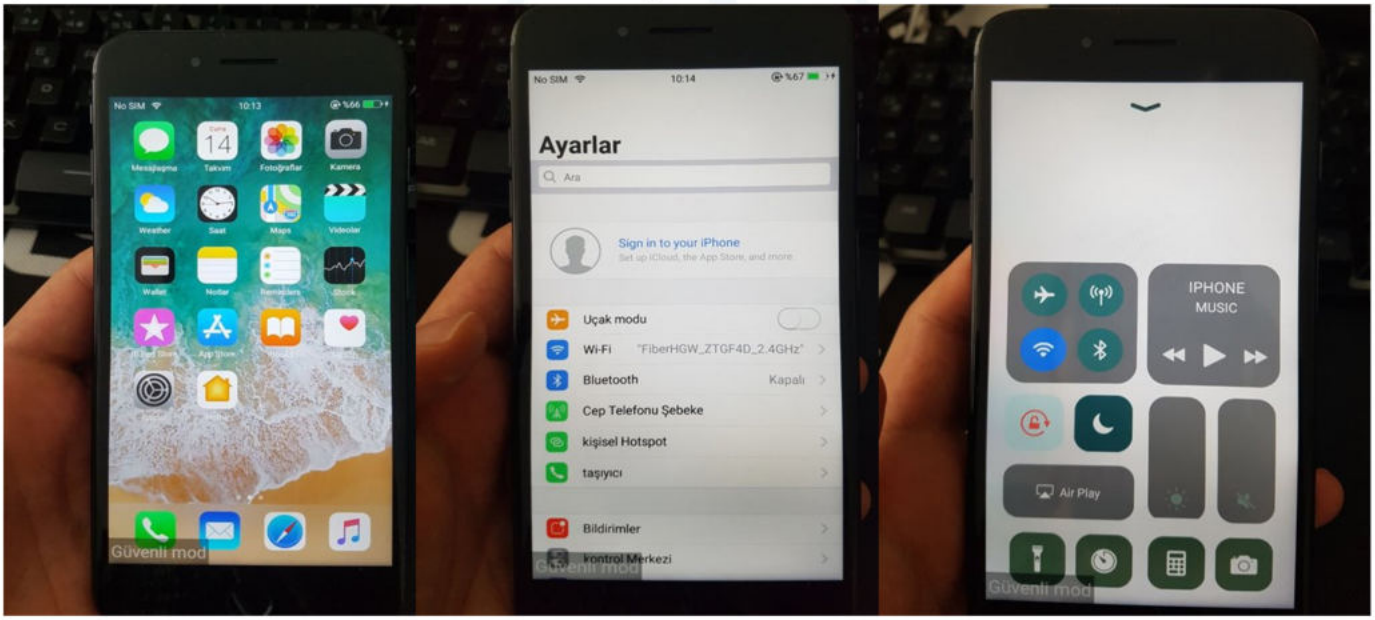
HUNTING MALWARE IN CLONE IPHONE

GAIS
Cyber Security

www.gaissecurity.com

Hunting Malware in Clone Iphone

Çin menşei merdiven altı üretilen bu cihazlar, parçaları farklı üreticilerden toplanarak, içerisine kasıtlı bir şekilde sisteme özel olarak tasarlanmış zararlı ve dahili yazılımlar yüklenerek paketlenirler. Ürünlerin, Türkiye dahil birçok ülkeye kaçak yollardan girişi sağlanmaktadır. Ayrı bölgelerde toplanan parçalar farklı bir bölgede paketlenmekte ve bu cihazlar kaçak yollarla ülkelerin pazarlarında yer almaktadır. Ürünler Çin merkezli e-ticaret sitelerinde farklı markalar altında satılmaktadır. Türkiye içerisinde rastgele bir telefoncudan edinilen bir clone Iphone cihaz incelenmek üzere satın alınmıştır.



Cihazlar uygun fiyatlarıyla satıldığından ve pahalı markaların dış görünüşlerine benzetilerek tasarlandığından ötürü birçok kullanıcıya ulaşmayı başarmaktadır. İlk bakışta bu cihazların üst sınıf imitasyon edildiği ürünlerden pek bir farkı görülmemektedir. Ancak donanım ve yazılım seviyesinde karşımıza farklılıklar çıkmaktadır. Klon bir Iphone içerisinde IOS değil android bulundurmaktadır. Ve donanım özellikleri inceleneceği üzere alt seviye olduğu görülecektir.

Hunting Malware in Clone Iphone

Cihazın özellikleri bir program aracılığıyla görüntülendiğinde sistem özelliklerinin Apple firmasına ait Iphone cihazı gibi gösterilmeye çalışılmıştır. Ancak başarılı olunmadığı anlaşılmaktadır. Cihazın mediatek firmasının üretmiş olduğu 6580 kodlu SoC kartı olduğu aşağıdaki görselde görülmektedir.

> adb shell getprop

```
[ro.board.platform]: [mt6580]
[ro.boot.bootreason]: [wdt_by_pass_pwk]
[ro.boot.hardware]: [mt6580]
[ro.fota.platform]: [MTK6580_6.0]
```

Cihaz bir lightning kablo ile bilgisayara bağlanmıştır ve ADB (Android Debug Bridge),iile çalıştırılan getprop komutu ile cihazın tüm sisteminin bilgileri görüntülenmektedir.

MEDIATEK MT6580 SoC

- 4x ARM Cortex-A7 MPcore
- Mali 400 MP GPU
- 4x ARM Cortex-A7 MPcore

Cihaz içerisine Telegram mesajlaşma uygulaması yüklendiği anda telefon hakkında bilgileri içeren otomatize bir mesaj gelen kutusuna düşmüştür. Bu gelen mesajın bir online bot tarafından atıldığı ve telefonun içerisinde backdoor içeren bir uygulama tarafından veri giden bir sunucuda çalıştığı öngörülmüştür. Ayrıca cihaz içerisindeki bir adware yazılımın ekrana bastığı reklam görülmektedir.

backdoor app ?

Hunting Malware in Clone Iphone

> Adb shell

> pm list packages

```
shell@8 plus:/ $ pm list packages
package:com.mediatek.ppl
package:com.snowfish.aios.launcher
package:com.google.android.youtube
package:org.simalliance.openmobileapi.uicc2terminal
package:com.android.providers.telephony
package:com.adups.fota.sysoper
package:com.google.android.googlequicksearchbox
package:com.mediatek.camera
```

> pm path %package%

```
shell@8 plus:/ $ pm path com.mediatek.dataprotection
package:/system/plugin/DataProtection/DataProtection.apk
```

Sırada cihaz içerisindeki yüklü paketlerin konumlarına ve apk dosyalarına ulaşılarak statik kod analizi çerçevesinde incelenmesi hedeflenmektedir. Adb ile öncelikle paketlerin konumu öğrenilmiş ardından işlemleri kolaylaştıracak scriptler yazılarak tüm dosyalara ulaşılmıştır.

```python
import os

filepath = 'v.txt'

with open(filepath) as fp:
    line = fp.readline()
    cnt = 1
    while line:
        os.system("adb.exe pull path {} D:/STUFF/TOOLS/platform-tools/apks".format(line.strip()))
        line = fp.readline()
        cnt += 1
```

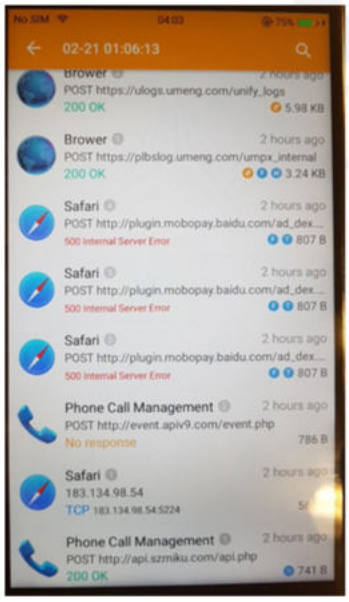
AdupsFota.apk	FprintCalibration.apk	MiraVision.apk	Uicc1Terminal.apk
AdupsFotaReboot.apk	framework-res.apk	MmsService.apk	Uicc2Terminal.apk
ApplicationsProvider.apk	FusedLocation.apk	MtkCalendar.apk	UserDictionaryProvider.apk
AtciService.apk	FwkPlugin.apk	MTKLogger.apk	VoiceCommand.apk
AutoDialer.apk	FWUpgrade.apk	MtkMms.apk	VoiceExtension.apk
Baidu_Location.apk	FWUpgradeProvider.apk	MusicFX.apk	VpnDialogs.apk
base.apk	Galaxy4.apk	MyFiles.apk	Wallet.apk
BasicDreams.apk	Gallery2.apk	NlpService.apk	WallpaperCropper.apk
BatteryWarning.apk	GoogleKorealME.apk	NoiseField.apk	webview.apk
Bluetooth.apk	GooglePartnerSetup.apk	Omacp.apk	WristService.apk
BluetoothMidiService.apk	GoogleServicesFramework.apk	OneTimeInitializer.apk	YGPS.apk
BSPTelephonyDevTool.apk	HoloSpiralWallpaper.apk	PackageInstaller.apk	zhixin-framework-res.apk

Çekilen uygulamaların zaman kazanmak ve ön bir filtrasyon işleminden geçirmek için aşağıdaki script vasıtası ile hashleri alınarak VirusTotal üzerinden sorgulatılmıştır.

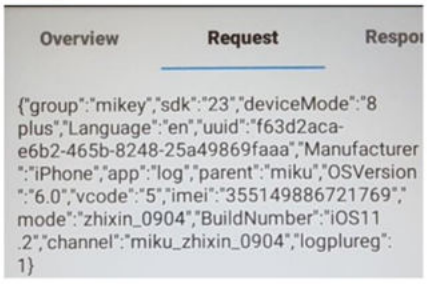
```python
from os import listdir
from os.path import isfile, join
import hashlib
import selenium

def md5(fname):
    hash_md5 = hashlib.md5()
    with open(fname, "rb") as f:
        for chunk in iter(lambda: f.read(4096), b""):
            hash_md5.update(chunk)
    return hash_md5.hexdigest()

onlyfiles = [f for f in listdir('D:/STUFF/TOOLS/platform-tools/apks') if isfile(join('D:/STUFF/TOOLS/platform-tools/apks', f))]

for i in onlyfiles:
    print(md5('D:/STUFF/TOOLS/platform-tools/apks/'+i))
    with open("md5sum.txt","a") as cart:
        cart.write(md5('D:/STUFF/TOOLS/platform-tools/apks/'+i)+'\n')
```

İşlem sonucunda geriye 12 adet apk dosyası kalmıştır. Bu apk dosyalarının VirusTotal tarafında zararlı olduğu tespit edilmiştir. Statik kod analizine başlanmasından önce cihazın internet trafiği kayıt altına alıp incelenmiştir.

AdupsFota.apk	14/02/2020 14:09	APK File	1,901 KB
ailfreeder.apk	21/02/2020 03:19	APK File	1,666 KB
denis.apk	21/02/2020 03:10	APK File	1,667 KB
FileManager.apk	21/02/2020 03:36	APK File	450 KB
nawdl.apk	21/02/2020 03:08	APK File	281 KB
nts.ppy.apk	21/02/2020 03:37	APK File	45 KB
qianqi.apk	21/02/2020 03:04	APK File	3,321 KB
randomstring.apk	21/02/2020 03:30	APK File	32 KB
Safari.apk	21/02/2020 03:33	APK File	4,486 KB
Telecom.apk	21/02/2020 03:44	APK File	509 KB
xamk-game.apk	21/02/2020 03:20	APK File	2,683 KB
zuyun.apk	21/02/2020 03:32	APK File	2,749 KB



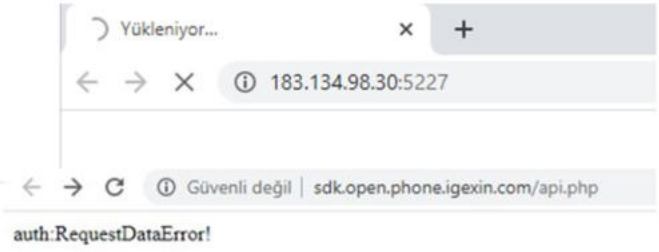
Cihaz üzerinde incelenen internet trafik kaydında görüleceği üzere cihaz üzerindeki bir takım uygulamalar Çin kaynaklı dış sunuculara post isteklerinde bulunmaktalar. Aşağıdaki resimlerde bu post isteklerine detaylı bakıldığında json formatında verilerin gittiği görülmekte.




```
GET /i?
data=eyJhcGkiOnsiYXBpX2tleSI6ImRnNHZzOWVzcDgifSwiY29sbGVjdGlvbiI6ImFkd
2ViX3JlcXVlc3QiLCJwcm9wZXJ0aWVzIjp7ImFwX3ZlciI6IjEuMDAuMjkuMDAiLCJjYWx
sX2Jyb3dzZXJfc3RhdHVzIjowLCJjb3VudCI6MSwiY291bnRyeSI6IlRSIiwiY3RhZyI6I
kNRUTMyMTgiLCJkZXZpY2VfaWQiOiJXWFBHWEgyT0pCS1ctMzE1ZTNkZTEtZjkwNiOOMzF
jLWEwMmUtYjNmZjljNTZmYTI3IiwiZXZlbnRfdmVyc2lvbiI6MSwicGtnIjoiY29tLmoyM
DE4MDUyMTE4MTUwMTA0Iiwicm9vdF9Oc3RhbXAiOjE1ODEyNzk3ODM2MDl9fQ== HTTP/
1.1
cg: 3
User-Agent: Mozilla/5.0 (Linux; Android 6.0; 8 plus Build/iOS11.2; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/
44.0.2403.119 Mobile Safari/537.36
Host: event.l1181.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

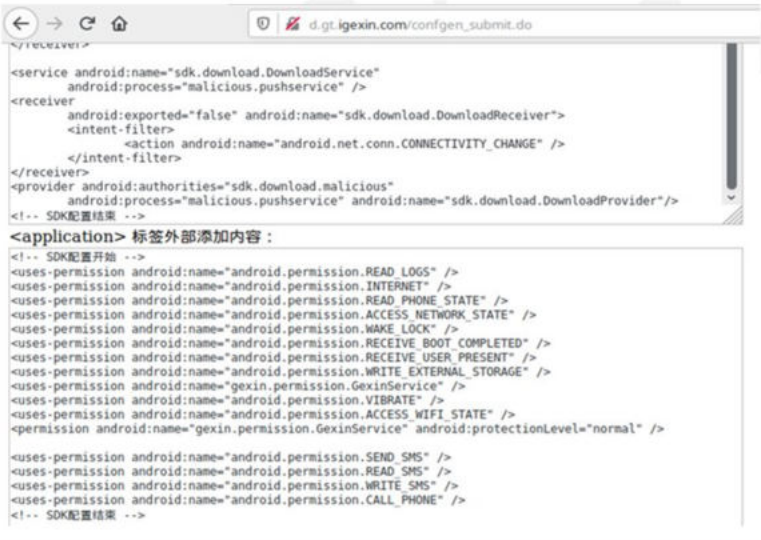
Cihaz içerisindeki TCP bağlantısı kurulan ve istek atılan sunucular trafikten export edilerek ziyaret edilmiştir. Ardından bu sunucular ziyaret edilerek üzerlerinde Apache Jetty Websocket çalıştığı görülmüştür. Çıkarılan ve iletişim kurulan sunucular aşağıdaki resimde görülmektedir.

http://sdk.open.lbs.igexin.com/api.htm
http://sdk.open.amp.igexin.com/
http://d.gt.igexin.com/api.htm
http://s-gt.getui.com/api.php
http://c-hzgt2.getui.com/
http://sdk.open.phone.igexin.com/api.php
http://sj54.nnmwm.com:90//upload/google_c.action



没有正确的查找到Json接口

İstek yapılan hostların arasında dikkat çeken ".igexin" alan adına sahip domainler bulunmaktadır. Igexin bir android reklam sdk sidir. Kullanıcılar hakkında veri toplar ilgi alanları, konum bilgileri vs. gibi. Her igexin sdk sürümü zararlı davranışlar göstermez. Ancak uygulama içerisinde bulunan igexin sürümü zararlı bir şekilde çalışmakta ve kullanıcıya ait hassas bilgileri Çin'de bulunan sunuculara aktarmaktadır. http: // sdk [.] Open [.] Phone [.] İgexin [.] com / api.php adresine istek atan igexin sdk sürümleri zararlı davranış sergilemektelerdir.



Resimde görüldüğü üzere sdk cihaz üzerinde sms ve telefon çağrılarına erişip aynı zamanda telefon çağrısı yapma ve sms gönderme gibi işlemleri yapabilmektedir.

Netstat komutu ile cihazın anlık olarak yaptığı bağlantılar görüntülenmekte. Görülen ip ler ve hostlar araştırıldığında sunuculara ve domainlere ulaşılmaktadır. Burada daha önce cnc panel olarak bir çok kez rapor edilmiş bir ip adresi, cihaza sürekli bağlantı kuran ve encrypted iletişim kuran bir ip adresi ayrıca sdk in veri gönderdiği sunucular tespit edilmiştir.

```
shell@8 plus:/ $ netstat -natp
(Not all processes could be identified, non-owned process info will not be shown, you would have
l.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp        57      0 192.168.1.53:59306      172.217.17.174:443      CLOSE_WAIT  -
tcp         0      0 192.168.1.53:56348      149.154.167.92:443      ESTABLISHED -
tcp         0      0 :::8100                 :::*                    LISTEN      -
tcp         0      0 :::51688                :::*                    LISTEN      -
tcp         0      0 :::48432                :::*                    LISTEN      -
tcp         0      0 ::ffff:192.168.1.53:35905 ::ffff:183.134.98.30:5227 ESTABLISHED -
tcp         1      0 ::ffff:192.168.1.53:60135 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp         0      0 ::ffff:192.168.1.53:60083 ::ffff:195.22.26.248:80 CLOSE_WAIT  -
tcp         1      0 ::ffff:192.168.1.53:56884 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp         1      0 ::ffff:192.168.1.53:56989 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp         1      0 ::ffff:192.168.1.53:42130 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp         0      0 ::ffff:192.168.1.53:56633 ::ffff:173.194.69.188:5228 ESTABLISHED -
```

172.217.17.174 : 443 -> google

149.154.167.92 : 443 -> telegram

183.134.98.30 : 5227 -> cm-10-39.igexin.com

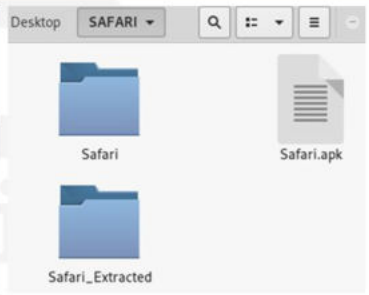
195.22.26.248 : 80 -> CnC Server

173.194.69.188 : 5228 -> google

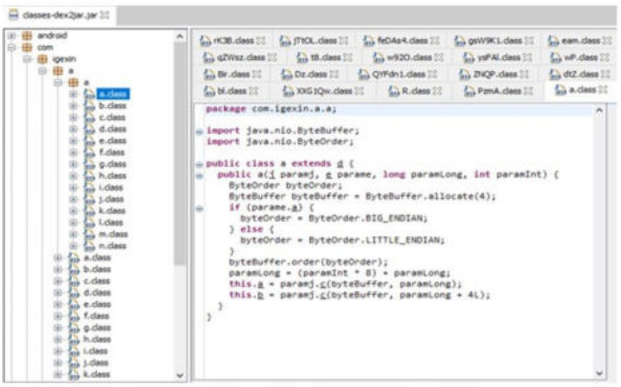
183.131.24.149 : 5226 -> cm-10-47.igexin.com

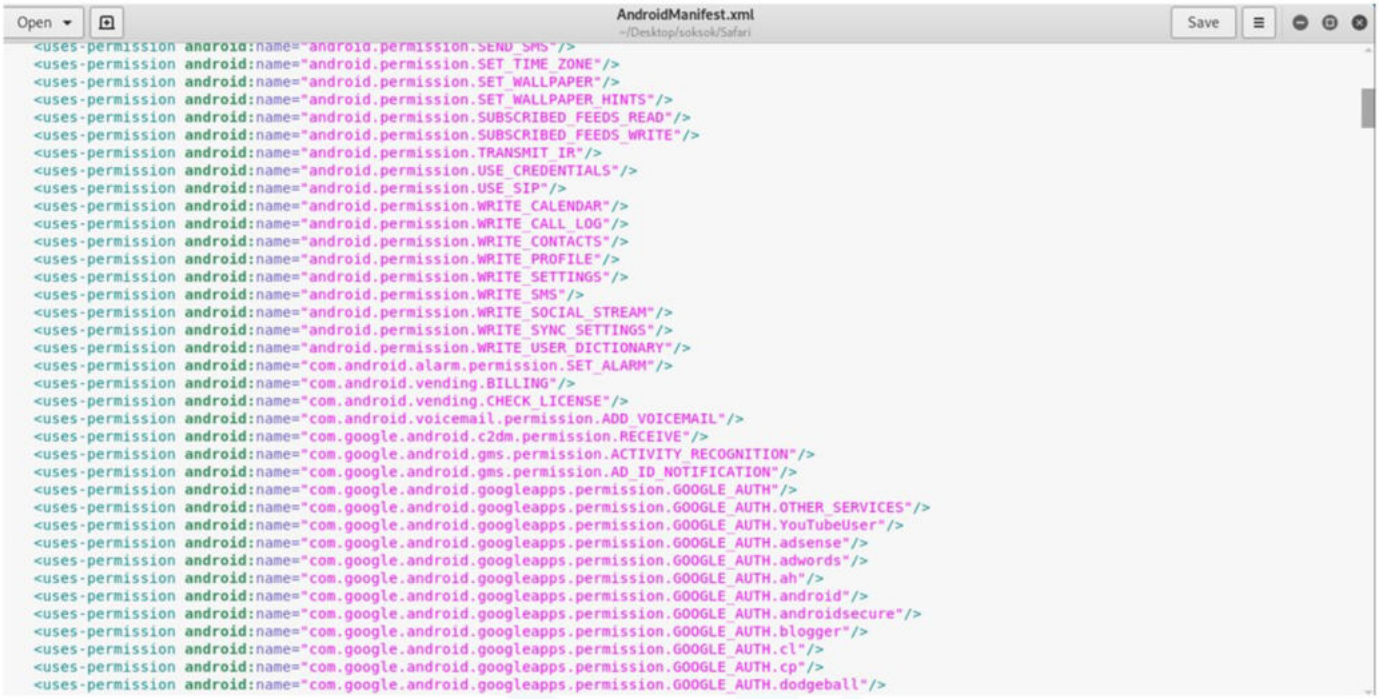
Statik kod analizi tarafında cihazdaki en çok trafiği yaratan ve veri gönderen Safari.apk dosyası ilk olarak ele alınmıştır. Apktool ve dex2jar araçları kullanılarak apk içerisindeki class lar okunur hale getirilmiş ve incelenmiştir.

```
root@not4her0:~/Desktop/SAFARI# apktool d Safari.apk
I: Using Apktool 2.3.4-dirty on Safari.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```




```
root@not4her0: ~/Desktop/SAFARI/Safari_Extracted
File  Edit  View  Search  Terminal  Help
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# ls
AndroidManifest.xml  assets  classes.dex  lib  META-INF  org  res  resources.arsc
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# d2j-dex2jar classes.dex
dex2jar classes.dex -> ./classes-dex2jar.jar
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# ls
AndroidManifest.xml  classes.dex         lib       org  resources.arsc
assets               classes-dex2jar.jar  META-INF  res
root@not4her0:~/Desktop/SAFARI/Safari_Extracted#
```





Uygulamanın isteklerine bakıldığında uygulamanın cihazın hemen her yerine ve her türlü kontrolüne erişim sağladığı görüntülenmektedir.

```
    iget-object v0, p0, Lw/Bir;->c8XA:Ldalvik/system/DexClassLoader;

    return-object v0
.end method

.method public final c8XA(Ldalvik/system/DexClassLoader;)V
    .locals 2

    iput-object p1, p0, Lw/Bir;->c8XA:Ldalvik/system/DexClassLoader;

    sget v0, Landroid/os/Build$VERSION;->SDK_INT:I

    const/16 v1, 0x33a

    if-le v0, v1, :cond 0
```

Uygulamanın içerisinde bir smali dosyası incelendiğinde DexClassLoader kullanıldığı fark edilmiştir. DexClassLoader yüklenen zararsız görünen bir uygulamanın sonradan internet üzerinden ulaştığı ve encrypt edilmiş halde indirdiği zararlı class ları yüklemek için kullanılır. Kötü amaçlı yazılımlar bunu gizlenmek için kullanırlar.

```
public class SDKUrlConfig {
  public static String[] AMP_ADDRESS_IPS;

  public static String[] BI_ADDRESS_IPS;

  public static String[] CONFIG_ADDRESS_IPS;

  public static String[] INC_ADDRESS_IPS;

  public static String[] LBS_ADDRESS_IPS;

  public static String[] LOG_ADDRESS_IPS;

  public static String[] STATE_ADDRESS_IPS;

  public static String[] XFR_ADDRESS_BAK;

  private static final Object a = new Object();

  private static String[] b;

  private static String c = "HZ";

  private static String[] d = new String[] { "socket://sdk.open.talk.igexin.com:5224", "socket://sdk.open.talk.getui.net:5224", "socket://sdk.open.talk.gepush.com:5224" };

  private static volatile String e;

  static {
    XFR_ADDRESS_BAK = new String[] { "socket://42.62.120.14:5224" };
    BI_ADDRESS_IPS = new String[] { "http://sdk.open.phone.igexin.com/api.php" };
    CONFIG_ADDRESS_IPS = new String[] { "http://c-hzgt2.getui.com/api.php" };
    STATE_ADDRESS_IPS = new String[] { "http://s-gt.getui.com/api.php" };
    LOG_ADDRESS_IPS = new String[] { "http://d.gt.igexin.com/api.htm" };
    AMP_ADDRESS_IPS = new String[] { "http://sdk.open.amp.igexin.com/api.htm" };
    LBS_ADDRESS_IPS = new String[] { "http://sdk.open.lbs.igexin.com/api.htm" };
    INC_ADDRESS_IPS = new String[] { "http://sdk.open.inc2.igexin.com/api.php" };
```

Uygulama içerisinde SDK class ları incelendiğinde uygulamanın bağlantı kurduğu ve veri gönderdiği adreslere ulaşılmaktadır.

```
public class p {
  public static void a() {
    try {
      Bundle bundle = (g.f.getPackageManager().getApplicationInfo(g.f.getPackageName(), 128)).metaData;
      if (bundle != null) {
        Iterator<String> iterator = bundle.keySet().iterator();
        while (iterator.hasNext()) {
          String str = iterator.next();
          if (str.equals("PUSH_DOMAIN")) {
            StringBuilder stringBuilder = new StringBuilder();
            this();
            a.b(stringBuilder.append("PUSH_DOMAIN:").append(bundle.getString(str)).toString());
            a(bundle.getString(str));
            break;
          }
        }
      }
    } catch (Exception exception) {
      a.b(exception.toString());
    }
  }

  private static void a(String paramString) {
    SDKUrlConfig.setXfrAddressIps(new String[] { "socket://xfr." + paramString + ":5224" });
    a.b("XFR_ADDRESS_IPS:" + SDKUrlConfig.getXfrAddress()[0]);
    SDKUrlConfig.XFR_ADDRESS_BAK = new String[] { "socket://xfr_bak." + paramString + ":5224" };
    a.b("XFR_ADDRESS_IPS_BAK:" + SDKUrlConfig.XFR_ADDRESS_BAK[0]);
    SDKUrlConfig.BI_ADDRESS_IPS = new String[] { "http://bi." + paramString + "/api.php" };
    a.b("BI_ADDRESS_IPS:" + SDKUrlConfig.BI_ADDRESS_IPS[0]);
    SDKUrlConfig.CONFIG_ADDRESS_IPS = new String[] { "http://config." + paramString + "/api.php" };
    a.b("CONFIG_ADDRESS_IPS:" + SDKUrlConfig.CONFIG_ADDRESS_IPS[0]);
    SDKUrlConfig.STATE_ADDRESS_IPS = new String[] { "http://stat." + paramString + "/api.php" };
    a.b("STATE_ADDRESS_IPS:" + SDKUrlConfig.STATE_ADDRESS_IPS[0]);
    SDKUrlConfig.LOG_ADDRESS_IPS = new String[] { "http://log." + paramString + "/api.php" };
    a.b("LOG_ADDRESS_IPS:" + SDKUrlConfig.LOG_ADDRESS_IPS[0]);
    SDKUrlConfig.AMP_ADDRESS_IPS = new String[] { "http://amp." + paramString + "/api.htm" };
    a.b("AMP_ADDRESS_IPS:" + SDKUrlConfig.AMP_ADDRESS_IPS[0]);
    SDKUrlConfig.LBS_ADDRESS_IPS = new String[] { "http://lbs." + paramString + "/api.htm" };
    a.b("LBS_ADDRESS_IPS:" + SDKUrlConfig.LBS_ADDRESS_IPS[0]);
    SDKUrlConfig.INC_ADDRESS_IPS = new String[] { "http://inc." + paramString + "/api.php" };
    a.b("INC_ADDRESS_IPS:" + SDKUrlConfig.INC_ADDRESS_IPS[0]);
  }
}
```

Burada daha sonra kötücül sunuculardan çekeceği ve veri göndereceği başka sunucuların domain yapılandırması görülmektedir. Çoğu aynı Apache Jetty WebsSocket sistemini kullanmaktadır.

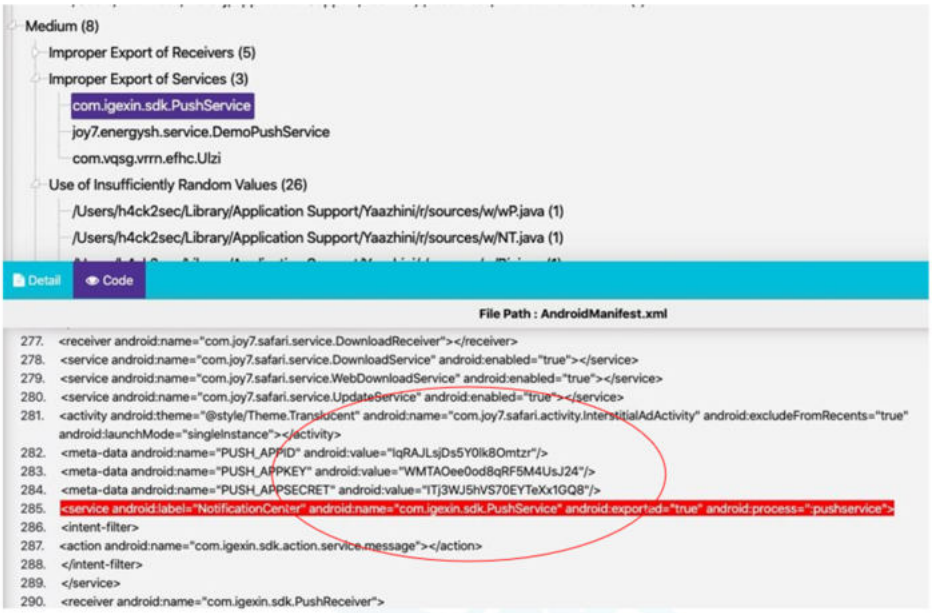
Aşağıdaki görselde cihazın root yetki kontrolü yaptığı görülmektedir.

```
public class ShellUtils {
  public static final String COMMAND_EXIT = "exit\n";

  public static final String COMMAND_LINE_END = "\n";

  public static final String COMMAND_SH = "sh";

  public static final String COMMAND_SU = "su";

  private ShellUtils() {
    throw new AssertionError();
  }

  public static boolean checkRootPermission() {
    boolean bool = true;
    if ((execCommand("echo root", true, false)).result != 0)
      bool = false;
    return bool;
  }
```

```
public static String MessageDigest(byte[] paramArrayOfbyte) throws Exception {
  return HexUtil.toHexString(MessageDigest.getInstance("SHA-1").digest(paramArrayOfbyte));
}

public static void RSACipher(byte[] paramArrayOfbyte) throws Exception {
  KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance("RSA");
  keyPairGenerator.initialize(1024);
  KeyPair keyPair = keyPairGenerator.generateKeyPair();
  Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
  cipher.init(1, keyPair.getPublic());
  paramArrayOfbyte = cipher.doFinal(paramArrayOfbyte);
  cipher.init(2, keyPair.getPrivate());
  paramArrayOfbyte = cipher.doFinal(paramArrayOfbyte);
  System.out.println("RSACipher----" + new String(paramArrayOfbyte));
}

public static void main(String[] paramArrayOfString) throws Exception {
  BASE64("Hello World".getBytes());
  MessageDigest("Hello World".getBytes());
  MD5MessageDigest("Hello World".getBytes());
  AESCipher("Hello World".getBytes());
  DESCipher("Hello World".getBytes(), "pass");
  RSACipher("Hello World".getBytes());
  DigitalSignature("Hello World".getBytes());
}
}
```

Soldaki görselde ise cihazın sunucularla veri alışverişi yapacağı sırada kullanacağı encryption ve encoding işlemlerini gerçekleştirdiği kısım görünmektedir.

Burada sdk in iletişimde kullanacağı id, key ve secret kodları görülmektedir.



_id	key	offerId	title	mainContent	iconImageUrl	mainImageUrl	bannerImageUrl
641	12548877	29319814	The Great Ottomans - Strat...	The first mobile MMORTS b...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/img...	http://gp.apiv7.con
642	12553287	369419	App Download - akbank dir...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
643	12551714	368907	App Download - akbank dir...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
644	12553023	369417	App Download - akbank dir...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
645	12561337	29376441	OlympTrade – Çevrimiçi Yat...	An easy and convenient mo...		http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
646	12558409	29368459	OlympTrade – Online Tradi...	An easy and convenient mo...		http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
647	12554628	28504665	Arkbank Incent CPE TR-[TR]	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
648	12566032	628012925	Akbank Direkt	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
649	12566033	51105999	Akbank Direkt	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
650	12490440	352460	Akbank Direkt_261025637_...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con

<long value="1543762745890" name="last_request_list_time"/>
<int value="0" name="uninstall_already_showTime"/>
<int value="1" name="log_level"/>
<string name="controlActive">100.0</string>
<string name="advertisingid">315e3de1-f906-431c-a02e-b3ff9c56fa27</string>
<string name="user_agent_string">Mozilla/5.0 (Linux; U; Android 6.0; tr-tr; 8 plus Build/iOS11.2) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Mobile Safari/537.36</string>
<int value="3" name="ad_retry_times"/>
<int value="0" name="noticebarshowTime"/>
<int value="0" name="install_already_showTime"/>
<int value="1" name="intercept_open"/>
<string name="cc_info">miku_zhixin_0904</string>
<string name="wrongRate">0.3</string>
<long value="1543819012341" name="strategyupdatetime"/>
<string name="white_list">null</string>
<int value="-1" name="show_dtime"/>
<string name="network_type">[redacted]</string>
<int value="1" name="chargeshowTime"/>
<int value="60" name="track_timeout"/>
<string name="intercept_interval">1.0</string>
<int value="0" name="unlockshowTime"/>
<int value="1" name="installshowTime"/>
<string name="retry_cdn">uc.gp.apiv6.com</string>
<string name="data_app">org.telegram.messenger,com.antutu.ABenchMark,org.iarr.iiyjj.zazyjbz.jqyrazi,com.baidu.map.location,cn.nts.ppy,com.samchristiansen.ioverlander.droid,</string>
<int value="20" name="in_delay"/>
<boolean value="false" name="nrp"/>
<string name="log_channel">miku_zhixin_0904</string>
<int value="0" name="ad_load_failed_time"/>
<long value="1543275969746" name="last_pop_time"/>
<long value="1557680680998" name="request_completed_time"/>
<boolean value="false" name="first"/>
<null name="sim_number"/>
<string name="listInterval">6.0</string>
<string name="referExpired">12.0</string>
<string name="supply_url"/>
<int value="0" name="bannershowTime"/>
<int value="5" name="intercept_num"/>
<string name="firstDelay">0.1</string>
<long value="1557680668722" name="last_upload_time"/>
<int value="6" name="chapingshowTime"/>
<long value="1557680666944" name="last_collect_time"/>
<int value="0" name="photo_num"/>
<int value="1" name="show_open"/>
<int value="1" name="preloadTime"/>
<string name="requestInterval">1.0</string>
<long value="1557680663985" name="last_act_gaid_time"/>
<long value="1557680663594" name="last_resume_download_time"/>
<string name="black_list">null</string>
<string
name="sys_app">com.mediatek.ppl,com.snowfish.aios.launcher,com.google.android.youtube,org.simalliance.openmobileapi.uicc2terminal,com.android.providers.telephony,com.adups.fota.sysoper,com.google.android.googlequic
<int value="0" name="rawshowTime"/>
<string name="headers">{s=720x1280, et=34361430016, ch=1300000, mf=iPhone, bo=APPLE A11, m=911323000413432, mt=2147432448, cpu=armeabi-v7a, rt=34361430016, a=splash_sdk, o=23, j=8 plus, ve=plug, br=APPLE,
r=3c3af20993b11c5e, al=/system/app_other/Settings/Settings.apk, pr=8 plus}</string>
<int value="1" name="uninstallshowTime"/>

Yandaki görselde uygulamanın cihaz hakkında depoladığı ve sunucu üzerinden gönderdiği bir xml dosyası bulunmaktadır. Burada telefon numarası dahil bir çok veri gönderilmektedir.

Bir başka uygulama incelendiğinde aynı şekilde içerisinde barındırdığı zararlı sdk üzerinden kullanıcıya ait hassas veriler uzak sunuculara toplanmak üzere gönderilmektedir.

zuyun.apk ??

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schem
android:compileSdkVersionCodename="9" package="com.zuyun.net" platformBuildVersionCode="28"
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
```

```
package com.umeng.commonsdk.stateless;

public class a {
  public static String a = "native";

  public static String b = "";

  public static long c = 2097152L;

  public static long d = 204800L;

  public static final String e = "stateless";

  public static String f = "https://plbslog.umeng.com";

  public static String g = f;

  public static String h = "https://ouplog.umeng.com";
}
```

```
public class UMServerURL {
  public static String DEFAULT_URL = "https://ulogs.umeng.com/unify_logs";

  public static String OVERSEA_DEFAULT_URL = "https://alogus.umeng.com/unify_logs";

  public static String OVERSEA_SECONDARY_URL = "https://alogsus.umeng.com/unify_logs";

  public static String SECONDARY_URL = "https://ulogs.umengcloud.com/unify_logs";
}
```

Özet

Türkiye pazarında da bulunan ve içerisinde bir çok zararlı yazılım ve arka kapı barındıran bu cihazlar kullanıcı hakkındaki hassas içerik ve verileri uzak sunuculara göndermektedir. Bu cihazların kullanımı oldukça yaygındır. Tamamen gizliliği ihlal etmektedir.