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 سايبركوف نحو الأمتين العربية والإسلامية ولتعم الفائدة على الجميع. كما تجب الإشارة أنه يُمنع نشر هذه الوثيقة او توزيعها دون الإشارة إلى شركة سايبركوف كمرجع لهذه الوثيقة.

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

معلومات عن الوثيقة

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

معلومات الاتصال

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

فهرس المحتويات

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 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 فبه 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 ولفريقها المتخصص بتحليل الأخطار الأمنية Cyberkov Security Incident Response team (CSIRT) عدد من برامج التجسس الإلكتروني التي تعمل على منصة الآندرويد والتي نجحت في استهداف مجموعة من السياسيين والنافذين 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 بتتبع 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 شكلا رئيسيا 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 معروفه حالياً لكن الشخص المستهدف لم يكن يستخدم "الحماية الثنائية" لحسابه الخاص بتطبيق تيليجرام وكنا قد أوصينا سابقاً في تدوينه بعنوان "دليلك نحو إستخدام تطبيق تيليجرام Telegram بأقصى درجة من السرية والأمان!" فكان استهدافه أسهل، ولأن الشخص المستهدف يفتقر الى الوعي الإلكتروني المطلوب قام بحذف تطبيق تيليجرام من جهازه الآندرويد 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 Massege.apk" على أنه ملف صوتي هام يجب تحميله والإستماع اليه، ونلاحظ هنا أن "عقارب ليبيا" أخطئوا في تسمية الملف فكلمة "Massege" 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 Massege.apk" هو في الحقيقة ملف خبيث وبرنامج تجسسي مدموج مع برنامج حقيقي خاص بالآندرويد 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 المُخترَقين والمُتَجسس عليهم.

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 "آندرويد".

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

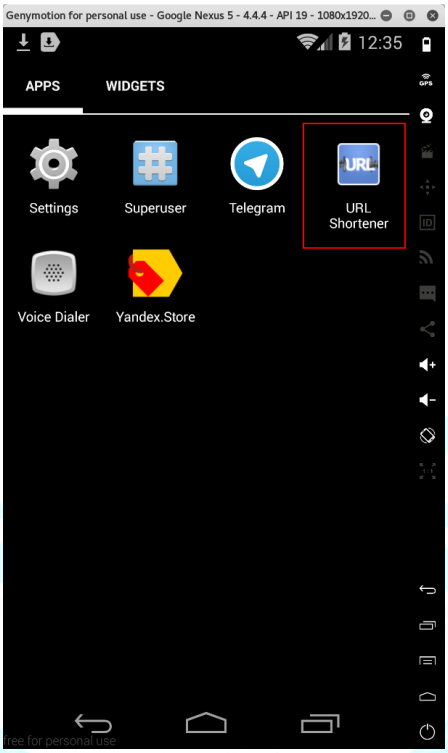
التكتيكات والتقنيات والإجراءات والخطط المستخدمة

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 بانه تم الدخول على الحساب الخاص بك من عنوان IP من أسبانيا بواسطة الـ"الويب":

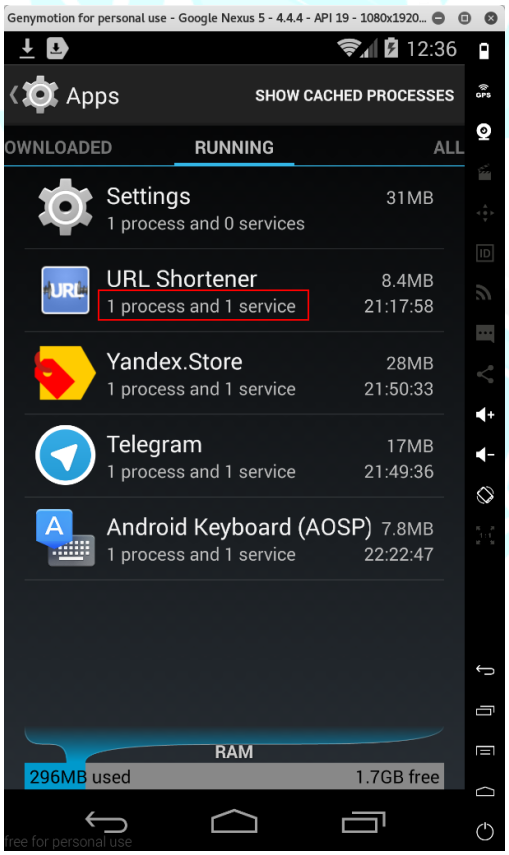
قام الشخص المستهدف ولقلة وعيه الأمني التقني بحذف برنامج تيليجرام ظناً منه بأن ذلك سيقوم بإيقاف اختراق الحساب.

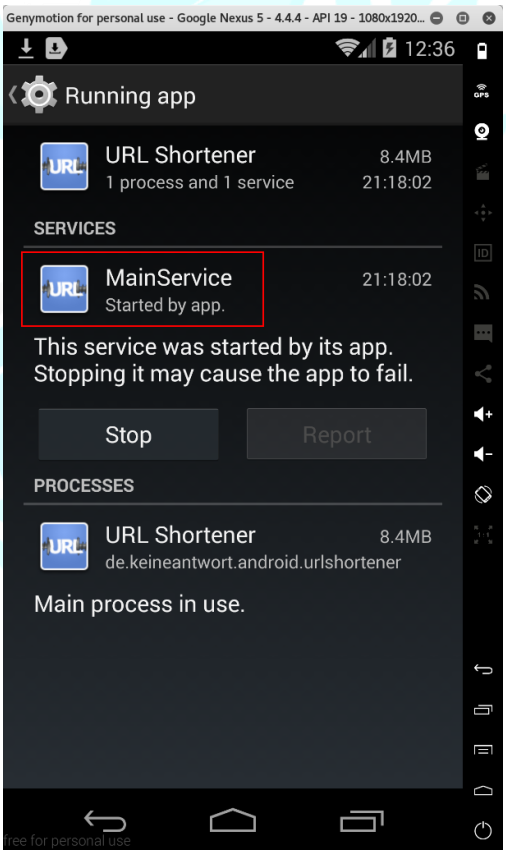
في اليوم التالي، قامت "عقارب ليبيا" (وعن طريق حساب تيليجرام المُخترَق) بإرسال رسالة تتضمن ملف خبيث بإسم "Voice Massege.apk" لكل الأشخاص في قائمة جهات الاتصال الخاصة بالشخص المخترق، معقبين على الملف برسالة **"للاطلاع وافادتنا لو سمح وقتك"** حتى يقوم الشخص بتحميل الملف وتنصيبه على جهازه يتم بعد ذلك اختراقه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

الملف الخبيث "Voice Massege.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 Android Service[1] باسم "MainService" تعمل بالخلفية لنظام التشغيل من حيث لا يعلم المستخدم.

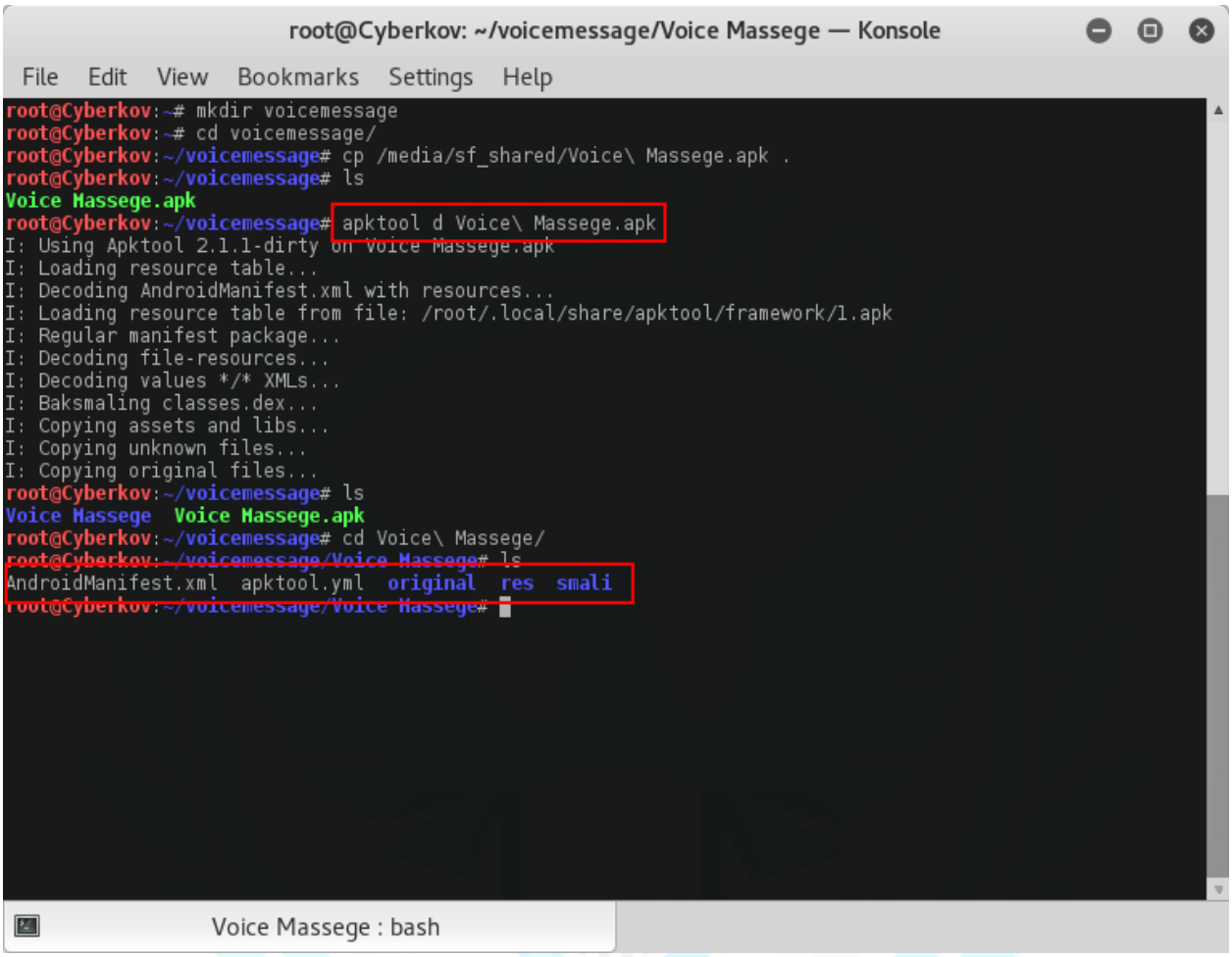




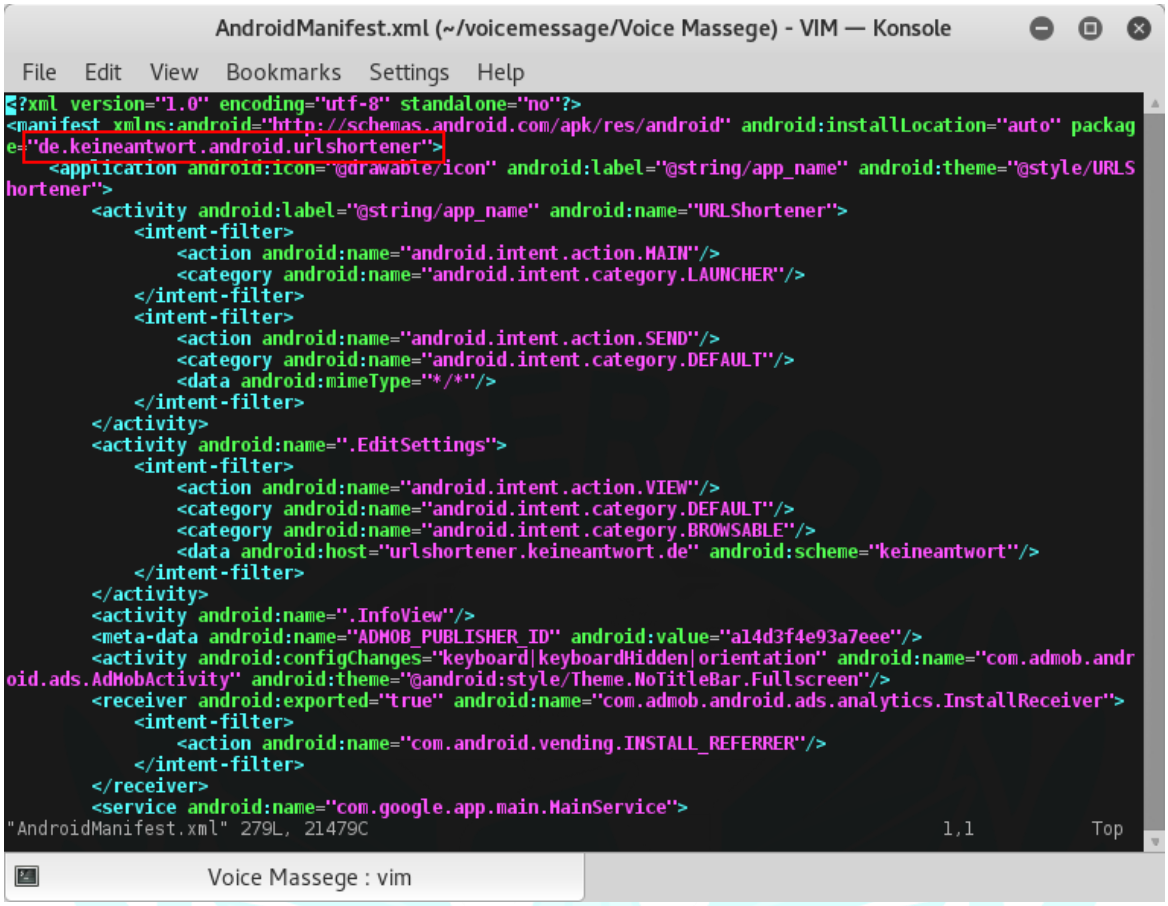
[1] https://developer.android.com/guide/components/services.html

تحليل الملف الخبيث

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

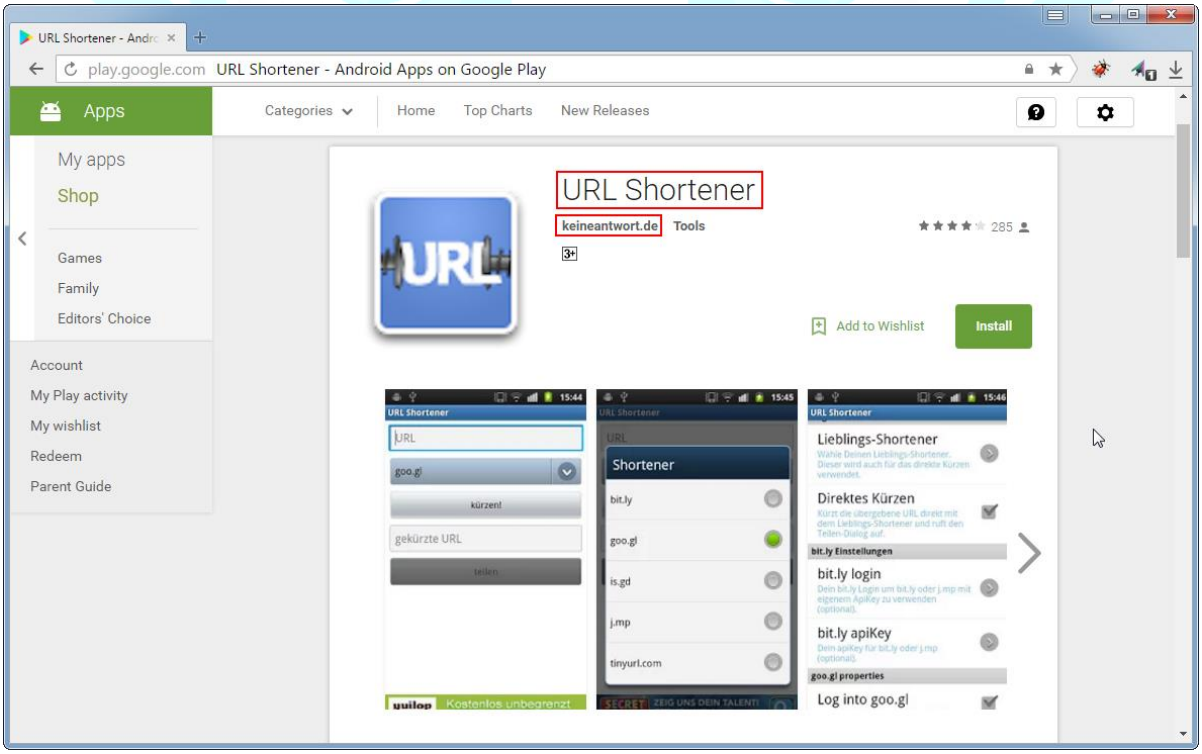


بعد تفكيك الملف باستخدام أداة apktool وقراءة ملف AndroidManifest.xml ندرك أن البرنامج عبارة عن ملف خبيث تم دمجه مع برنامج حقيقي يحمل اسم Java package: **de.keineantwort.android.urlshortener**



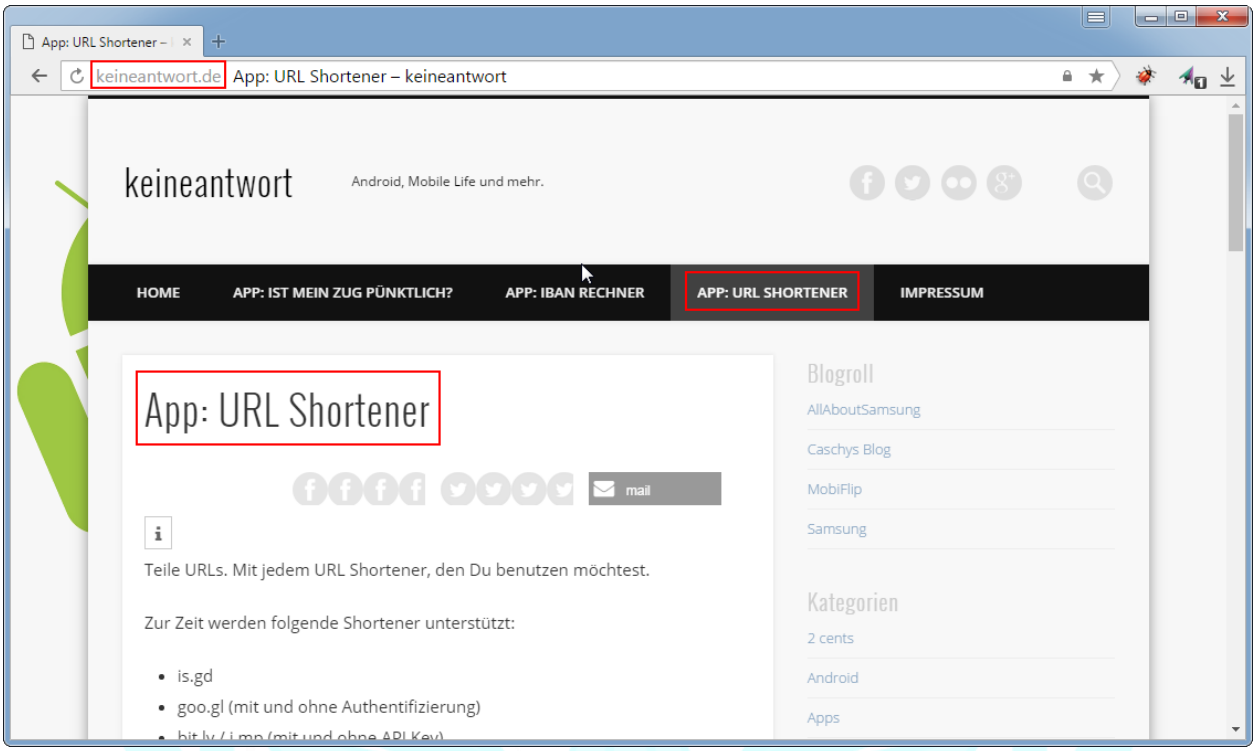
وعند البحث باسم الـ Java Package في متجر قوقل للآندرويد

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



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، قمنا بالتأكد من ذلك عن طريق الموقع الخاص بهم:

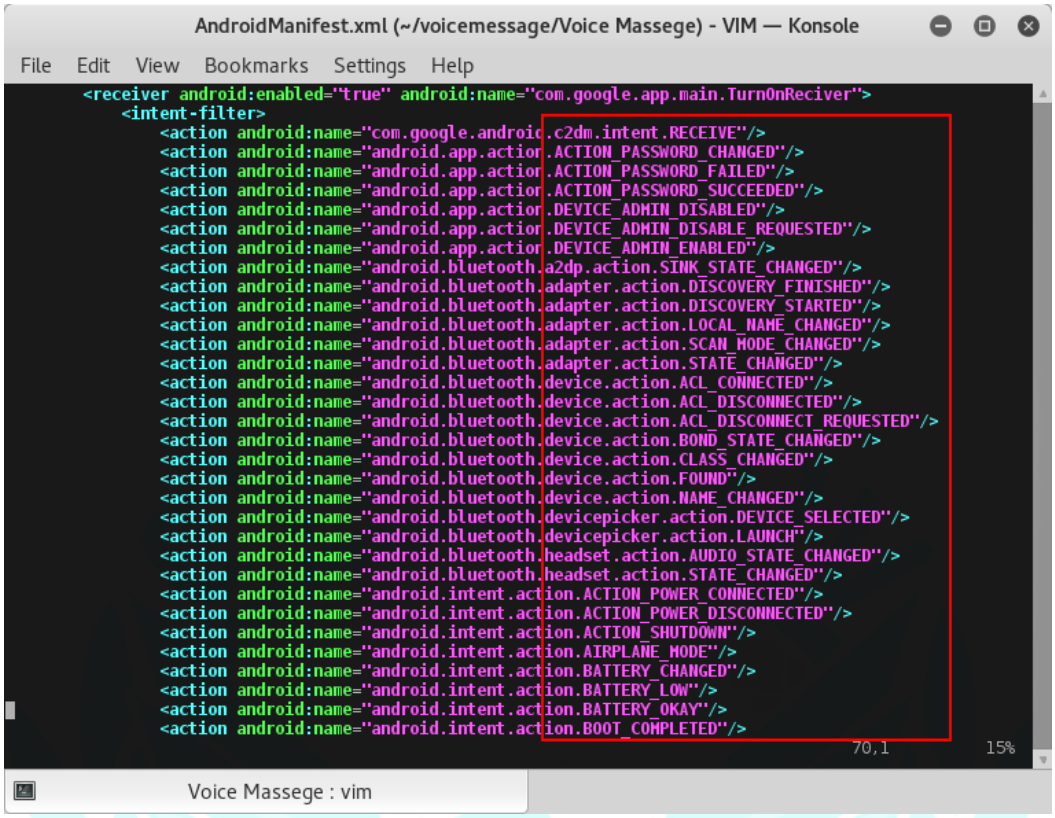


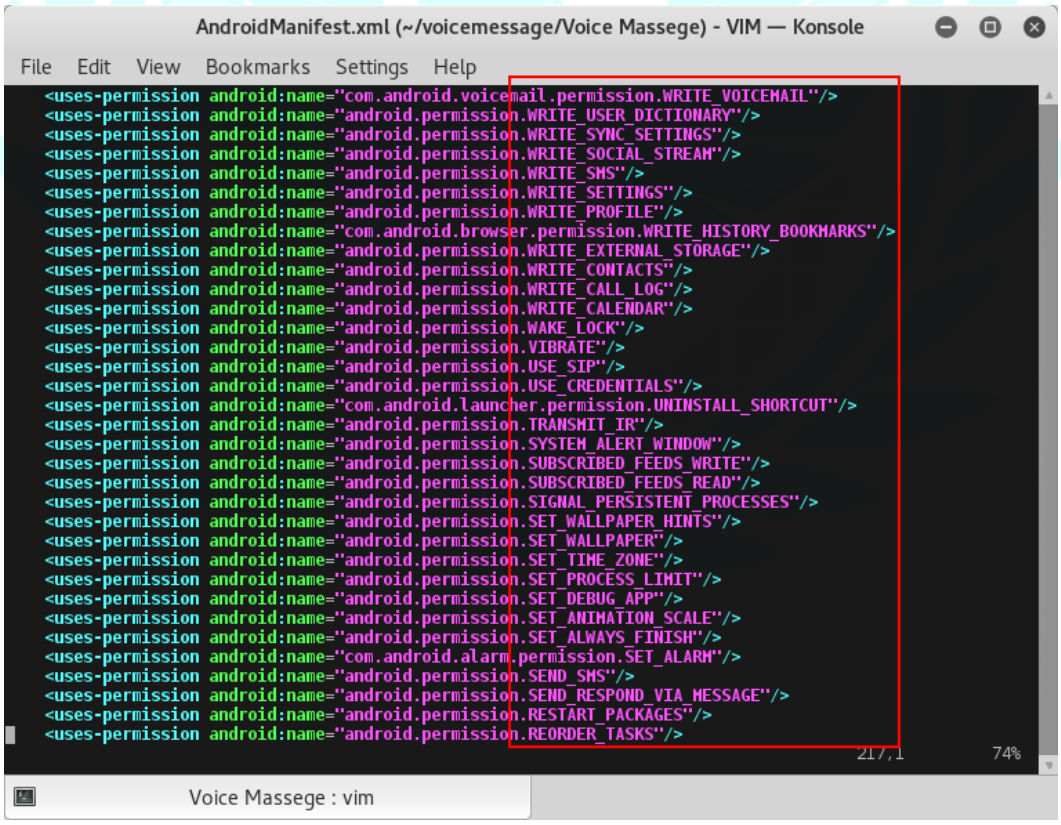
بمتابعة قراءة ملف AndroidManifest.xml نلاحظ بأن البرنامج التجسسي يقوم بتسجيل نفسه كـ Receiver لكل الـ Intent المتوفرة في نظام أندرويد تقريباً وكذلك يقوم بطلب كامل الصلاحيات المتوفرة في نظام أندرويد.

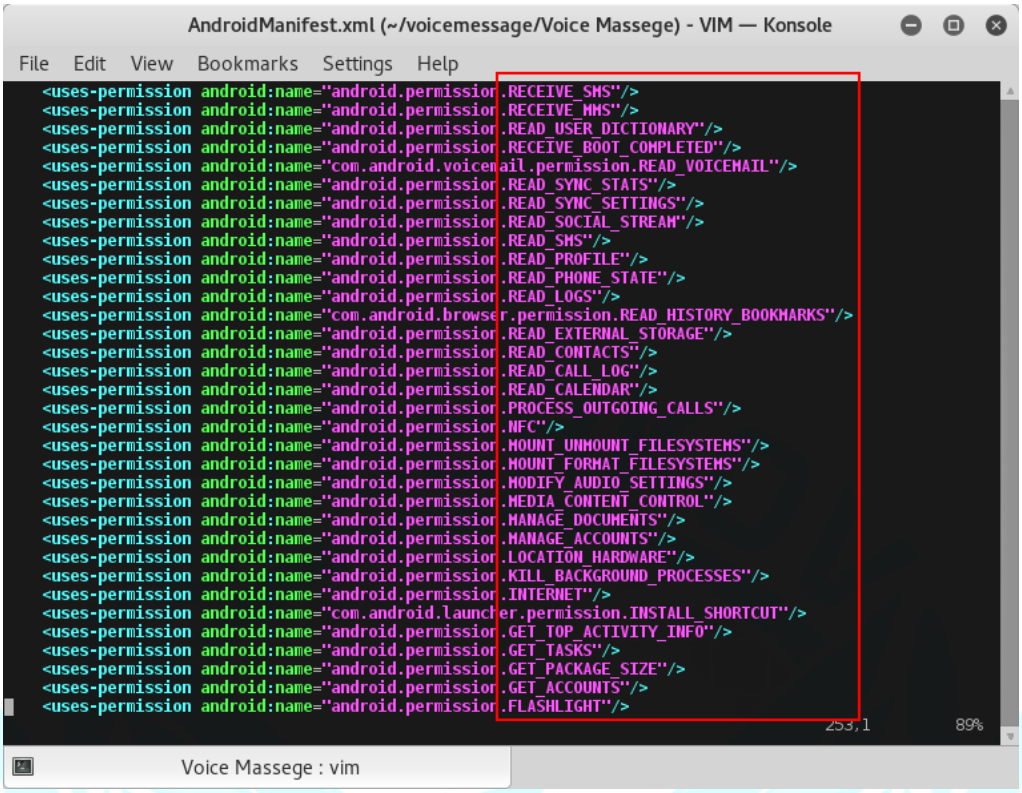
ويقوم البرنامج التجسسي ومن خلال حصوله على كامل الصلاحيات في النظام بالقدرة على التالي:

- القدرة على فتح الكاميرا الأمامية والخلفية للجهاز دون شعور المستخدم
- القدرة على تصوير المستخدم 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:

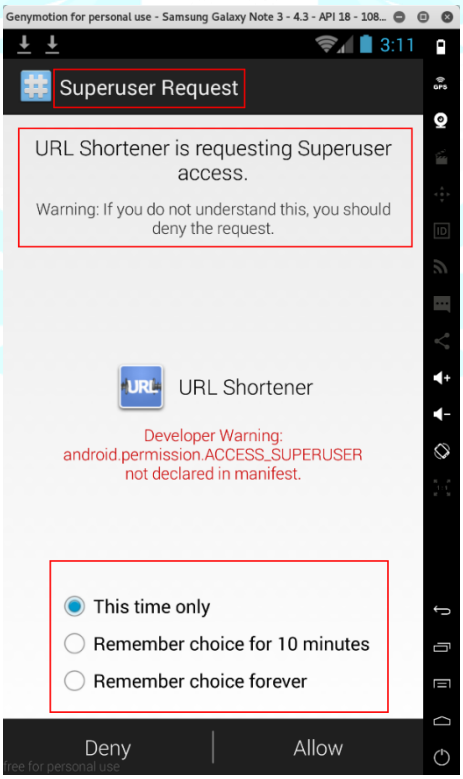

AndroidManifest.xml (~/voicemessage/Voice Massege) - VIM — Konsole
File Edit View Bookmarks Settings Help
<receiver android:enabled="true" android:name="com.google.app.main.TurnOnReciver">
<intent-filter>
<action android:name="com.google.android.c2dm.intent.RECEIVE"/>
<action android:name="android.app.action.ACTION_PASSWORD_CHANGED"/>
<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.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"/>
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

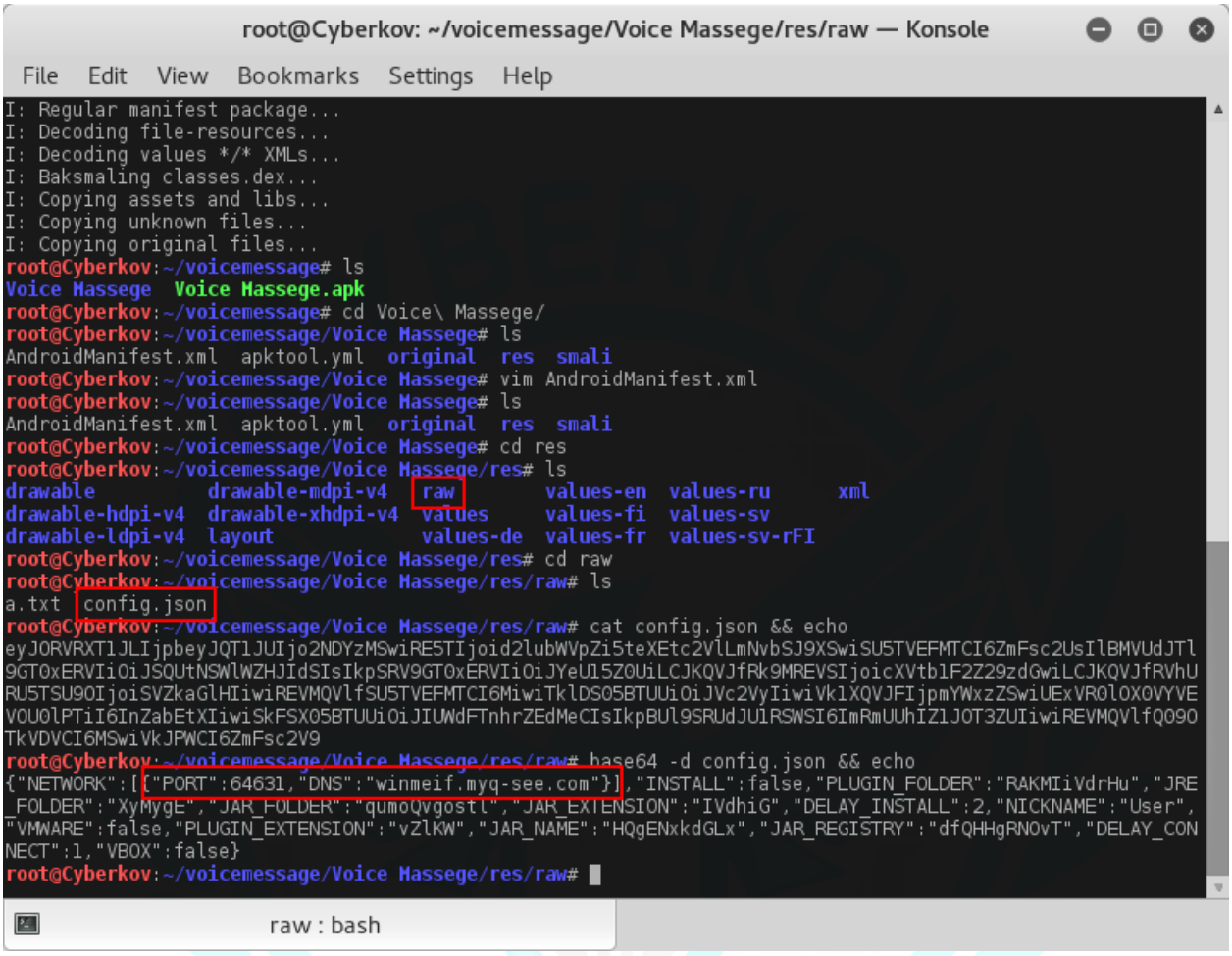


يقوم الفايروس بطلب صلاحيات الدخول على مكان الجهاز وحالة الاتصال بالشبكة ومقدار البطارية المتبقية في الجهاز والبلوتوث والكاميرا والميكروفون وصلاحيات الدخول على الانترنت.

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.



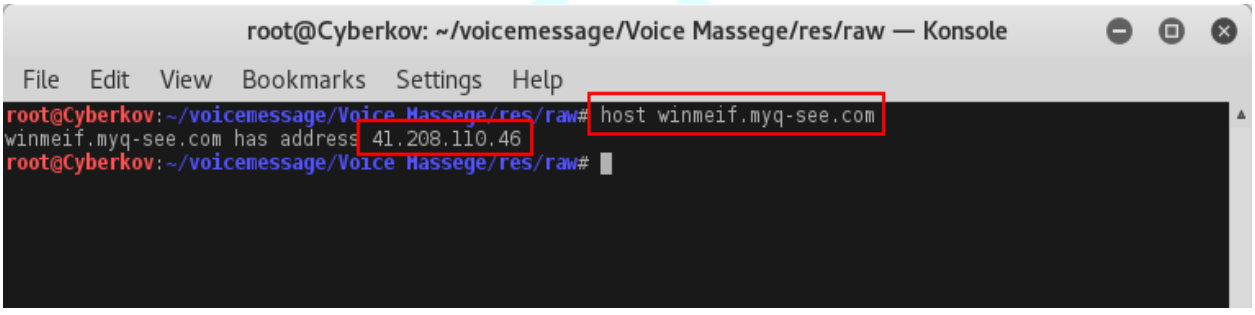
وبمتابعة تحليل البرنامج التجسسي نجد ملف باسم "config.json" وهو ملف بصيغة JSON تم تشفيره بخوارزمية Base64، بعد فك تشفير الملف تبين أنه يحتوي على تفاصيل مركز القيادة والتحكم (Command and Control – C2) الخاصة بمجموعة "عقارب ليبيا"، كما تبين أن خصائص البرنامج التجسسي ووظائفه تشابه إلى حد كبير خصائص ووظائف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



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.



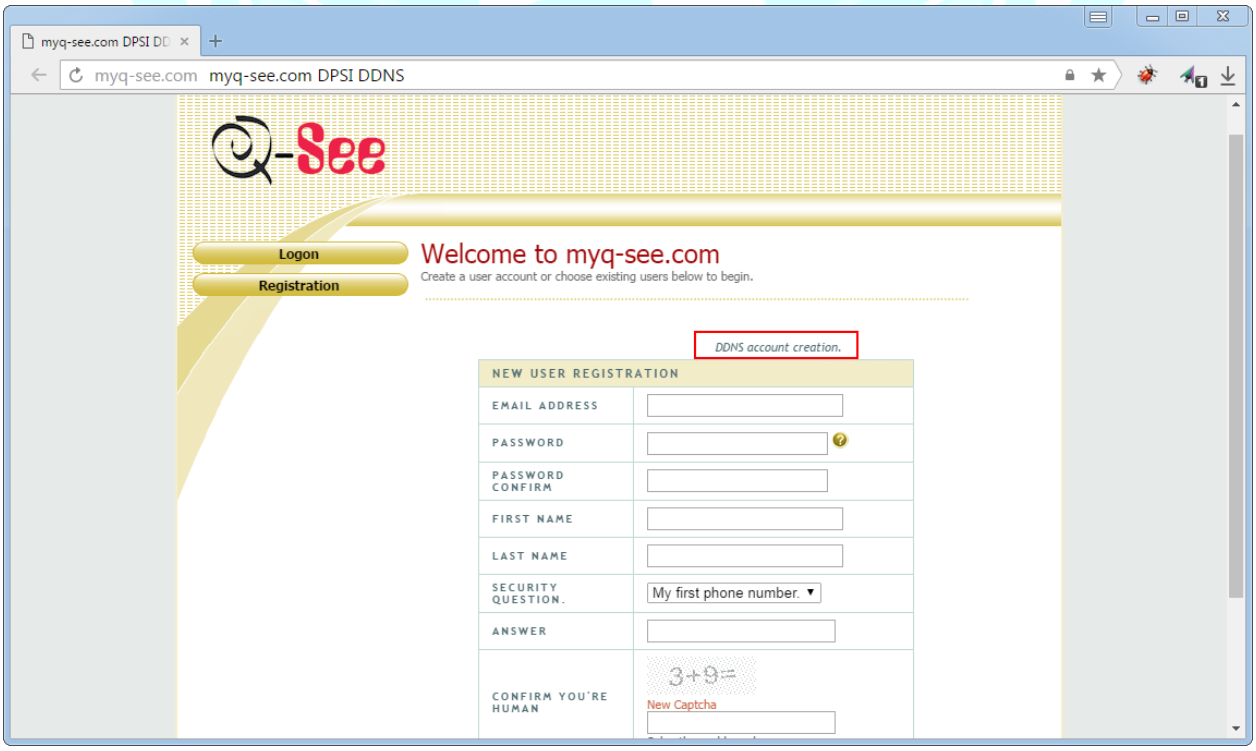
Geolocation data from IP2Location (Product: DB6, updated on 2016-8-1)

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

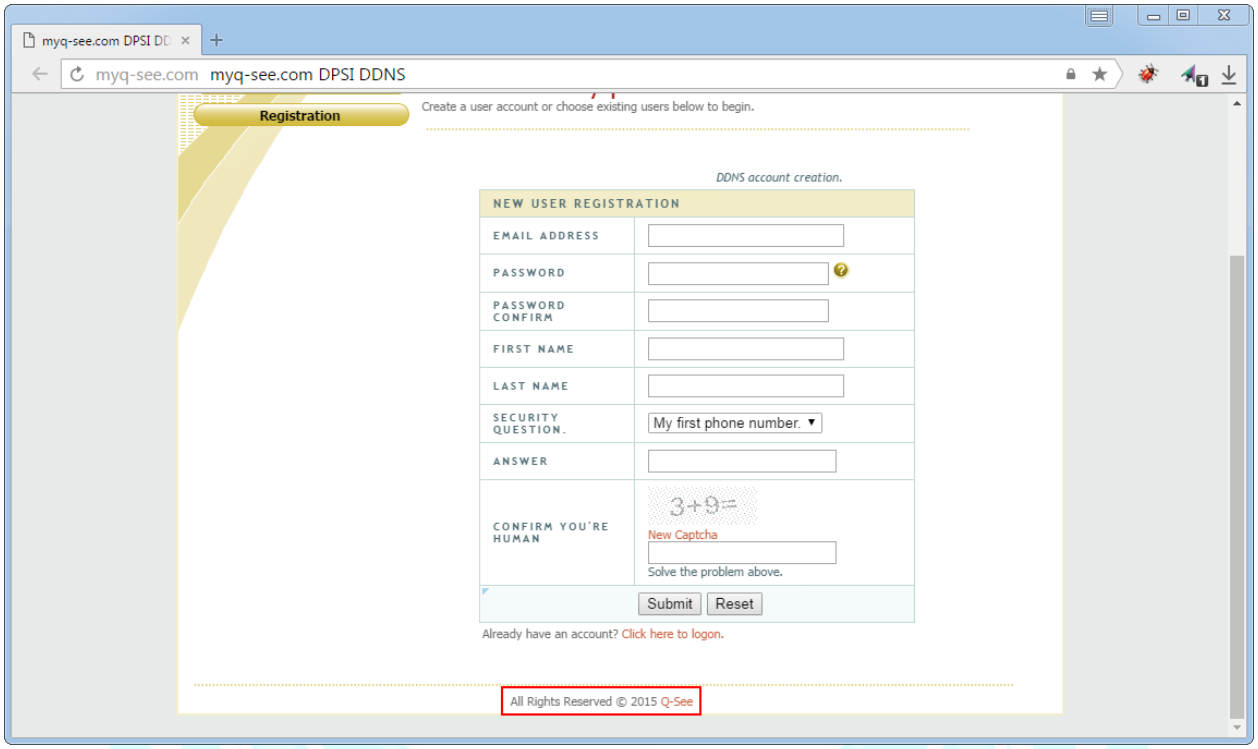
Geolocation data from ipinfo.io (Product: API, real-time)

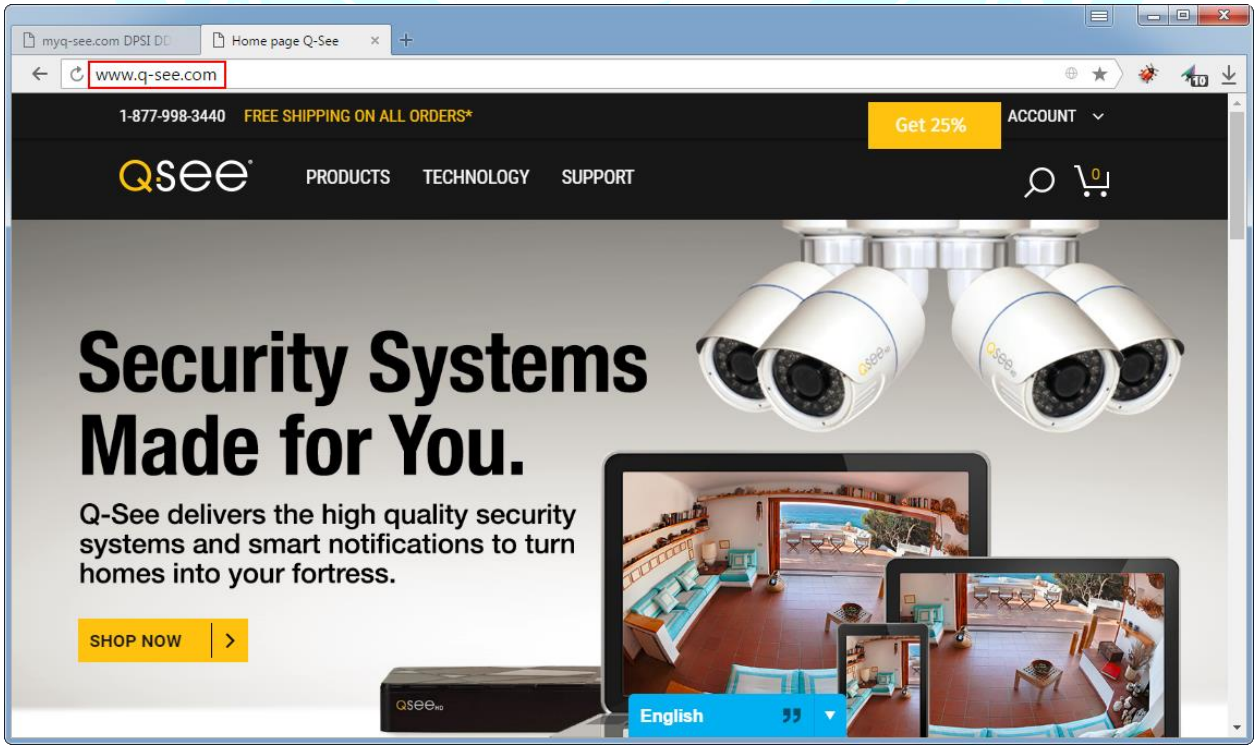
IP Address	Country	Region	City
41.208.110.46	Libya	Not Available	Not Available
ISP	**Organization**	**Latitude**	**Longitude**
General Post and Telecommunication Company (GPTC)	Libya Telecom and Technology Backbone L.L Pool	25.0000	17.0000

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.

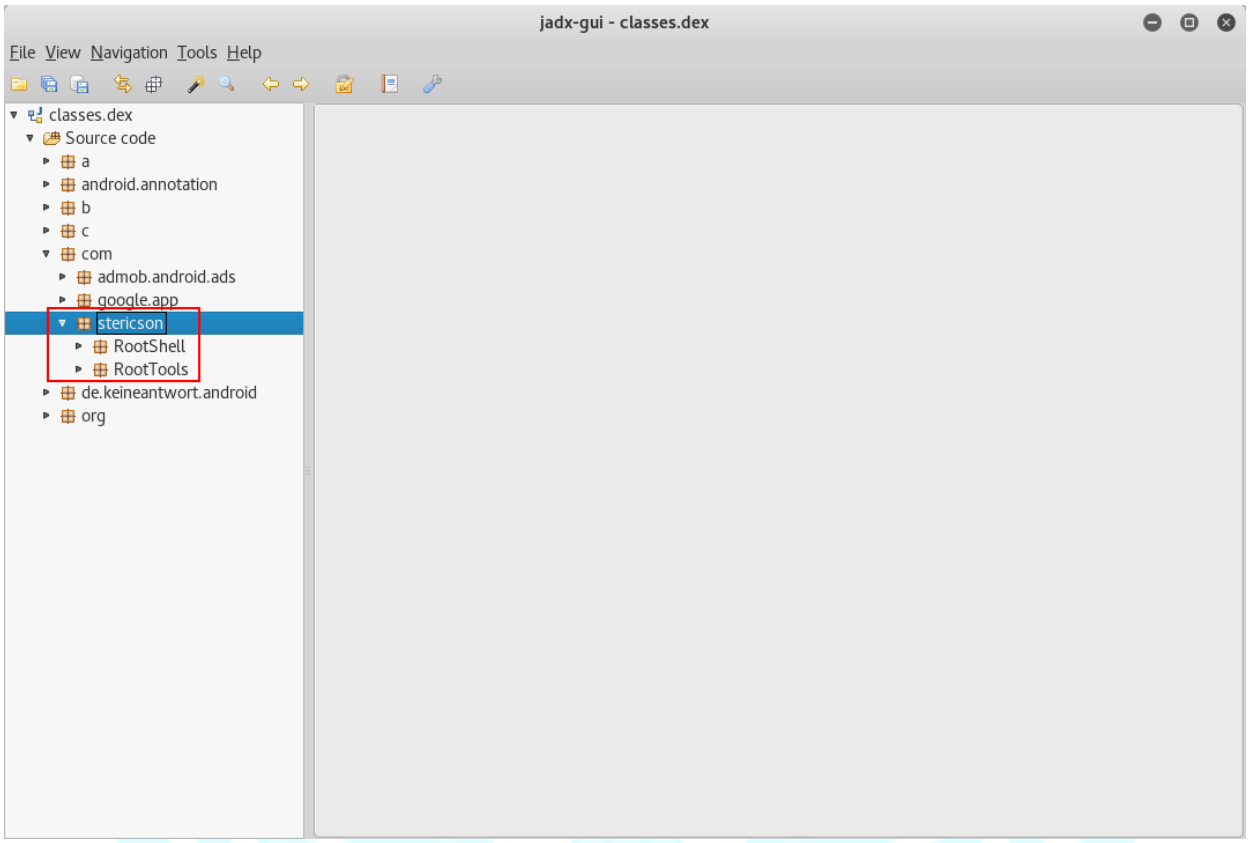


عند الدخول على الموقع والنزول إلى أسفل الصفحة نلاحظ أن الخدمة تابعة لشركة باسم Q-See وهي شركة تقوم ببيع الكاميرات وقد قامت بإنشاء هذه الخدمة للتسهيل على زبائنها عند تركيب الكاميرات للدخول عليها عبر الانترنت، فبدل حفظ عنوان الـ IP الخاص بالكاميرا يمكن حجز نطاق سهل وإعداد الكاميرا لاستخدامه.

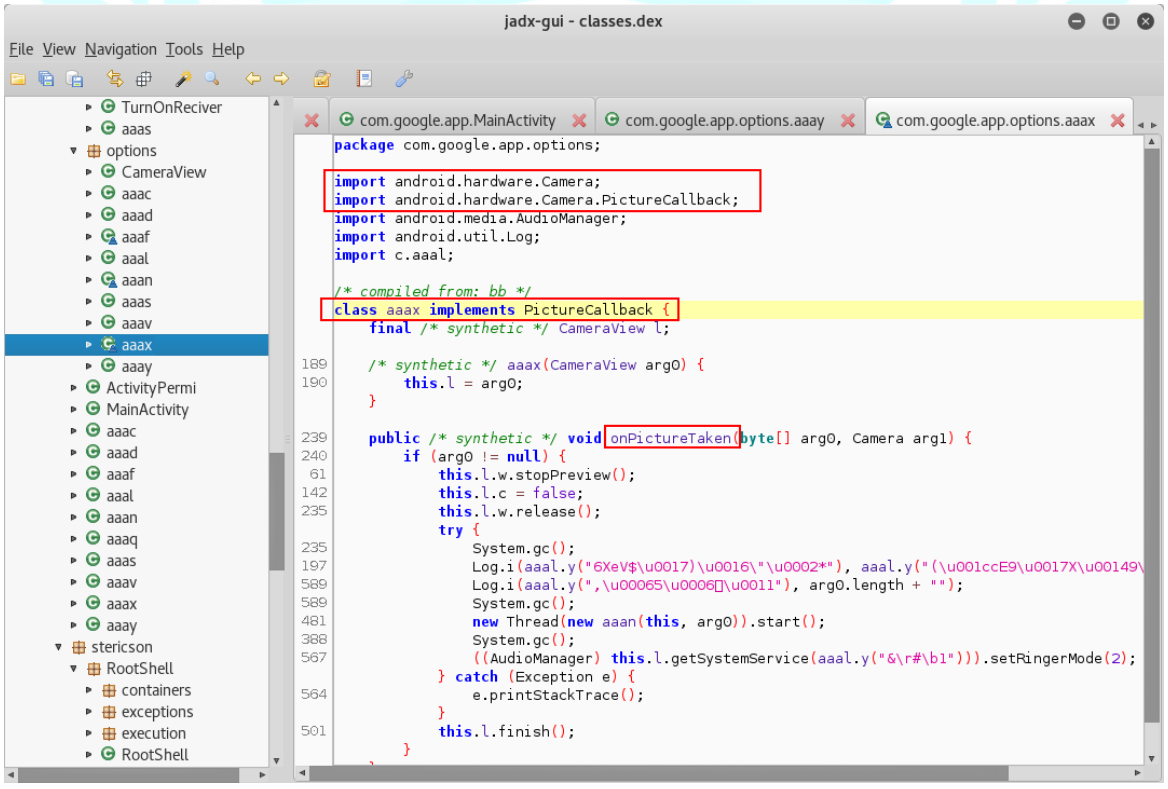

myq-see.com DPSI DD
myq-see.com myq-see.com DPSI DDNS
Registration
Create a user account or choose existing users below to begin.
DDNS account creation.
NEW USER REGISTRATION
EMAIL ADDRESS
PASSWORD
PASSWORD CONFIRM
FIRST NAME
LAST NAME
SECURITY QUESTION.
My first phone number.
ANSWER
CONFIRM YOU'RE HUMAN
3+9=
New Captcha
Solve the problem above.
Submit
Reset
Already have an account? Click here to logon.
All Rights Reserved © 2015 Q-See


myq-see.com DPSI DD
Home page Q-See
www.q-see.com
1-877-998-3440
FREE SHIPPING ON ALL ORDERS*
Get 25%
ACCOUNT
Qsee
PRODUCTS
TECHNOLOGY
SUPPORT
Security Systems Made for You.
Q-See delivers the high quality security systems and smart notifications to turn homes into your fortress.
SHOP NOW
English

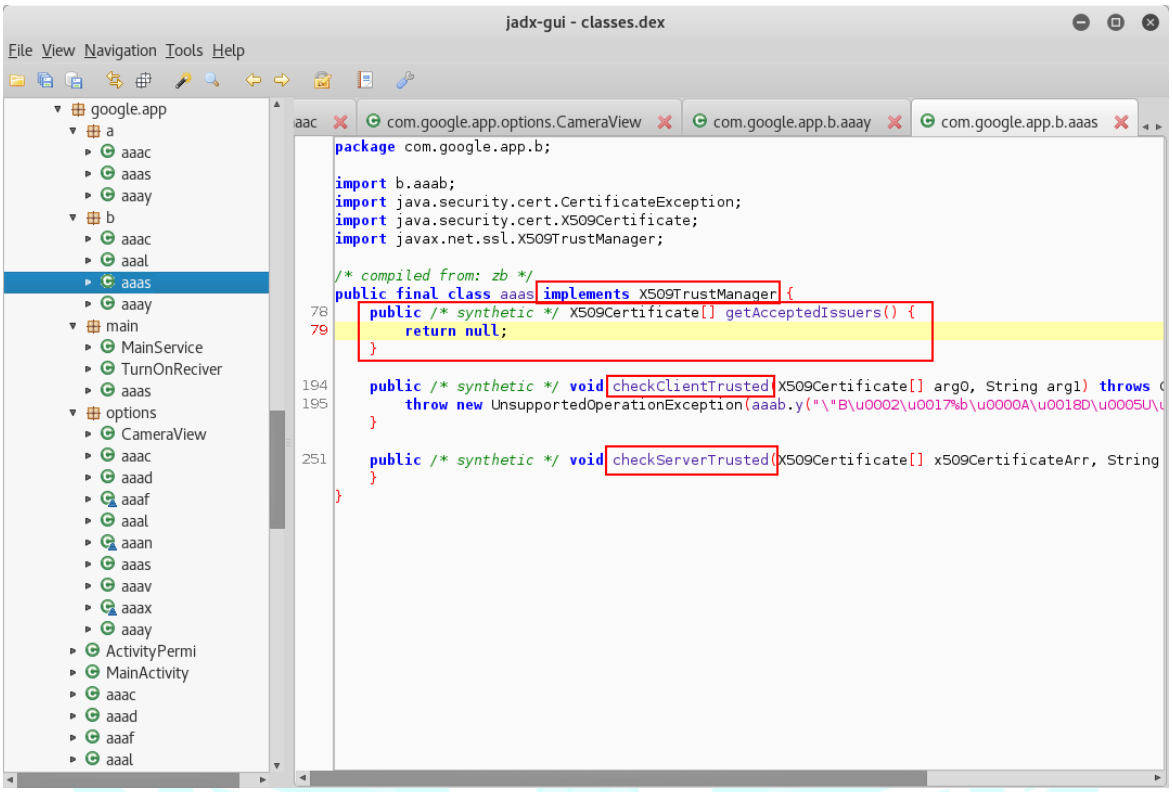
يقوم الفايروس باستخدام أدوات مشهورة لتسهيل عمليات الـ Root في جهاز أندرويد وهي RootTools و RootShell.



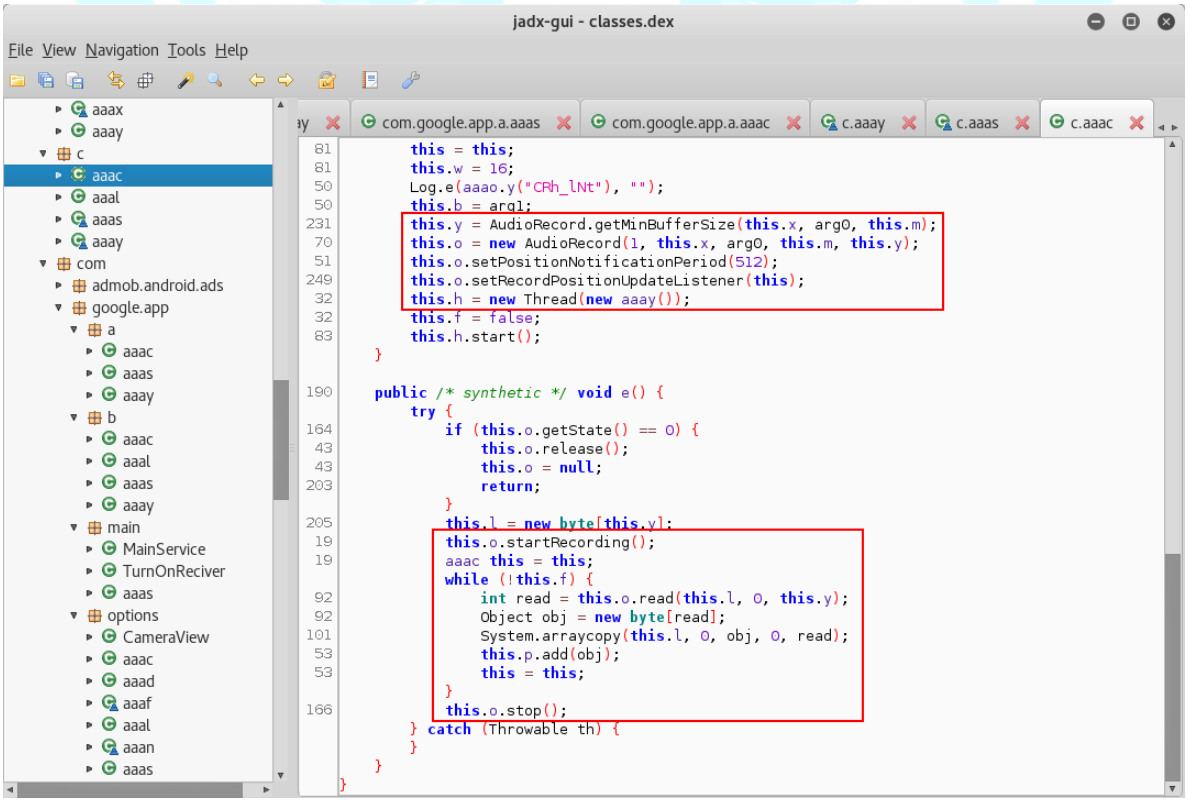
كما يستطيع الفايروس التقاط الصور من كاميرا الجهاز ورفعها لمركز القيادة والتحكم التابع لمجموعة "عقارب ليبيا".



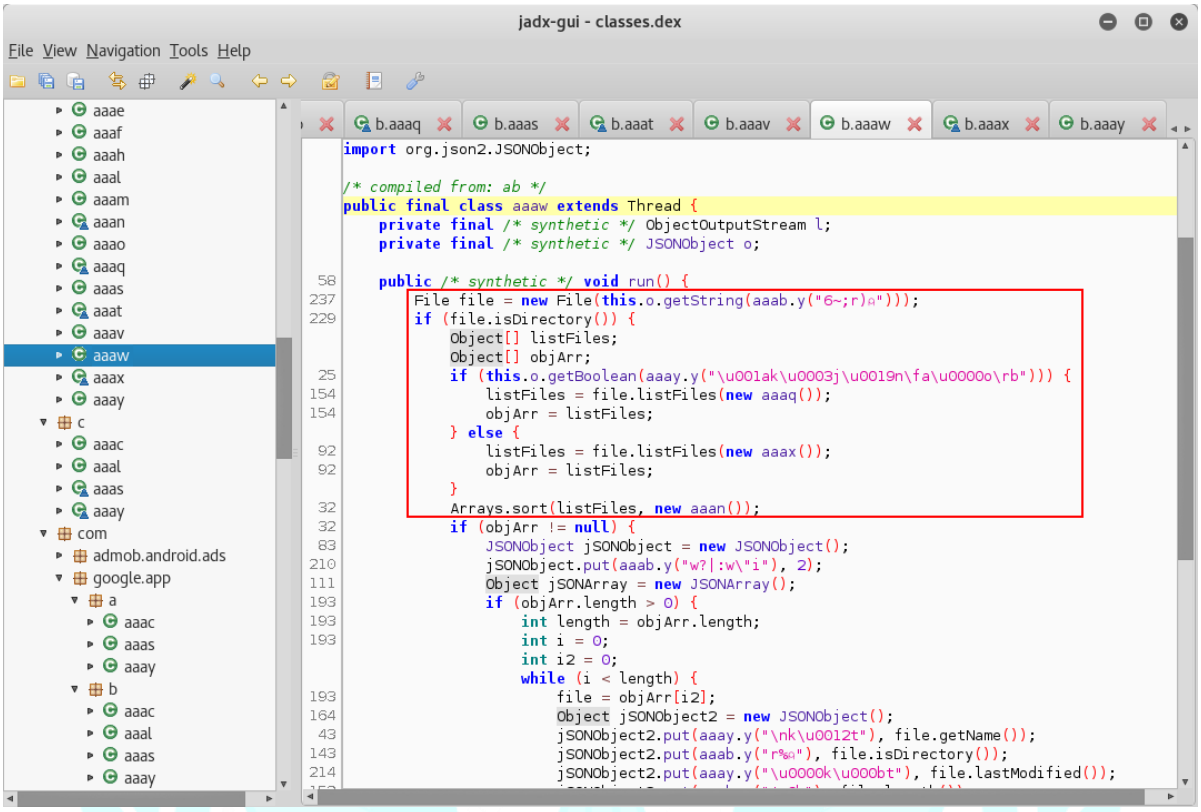
أيضا يقوم الفايروس بقبول جميع شهادات التشفير Accept All Certificates حال الاتصال بمركز القيادة والتحكم وذلك لتفادي ومنع أي مشكلة تختص في بروتوكول التشفير SSL حال التواصل مع الضحايا.



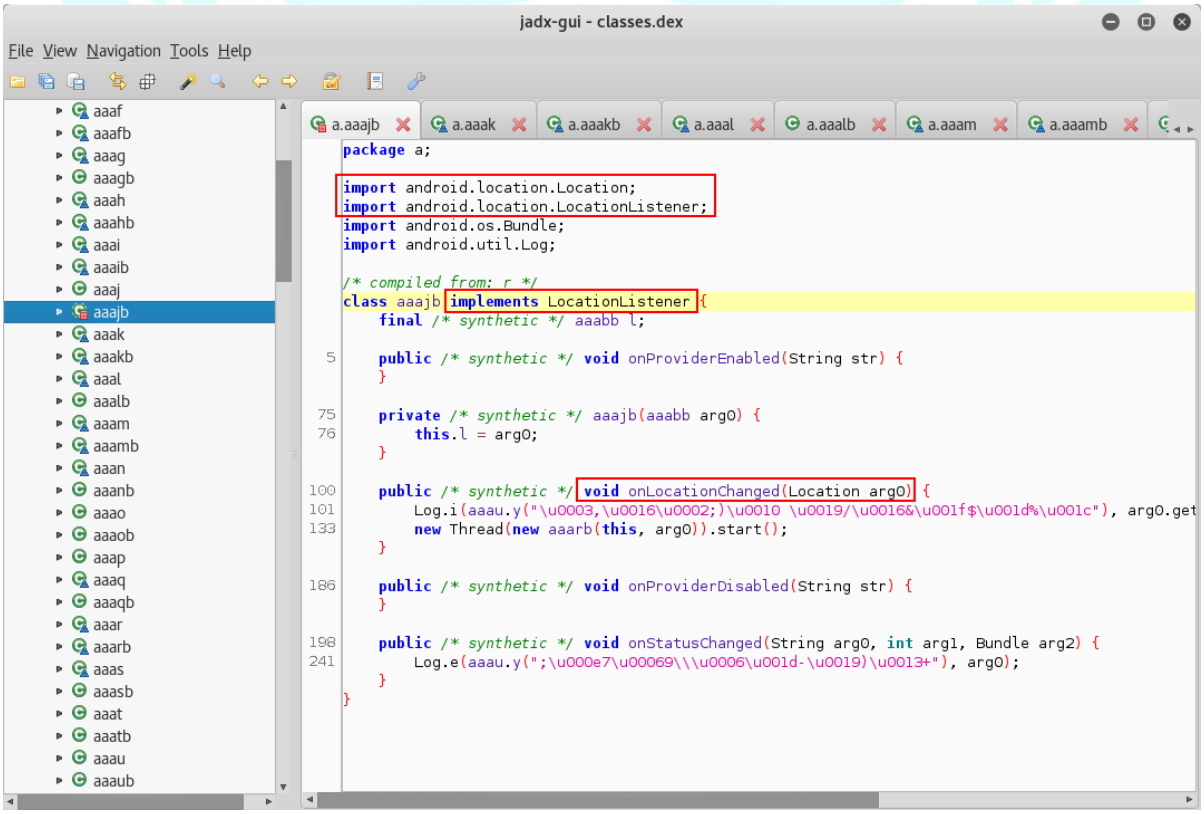
كما يستطيع الفايروس تحويل جهاز الأندرويد التابع للضحية إلى جهاز تنصت من حيث لا يشعر مستخدمه ثم تسجيل المحادثات التي تدور حول الجهاز ثم ارسالها لمركز القيادة والتحكم التابع لمجموعة "عقارب ليبيا" للاستماع اليها.



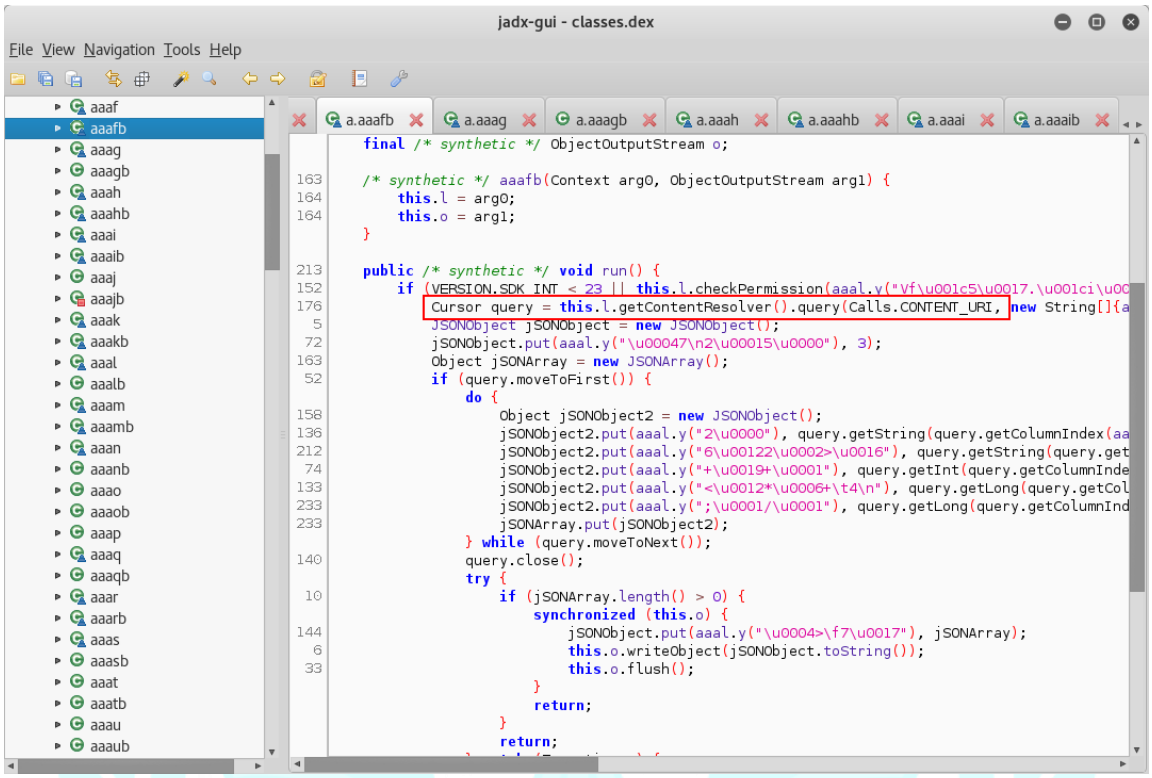
كما أن الفايروس قادر على تصفح كامل ملفات الضحية من صور وأفلام وملاحظات وغيرها من الملفات المحفوظة في ذاكرة الجهاز.



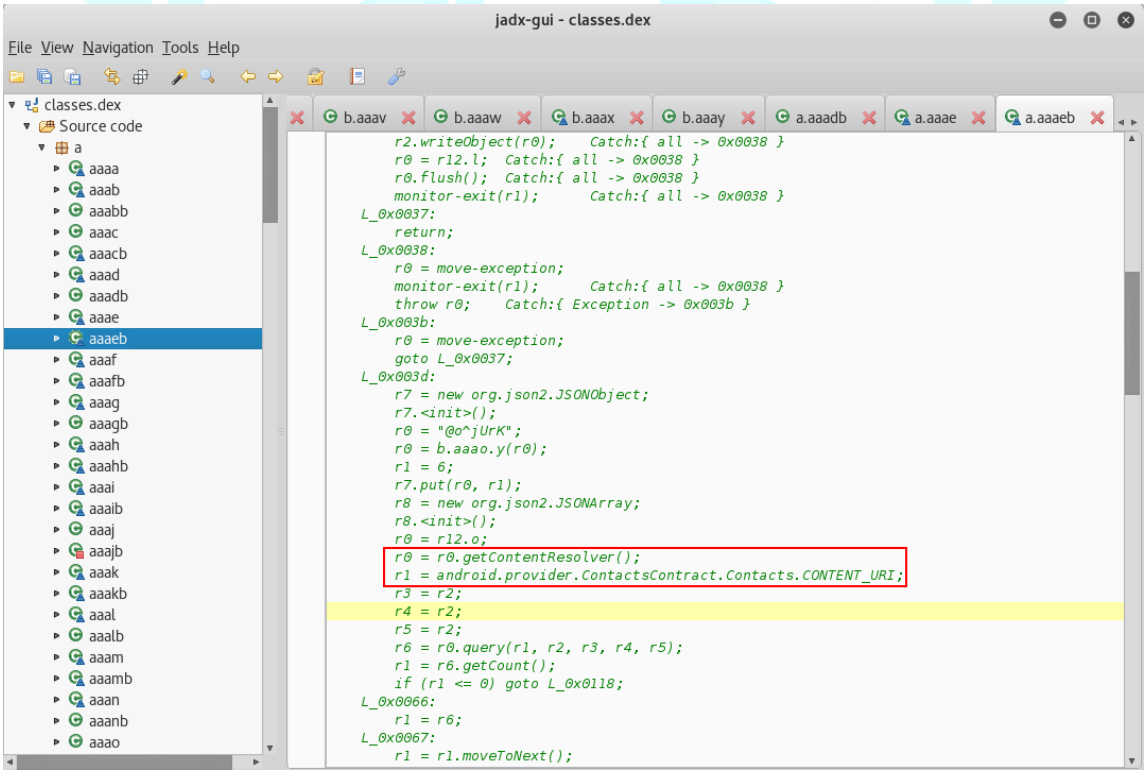
يستطيع الفايروس تحديد مكان الجهاز بالضبط على وجه الأرض بخطوط الطول ودوائر العرض ومنها يمكن معرفة مكانه ودراسة تحركاته أو استهدافه.



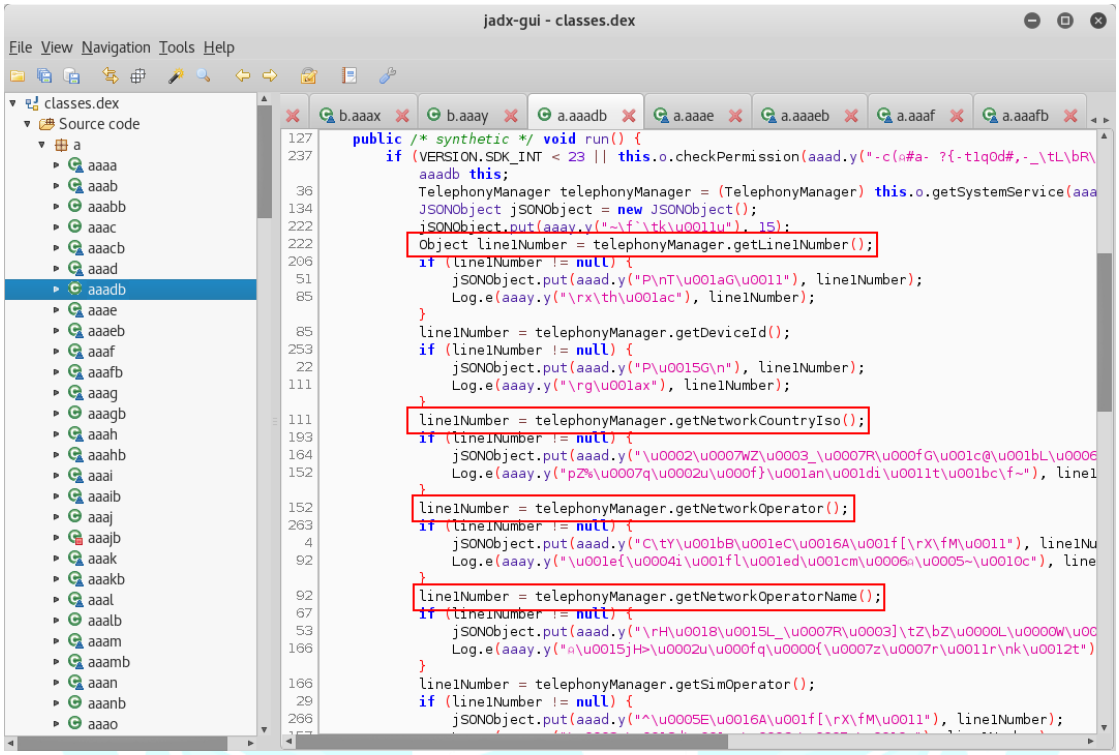
كما يمكن للفايروس أن يقوم بجمع سجلات الاتصال مع كامل تفاصيلها مثل ارقام التلفونات للأطراف المتصلة ومدة المكالمات وتاريخها ووقتها بالضبط.



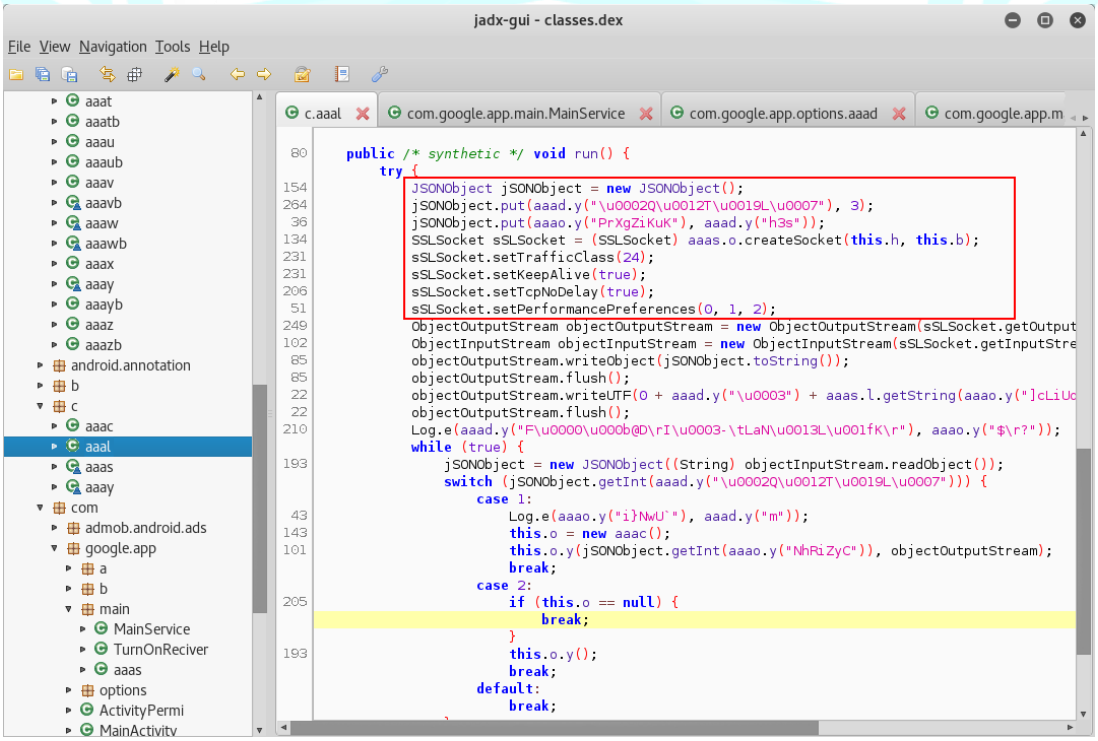
كما يستطيع الفايروس قراءة رسائل SMS القصيرة دون علم الضحية ومن هنا تستطيع مجموعة "عقارب ليبيا" الدخول على حسابات تيليجرام التابعة للضحايا عن طريق استخدام نسخة الـ Web من برنامج تيليجرام ثم وضع رقم الهاتف الخاص بالهدف ثم قراءة رمز الدخول والذي يتم ارساله عبر رسالة SMS.



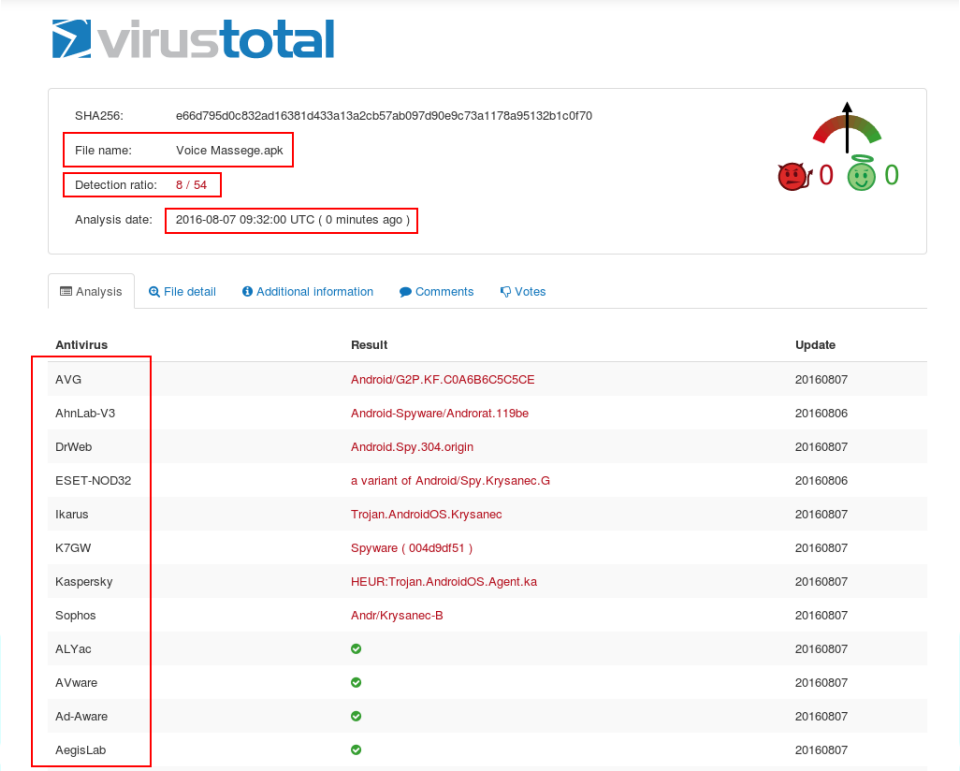
كما يستطيع الفايروس تحديد رقم هاتف الضحية ودولته واسم مشغل الشبكة من أبراج الاتصالات التابعة لشركة الاتصالات المتصلة بالجهاز.



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



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 Massege.apk

Detection ratio: 8 / 54

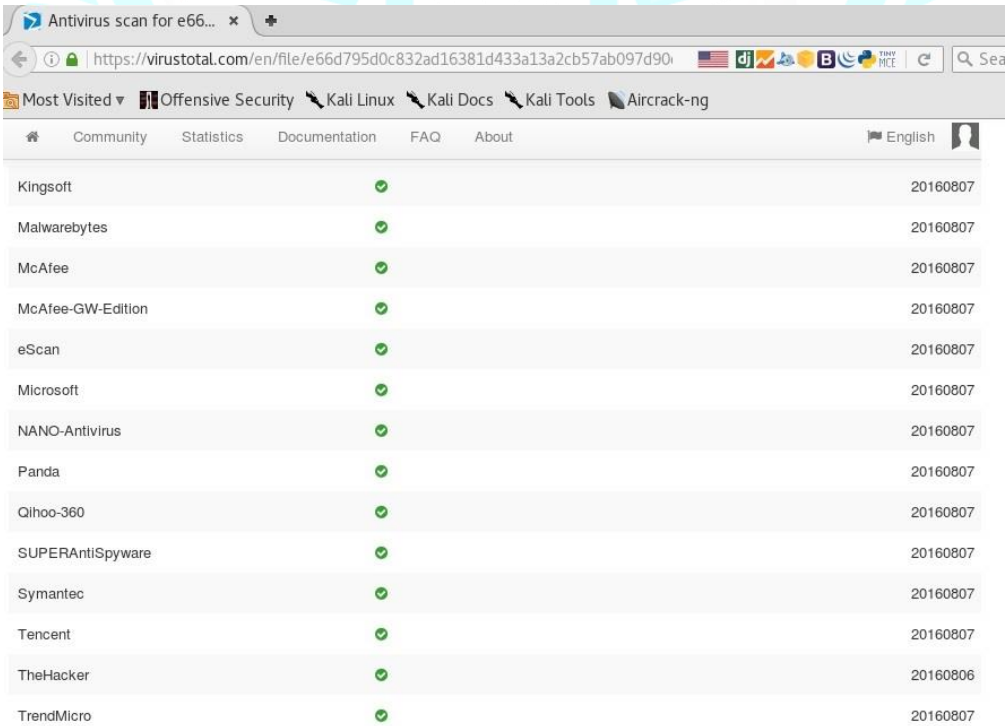
Analysis date: 2016-08-07 09:32:00 UTC (0 minutes ago)

0 0

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 سايبركوف 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 "قارتنر" 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

Kingsoft	✓	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

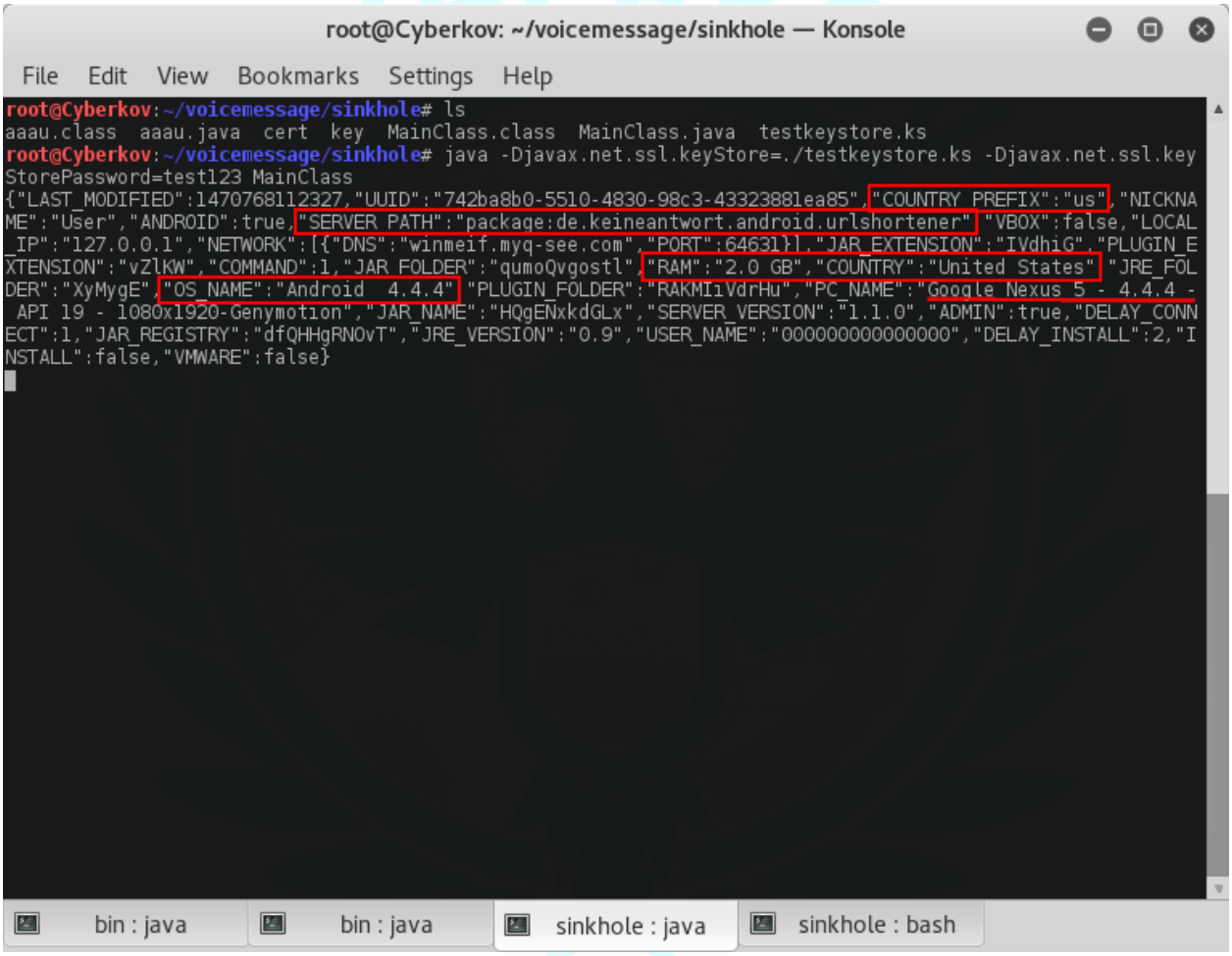
تحليل الاتصال مع مركز القيادة والتحكم

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

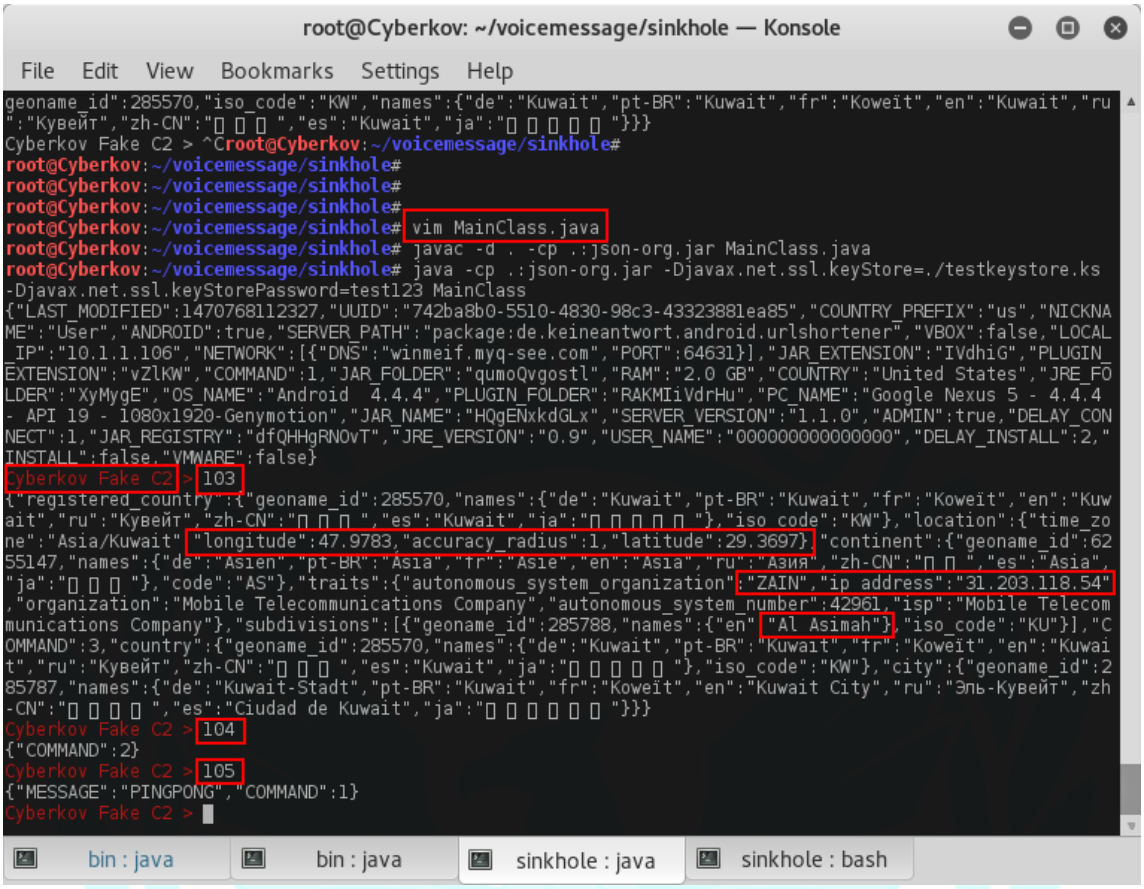
إعادة توجيه الاتصال Sinkhole

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

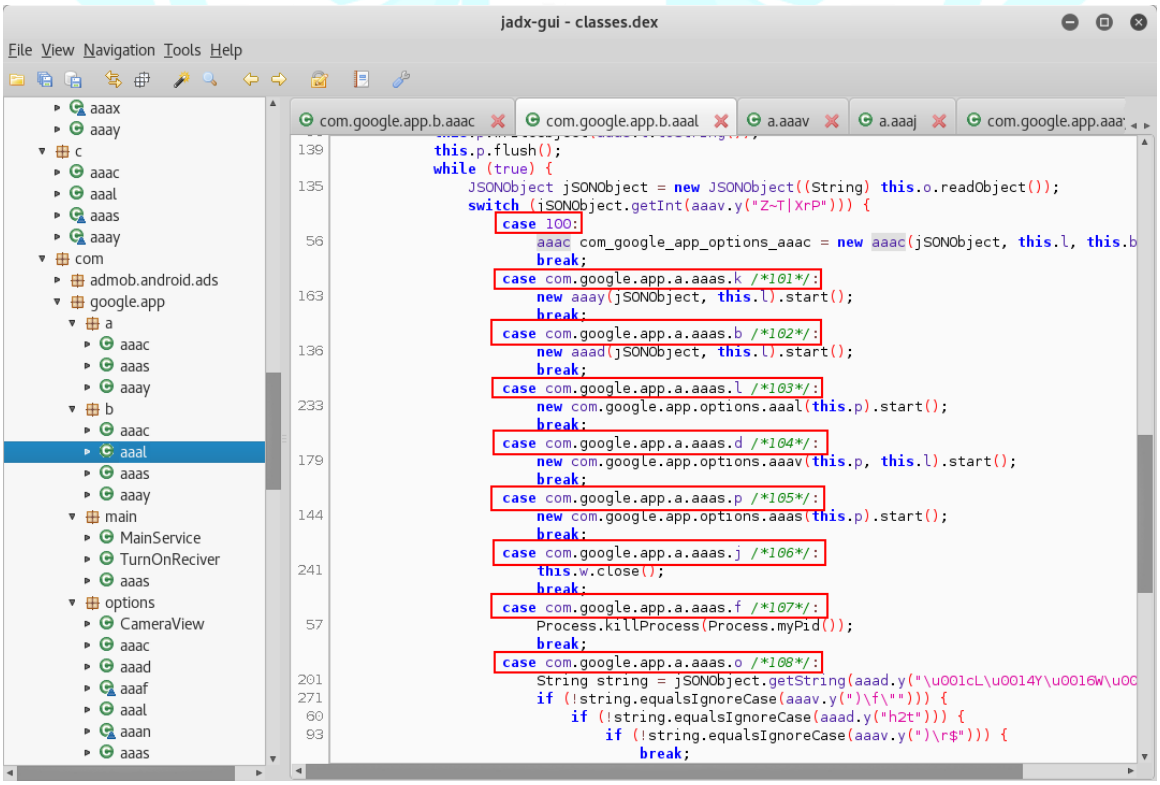
بعد تشغيل الفايروس وعند الاتصال بمركز القيادة والتحكم يقوم الفايروس بإرسال معلومات كثيرة عن الضحية الى المركز ومن ضمن هذه المعلومات: دولة الضحية وعنوان الـ IP الخاص به وسعة ذاكرة الجهاز وإصدار الأندرويد الخاص به ونوع الجهاز وغيرها من المعلومات.



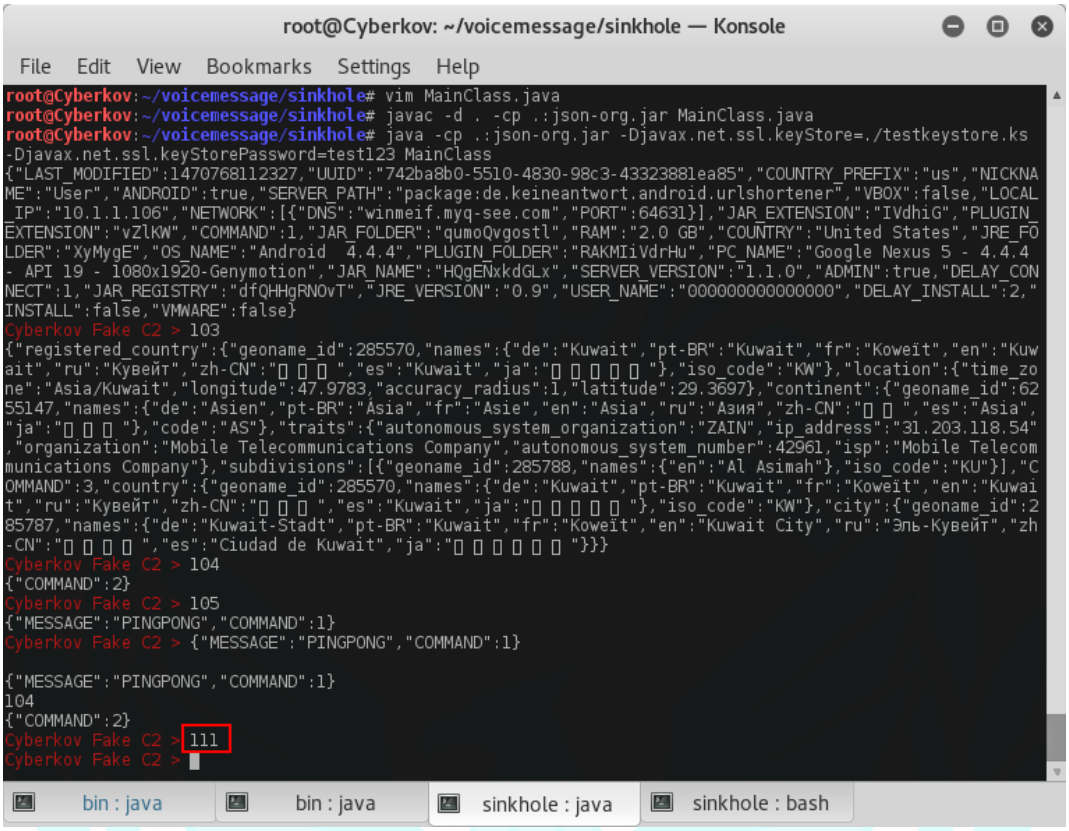
خادم سايبركوف المزيّف يستطيع ارسال الأوامر وقراءة الردود من الفايروس ومنها يمكن التحكم بالفايروس بشكل كامل.



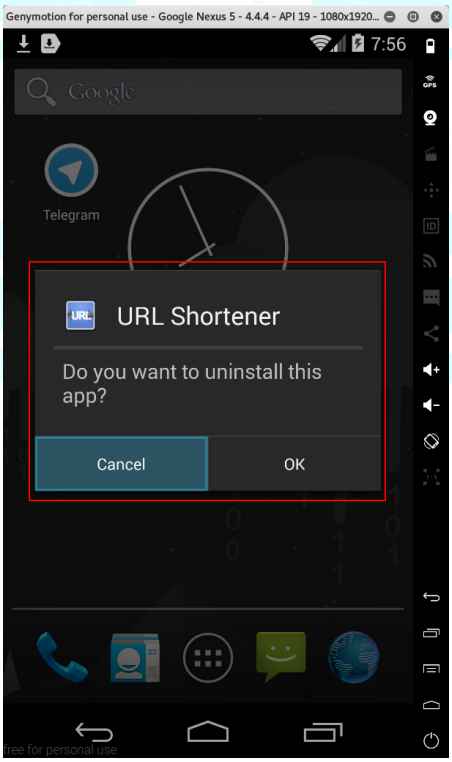
نلاحظ هنا أن الأوامر التي تم ارسالها الى الفايروس وهي 103 و 104 و105 متعلقة بالقائمة التالية والتي وجدناها معرفة داخل الفايروس:



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 سايبركوف المزيّف)، فمثلاً عند ارسال الأمر 111 يقوم الفايروس بإلغاء تنصيب البرنامج الحقيقي URL Shortener:

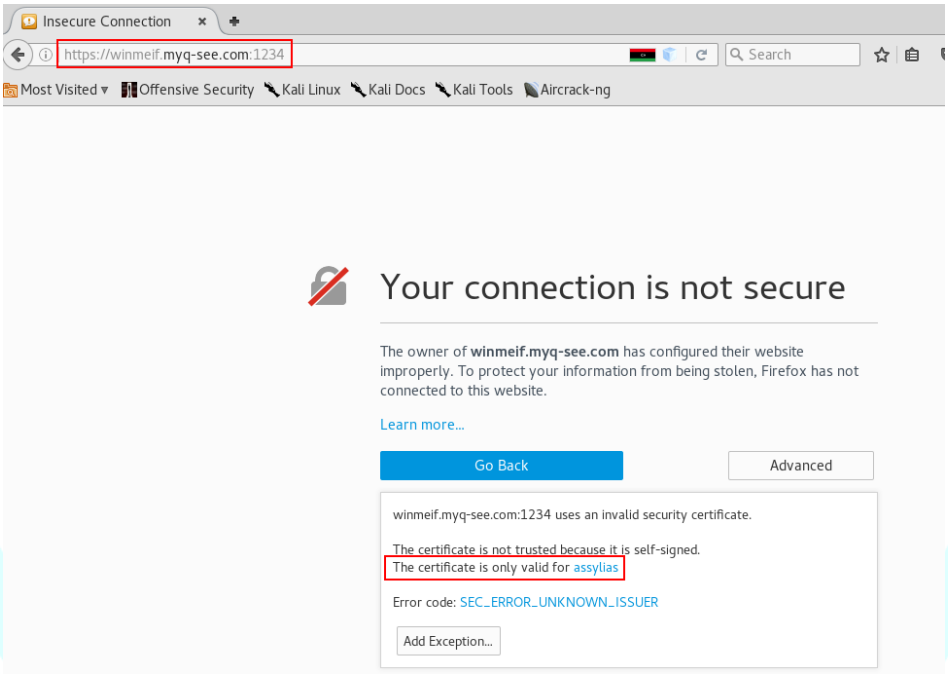


بعد ارسال الأمر تظهر هذه النافذة في جهاز الضحية:

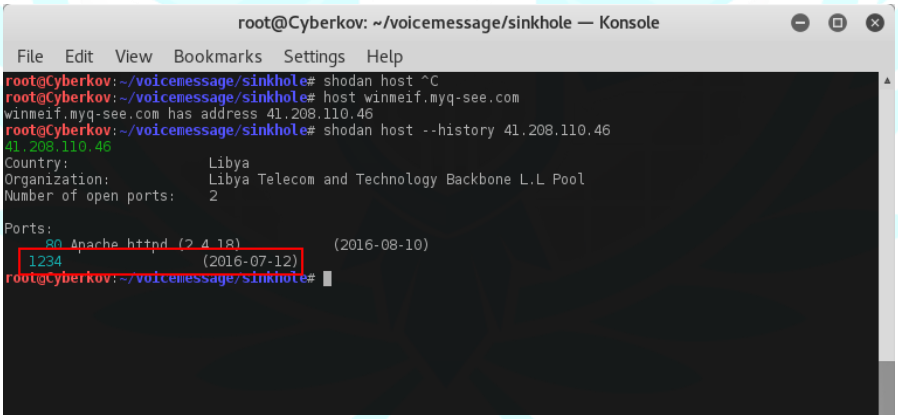


مركز القيادة والتحكم الحقيقي

قام فريق 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 assylias[2].



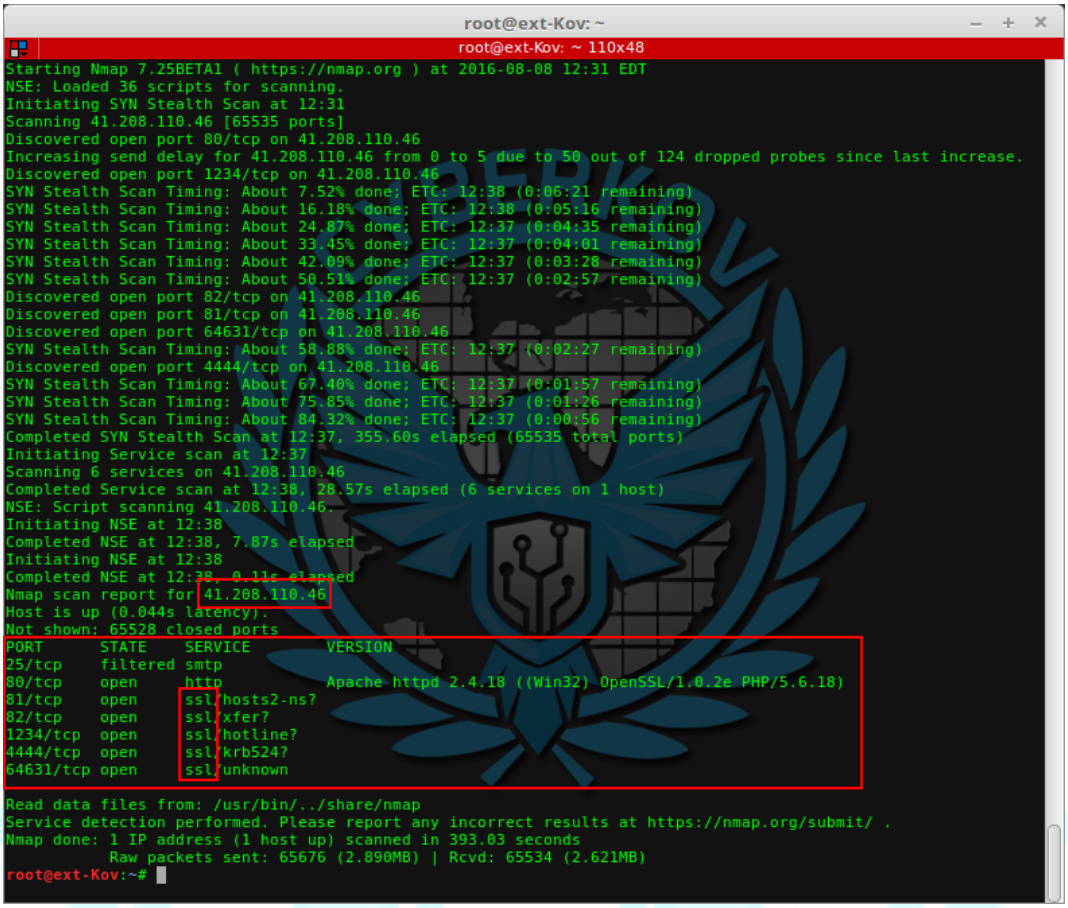
بناء على خدمة Shodan المتخصصة بمتابعة منافذ الخوادم في العالم، تم فتح منفذ 1234 في خادم مجموعة "عقارب ليبيا" بتاريخ 12-07-2016 وبهذا التاريخ قد يكون انتشار الفايروس تم قبل 25 يوم من كشف سايبركوف له.



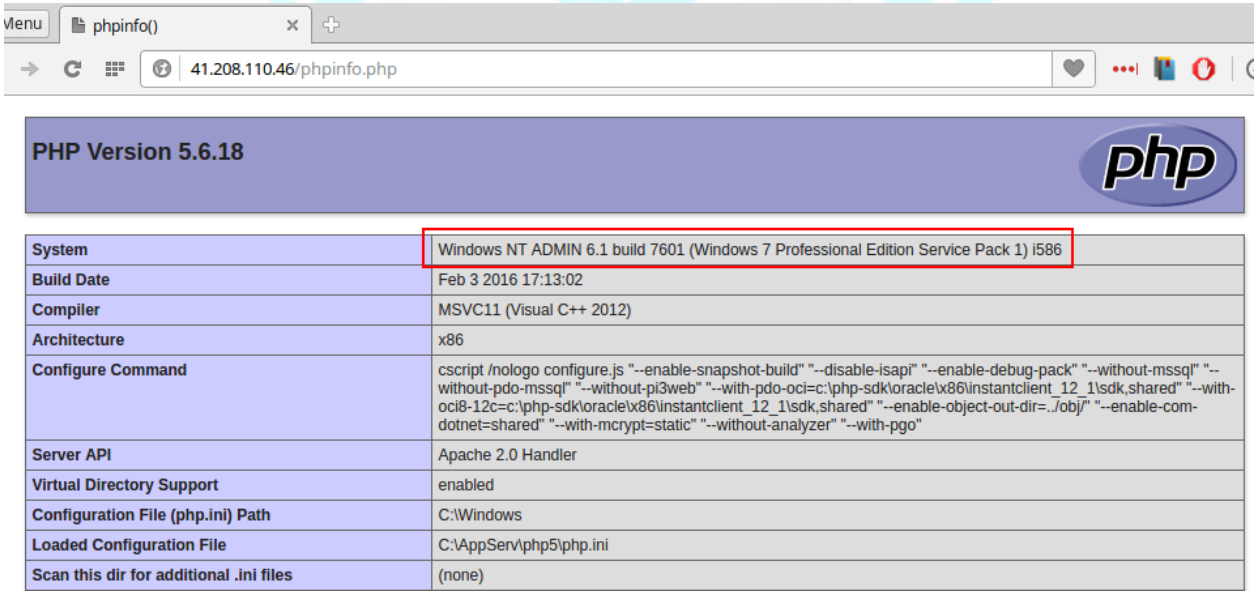
2 https://www.fidelissecurity.com/sites/default/files/FTA_1019_Ratcheting_Down_on_JSocket_A_PC_and_Android_Threat_FINAL.pdf

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.

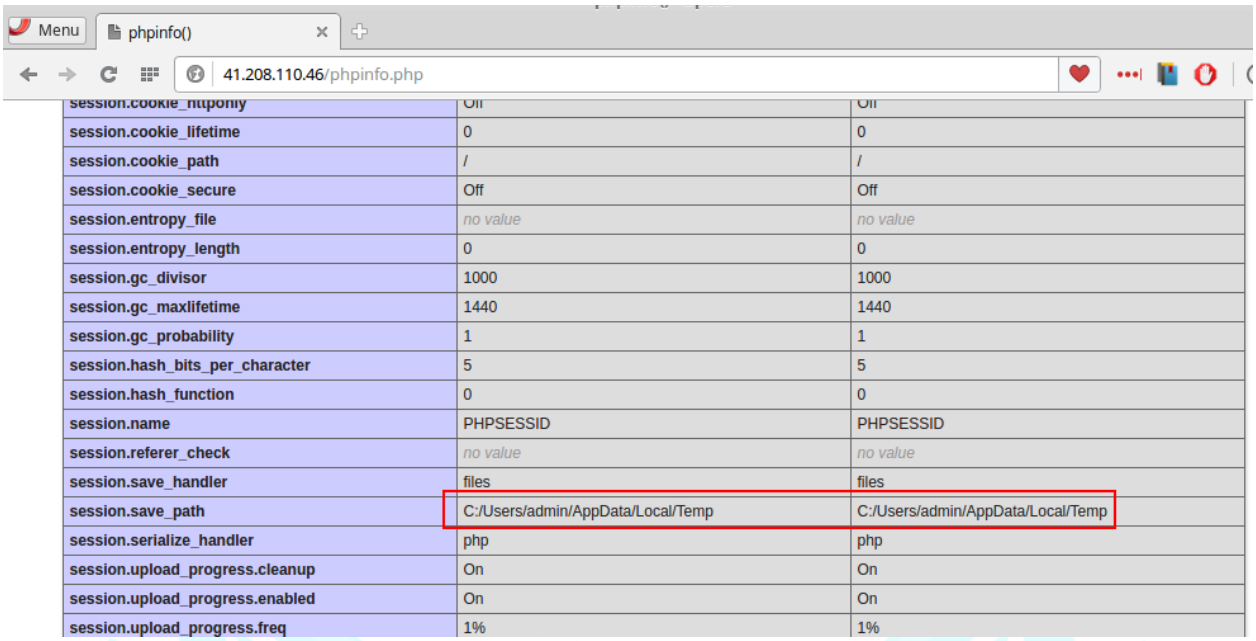


أيضا قامت مجموعة "عقارب ليبيا" دون قصد بوضع ملف باسم phpinfo.php في مركز القيادة والتحكم والذي بدوره يكشف معلومات مفيدة جدا عن أدوات وبرامج المجموعة أولها أن مركز القيادة والتحكم يعمل على نظام Windows 7 Professional Service Pack 1.



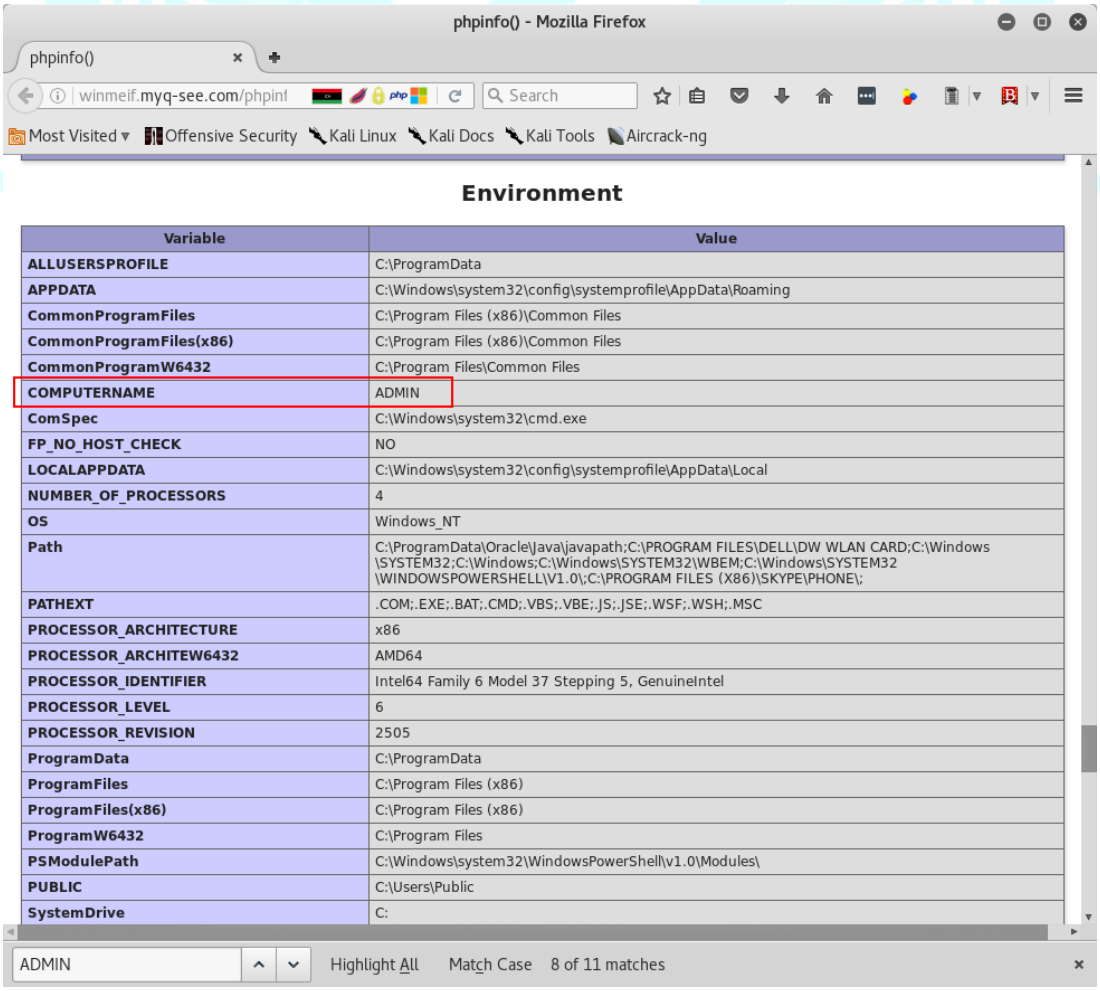
System	Windows NT ADMIN 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586
Build Date	Feb 3 2016 17:13:02
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--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"
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**.



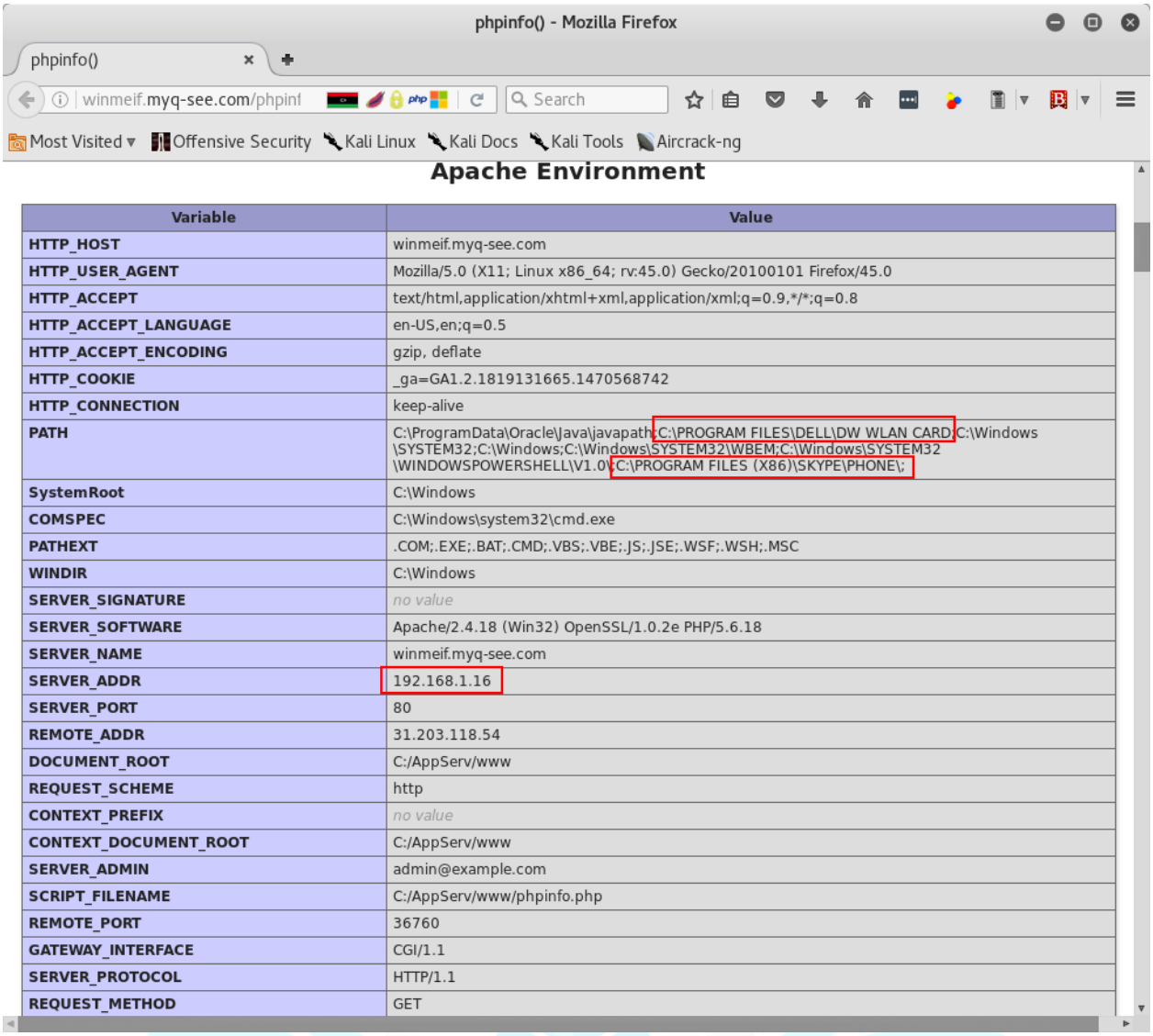
session.cookie_httponly	Off	Off
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_secure	Off	Off
session.entropy_file	no value	no value
session.entropy_length	0	0
session.gc_divisor	1000	1000
session.gc_maxlifetime	1440	1440
session.gc_probability	1	1
session.hash_bits_per_character	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:

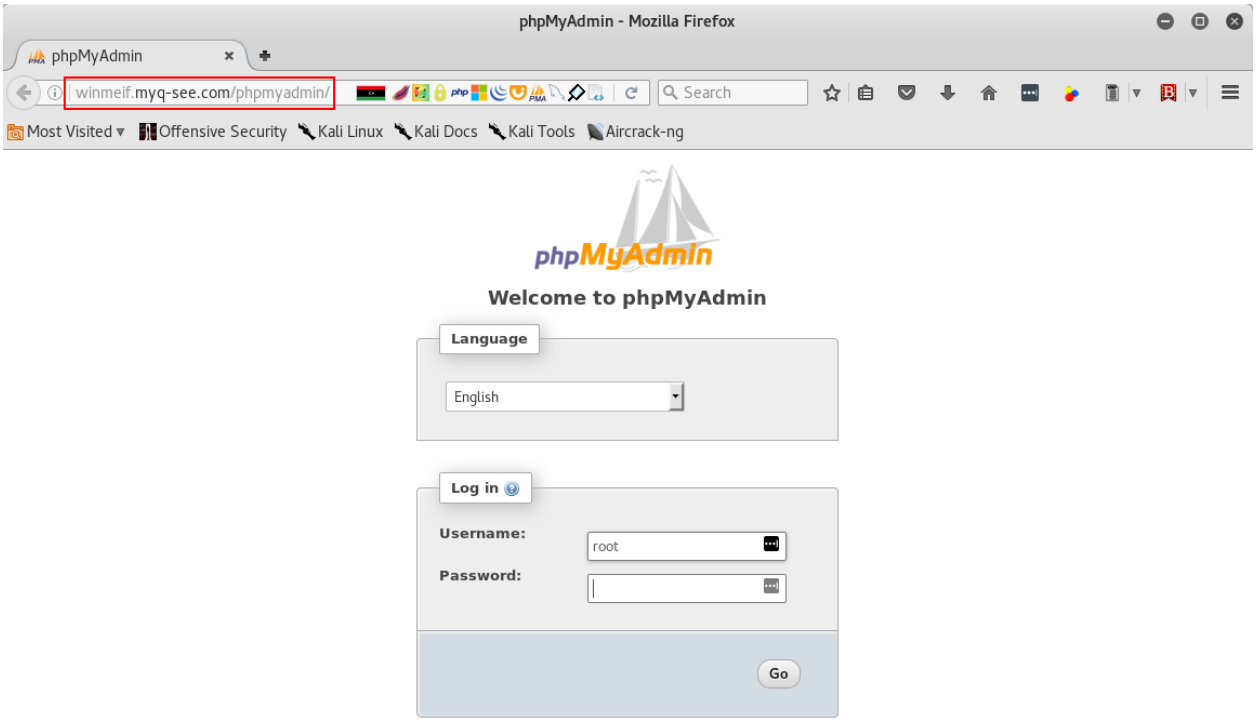
مجموعة "عقارب ليبيا" تستعمل أجهزة محمولة (لاب توب) من نوع Dell وتستخدم برنامج Skype وعنوان IP الداخلي لمركز القيادة والتحكم هو **192.168.1.16**.



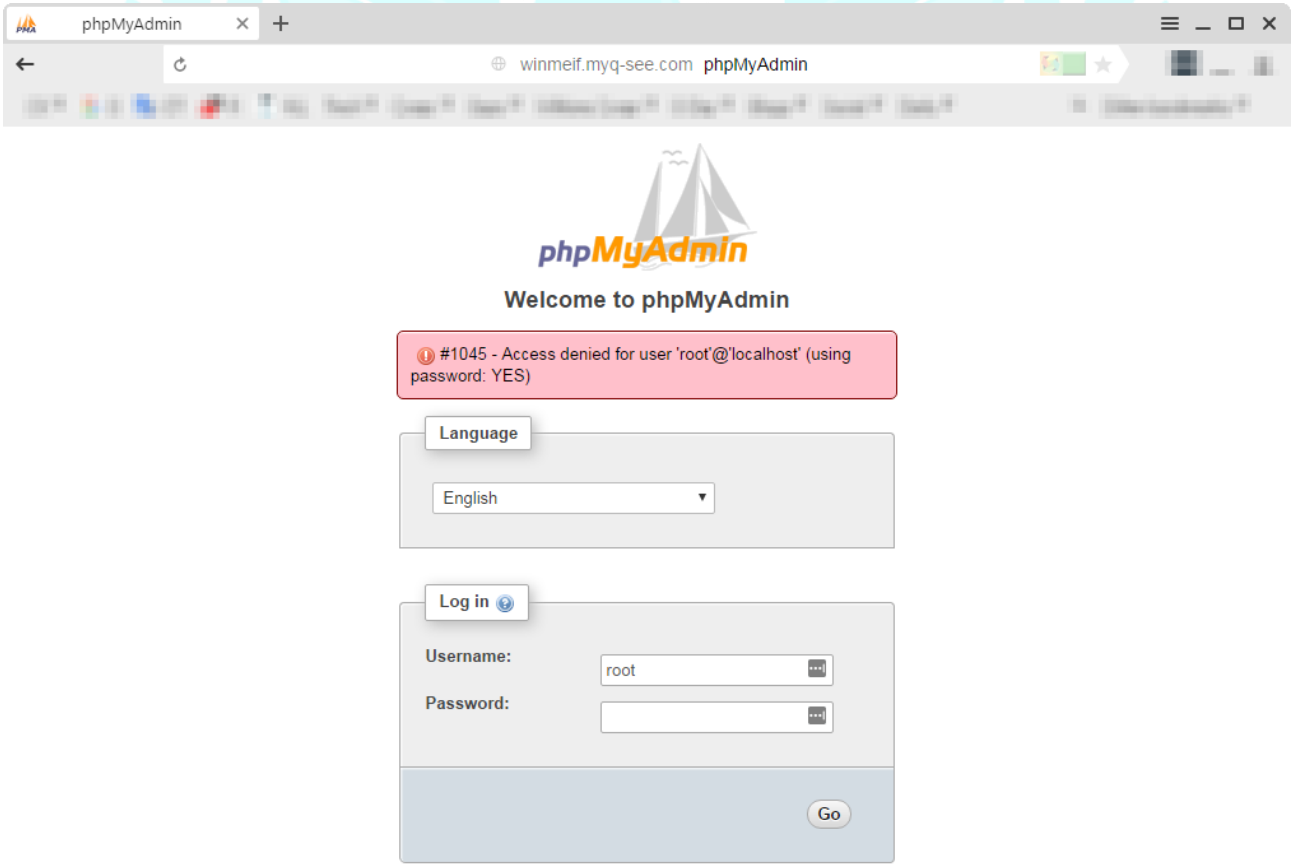
Apache Environment

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 سكربت PhpMyAdmin لادارة قواعد البيانات الخاصة بهم:



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

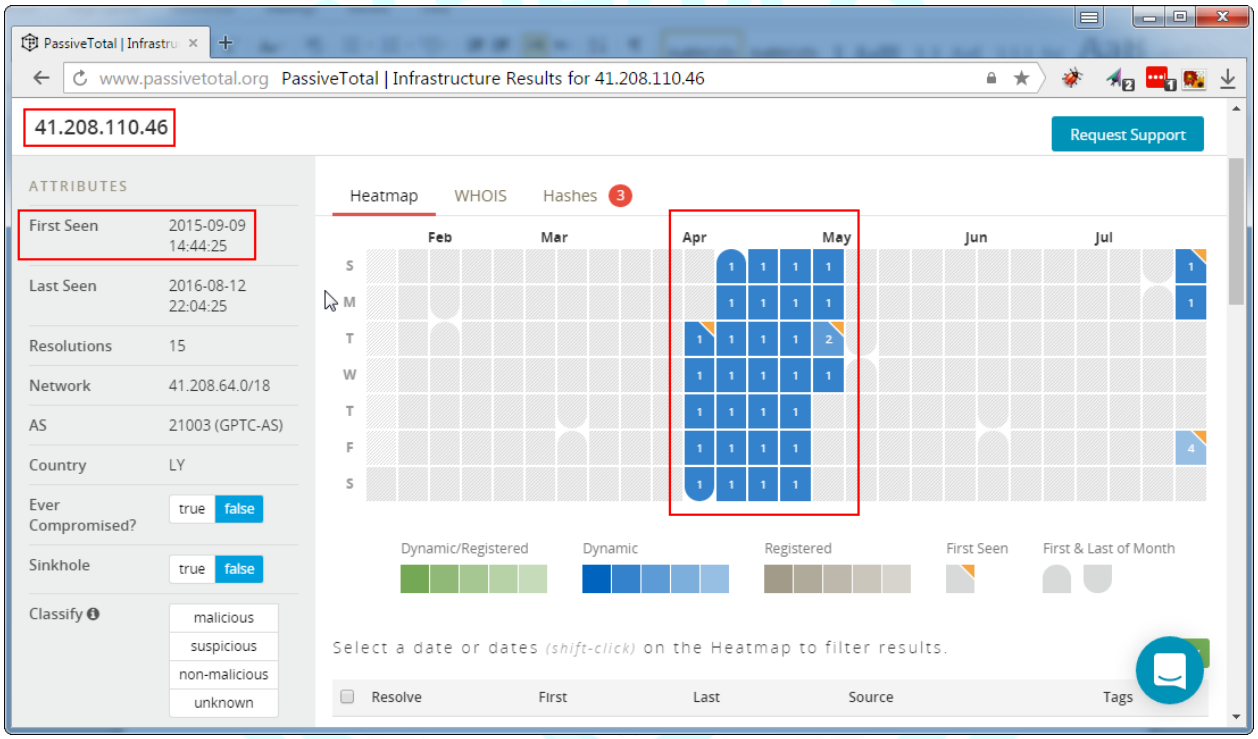


البنية التحتية لمجموعة عقارب ليبيا

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.

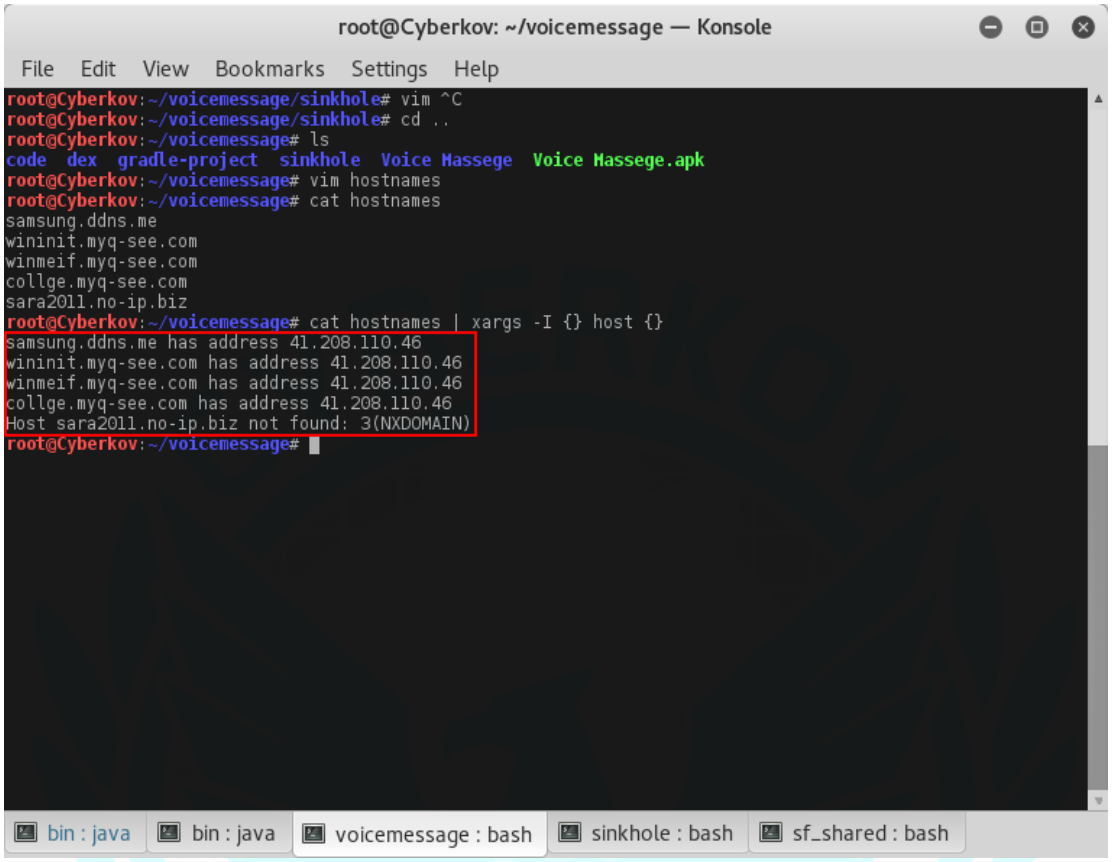
يتبين من الخريطة التالية أن مجموعة "عقارب ليبيا" بدأت عمليات الاختراق في 2015-09-09 (منذ سنة تقريبا من تاريخ نشر هذا التقرير) وخلال هذه السنة قامت المجموعة باستخدام 5 نطاقات للتحكم بالضحايا.



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

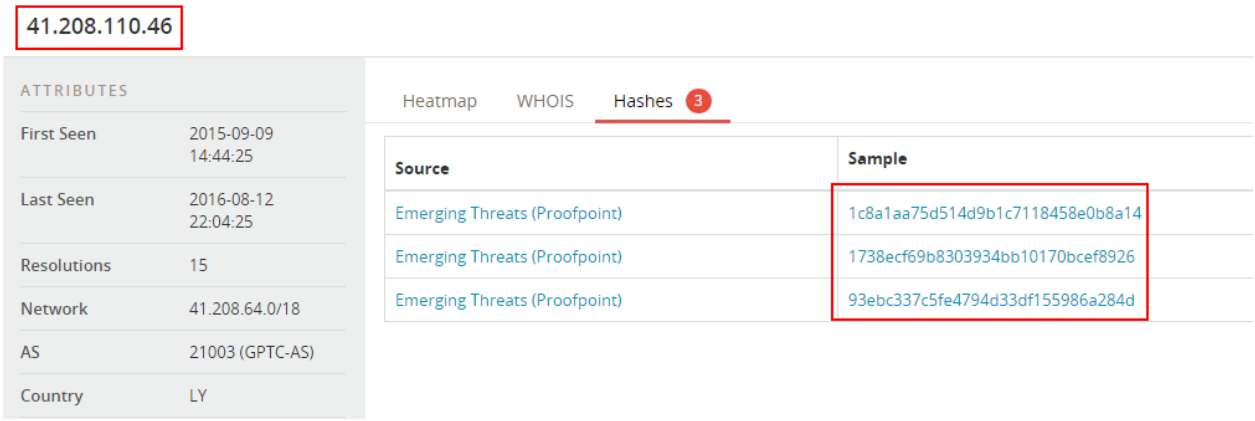
Hostname	First Seen	Last Seen
Samsung.ddns.me	26-04-2016	12-08-2016
Wininit.myq-see.com	24-05-2016	12-08-2016
Winmeif.myq-see.com	07-08-2016	12-08-2016
Collge.myq-see.com	09-09-2015	12-08-2016
Sara2011.no-ip.biz	08-10-2015	08-10-2015

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



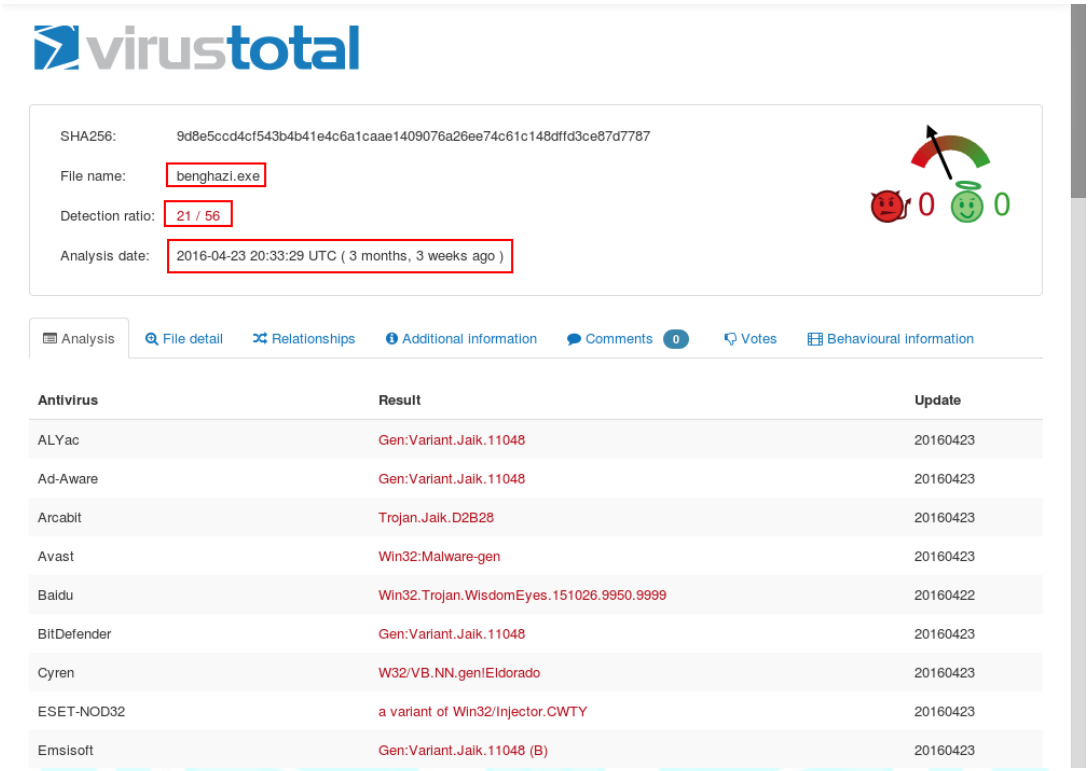
أيضا باستخدام منصة PassiveTotal يتبين أن هناك برامج تجسس أخرى مرتبطة بمجموعة "عقارب ليبيا"، هذه البرامج تحمل البصمات الرقمية (الهاشات) التالية (وهي من نوع MD5):

- 1738ecf69b8303934bb10170bcef8926
- 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 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: 9d8e5ccd4cf543b4b41e4c6a1caae1409076a26ee74c61c148dffd3ce87d7787

File name: benghazi.exe

Detection ratio: 21 / 56

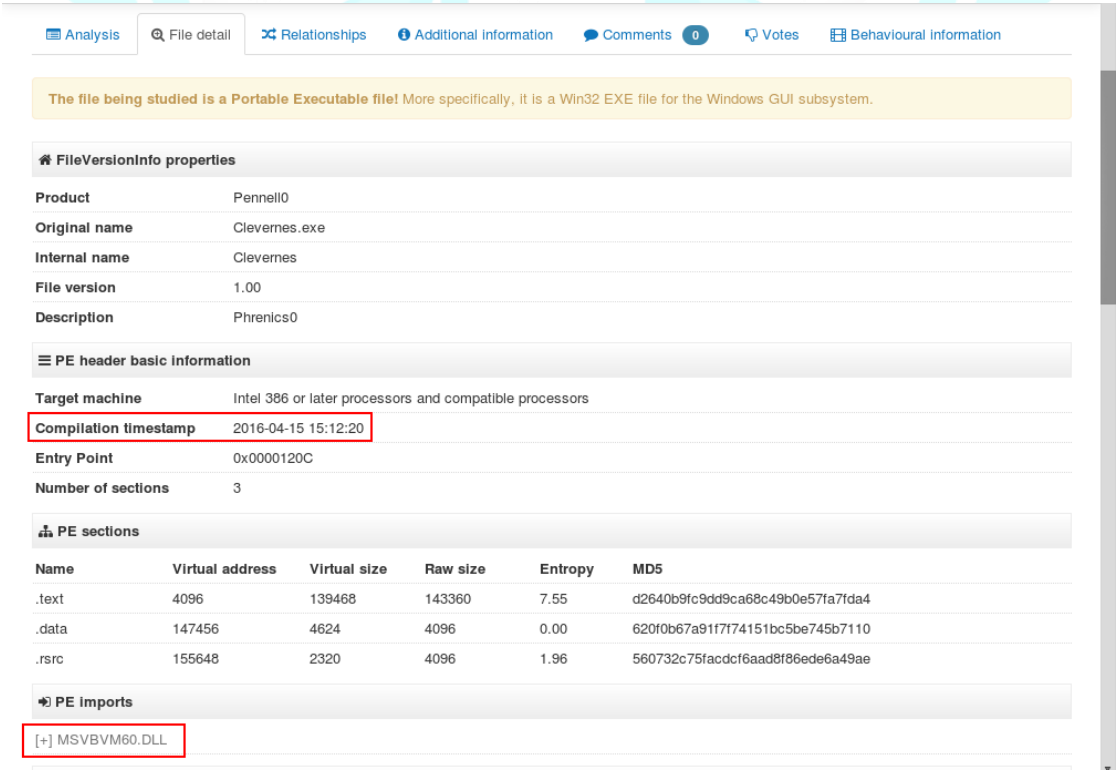
Analysis date: 2016-04-23 20:33:29 UTC (3 months, 3 weeks ago)

0 0

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
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.



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	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

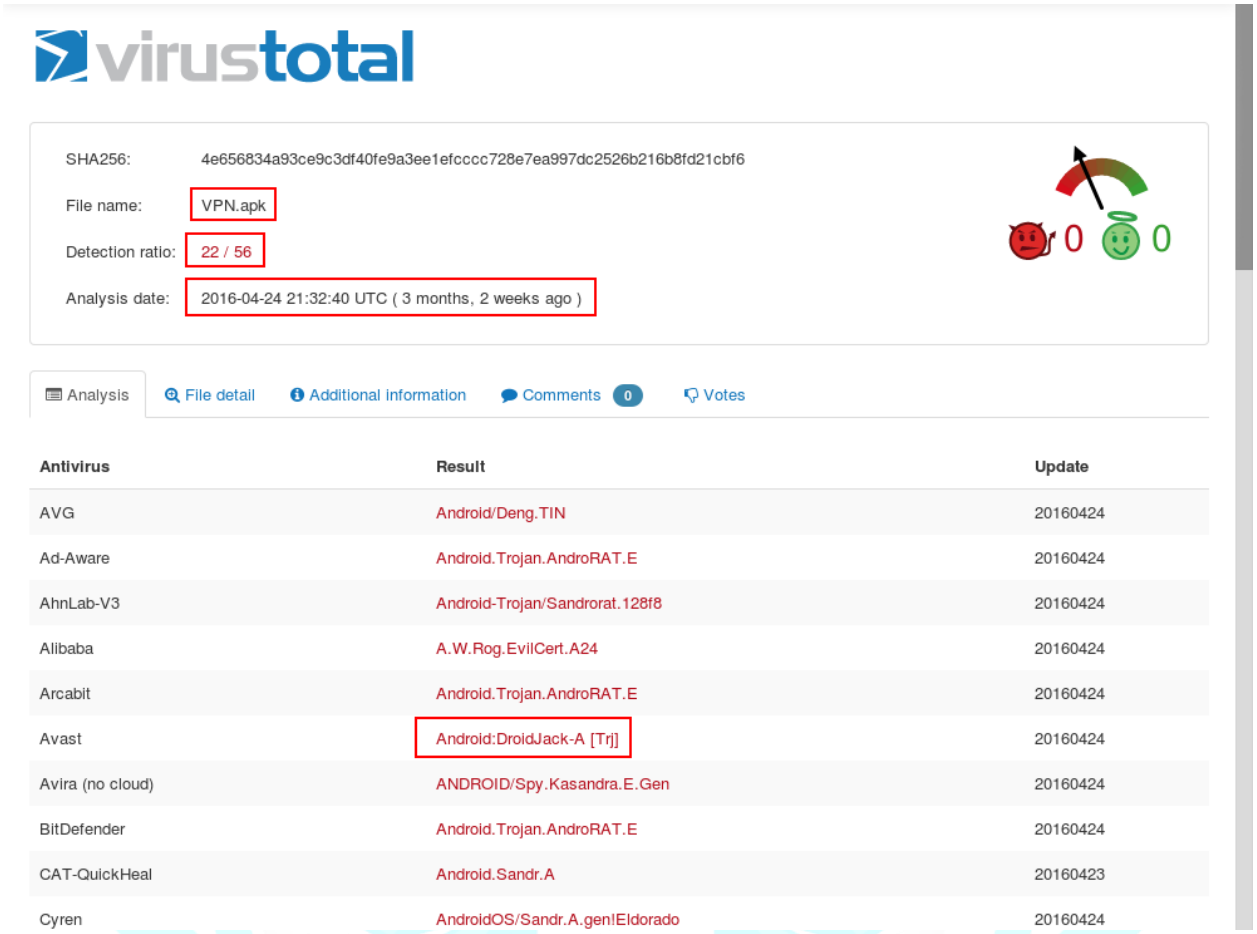
PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	139468	143360	7.55	d2640b9fc9dd9ca68c49b0e57fa7fda4
.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.



virustotal

SHA256: 4e656834a93ce9c3df40fe9a3ee1efcccc728e7ea997dc2526b216b8fd21cbf6

File name: VPN.apk

Detection ratio: 22 / 56

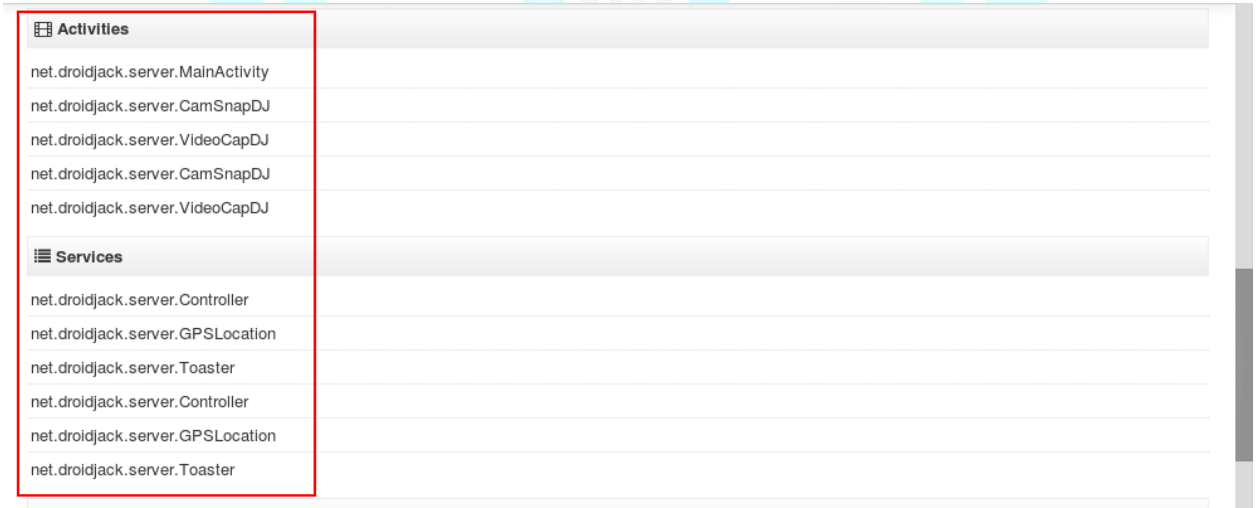
Analysis date: 2016-04-24 21:32:40 UTC (3 months, 2 weeks ago)

0 0

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.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 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

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 إلكترونيا.

توصيات أمنية لحماية أجهزة أندرويد من عقارب ليبيا

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

- التحديث المستمر لجهازك الأندرويد
- استخدام برنامج مكافحة الفايروسات DrWeb Security Space بنسخته الكاملة من هنا لحمايتك من البرامج الخبيثة
- إستخدام الـDrWeb 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 إستخدام تطبيق تيليجرام Telegram 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 للمساعده في المساهمة في كشف برامج "عقارب ليبيا" التجسسية:

Type	Indicator
Sha256	9d8e5ccd4cf543b4b41e4c6a1caae1409076a26ee74c61c148dffd3ce87d7787
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