Cyberkov Co. Ltd.
www.cyberkov.com
info@cyberkov.com

Hunting Libyan Scorpions

Investigating a Libyan Cyber Espionage Campaign Targeting High-Profile Influentials

TLP: White

For public distribution

18/September/2016

Legal Notice:

This document is intended for public use and distribution. Unauthorized use or reproduction of this document without referencing Cyberkov is prohibited.

This document has been prepared by Cyberkov Co. Ltd.

Document Control

Document Title	Hunting Libyan Scorpions
TLP Classification	White
Document Version	1.0
Creation Date	01/September/2016
Last Modification Date	18/September/2016
Distribution	Public Distribution
Reference	PD-001

Cyberkov Contact Details

Name	Cyberkov Media Office
Email	media@cyberkov.com
Phone Number	+965 22445500
Fax Number	+1 (888) 433-3113
Office Number	+965 22445500
General query	info@cyberkov.com

Table of Contents

Executive Summary

Libya maybe known in non-stable political system, civil war and militant groups fighting for the land and oil control but it is definitely not known in cyber malicious activities, cyber espionage and hacking groups. No parties in Libya before this analysis reported to use cyber attacks, malwares nor recruit hackers to spy on their rivals. Today we have a different story.

In the past weeks on 6 August 2016, Cyberkov Security Incident Response Team (CSIRT) received a numerous Android malwares operating in different areas in Libya especially in Tripoli and Benghazi.

The malware spreads very fast using Telegram messenger application in smartphones, targeting high-profile Libyan influential and political figures.

The malware first discovery was after a highly Libyan influential Telegram account compromised via web Telegram using IP address from Spain.

The following day, the attackers spread an Android malware binded with legitimate Android application from the compromised Telegram account to all his contacts pretending it is an important voice message (misspelled it by "Voice Massege.apk") which indicates a non-english (maybe an Arabic) attacker.

After spreading the malware, more Android smartphones has been infected using the same technique (via Telegram) and then repost the malware again and again making a network of victims.

Analysis of this incident led us to believe that this operation and the group behind it which we call **Libyan Scorpions** is a malware operation in use since September 2015 and operated by a politically motivated group whose main objective is intelligence gathering, spying on influentials and political figures and operate an espionage campaign within Libya.

Also, the analysis of the incident led to the discovery of multiple malwares targeting Android and Windows machines.

Libyan Scorpions threat actors used a set of methods to hide and operate their malwares. They appear not to have highly technical skills but a good social engineering and phishing tricks. The threat actors are not particularly sophisticated, but it is well-understood that such attacks don't need to be sophisticated in order to be effective.

> *Using malwares as weapon in an active warzone such as Libya, make the victims easy targets for assassination or kidnapping by tracking their physical locations and monitoring them day and night.*

Tactics, Techniques and Procedures (TTPs)

Libyan Scorpions is believed to be a political motivated group targeting a high-level influential and political figures in multiple cities within Libya.

Libyan Scorpions first compromised a personal Telegram account for a Libyan influential person with unknown vector. The victim received a push notification from his Telegram app that someone from Spain is logged into his account:


The victim mistakenly deleted Telegram application from his phone thinking that this is going to stop the attacker(s).

Second day, the attacker used the victim phone number to spear phish his contacts in Telegram by pretending that the real person is sending a voice message while the file is actually a malicious APK (Android Package) file.

This APK file targets only Android-based smartphones. Once the new victim click on the APK file, the application installs itself in the device without any problem and is fully functional. The icon of the application appears in the Apps menu named (URL Shortener).
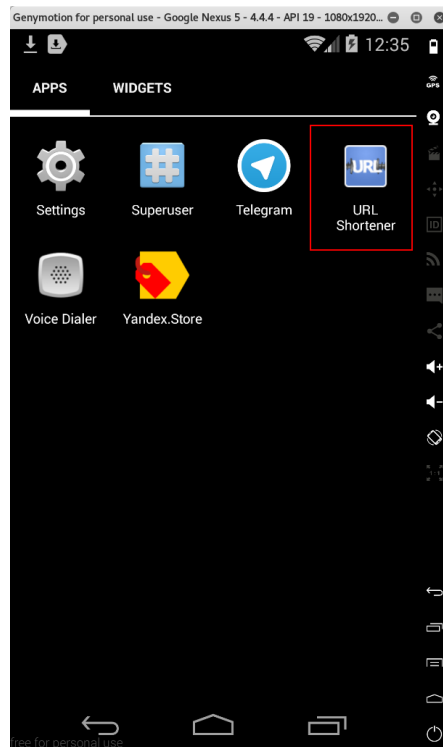
The real malicious code is running in the background as Android service[1].

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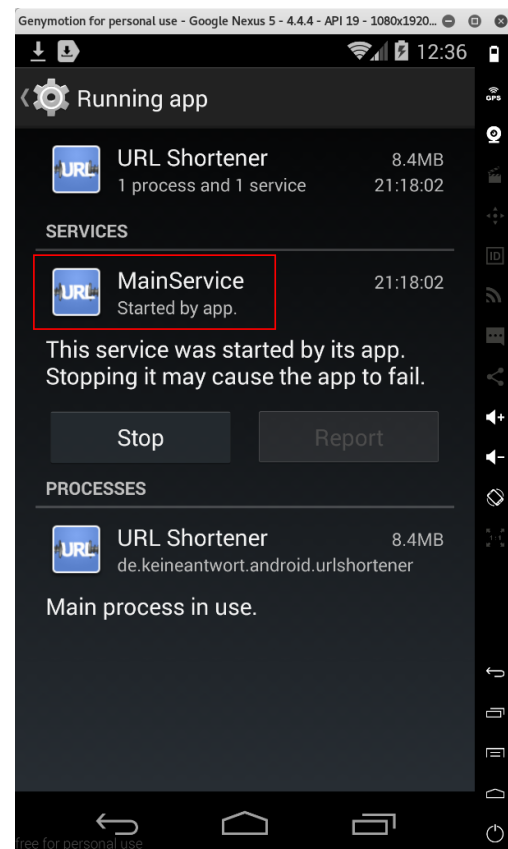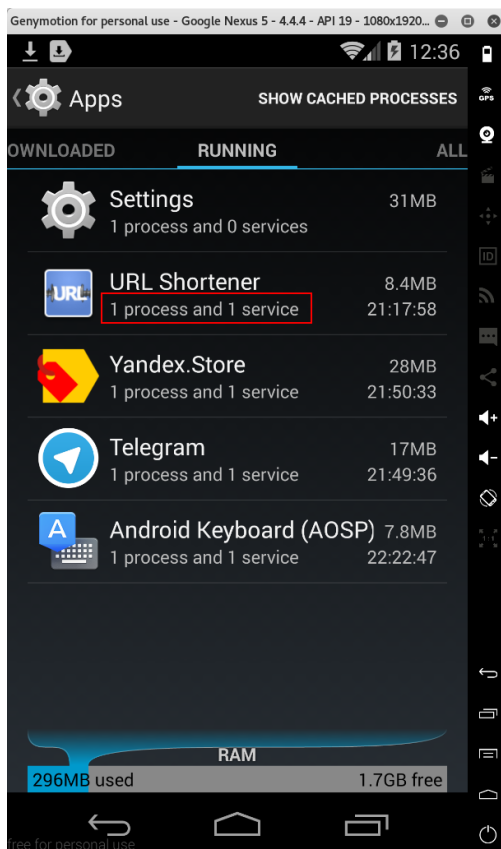
Malware Analysis

Cyberkov Security Incident Response Team (CSIRT) started analyzing the APK file (malware) and the first step was to unpack it.

After unpacking with apktool and reading (AndroidManifest.xml) file, it appears that the application is a malware injected inside a legitimate application having java package name:
de.keineantwort.android.urlshortener.

Searching for the application in Google Play store with that specific package name (https://play.google.com/store/apps/details?id=de.keineantwort.android.urlshortener) yields:
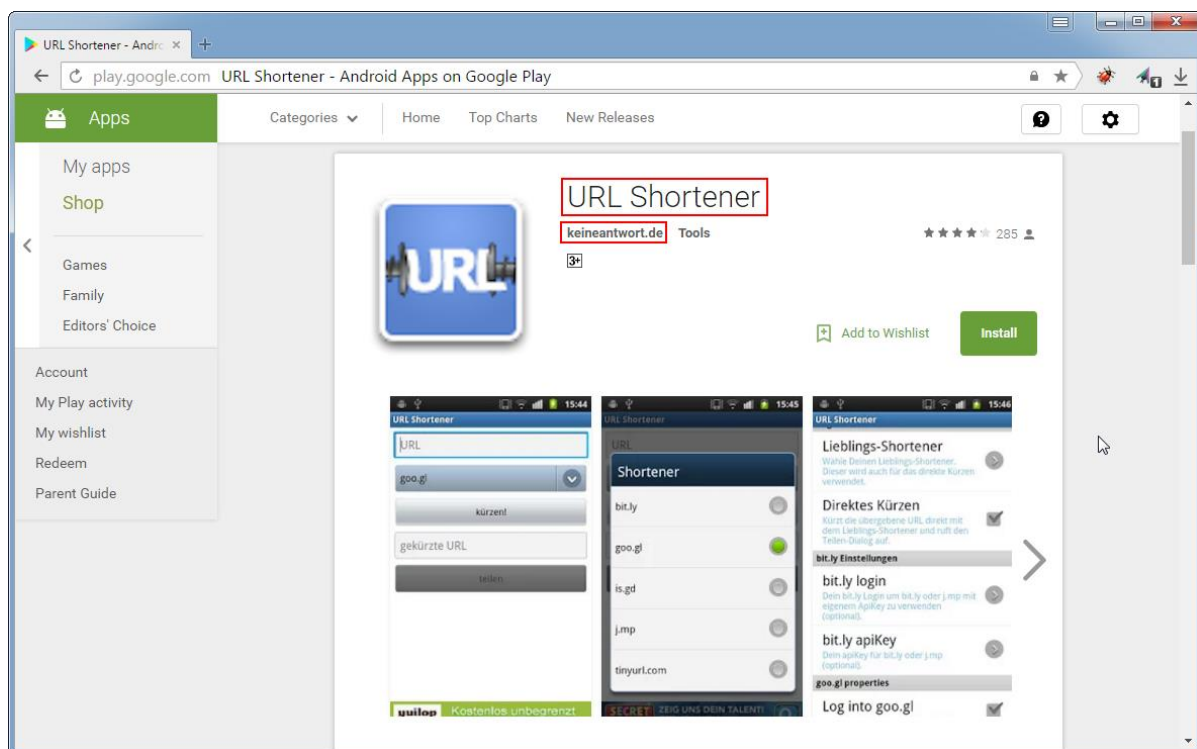
The application exists in the store and the Libyan Scorpions hacking group took an instance of the APK and injected their malware into that legitimate application to spread it.

The real application is created by keineantwort.de and we have verified it from their main website:
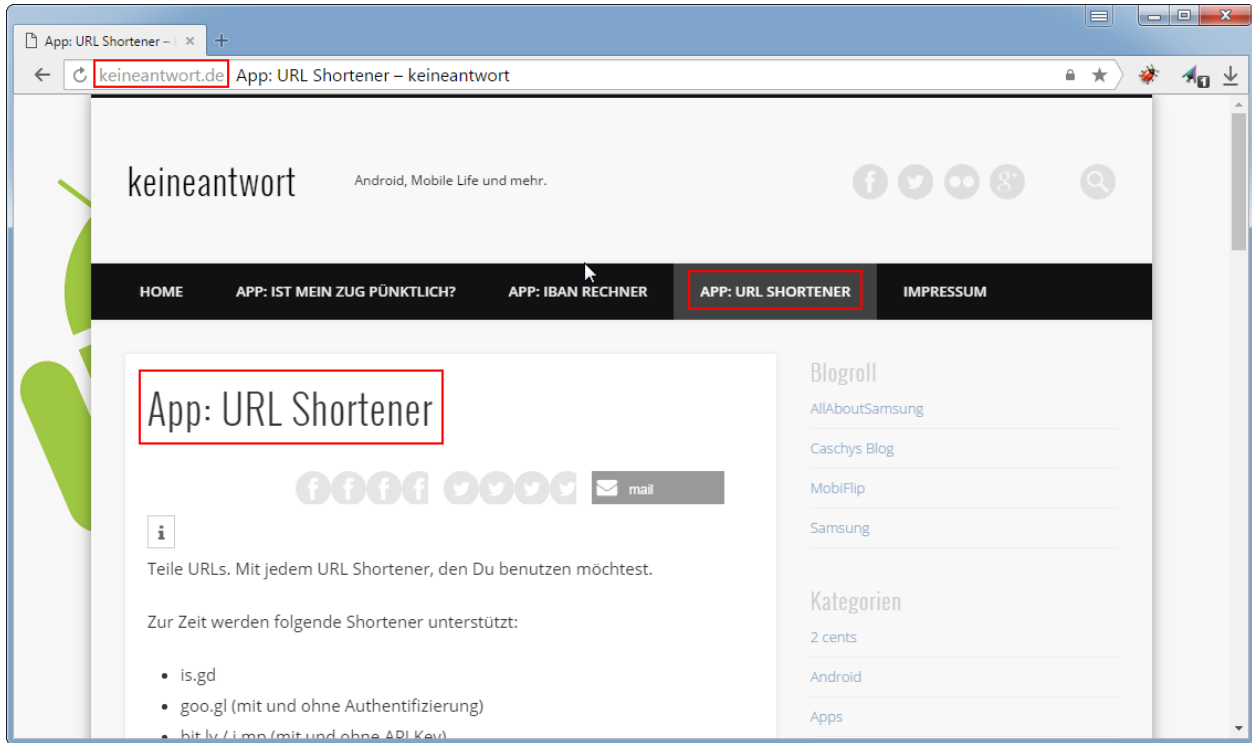
Going back to (AndroidManifest.xml) file, the malware register itself as receiver of almost all intents and request almost all permissions available in Android system!

The malware can access location, network state, battery status, Bluetooth, camera, capturing audio, internet, …, etc.

After launching the malicious application for the first time, it checks if the Android device is rooted or not and if rooted, it asks for root permission.

Carrying on the reverse engineering of the malware, we found a file called "**config.json**" which is a base64 encoded json file containing the configuration of the malware and its Command and Control **(C2)**. The characteristics of the malware ("a.txt" and "config.json" files) and the functionality of it is very similar to JSocket and AlienSpy famous Android Remote Access Tools (RATs).

Decoding the "config.json" file using base64 decoder shows that the C2 hostname/domain is:

winmeif.myq-see.com using the port **64631**

Resolving the hostname gives: **41.208.110.46** which is a static Libyan IP address owned by **Libya Telecom and Technology Backbone**.

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

Going back to the domain/hostname used by the Libyan Scorpions hacking group, it appears that **myq-see.com** is a dynamic DNS service open for the public.

Scrolling down the web page, it is created by Q-See which is a company that sells cameras and it seems that Q-See published this service to help their customers to connect to their IP cameras regardless of IP changes.

The malware uses RootTools and RootShell components to make root privileged tasks easy in Android.
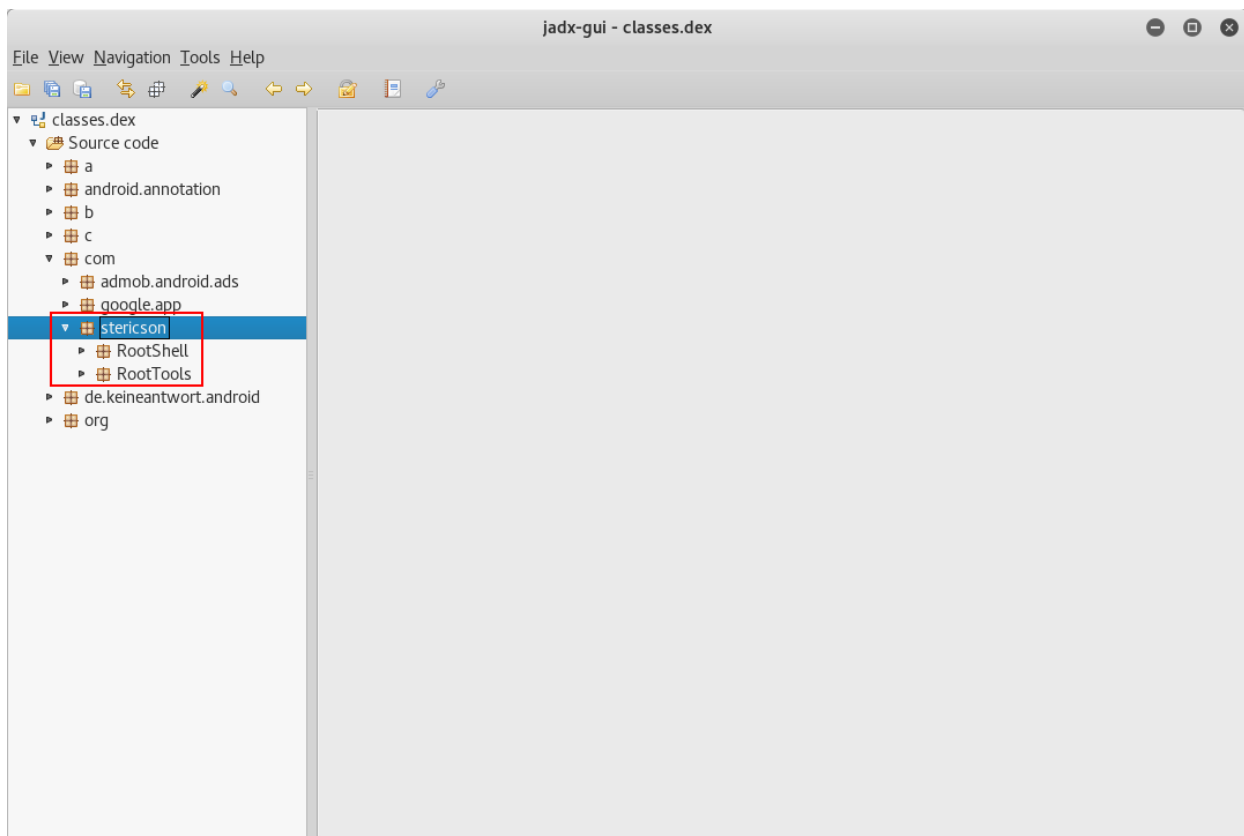
The picture below showing that the malware is capable of taking pictures from the camera of the compromised device and upload it to the C2.

The malware begins by implementing a Trust Manager that **accepts all certificates** so that Libyan Scorpions hackers are sure no victim left disconnected due to SSL certificates issues.

The malware is able to turn the Android phone into a remote listening bug by opening the Microphone and recording the audio then send it to the C2.

The malware is able to browse the files and folders stored inside the Android device.

The malware is able to monitor the physical location of the compromised Android device.

The malware is able to get the call logs along with phone numbers, duration and date and time of each call.

The malware is able to read the SMS messages and the list of contacts saved in the device.

Besides, the malware is able to get the phone number, country and network operator name from cellular towers of the telecom company of the target.

The malware uses Allatori Java Obfuscator to protect the code and make it harder to reverse engineer and it obviously uses communication protocol based on Java JSON objects encapsulated in SSL connection wrapper. Again, this behavior and characteristics of the malware is very similar to JSocket and AlienSpy Android RATs.

After finalizing the analysis of the Android malware, Cyberkov uploaded it to VirusTotal to see if it has been uploaded before and what information we can get from it:

Cyberkov discovered that the malware has not been uploaded to VirusTotal before and the first sample of this malware has been uploaded by us. However, 8 out of 54 AntiVirus engines detect it which is a very low detection rate (15%). Most and major American top Gartner Antivirus companies did not detect it!!

Command and Control Communication

Cyberkov tried to discover the attacker behind this malicious application by sinkholing the malware and analyzing the real C2.

Sinkhole

Cyberkov created a fake server simulating the real C2 of the Libyan Scorpions hacking group and sinkholed the malware to study the behavior of the malware deeply.

Upon connection to the C2, the malware sends a lot of information about the target including: Country, Malware Path, Local IP Address, RAM, Android Version, Device Name, …, etc.

The fake C2 server is able to send fake commands to the malware and read the reply as well.

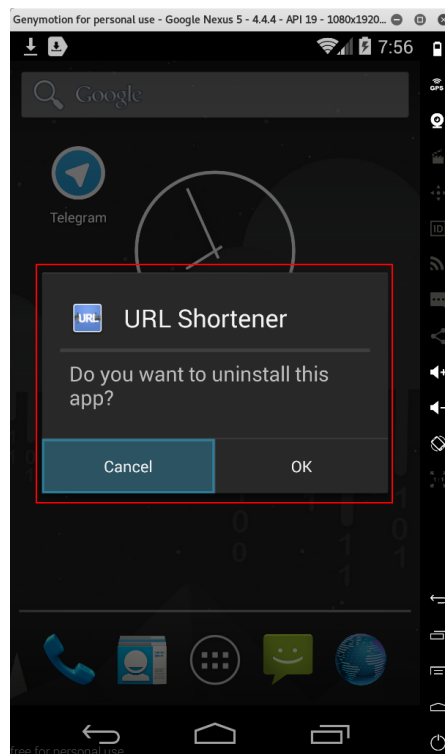Those commands (103, 104 and 105) correspond to the following list of commands defined in the malware:

Each number corresponds to one command to be done by the malware. For example, the command (111) uninstalls the real application "URLShortener":
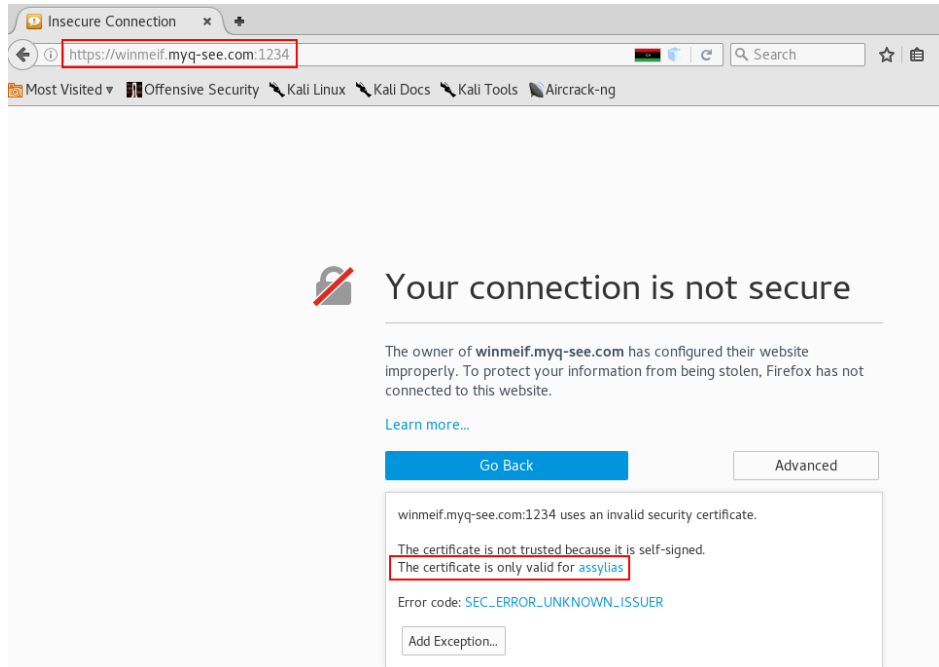

Will result in:

Real C2

By connecting to the real C2 IP address, Cyberkov found that the malware is really of JSocket/AlienSpy family of RATs since that family of RATs open the port 1234 with a self-signed certificate of "assylias"[2].

According to Shodan, the port (1234) has been spotted open since 12-07-2016 which is 25 days before the first discovery.

---

[2]

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

Threat Actor and Attribution

Seems like the Libyan Scorpions threat actors are running multiple Android RATs since numerous ports protected by SSL layer are open in (**winmeif.myq-see.com**) machine.

Also, the Libyan Scorpions threat actors left **phpinfo.php** script on the webserver running on port 80 with useful information that could expose them. Their machine is running Windows 7 Professional Service Pack 1.

Username of the Windows machine is **admin**.

The computer name of Windows machine is **ADMIN**.

The Libyan Scorpions threat actors use a **Dell laptop** and have Skype installed and are setting behind a NAT and their internal IP address is **192.168.1.16**

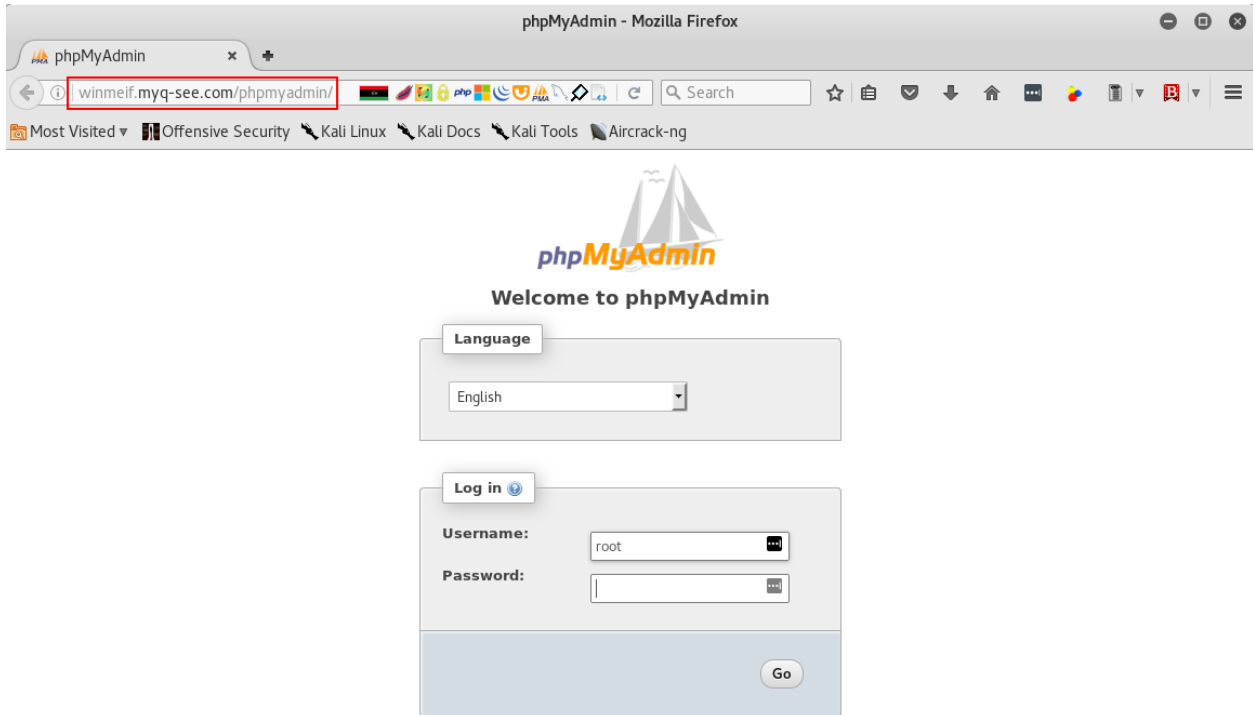The attackers also have a PhpMyAdmin script installed in their machine:

Cyberkov Security Incident Response Team (CSIRT) tried to brute force the password of the database using the top most common 100 passwords. Unfortunately, the attempt failed.
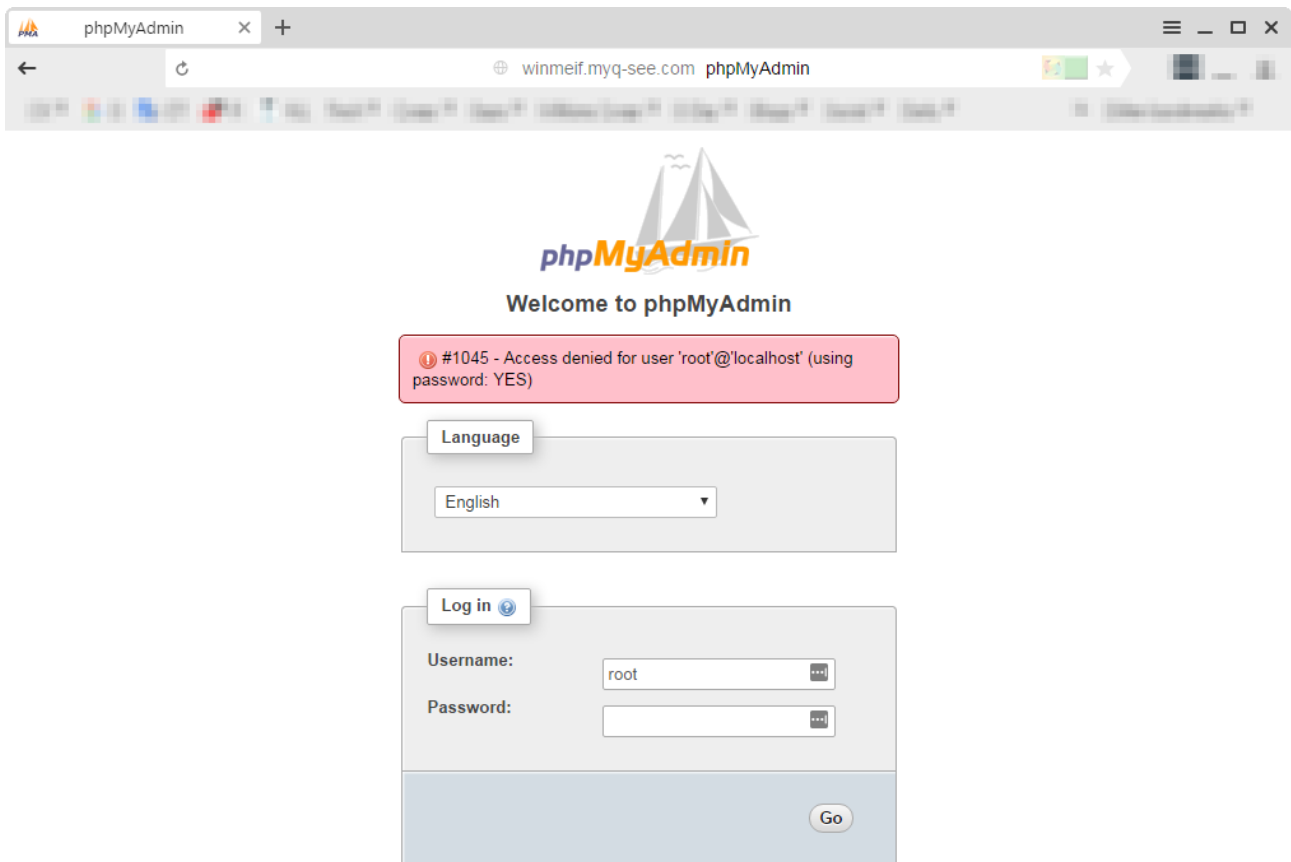
Threat Actors Infrastructure

Going back to the IP address of the attackers (41.208.110.46), it is very important to discover the attackers infrastructure that maybe used to launch wider attacks using multiple RATs on multiple platforms.

By using Threat Intelligence Platforms and Feeds such as PassiveTotal, Cyberkov was able to discover more activities and campaigns run by Libyan Scorpions.

The following Heatmap shows that the IP address (41.208.110.46) has been used to launch attacks since 9/9/2015 until the time of writing this report using 5 different hostnames and multiple malicious malwares.
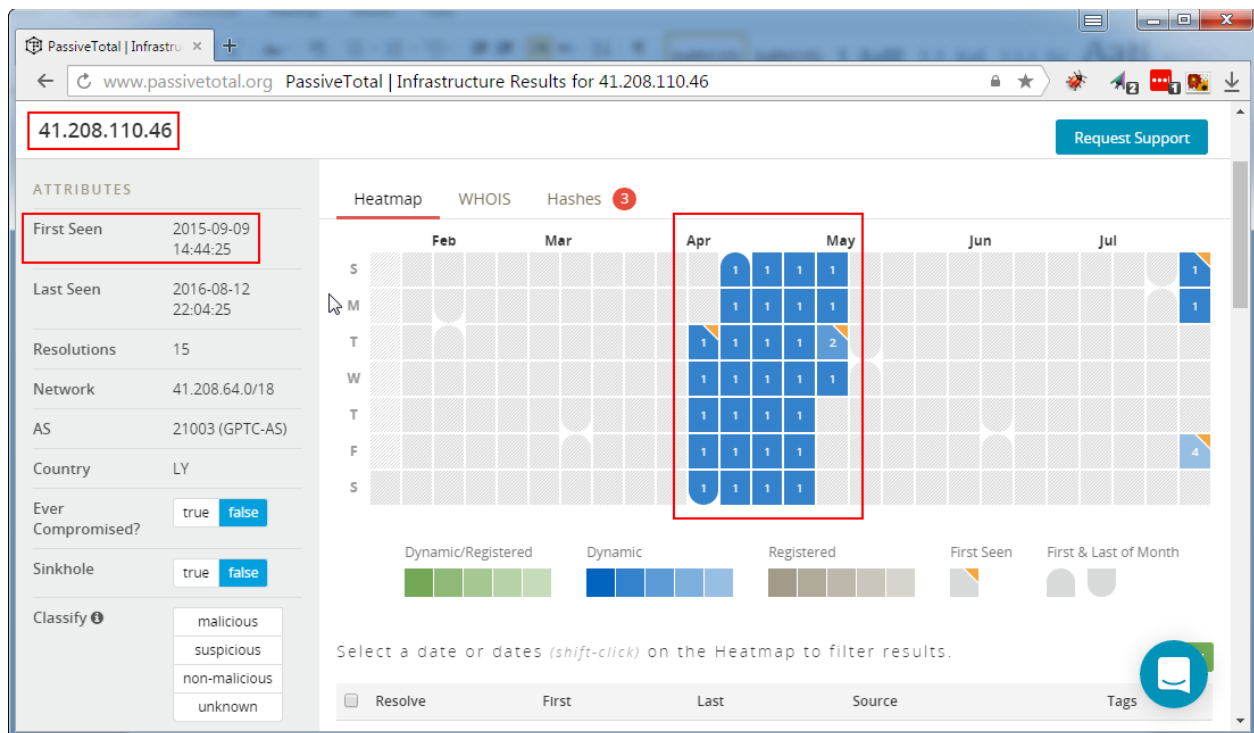
The following table summarizes the list of hostnames used by the attacker(s):

Hostname	First Seen	Last Seen
Samsung.ddns.me	26-04-2016	08-09-2016
Wininit.myq-see.com	24-05-2016	22-08-2016
Winmeif.myq-see.com	07-08-2016	22-08-2016
Collge.myq-see.com	09-09-2015	22-08-2016
Sara2011.no-ip.biz	08-10-2015	08-10-2015

All of the hostnames point to the same C2 IP address used by the attackers (but sara2011.no-ip.biz):

Also, using PassiveTotal, the C2 is connected to 2 more malwares used by the attackers having the following hashes (MD5):

- 1738ecf69b8303934bb10170bcef8926
- 93ebc337c5fe4794d33df155986a284d

The first hash in the above picture is for the malware "Voice Massege.apk" which we have analyzed already.

The second hash (1738ecf69b8303934bb10170bcef8926) is named **(Benghazi.exe)** and have detection rate of 21 out of 56 (37.5%) and has been uploaded first time to VirusTotal on 23-04-2016.

Notice that this malware targets Windows machines and not Android smartphones. It is compiled on 15-04-2016 and is coded in Visual Basic.

The third hash **(93ebc337c5fe4794d33df155986a284d)** is a DroidJack, a malicious attacking platform, targeting android smartphones.

Also, the name of activities and services contains **net.droidjack.server** name which makes us sure it is **DroidJack** malware.

To Be Continued…

Cyberkov will continue investigating Libyan Scorpions hacking group operating in Libya and will update this report with a follow-up reports regarding any future cyber activities.

Mitigating Libyan Scorpions Attacks on Android

Cyberkov recommends the following points in order to protect the victims from such malwares:

- Update your Android operating system regularly
- Install DrWeb Security Space for Android (A leading Russian AntiVirus Company)
- Use of DrWeb Telegram Bot (DrWebBot) to scan links and files shared on Telegram chats or groups
- Install Zemana Mobile AntiVirus (A leading Turkish AntiMalware and AntiFraud Company)
- Never install applications from unknown sources
- Use Telegram with Secret Chat feature only
- Always verify with your partners when sending and receiving files

Indicators of Compromise (IOCs)

The following table summarizes the list of indicators to detect the malware:

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