Hunting Libyan Scorpions

CYBERKOV
Hunting Libyan Scorpions
Investigating a Libyan Cyber Espionage Campaign Targeting High-Profile Influentials

Overview

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.

To read the full investigation, please download the report below (In Arabic or English). We also have compiled the list of indicators of compromise (IoCs) to help security community mitigating this threat.

"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."

DOWNLOAD ENGLISH REPORT

DOWNLOAD "ARABIC" REPORT

DOWNLOAD INDICATORS LIST