Libyan Scorpions - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:18:09 UTC

APT group: Libyan Scorpions

Names	Libyan Scorpions *(Cyberkov)*
Country	Libya
Motivation	Information theft and espionage
First seen	2015
Description	(Cyberkov) 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 webTelegram using IP address from Spain. 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.
Observed	Sectors: Influencers and political figures. Countries: Libya.
Tools used	Voice Massege.apk, Benghazi.exe.

Information	<https://cyberkov.com/wp-content/uploads/2016/09/Hunting-Libyan-Scorpions-EN.pdf>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
