LIBYAN SCORPIONS

AXIAL

LIBYAN SCORPIONS

LIBYA

INFLUENCERS AND POLITICAL FIGURES

VOICE MASSEGE.APK, BENGHAZI.EXE

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON LIBYAN SCORPIONS ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Libyan Scorpions is a threat group based out of Libya focusing on information theft and espionage.

II. TARGETS

The target/s of this threat group mainly focuses on influencers and political figures.
.

III. METHODS USED

The methods used by this group used are various malicious applications and social media accounts compromise, these threat actors also use various methods to hide and operate their malwares.

IV. CAMPAIGNS

This threat group has been linked to campaigns related to delivering numerous Android malware operating in different parts of Libya especially in Tripoli and Benghazi, also they have been linked to compromise of social media accounts of influencers.

ATTRIBUTION

This threat group is attributed to be based out of Libya as thry are believed to be a political motivated group targeting a high-level influential and political figures in multiple cities within Libya.

[Cited from CYBERKOV]

V. IOCS

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

Cited from Cyberkov

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Libyan%20Scorpions