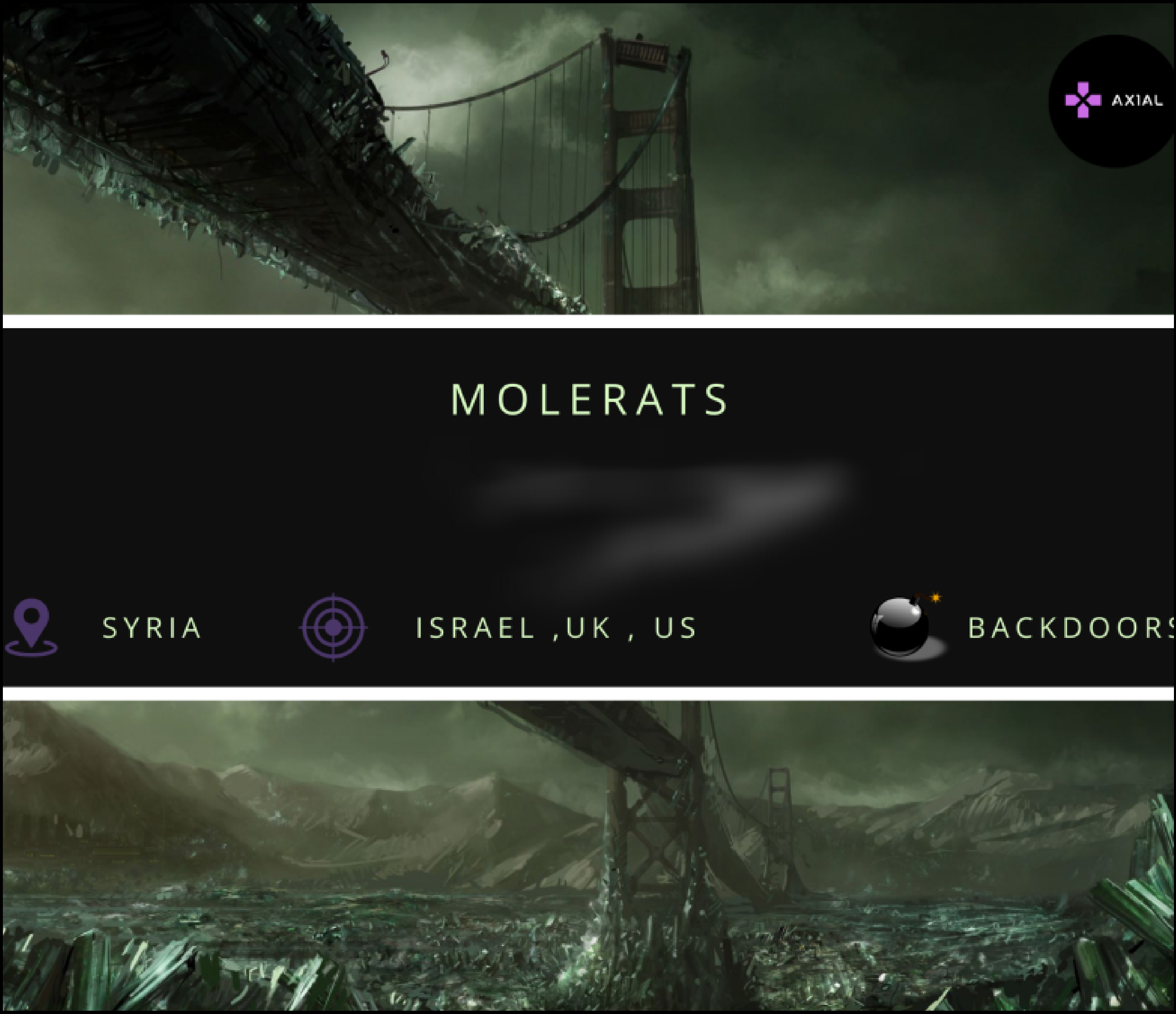
MOLERATS



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON MOLERATS: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Molerats is a threatb group which also goes by the name extreme Jackal ,ATK 89 based out of Syria ,sponsored by Hamas
.

II. TARGETS

Molerats focuses on aerospace , defense , embassies , Energy, Financial, Government, High-Tech, Media, Oil and gas, Telecommunications and journalists and software developers onto multiple countries .

III. METHODS USED

Molerats has been using various tools like BadPatch , Downeks , Dustysky ,

Molerats have also been found using XtremeRat samples
Moleats have also been found using Poison Ivy Samples with Middle Eastern Themes.

Molearts have been using spear phising to deliver weaponized RAR files containing their malicious payloads to their victims in at least two different ways. The Molerats actor will in somecases attach the weaponized RAR file directly to their spear- phishing-emails. We also believe that this actor sends spear-phishing emails that include links to RAR files hosted on third-party platforms such as Dropbox.

IV. CAMPAIGNS

- Molerats have been involved in defacing Isreal fire service based website.
- Molerats have been identified as identified malware attacks against Israeli government targets.

- Molearts have been found involved in operation Moonlight which uncovered the activities of a group of individuals currently engaged in targeted attacks against entities in the Middle East.
- FireEye Labs identified several new Molerats attacks targeting at least one major U.S. financial institution and multiple, European government organizations.
- Molerats have been also linked to operation Pierogi , Sneakypass .

ATTRIBUTION

Molerats have been attributed to Syria , also according to operation DustSky Pt.2 attacks against all targets in the Middle East stopped at once, after we published our first report. However, the attacks against targets in the Middle East (except Israel)were renewed in less than 20 days. In the beginning of April 2016, we found evidence that the attacks against Israel have been renewed as well. Based on the type of targets, on Gaza being the source of the attacks, and on the type of information the attackers are after -we estimate with medium-high certainty that the Hamas terrorist organization is behind these attacks.

[cited from ClearSky reports]

AXIAL

V. IOCS

MD5 Hashes

d9a7c4a100cfefef995785f707be895c
9dff139bbbe476770294fb86f4e156ac
16346b95e6deef9da7fe796c31b9dec4
fc554a0ad7cf9d4f47ec4f297dbde375
b0a9abc76a2b4335074a13939c59bfc9
fc554a0ad7cf9d4f47ec4f297dbde375

C2's

hxxps://dl[.]dropboxusercontent[.]com/s/uiod7orcpykx2g8/Ramadan.rar?token_hash=AAHAVuiXpTkOKwar9e0WH-EfrK7PEB9O7t7WC6Tgtn315w&dl=1
toornt.servegame.com
updateo.servegame.com
egypttv.sytes.net
skype.servemp3.com
natco2.no-ip.net
209.200.39.88
209.200.39.48

VI. REFRENCES

https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Molerats%2C%20Extreme%20Jackal%2C%20Gaza%20Cybergang

https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

https://attack.mitre.org/groups/G0021/