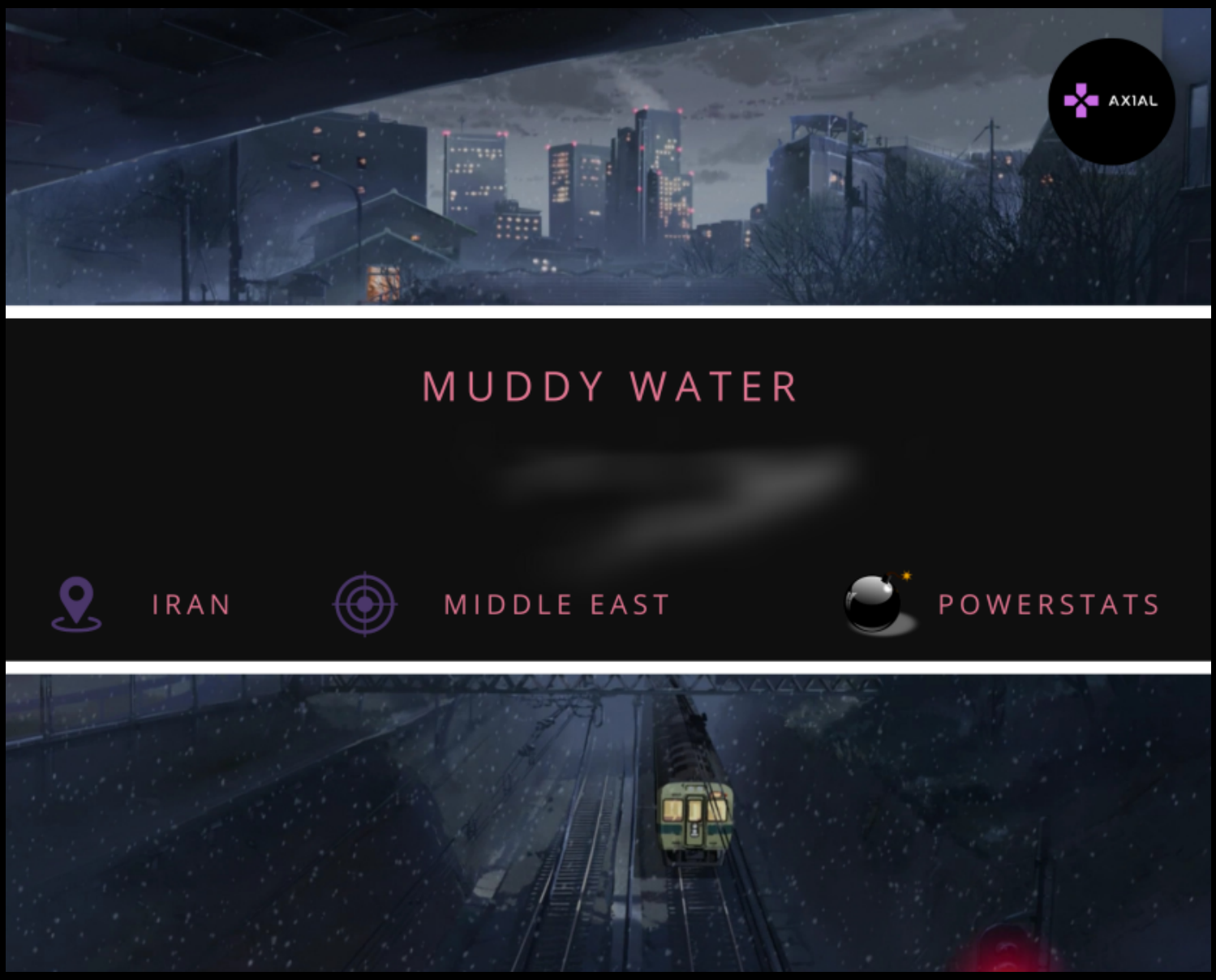
MUDDY WATER



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

MuddyWater is a group based out of Iraq and is a state sponsored threat group targetting victims in Middle East .

II. TARGETS

Governments, Telcos and Oil Companies.

III. METHODS USED

MuddyWater has been seen using the infection vector for all of the attacks involved in this campaign are macro-based documents sent as an email attachment.

MuddyWater has also been seen using spearphishing as their targets .

Muddywater has also been seen using Indirect Code Execution through INF and SCT .

IV. CAMPAIGNS

- The MuddyWater attacks are primarily against Middle Eastern nations., however, we have also observed attacks against surrounding nations and beyond, including targets in India and the USA.
- This actor has engaged in prolific spear phishing of government and defense entities in Central and Southwest Asia.
- This threat group has also been noticed a large amount of spear phishing documents that appear to be targeting government bodies, military entities, telcos and educational institutions in Jordan, Turkey, Azerbaijan and Pakistan, in addition to the continuous targeting of Iraq and Saudi Arabia, other victims were also detected in Mali, Austria, Russia, Iran and Bahrain..

ATTRIBUTION

The operators behind MuddyWater are likely espionage motivated, this information has been derive this information from the analysis of data and backdoors and their behaviors. We also find that despite the strong preponderance of victims from Pakistan, the most active targets appear to be Saudi Arabia, UAE and Iraq and the originating country is likely to be Iran.

[cited from ThaiCERT reports]

AX1AL

V. IOCS

SHA256 Hashes

eff78c23790ee834f773569b52cddb01d3c4dd9660f5a476af044ef6fe73894
76e9988dad0278998861717c774227bf94112db548946ef617bfaa262cb5e38
6edc067fc2301d7a972a654b3a07398d9c8cbe7bb38d1165b80b05e5ac
3da24cd3af9a383b731ce178b03c68a813ab30f4c7c8dfbc823a328106fb
9038ba1b7991ff38b802f28c0e006d12d466a8e374d2f2a83a039aabcbe76f5c
aa60c1fae6a0ef3b9863f710e46f0a7407cf0feffa240b9a4661a4e8884ac627
5550615affe077ddf66954edf132824e4f1fe16b3228e087942b0cad0721a6af

C2's&Proxy URLs

hxxp://alessandrofoglino[.]com//db_template.php
hxxp://www.easy-home-sales[.]co.za//db_template.php
hxxp://www.almaarefut[.]com/admin/db_template.php
hxxp://chinamall[.]co.za//db_template.php
hxxp://amesoulcoaching[.]com//db_template.php
hxxp://www.antigonisworld[.]com/wp-includes/db_template.php
hxxps://anbinni.ba/wp-admin/db_template.php
hxxp://arctistrade[.]de/wp/db_template.php
hxxp://aianalytics[.]ie//db_template.php
hxxp://www.gilforsenate[.]com//db_template.php
hxxp://mgamule[.]co.za/oldweb/db_template.php
hxxp://chrisdejager-attorneys[.]co.za//db_template.php
hxxp://alfredocifuentes[.]com//db_template.php
hxxp://alxcorp[.]com//db_template.php
hxxps://www.aircafe24[.]com//db_template.php
hxxp://agencereferencement.be/wp-admin/db_template.php
hxxp://americanlegacies[.]org/webthed_ftw/db_template.php
hxxps://aloefly[.]net//db_template.php
hxxp://www.duotonedigital[.]co.za//db_template.php
hxxp://architectsinc[.]net//db_template.php

VI. REFRENCES

https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=MuddyWater%2C%20Seedworm%2C%20TEMP%2EZagros%2C%20Static%20Kitteng