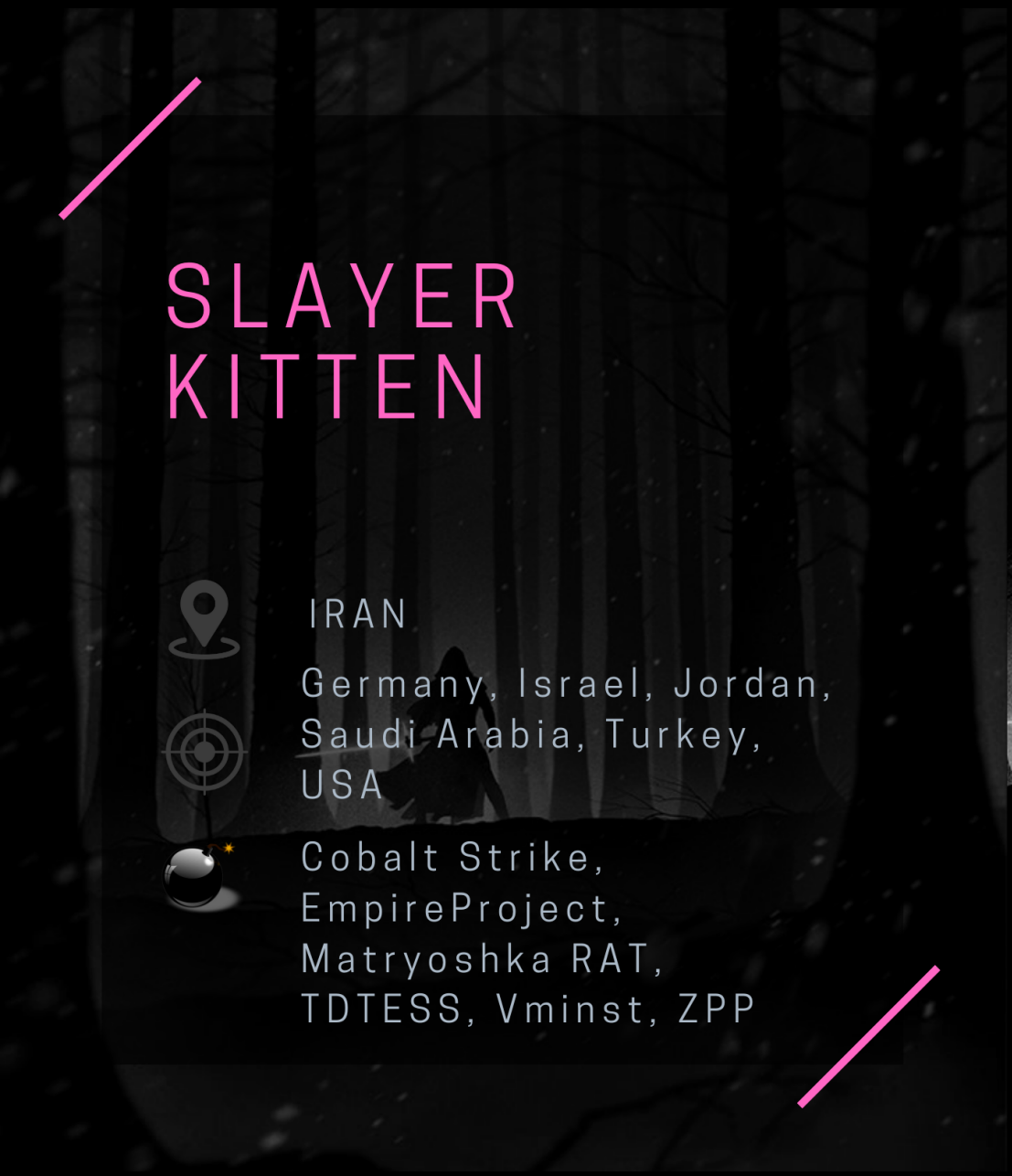
SLAYER KITTEN



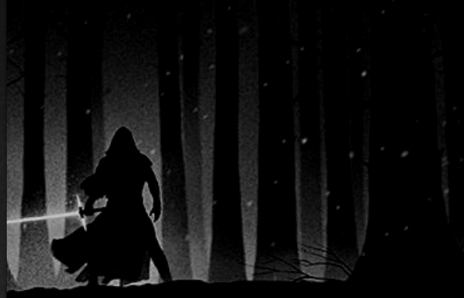
AXIAL

SLAYER KITTEN

IRAN

Germany, Israel, Jordan, Saudi Arabia, Turkey, USA

Cobalt Strike, EmpireProject, Matryoshka RAT, TDTESS, Vminst, ZPP



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SLAYER KITTEN ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Slayer Kitten is a threat group based out of Iran which focuses on Information theft and espionage.

II. TARGETS

The target/s of this threat group mainly focuses on Defense, Education, Government, IT, Media on multiple countries like Germany, Israel and many others.
.

III. METHODS USED

The methods used by this groups are exploiting CVE-2017-0199, embedding OLE objects and macros, also fake social media entities impersonating known entities.They also used multiple tools like Havij, sqlmap and Acunetix. Backdoors like TDTESS and Matreyoshka were also used by this threat group.

IV. CAMPAIGNS

This threat group has been linked to Operation Wilted Tulip .
This threat group has also been linked to breach of the Israeli newspaper Jerusalem Post.
This threat group has also been linked to a three-wave of cyberattacks in 2015.

The methods used by this groups are exploiting CVE-2017-0199, embedding OLE objects and macros.

ATTRIBUTION

This threat group is attributed to be based out of Iran and has been targeting Israeli newspapers.

[Cited from Clearsky]

V. IOCS

IPv4Address206.221.181.253
IPv4Address66.55.152.164
IPv4Address68.232.180.122
IPv4Address173.244.173.11I
IPv4Address173.244.173.12
IPv4Address173.244.173.13I
Pv4Address209.190.20.149
IPv4Address209.190.20.59
IPv4Address209.190.20.62
IPv4Address209.51.199.116
IPv4Address38.130.75.20
IPv4Address185.92.73.194
IPv4Address144.168.45.126
IPv4Address198.55.107.164
IPv4Address104.200.128.126
IPv4Address104.200.128.161
IPv4Address104.200.128.173
IPv4Address104.200.128.183
IPv4Address104.200.128.184
IPv4Address104.200.128.185I
Pv4Address104.200.128.187
IPv4Address104.200.128.195
IPv4Address104.200.128.196

VI. REFRENCES

https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=CopyKittens%2C%20Slayer%20Kitten