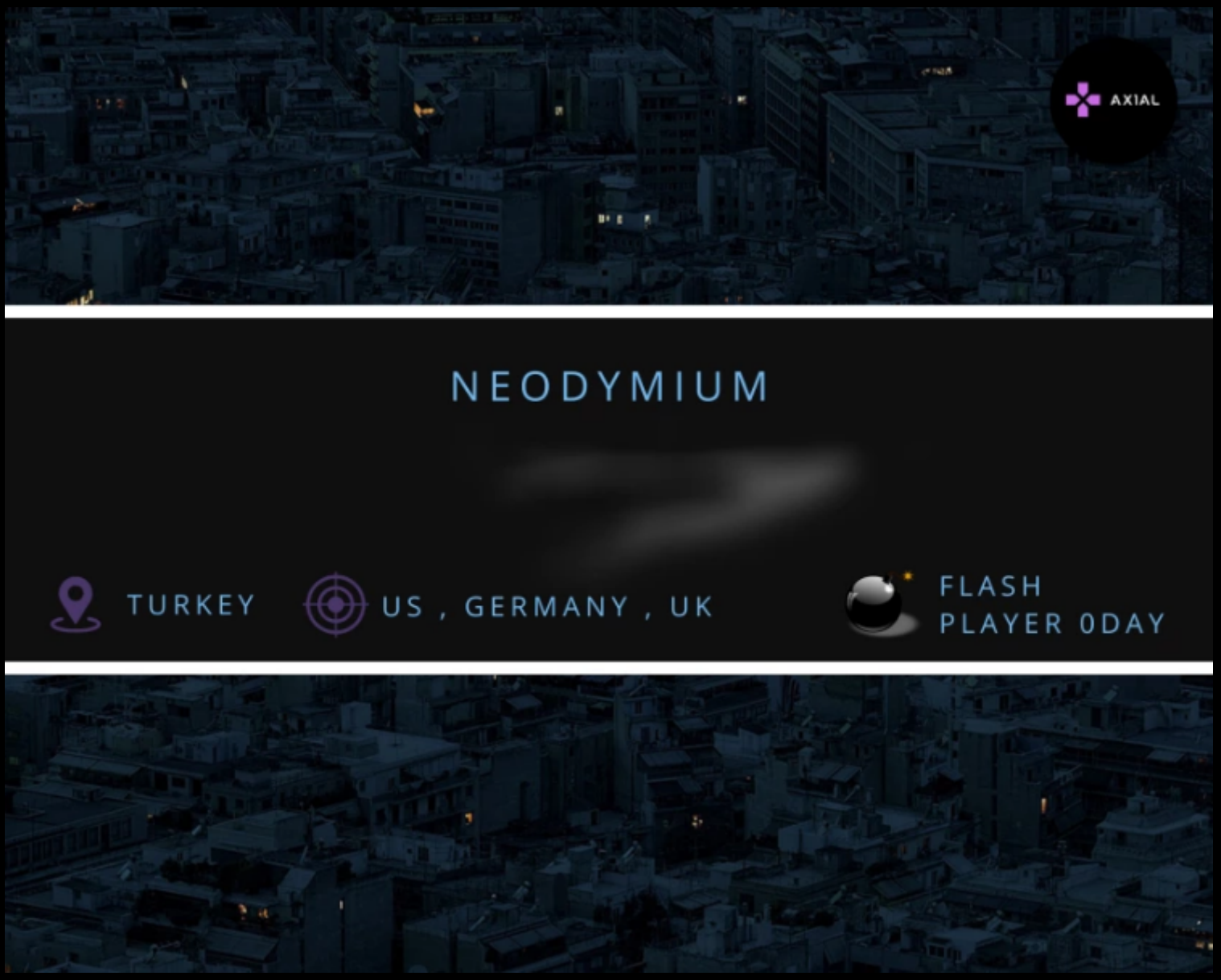
NEODYMIUM



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Neodymium is a threat group based out of turkey which focuses on Information theft and espionage .

II. TARGETS

Neodymium focuses on information theft and espionage , also has heavily targeted Turkish Victims and multiple countries like Australia , and various parts of Europe.

III. METHODS USED

Neodymium has used exploit for CVE-2016-4117 , a vulnerability in Adobe Flash Player . NEODYMIUM used well-tailored spear-phishing emails with attachments that delivered the exploit code, ultimately leading to Wingbird's installation on victim computers.
Neodymium uses the W32/Wingbird.A!dha backdoor to spy on users.

IV. CAMPAIGNS

- Neodymium has been associated with twin zero day attacks which have targeted individuals in Europe .

ATTRIBUTION

Neodymium is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called Promethium, StrongPity due to overlapping victim and campaign characteristics. Neodymium is reportedly associated closely with BlackOasis operations
[cited from Malpedia]

AX1AL

V. IOCS

Hashes

To be added

C2's

To be added

h

VI. REFRENCES

https://www.itnews.com.au/news/finfisher-like-government-spyware-found-in-apt-attacks-444726

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Neodymium

AXIAL