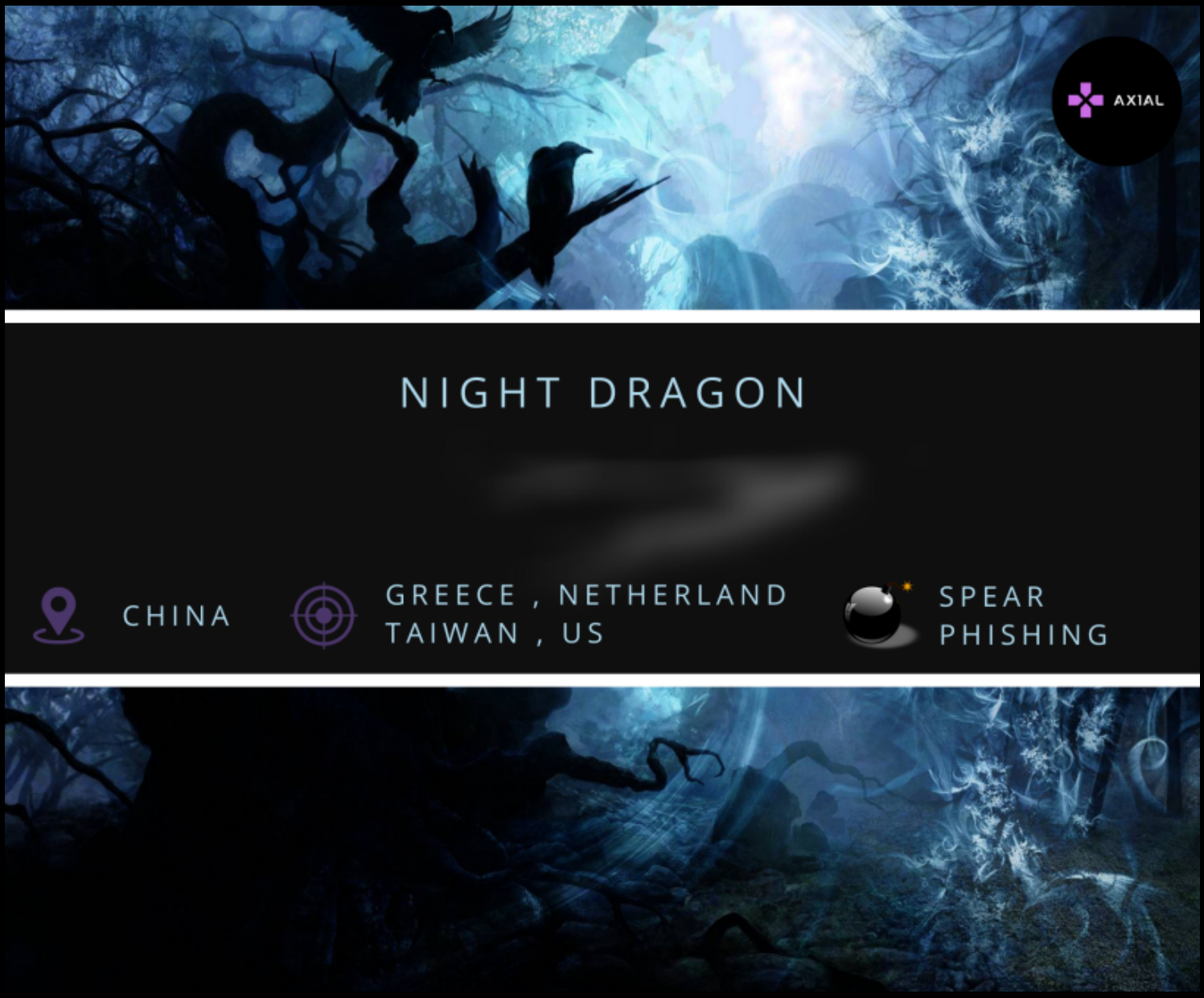
NIGHT DRAGON



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON NIGHT DRAGON ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Night Dragon is a threat group based out of China which focuses on information theft and espionage .

II. TARGETS

Energy , Petrochemical & global oil .

III. METHODS USED

Night Dragon has been using tools like ASPSXSpy , zwShell & Cain & Abel .

The Night Dragon attacks work by methodical and progressive intrusions into the targeted infrastructure.
The Night Dragon has also been using RAT Malware which they have been using to connect to other machines and further exfiltrating archives and other sensitive documents.

IV. CAMPAIGNS

- Night Dragon has been involved in cyberattacks that started in mid-2006
- Night Dragon has been involve din Operation Aurora
- Night Dragon has bene involved in attacks related to Energy Companies .

ATTRIBUTION

Attackers using several locations in China have leveraged C&C servers on purchased hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the United States to acquire proprietary and highly confidential information.
Night Dragon may also be related to other threat actors like APT 18 .
[cited from Malpedia]

AX1AL

V. IOCS

Hashes

A6CBA73405C77FEDEAF4722AD7D35D60
6E31CCA77255F9CDE228A2DB9E2A3855
093640a69c8eafbc60343bf9cd1d3ad3
18801e3e7083bc2928a275e212a5590e
85df6b3e2c1a4c6ce20fc8080e0b53e9

C2's

is-a-chef.com
thruhere.net
office-on-the.net
selfip.com

VI. REFRENCES

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

McAfee Reports

https://us-cert.cisa.gov/ics/advisories/ICSA-11-041-01A