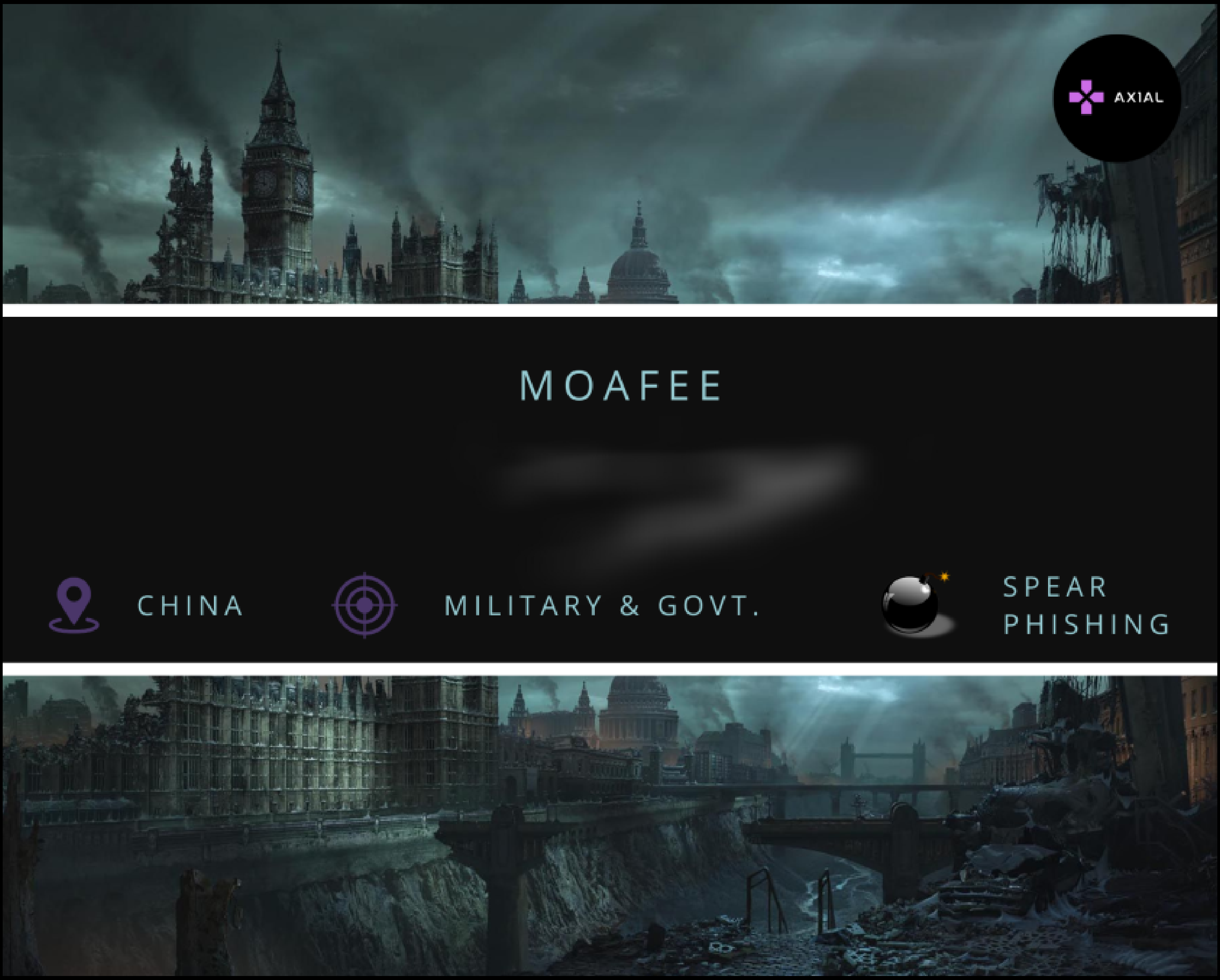
MOAFEE



AXIAL

MOAFEE

CHINA

MILITARY & GOVT.

SPEAR PHISHING

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

It is a state sponsored threat group based out of China also goes by the name BRONZE OVERBROOK which have been targeting Japanese Organization with phishing mails.

II. TARGETS

MMilitary and government artifacts based on those who have national interests in the South China Sea

III. METHODS USED

- MOAFEE has been using variety of malware including Sysget , PlugX and PosonIvy , FormerFirstRat.
- MOAFEE has been using HTran
- MOAFEE has been known to employ binary padding
- MOAFEE has also been spear phishing it's targets .

.

IV. ATTRIBUTIONS

A group of cyber actors utilizing various tools like PlugX malware and this group seems to operate from the Guandong Province of China also due to overlapping TTPs with the threat group DragonOK also this group targets military organizations of countries whose national interests are in with the South China Sea .

This group has been noticed targeting organizations within the US defense industrial base.

[Cited from Malpedia]

VII. IOCS

Mspoiscon.exe:
79ad835d5068c9967f383f9450502bfb[MD5]
IVYVARIENT[POISONRAT]
E7931270A89035125E6E6655C04FEE00798C4C2D1584694
7E41DF6BBA36C75AE[SHA-256]

URLs:
happyy.7766.org
hxxp://203.248.116.182/images/Thumbs.bmp

V. REFERENCES

1. www.fireeye.com
2. www.attack.mitre.org
3. www.securelist.com
4. Malpedia
5. THAICERT
6. Fortinet
7. Wikileaks