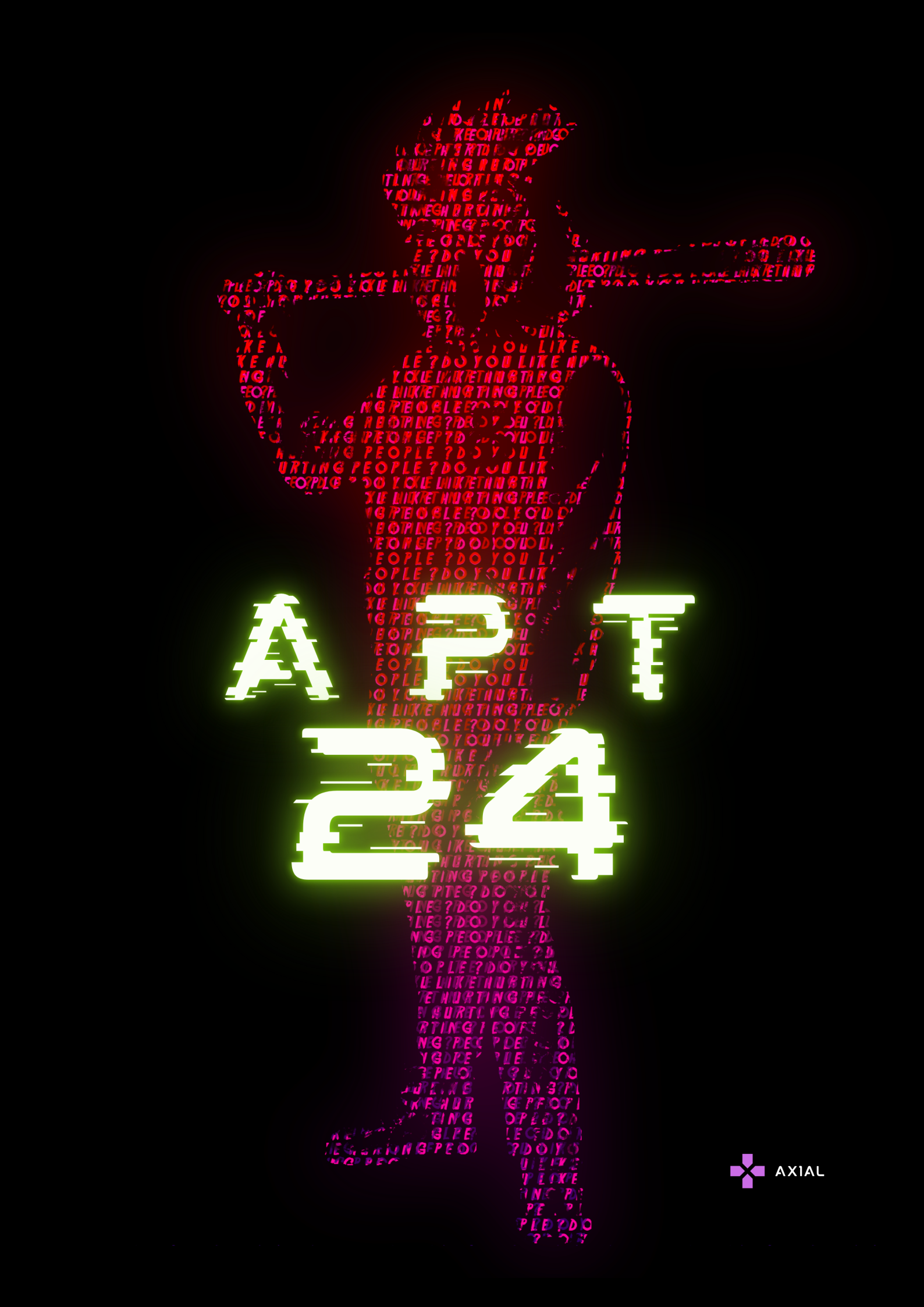
APT
24
AXIAL

A SURVEY ON APT24: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

PittyTiger also known as Manganese or Pitty Panda is an Threat Actor of Chinese Origin and has been active since 2011 though some research states that they have been active for far longer. They commonly engage in Information theft and espionage and target European Organizations as well as Taiwan. Pitty Tiger prefer to use custom malware, developed for the group's exclusive usage. Pitty Tiger group is fairly small compared to other APT groups, hence their Operations are limited.

II. TARGET SECTORS

Pitty Tiger tends to target Defence, Government, Telecom and Web Development.

III. METHODS USED

Pitty Tiger mostly uses spear-phishing in order to get an Initial foothold. They exploit known vulnerabilities in Microsoft Office products(mostly CVE-2012-0158 and CVE-2014-1761) to infect the targets with malware. They also have been seen using HeartBleed vulnerability.

IV. ENGAGEMENTS

- In 2011, Operation PittyTiger was revealed by Airbus Defence and Space, when they investigated particular malware samples affiliated with the group.
- In 2014, A French company was the target of PittyTiger. The attackers sent simple, straightforward messages in English and French from free email addresses using names of actual employees of the targeted company.

V. ATTRIBUTIONS

- Several Chinese tools have been used and found on the C2 servers of the attackers: 8uFTP, a Chinese version of calc.exe, etc.
- Two of the used RATs have been developed by the same developers: CT RAT and PittyTiger RAT. The controllers for these RATs show Chinese language.
- Several binaries used by the attackers show either “Chinese - China” or “Chinese-Taiwan” language ID in their resources

AX1AL

VI. IOC

C&C

1. acers.com[.]tw
2. kimoo.com[.]tw
3. paccfic[.]com
4. foxcom[.]com[.]tw
5. dopodo[.]com[.]tw
6. trendmicroup[.]com
7. lightening[.]com[.]tw
8. avstore[.]com[.]tw
9. helosaf[.]com[.]tw
10. trendmicro[.]org[.]tw
11. stareastnet[.]com[.]tw
12. symantecs[.]com[.]tw
13. seed01[.]com[.]tw
14. skypetm[.]com[.]tw

MD5

PittyTiger RAT

- a1ea6dc12b983c7262fe76c1b3663b24
- d5da60d678d5a55a847e1e6723c7a4d0
- 55e456339936a56c73a7883ea1ddb672
- abb0abfab252e45bfb9106273df3c1c2

Troj/ReRol.A

- 4ab74387f7a02c115deea2110f961fd3
- b6380439ff9ed0c6d45759da0f3b05b8
- ce15fa3338b7fe780e85c511d5e49a98
- 5e2360a8c4a0cce1ae22919d8bff49fd

Paladin RAT (Variant of Gh0st RAT)

- 33714886dad497d6f0ecc255f0399004
- 3b498f19d467d2b8d4c778a92cacae9a
- f71b374d341dc55b9b825531ba843f6d

MM RAT (Troj/Goldsun-B)

- 81fa811f56247c236566d430ae4798eb

LeoRAT

- 3654496539faedfe137a1f989359aef0

VII. LINKS TO OTHER THREAT GROUPS

- Researchers have found that there is some overlap with APT 5, Keyhole Panda.

VIII. REFERENCES

- https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.07.11.Pitty_Tiger/Pitty_Tiger_Final_Report.pdf
- https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html