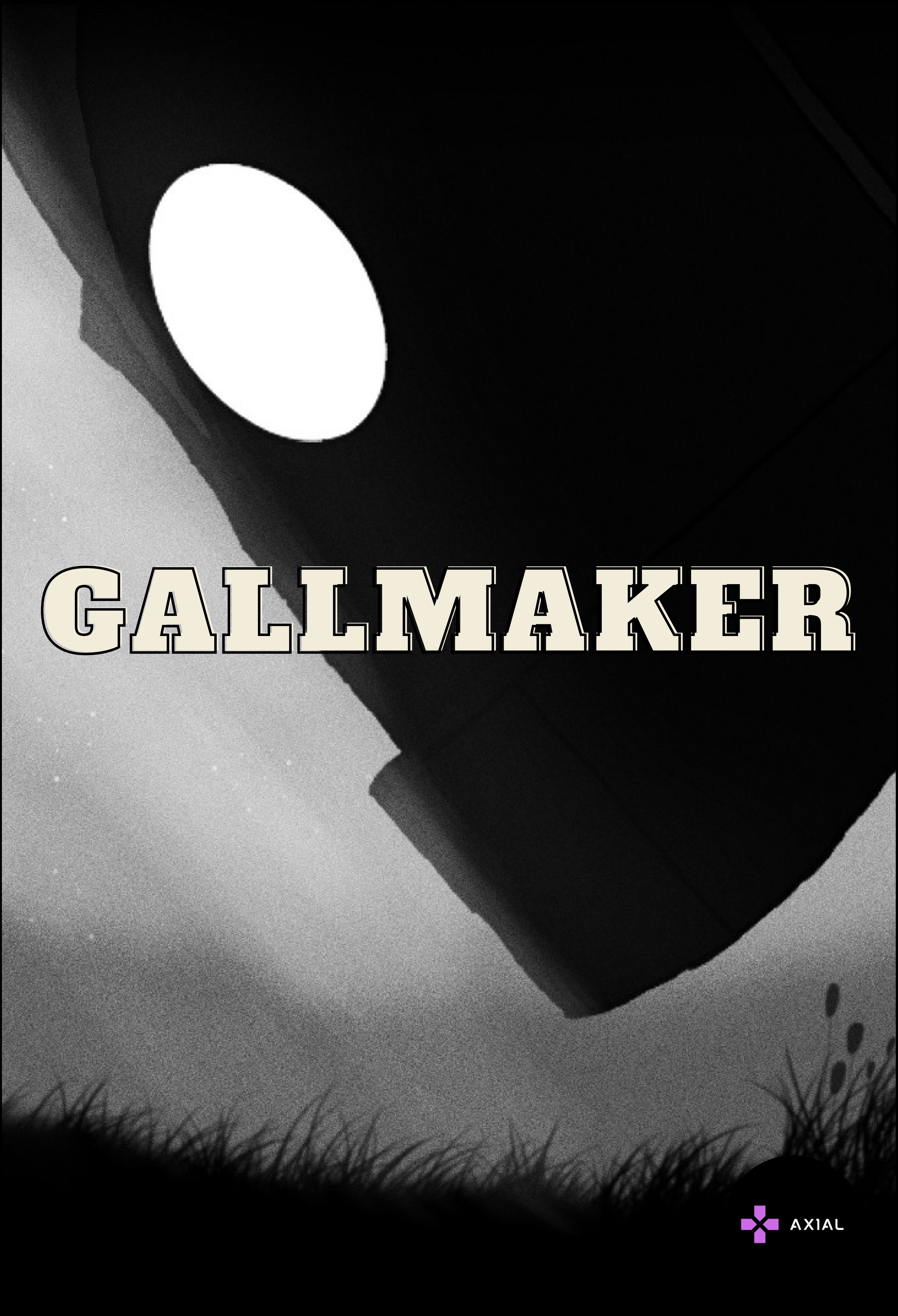

GALLMAKER

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

Gallmaker is a cyberespionage group that has targeted victims in the Middle East and has been active since at least December 2017. The group has mainly targeted victims in the defense, military, and government sectors.

II. TARGET SECTORS

Defense, Embassies, Government.

III. METHODS USED

The group delivers a malicious Office lure document to victims, most likely via a spear-phishing email.

IV. ENGAGEMENTS

- The group has carried out attacks most months since December 2017.
- Its activity subsequently increased in the second quarter of 2018, with a particular spike in April 2018.

V. COMMON ATTRIBUTIONS

- They use lure documents titles with government, military, and diplomatic themes, and the file names are written in English or Cyrillic languages. These documents are not very sophisticated, but evidence of infections shows that they're effective. The attackers use filenames that would be of interest to a variety of targets in Eastern Europe,
- These lure documents attempt to exploit the Microsoft Office Dynamic Data Exchange (DDE) protocol in order to gain access to victim machines. When the victim opens the lure document, a warning appears asking victims to “enable content”. Should a user enable this content, the attackers are then able to use the DDE protocol to remotely execute commands in memory on the victim's system. By running solely in memory, the attackers avoid leaving artifacts on disk, which makes their activities difficult to detect.

V. IOC

Network

1. **111[.]90.149.99/o2**
2. **94[.]140.116.124/o2**
3. **94[.]140.116.231/o2**

Filenames

1. **bg embassy list.docx**
2. **Navy.ro members list.docx**
3. **БГ в чуждите медии 23.03.2018-1.docx**
4. **A-9237-18-brasil.docx**

VI. REFERENCES

- https://attack.mitre.org/groups/G0084/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/gallmaker-attack-group
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Gallmaker&n=1