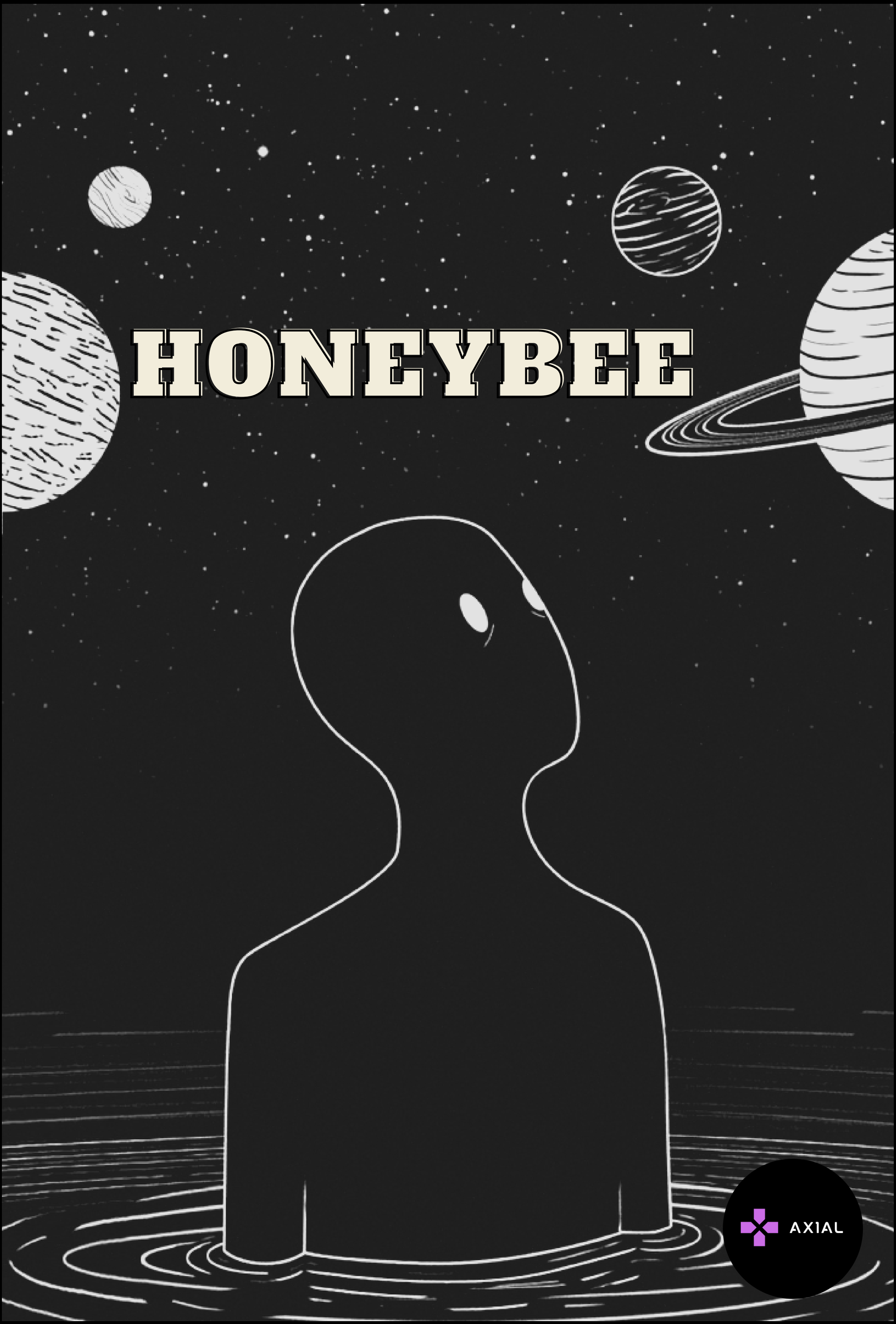
HONEYBEE



AXIAL

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

-NERDS OF AX1AL

I. ABOUT

The honeybee is a campaign led by an unknown actor that targets organizations involved in humanitarian aid and inter-Korean affairs and has been active in Vietnam, Singapore, Argentina, Japan, Indonesia, and Canada. It has been an active operation since August of 2017 to February 2018.

II. TARGET SECTORS

Organizations involved in humanitarian aid and inter-Korean affairs.

III. METHODS USED

Generally, they use malicious documents such as the lure messages that contain a Visual Basic macro.

IV. ENGAGEMENTS

- The actor behind Honeybee has been operating with new implants since at least November 2017 with the first known version of NTWDBLIB installer.
- On 15 January 2018, Advanced Threat Research discovered an operation using a new variant of the SYSCON backdoor.
- On 17 January 2018, a Korean-language Word document manual.doc appeared in Vietnam, with the original author name of Honeybee.

V. COMMON ATTRIBUTIONS

- Contain the same Visual Basic macro code and author name as Honeybee.
- Used the same macro and same type of implant,
- These documents do not contain the typical lures by this actor, instead of using Word compatibility messages to entice victims into opening them.

VI. IOC

C&C

1. **ftp.byethost31.com**
2. **ftp.byethost11.com**
3. **1113427185.ifastnet.org**
4. **navermail.byethost3.com**
5. **nihon.byethost3.com**

MD5

1. **fe32d29fa16b1b71cd27b23a78ee9f6b7791bff3**
2. **f684e15dd2e84bac49ea9b89f9b2646dc32a2477**
3. **1d280a77595a2d2bbd36b9b5d958f99be20f8e06**
4. **19d9573f0b2c2100accd562cc82d57adb12a57ec**
5. **f90a2155ac492c3c2d5e1d83e384e1a734e59cc0**

VII. REFERENCES

- https://attack.mitre.org/groups/G0072/
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Honeybee&n=1