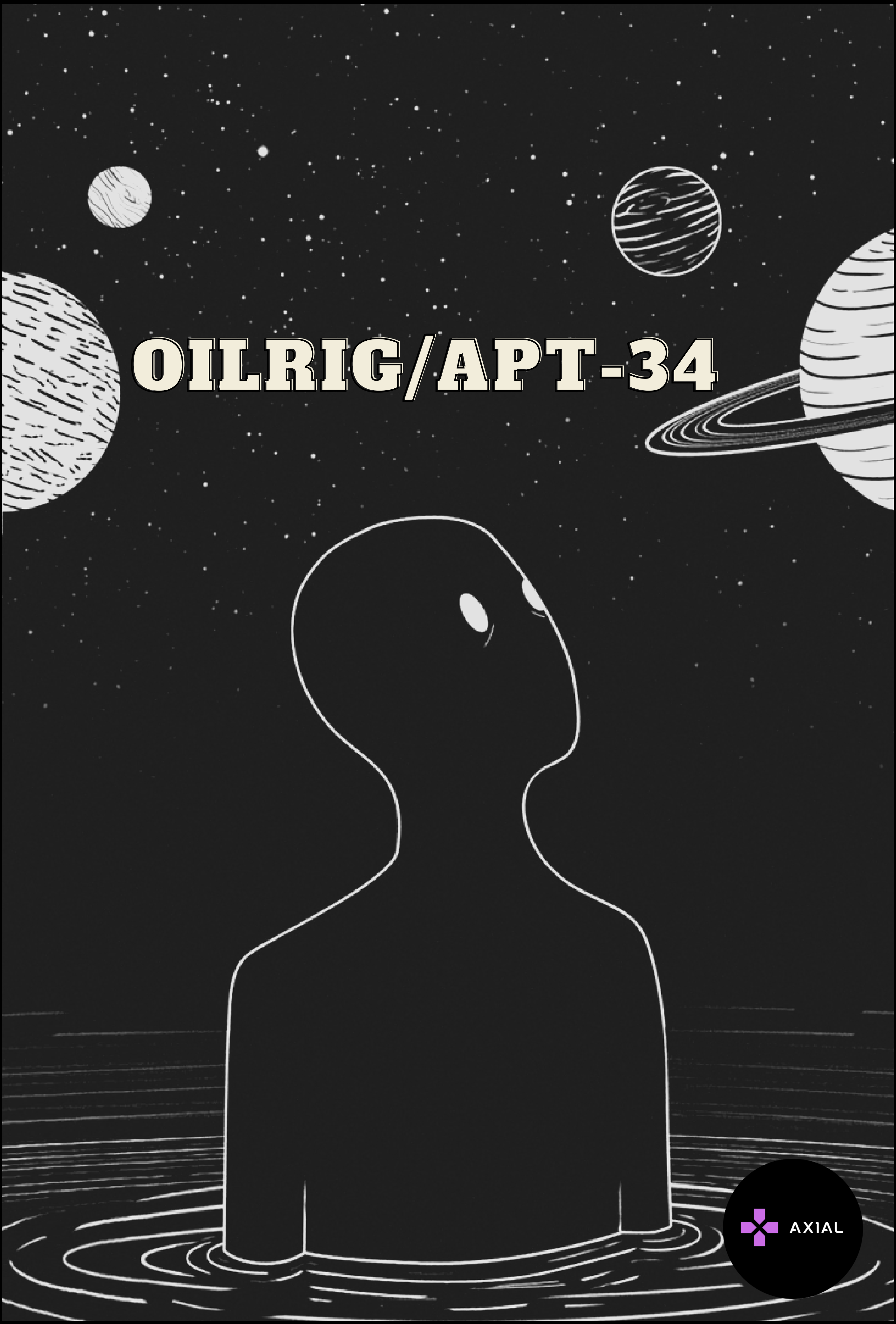
OILRIG/APT-34



AXIAL

A SURVEY ON OILRIG/APT-34: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

OilRig is a threat group that is su expected to have it's origin based out of Iran, which is also known as APT 34 or Twisted Kitten.

II. TARGET SECTORS

Aviation, Defense, Energy, Financial, Government, IT, Media, NGOs, Pharmaceutical, Think Tanks on multiplecountries.

III. METHODS USED

- OilRig has been using W32.Disttrack is a new threat that is being used in specific targeted attacks against at least one organization in the energy sector. It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable.

- In the recent attacks, they set up a fake VPN Web Portal and targeted at least five Israeli IT vendors, several financial institutes, and the Israeli Post Office.

- OilRig group using a tool they developed called ISMAgent in a new set of targeted attacks. The OilRig group developed ISMAgent as a variant of the ISMDoor Trojan.

IV. ENGAGEMENTS

- OilRig has been linked to Shamoon attacks in the energy sector.

- Targeted attacks against the banks in the Middle East.

- Government organizations of Turkey, Isreal, and the US.

- Oilrig has also been attributed for carrying out various operations against insurance-based companies in the Middle East.

V. COMMON ATTRIBUTIONS

OilRig has been attributed by Fireeye and they have linked this campaign to APT34, a Suspected Iranian cyber-espionage threat group that believed has been active since at least 2014.

V. IOC

HASHES

1. **742a52084162d3789e19…**
2. **f1de7b941817438da2a4…**
3. **b142265bb4b902837d83…**
4. **2e226a0210a123ad8288…**
5. **299bc738d7b0292820d9…**
6. **d64b46cf42ea4a7bf291…**

Format of subdomains used in DNS C2 protocol:

1. **[00][botid]00000[base36 random number]30**
2. **[00][botid]00000[base36 randomnumber]232A[hex_filename][i-counter]**
3. **[00][botid][cmdid][partid][base36 random number][48-hex-char-of-file-content]**

VI. REFERENCES

- https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi g=OilRig%2C%20APT%2034%2C%20Helix%20Kitten%2C%20Chrysene
- https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html