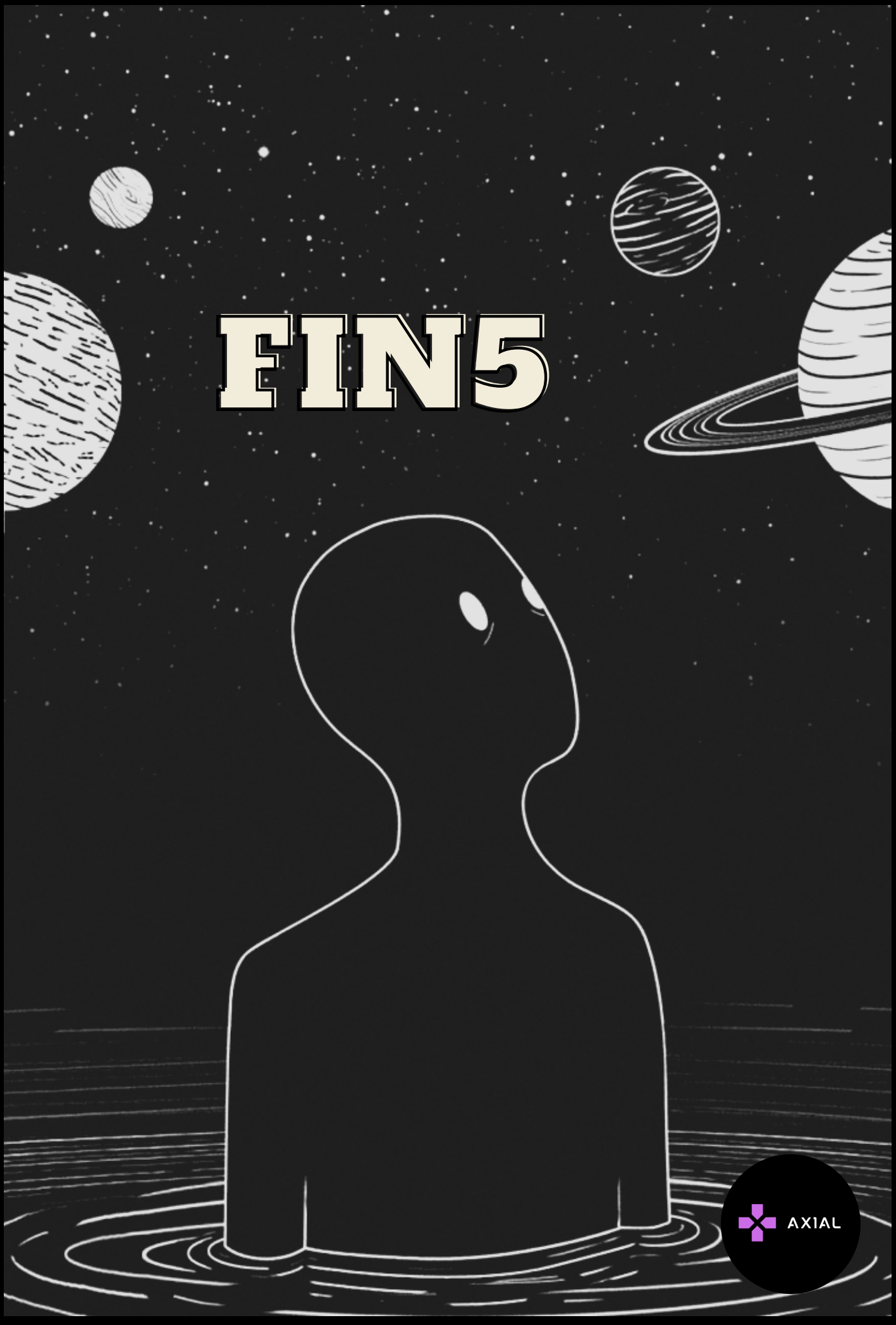
FIN5
AXIAL

A SURVEY ON FIN5: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian.

II. TARGET SECTORS

Gaming, Hospitality.

III. ENGAGEMENTS

- This group has been targeting the restaurant, gaming, and hotel industries since 2008.
- 2014, FireEye investigated a massive breach at a casino hotel with 1,200 endpoints that suffered losses to more than 150,000 payment cards. Vengerik declined to name the hotel.

IV. METHODS USED

The attackers first target the Active Directory to get to the card data and use tools such as Windows Credentials Editor in their quest for legit credentials. They also created several custom tools for covering their tracks and cleaning up any traces of the malware, as well as proxy tools for accessing segregated network segments.

AX1AL

V. ATTRIBUTIONS

- FIN5 is attributed by MITRE ATT&CK that the group is made up of actors who likely speak Russian.

VI. IOC

- No public IOCs found.

VII. REFERENCES

- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=FIN5&n=1
- https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645
- https://malpedia.caad.fkie.fraunhofer.de/actor/the_gorgon_group
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Gorgon%20Group&n=1