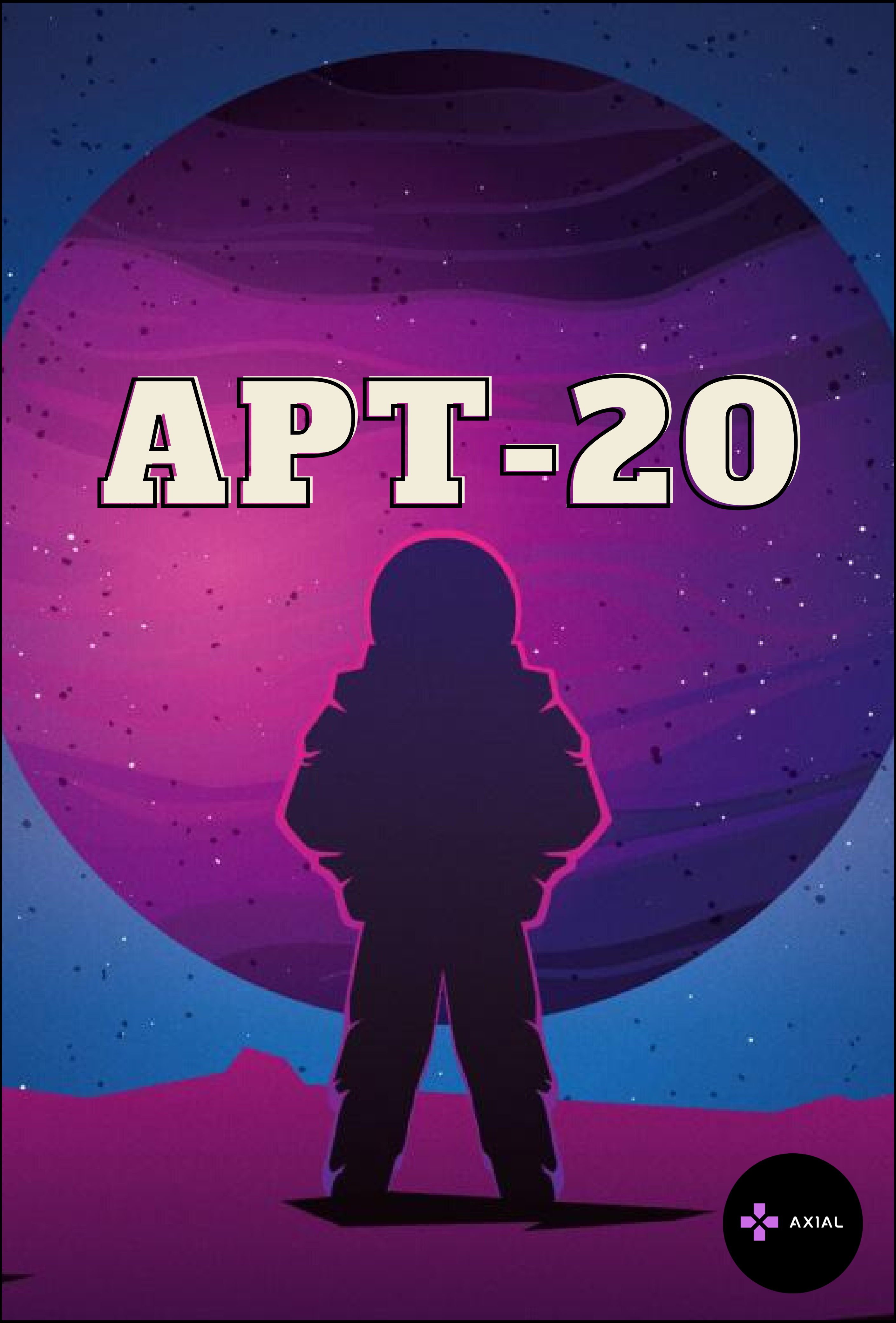

APT-20

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

Violin Panda also known as Twivy, is a threat group working out of China. They are also known as Th3bug named for the password the actors often use with their Poison Ivy malware. APT 20's goal is data theft and espionage of the person associated with the Organization or Industry. The Threat Group was active from 2009 to 2014, but recently as of 2019, they have re-emerged. What makes them different from other APT groups is the ability to compromise legitimate websites and install malware on them for people who will visit them.

II. TARGET SECTORS

Violin Panda has been known to target sectors that are Finance, insurance, healthcare, aviation, or energy. They also target Non-profit organizations.

III. ENGAGEMENTS

In 2014, Violin Panda executed a Watering Hole attack targeting US-Based Companies in East Asia, US University, Telecom Providers

In December 2019, APT 20 exploited a vulnerability in Jboss web servers, gaining access to networks and spreading widely into the networks all the while dumping passwords to admin accounts to maximize their access.

They also successfully maintained access to said systems by logging into VPN accounts protected by MFA.

IV. METHODS USED

APT 20 strategically compromise legitimate websites and install malware to compromise website visitors.

V. IOC

C&C

1. diff.qohub.info
2. app.qohub.info
3. 2014year.qpoe.com

MD5

1. 0cabd6aec2555e64bdf39320f338e027
2. efad656db0f9cc92b1e15dc9c540e407
3. 7b0cb4d14d3d8b6ccc7453f7ddb33997
4. 1ea41812a0114e5c6ae76330e7b4af69
5. 14f3514feb74a943b17596ebf0811eb0
6. fdba8a1e7624f4e14267366e4f83afc4

VI. Attributions

- Use malwares such as CAKELOG, CANDYCLOG, PlugX, ZXSHELL, Poison Ivy, BEACON, HOMEUNIX, STEW.
- Return was attributed to their signature malware CETTRA and COOKIECLOG.
- Leaked Language Settings used by the actor as well as the Registration details of one of the servers cited the actor to be of Chinese Origin, stated through report of Operation Wocao.

VII. References

- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?u=110ed515-11db-4bf1-af41-a66f513ecf70
- https://unit42.paloaltonetworks.com/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/
- https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf