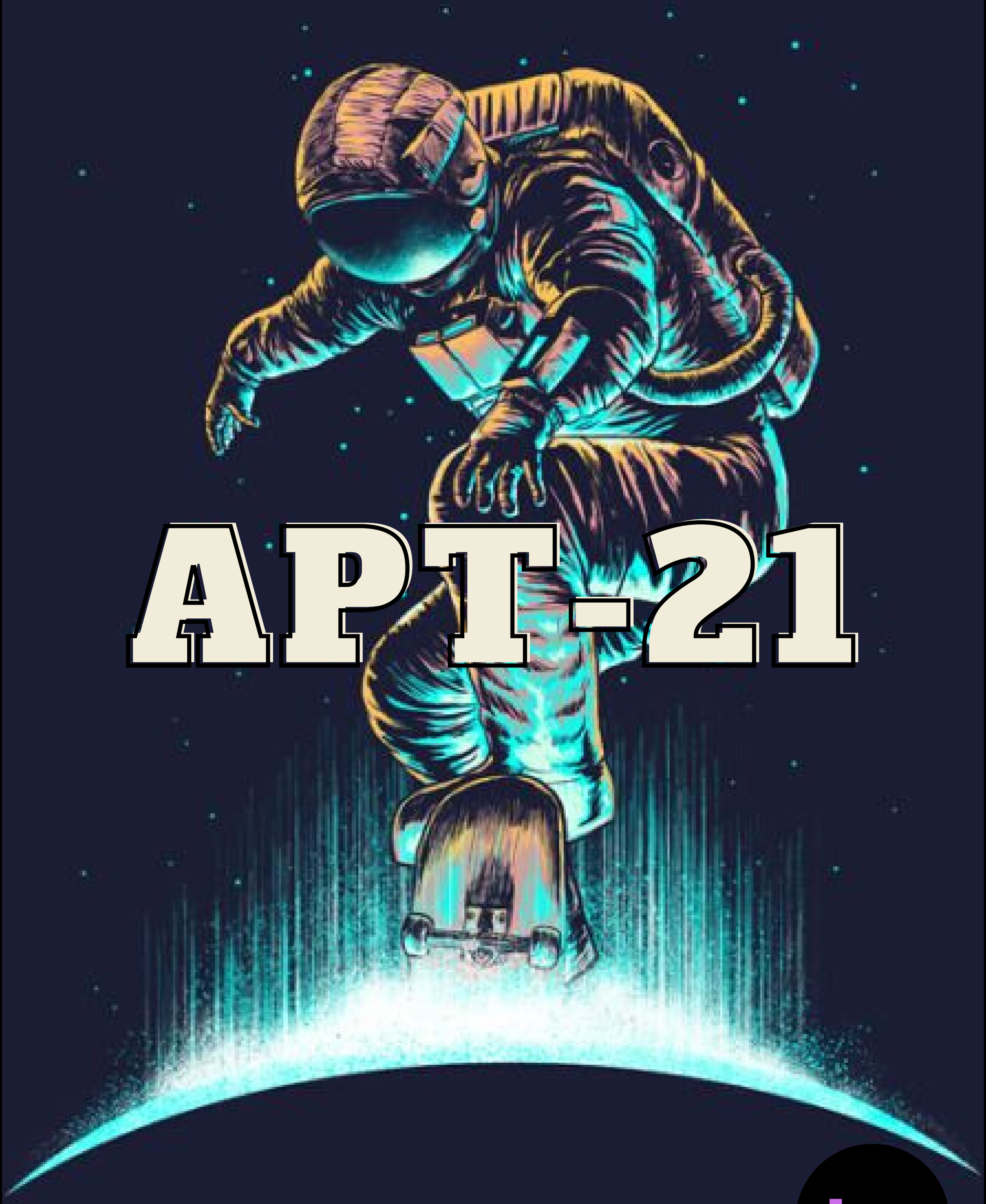
APT-21



AXIAL

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

-NERDS OF AX1AL

I. ABOUT

APT 21 also known as Hammer Panda, Zhenbao or NetTraveler is a Threat Group of Chinese Origin. Their key targets are Russian Organizations with the motivation of Data Theft and Espionage. Hammer Panda has been active since 2004 however their highest volume of activity occurred from 2010-2013. They send spear-phishing emails to exploit High-Value Individuals. They also engage in Social Engineering attacks as well as Waterhole attacks in the past.

II. TARGET SECTORS

Hammer Panda has been known to target sectors that are in Government Sectors, Defence, Embassies, Scientific Researches, and many more.

III. ENGAGEMENTS

- In August 2014, Operation NetTraveler had completed 10 years. Kaspersky had found out that there is an updated version of NetTraveler targetting Uyghur and Tibetan supporters
- In December 2015, a spear-phishing attack against an individual working for the Foreign Ministry of Uzbekistan in China came to light. The email was spoofed to look like it was sent by the Russian Foreign Ministry. This attack took place a few months later after SCO BRICS Summit.

IV. METHODS USED

Hammer Panda uses spear-phishing to target high profile people by sending malicious Microsoft Office attachments that are rigged with two highly exploited vulnerabilities (CVE-2012-0158 and CVE-2010-3333)

V. IOC

C&C

1. ssdcru.com
2. Uygurinfo.com
3. Samedone.com
4. Gobackto.com
5. cultureacess.com
6. discoverypeace.org
7. drag2008.com
8. eaglesey.com
9. enterairment.net
10. faceboak.net

MD5

1. b2385963d3afece16bd7478b4cf290ce
2. 2a43c23a17cd2bc9074a486c47444e7c
3. 29a420e52b56bfadf9f0701318524bef
4. 3c0ea91ea42f2bf6686e9735998e406e
5. 6eb5932b0ed20f11f1a887bcfbdde10f
6. 917e36946c67414a988f6878d9d0cdfe
7. 059a7482efee3b2abf67c12d210cb2f7
8. 36ed86602661bb3a7a55e69fde90ee73

VI. Attributions

- Associated Malware like SOGU, TEMPFUN, Gh0st, TRAVELNET, HOMEUNIX, ZEROTWO as well frequently using two backdoors known as TRAVELNET and TEMPFUN.
- Kaspersky estimates the group contains about 50 individuals, most of whom are native Chinese speakers and have a working knowledge of English.

VII. References

- https://securelist.com/nettraveler-apt-gets-a-makeover-for-10th-birthday/66272/
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=NetTraveler%2C%20APT%2021%2C%20Hammer%20Panda&n=1
- https://unit42.paloaltonetworks.com/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080841/kaspersky-the-net-traveler-part1-final.pdf