APT-23

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

APT 23, also known as KeyBoy, Tropic Trooper, or Pirate Panda, is a Chinese State-sponsored Threat actor whose prime motivation is Information Theft and Espionage. Pirate Panda has been active since 2011. Pirate Panda has led targeted campaigns against the Philippines, Taiwan, and Hong Kong.

II. TARGET SECTORS

Pirate Panda's known for targeting government and political organizations, healthcare, transportation. The group also leverages Poison Ivy for their campaigns.

III. ENGAGEMENTS

- In 2012, the Philippines Military Agencies and Taiwanese Government were targeted by Operation Tropic Trooper.
- In 2013, Tropic Trooper used a custom backdoor known as KeyBoy against Vietnam and India.
- In 2014, Pirate Panda targeted the Taiwanese and Philippine military's physically isolated network through a USBferry attack.
- In 2016, Pirate Panda targeted the Tibetan community using a new version of the KeyBoy backdoor. They had used CVE-2012-0158 and CVE-2015-1641
- In April 2020, Pirate Panda targeted Vietnam's government employees using spear-phishing email campaigns.

IV. METHODS USED

Pirate Panda uses spear-phishing campaigns. As of February 2020, they were observed using COVID-19 themed lure documents.

V. IOC

C&C

1. skypechatvideo[.]online
2. phdns01[.]com
3. phmail[.]us
4. qpoe[.]com
5. wikaba[.]com
6. tibetnews[.]today
7. dns-stuff[.]com
8. 2waky[.]com

SHA-256

1. 1d128fd61c2c121d9f2e1628630833172427e5d486cdd4b6d567b7bdac13935e (CVE-2018-0802.ZTFC)
2. 01087051f41df7bb030256c97497f69bc5b5551829da81b8db3f46ba622d8a69 (BKDR_TCLT.ZDFB)
3. 6e900e5b6dc4f21a004c5b5908c81f055db0d7026b3c5e105708586f85d3e334 (BKDR64_TCLT.ZTFB)
4. 49df4fec76a0ffaee5e4d933a734126c1a7b32d1c9cb5ab22a868e8bfc653245 (TROJ_SCLT.ZTFB)
5. b0f120b11f727f197353bc2c98d606ed08a06f14a1c012d3db6fe0a812df528a
6. d65f809f7684b28a6fa2d9397582f350318027999be3acf1241ff44d4df36a3a
7. 85d32cb3ae046a38254b953a00b37bb87047ec435edb0ce359a867447ee30f8b (TROJ_TCDROP.ZTFB)
8. 02281e26e89b61d84e2df66a0eeb729c5babd94607b1422505cd388843dd5456
9. fb9c9cbf6925de8c7b6ce8e7a8d5290e628be0b82a58f3e968426c0f734f38f6 (TROJ_TCLT.ZDFB)

VI. References

- https://www.trendmicro.com/en_us/research/20/e/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments.html
- https://citizenlab.ca/2016/11/parliament-keyboy/
- https://www.anomali.com/blog/anomali-suspects-that-china-backed-apt-pirate-panda-may-be-seeking-access-to-vietnam-government-data-center
- https://www.trendmicro.com/en_us/research/18/c/tropic-trooper-new-strategy.html