
APT
30
AXIAL

A SURVEY ON APT30: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT30, also known as PLA Unit 78020, OverridePanda, LotusPanda, Hellsing, BronzeGeneva, or APT.Naikon is a Chinese State-sponsored Threat Group that has been active since 2005. Their mission focuses on acquiring sensitive data from a variety of targets and they show how a group can persistently compromise victims across an entire region and subcontinent, with little to no need to change to their modus operandi.

II. TARGET SECTORS

APT30 targets sectors that are in Defence, Energy, Government, Law enforcement, Media. The countries that are the main focus of the group are All ASEAN Members, Australia, China, India, Nepal, Saudi Arabia, South Korea, USA.

IV. METHODS USED

APT27 has extensively used Strategic Web Compromises to lure targets for espionage purposes.

III. ENGAGEMENTS

- In 2013, MsnMM Campaign was launched by APT30 deploying backdoors and tools against victim systems. They were delivered to victims using spear-phishing and were laced with CVE-2012-0158.
- In the same year, several industries across Asia were hit by RARSTONE RAT. The attacks were carried out using spear-phishing with messages related to diplomatic discussions in the APAC region.
- One of the biggest operations of the APT30 group was launched in March 2014, in the wake of the MH370 tragedy that took place on March 8th. APT30 group was actively hitting most of the nations involved in the search for MH370.
- In 2017, Check Point Research discovered evidence of an ongoing cyber-espionage operation against several government entities in the APAC region. This operation was attributed to the APT30 group, which used a new backdoor named Aria-body, to take control of the victims' networks.

AX1AL

V. ATTRIBUTIONS

- The use of Backspace, Neteagle, 8.t Dropper, Spaceship, Naikon, LoTL (Living off the Land), RARSTONE, PlugX which is observed with other Chinese Threat Actors shows that the Adversary is of Chinese Origin and their Toolkit is vast.

VI. IOC

C&C

1. kabadefender[.]com
2. gordeneyes[.]com
3. techmicrost[.]com
4. hxxp://103.233.10[.]152:4433
5. hxxp://172.247.197[.]189:443
6. newpresses[.]com
7. appsecnic[.]com
8. km153[.]com

ASN

- CNSERVERS LLC (40065),
- ABCDE GROUP COMPANY LIMITED (133201),
- Zenlayer Inc (21859).

MD5

- d9c42dacfae73996ccdab58e429548c0
- 101bda268bf8277d84b79fe52e25fee4
- f4f8f64fd66a62fc456da00dd25def0d
- 56725556d1ac8a58525ae91b6b02cf2c
- e39756bc99ee1b05e5ee92a1cdd5faf4
- c2acc9fc9b0f050ec2103d3ba9cb11c0
- 28f2396a1e306d05519b97a3a46ee925
- 80e39b656f9a77503fa3e6b7dd123ee3
- bbb3cb030686748b1244276e15085153
- 7c307ca84f922674049c0c43ca09bec1
- a813eba27b2166620bd75029cc1f04b0
- cb1087b2add3245418257d648ac9e9a7
- c90f798ccfbedb4bbe6c4568e0f05b68
- ab153afbfbcfc8c67cf055b0111f0003

VIII. REFERENCES

- https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf
- https://malpedia.caad.fkie.fraunhofer.de/actor/naikon
- https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf
- https://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/