APT40

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

Also known as TEMP.Periscope, Leviathan, Gadolinium, and Mudcarp is a threat group originating from China that targets countries strategically important for the Belt and Road Initiative and have been operational since 2013. Historically, it has also conducted campaigns against entities in the APAC region. The group has targeted engineering, transportation, and the defence industry, especially where these sectors overlap with maritime technologies. FireEye Intelligence believes that APT40's operations are a cyber counterpart to China's efforts to modernize its naval capabilities.

II. TARGET SECTORS

APT40 has vast target sectors ranging from Defense, Engineering, Government, Manufacturing, Research, Shipping and Logistics, Transportation to other Maritime-related targets across multiple verticals.

III. ENGAGEMENTS

- In 2014, APT40 was involved in spear-phishing organizations and high-value targets in defence and government. They had exploited vulnerabilities CVE-2017-0199 and CVE-2017-8759.
- In 2018, a UK based engineering company was targeted by a spearphishing campaign. The campaign also targeted a freelance journalist based in Cambodia who covers Cambodian politics, human rights, and Chinese development.
- In the same year, APT40 was targeting Cambodian entities with active compromises, that are related to the country's electoral system. The targeted entities include Entities charged with overseeing the elections as well as targeting opposition figures.

IV. METHODS USED

Use of RTF Phishing followed by shellcode executed via an OLE package dropping distinctive source file.

V. ATTRIBUTIONS

- The group’s targeted victims are linked to Chinese state interests, and various technical artifacts are supporting the fact that this actor is based in China. Also, the operational times of this group’s activities indicate that it is probably centered around China Standard Time.
- APT40 has been observed using at least 51 different code families. Of these, 37 are non-public. At least seven of these non-public tools (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDETONE) are shared with other suspected China-nexus operators.

VI. IOC

C2

1. scsnewstoday[.]com
2. thyssenkrupp-marinesystems[.]org
3. hxxp://www.vitaminmain[.]info
4. tomema.myddns.me
5. armybar.hopto.org
6. 185.106.120[.]206
7. 193.180.255[.]2
8. 68.65.123[.]230
9. 82.118.242[.]242
10. 82.118.242[.]243
11. hxxp://185.106.120[.]206/favicon.ico
12. ftp://185.106.120[.]206/pub/readme.txt
13. 139.162.44.81:80
14. 45.32.123.142:80
15. 167.99.72.82:80
16. 195.12.50.168:80

MD5

- 00f952c54f1189bf9583d9fb066be54a
- 055bc765a78da9cc759d1ba7ac7ac05e
- 0cb26112cb09d268ccbfe10ac59765df
- 0dfed59e581c181baeabb5d936c902ce
- 10c6029fbc0a2770b9686cf31d58067a
- 166694d13ac463ea1c2bed64fbbb7207
- 17dbbda8cd63c255d647ab7c423367e5
- 1c35a87f61953baace605fff1a2d0921
- 1c6ef040cd7121915245677eef5a3180
- 2366918da9a484735ec3a9808296aab8
- 25fc656f3756c7d58aa15aa7e9fae2dc
- 2754975fb01c931f070d880b224eaee7
- 2a38ff33240e20caabfc53524a840dfd
- 2bf998d954a88b12dbec1ee96b072cb9
- 302003a7ee0d848c98df4bb2b7c720cd
- 35b82e945de3c49d52283f2caea979f5

VIII. REFERENCES

- https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
- https://lab52.io/blog/leviathan-geostrategy-and-ttp-technical-tactics-and-procedures/
- https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/
- https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html