
APT
17
AXIAL

A SURVEY ON APT17: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Also known as Tailgater Team, Elderwood, Sneaky Panda, SIG22, Beijing Group, Dogfish, Deputy Dog, TEMP.Avengers and ATK2 is a state-sponsored threat group originating from China. They were active from 2009. They have been known to use multiple 0day exploits, attacking supply chain manufacturers, and shifting to SWC attacks. APT17 tends to target Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK, USA.

II. TARGET SECTORS

APT17 targets Defence, Education, Energy, Financial, Government, High-Tech, IT, Media, Mining, NGOs and Lawyers.

III. METHODS USED

The threat group took advantage of the ability to create profiles and post in forums to embed encoded C2 for use with a variant of the malware it used. This technique can make it difficult for network security professionals to determine the true location of the C2, and allow the C2 infrastructure to remain active for a longer period.

IV. ENGAGEMENTS

- In March 2010, RSA was breached. APT17 had breached security systems designed to keep out intruders by creating duplicates to “SecurID” electronic keys from EMC Corp’s EMC.N RSA security division.
- Operation "DeputyDog" went live in August 2013, targeting organizations in Japan leveraging the then-recently announced zero-day CVE-2013-3893.
- Operation "Ephemeral Hydra" went live in November 2013 targeting strategically important websites that are known to draw visitors that are interested in National and International Security Policy.
- In August 2017, Proofpoint observed a targeted email campaign attempting a spear-phishing attack using a Game of Thrones lure. The malicious attachment, which offered spoilers and video clips, attempted to install a “9002” remote access Trojan (RAT) historically used by APT17.
- In 2017, Talos observed a case where the download servers used by software vendors to distribute a legitimate software package were leveraged to deliver malware to unsuspecting victims. For a period of time, the legitimate signed version of Ccleaner 5.33 being distributed by Avast also contained a multi-stage malware payload that rode on top of the installation of Ccleaner.

AX1AL

V. ATTRIBUTIONS

- Intrusion Truth, after an extended research period, found out that APT17 is run by the Jinan Bureau of the Chinese Ministry of State Security. A few months after, cyber-security firm Recorded Future independently confirmed Intrusion Truth findings -- which later resulted in DOJ charges, giving the group immense credibility.

VII. IOC

C2

1. matrix.bcvziy.com
2. back.teledynegroup.com
3. rsc-to.teledynegroup.com
4. www.missll.com
5. 1si2.yqdac.com
6. dpc0p.com
7. yahxi123.cn
8. access.wscsvc.net
9. whoi.usdagroup.com
10. ns1.wscsvc.net
11. pir0i.com

MD5

- 0777ae914c11045d00159744ccdc8109
- 007cf8d976ee0862487c78ec071ce2e7
- fb13c3cf930f5714f9081a49844209e7
- d901a5737d7a0c37aa42798cb523150f
- d1a326be4a422e92308bbcf8ea154f6d
- de56eb5046e518e266e67585afa34612
- da88e711e4ffc7c617986fc585bce305
- c016af303b5729e57d0e6563b3c51be4
- ac169b7d4708c6fa7fee9be5f7576414
- 5f2fcba8bd42712d9975da208a1cc0ca
- 5d16e5ee1cc571125ab1c44ecd47a04a

VIII. REFERENCES

- https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/
- https://www.theregister.com/2010/11/11/amnesty_international_hosts_ie_exploit/
- https://www.darkreading.com/attacks-and-breaches/chinese--hidden-lynx--hackers-launch-widespread-apt-attacks/d/d-id/1111589?page_number=2
- https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
- https://www.infosecurity-magazine.com/news/chinese-espionage-group-widescale/
- https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html