APT 3

AXIAL

A SURVEY ON APT3: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT3 also known as Gothic Panda, Buckeye, TG-0110, Bronze Mayfair, UPS Team, and Group 6 is a Chinese State-sponsored Threat Group that has been active since 2007. Extensive analysis by Intrusion Truth revealed the Threat Group to be Boyusec - the Guangzhou Boyu Information Technology Company, Ltd, and Ministry of State Security.

II. TARGET SECTORS

APT3 targets and compromises entities in the Aerospace and Defence; Construction and Engineering; Energy; High Tech; Nonprofit; Telecommunications; Transportation. Up until 2015, it was primarily focused on U.S. and UK entities, but it shifted to Hong Kong based targets afterward.

III. METHODS USED

APT3 utilizes a broad range of tools and techniques including spear-phishing attacks, zero-day exploits, and numerous unique and publicly available remote access tools (RAT). Tools like Shotput, Pirpi, PlugX/Sogu, Kaba, Cookie Cutter, many 0days: IE, Firefox, and Flash, SportLoader, Shadow Brokers exploits, DoublePulsar, Bemstour, Filensfer.

IV. ENGAGEMENTS

- In 2007, Symantec disclosed a 0day in Microsoft's IE v6,7 and 8. They also revealed one malware that was actively exploiting this 0day namely 'Backdoor.Pirpi'. Later, FireEye revealed malware exploiting the same 0day. It was named 'Hupigon'.
- In April 2014, Operation "Clandestine Fox" took place. Researchers at FireEye identified a new IE 0day exploit being used in targeted attacks. The vulnerability affected IE6 to IE11.June 2014, Operation "Clandestine Fox" resumed in the form of Social Engineering.
- November 2014, Operation "Double Tap" took place which targeted multiple organizations exploiting CVE-2014-6332 and CVE-2014-4113.
- In June 2015, APT3 actors launched a large-scale phishing campaign against organizations in the following industries: Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, and Transportation. Also known as Operation "Clandestine Wolf"
- APT3 was active once again in 2016 with a variant of Backdoor.DoublePulsar. It was Initially delivered to targets using Trojan.Bemstour.
- APT3 compromised political entities in Hong Kong by sending malicious emails to targets in June 2015.

AX1AL

V. ATTRIBUTIONS

- The use of malwares that was used by other Chinese Threat Actors such as PlugX, HTran, etc shows that APT3 is of Chinese Origins.
- Intrusion Truth's in-depth analysis of the group revealed the group's company and their links to MSS.

VI. COUNTER OPERATIONS

- In November 2017, Department of Justice indicted APT3 group members, Wu Yingzhuo, Dong Hao and Xia Lei, who had involvement in stealing data from Companies, including Siements AG, Moody's Analytics, and Trimble. The group operated for a Chinese-based Internet Security Firm Boyusec.

VII. IOC

C2

1. psa.perrydale[.]com
2. link.angellroofing[.]com
3. 107.20.255.57
4. 23.99.20.198
5. securitywap.com
6. join.playboysplus[.]com
7. walterclean[.]com

MD5

- 7020bcb347404654e17f6303848b7ec4
- aacfef51a4a242f52fbb838c1d063d9b
- c2f902f398783922a921df7d46590295
- a3932533efc04ac3fe89fb5b3d60128a
- a469d48e25e524cf0dec64f01c182b25
- 0d2d0d8f4989679f7c26b5531096b8b2
- 58f784c7a292103251930360f9ca713e
- 6458806a5071a7c4fefae084791e8c67

VIII. REFERENCES

- https://www.fireeye.com/blog/threat-research/2010/11/ie-0-day-hupigon-joins-the-party.html
- https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html
- https://intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/
- https://www.recordedfuture.com/chinese-mss-behind-apt3/
- https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/
- https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html
- https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations