APT1

A SURVEY ON APT1: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT 1, also known as Comment Crew Was Identified by Mandiant as 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's(GSD) 3rd Department aka unit 61398. Members of APT 1 Was Very Professional in Computer Security, Network Operations and English. Stole Hundreds of Terabytes of data from 141 Companies with 20 Different Industries. Reason for Naming is that they was the first APT Group to be Name by Mandiant. Their Goals was Mainly Cyberespionage and Data Theft.

II. TARGET SECTORS

APT 1 Targeted Various Industries and Organizations Including: Information Technology, Transportation, High-Tech Electronics, Finance, Navigation, Legal Services, Engineering Services, Media, Advertising and Entertainment, Food and Agriculture, Satellites and, Telecommunications, Chemicals, International, Organizations, Scientific Research and Consulting. Education, Energy, Metals and Mining, Construction, and Manufacturing and Aerospace. They Targeted Industries that supports their Economic Plan aka Five-year plans of China it was first issued in 1953 and still continuing until now It wasn't Five Years It was like Every Five Years like from 1953 to 1957 and then from 1958 to 1962.

III. ENGAGEMENTS

- APT 1 Engaged in Several Attack Since 2006 it was Operation Seasalt They Targeted 140 Companies for Cyber-Espionage and Data Theft Goals It Continued to 2010.

- In 2011-2012 They Hacked Three Israel Companies Elisra Group, Israel Aerospace Industries, and Rafael Advanced Defense Systems. These Companies was Responsible for Building Iron Dome it was air-defense system made to protect israel against rocket attacks. Their Goals was to steal sensitive data and documents.

- In Feb 2014 TrendMicro Reported Operation Siesta, FireEye Examined their tools found that they same tools and code are that which APT1 used. The Attacks was spread using Spear-Phishing Containing Malicious Zipped Files. FireEye Examined the PE Files of this attack found that they belong to Menupass group which is a threat group also originated from china. Two Assumptions either they are the same group or they just shared resources. FireEye said that they are unlikly the same group but instead they look like they shared the Binder tool. which is used to add an icon like pdf to a malware.

IV. METHODS USED

APT 1 Used Spear-Phishing for as an Initial Access Technique Emails with attachments mostly was zipped but not always Example an email containing a malicious pdf document. They Maintained Persistence for average 356 day. They Used Multiple Tools and Backdoors. We Are Sure That They were Mostly Developed by Them.

V. IOC

C&C

1. domain.busketball.com
2. domain.arrowservice.net
3. 40gmail.com
4. 208.239.156.123:443
5. s.gb
6. camaya.net
7. passport.ne
8. header.id

SHA-256

1. 225e33508861984dd2a774760bfdfc52 (WEBC2-Y21K)
2. fd66b9718e650978eb0fff32b9edb377 (AURIGA)
3. 57353ecbaece29ecaf8025231eb930e3 (BOUNCER)
4. 497f07f54a4c29fe3be1a15f4516e32d (BISCUIT)
5. fa14d823a5d1854131db0dc9eef27022 (COMBOS)
6. 8dc3561ca52bfe40089f3ee0af7fdd9d (WEBC2-ADSPACE)
7. 16c390a32f9a60bf50396fc86aea0f9d (CALENDAR)
8. 36ca55556280f715e2de8b4b997a26c9 (GETMAIL)
9. 3de1bd0f2107198931177b2b23877df4 (GLOOXMAIL)
10. bce4b77a4e4acc70a3f6f52ec0a2f033 (GOGGLES)

VI. References

- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Comment%20Crew%2C%20APT%201&n=1
- https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html
- https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/
- https://attack.mitre.org/groups/G0006/
- https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf