APT-18

AXIAL

APT- 18

WEKBY

CHINA

US

Gh0st RAT

HAWK BASE

HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-18 ABOUT , WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

APT-18 also known as Dynamite Panda is a threat group based out of China they mainly targeted United States their Goals were Cyber-Espionage and Data theft.

II. TARGETS

APT-18 Mainly targeted United States their targets include: Aerospace and Defense, Construction and Engineering, Education, Health and Biotechnology, High Tech, Telecommunications, transportation.

III. METHODS USED

. APT-18 Weaponized Mutilple Zero Day Vulnerabilites. Example was (CVE-2015-5119) which was an Adobe Flash Vulnerability. The Vulnerability was leaked by Hacking Team.

. They Used Gh0st Rat as their Malware the Malware has the ability to profile the system, steal use info, process manipulation, capture screen and audio and perform C2 Communications.

They Used Phishing Emails in order to install their Malware and Get Into the Victim Organization. The Email is a Spoofed Email Pretending to be Adobe Telling It's users to update once the user clicks on the link it will install a malicious Adobe flash which then takes advantage of (CVE-2015-5119) which lead to installation of Gh0stRat.

IV. CAMPAIGNS

.The Attack Time Scale was From 2009 till May 2016.

. In April 2018 They Breached Community Health Systems which is based in Franklin, Tennessee United States. They Stole Patient and Health Care Information. Experts say That This was campaign was for the support of Economic Plan of China so they can Develop their Health Care Systems.

ATTRIBUTION

This threat group is linked to Night Dragon which is one of the group attributed to China, therefore APT-18 or Wekby is somehow related to China and many other attributes like campaigns which were carried out by this group which claimed has direct links to the support of Economic Plans of China.

[cited from ThaiCERT]

V. IOCS

Hashes (MD5)

079a440bee0f86d8a59ebc5c4b523a07

d0f79de7bd194c1843e7411c473e4288

e5414c5215c9305feeebbe0dbee43567

985eba97e12c3e5bce9221631fb66d68

e4968c8060ea017b5e5756c16b80b012

e8d58aa76dd97536ac225949a2767e05

C2:

223.25.233.248

VI. REFRENCES

https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/

https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2018%2C%20Dynamite%20Panda%2C%20Wekby&n=1