APT-12

AXIAL

APT- 12

IXESHE \
NUMBERED PANDA

CHINA

JAPAN , TAIWAN

RIPTIDE BACKDOORS

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-12: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

APT-12 or Numbered Panda is a Chinese APT Group. They Targeted multiple Sectors and Governments. Most of the Attacks was Targeted to Taiwan. They Mainly Focused on Spear-Phishing as an Initial Access Technique.

II. TARGETS

APT-12 Targeted Multiple Industries Including: Defense, Government, High-Tech, Media, Telecommunications and Electronics and journalists. Their Attacks Focused on Taiwan But They Also Targeted Countries like: Germany, Japan, USA and East Asia

III. METHODS USED

APT-12 Used Spear-Phishing Emails with Malicious Attachments The Attachment maybe a office malicious Document containing malicious macro code that will download the main payload from the c2 server. they exploited different office vulnerabilities like: CVE-2009-3129, CVE-2012-0158. Also The Attachment maybe a PDF Document They Exploited 4 Vulnerabilities in for that CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611. In Their Campaigns They Used Multiple Tools and Backdoors including: AUMLIB, ETUMBOT, IHEATE, IXESHE, RapidStealer, THREEBYTE, WaterSpout

IV. CAMPAIGNS

- APT-12 Engaged in about 10 Campaigns From 2009-2016
- First Campaign Observed was in July 2009 They East Asian governments, Taiwanese electronics manufacturers and a telecommunications company the Attack was then named "IXESHE" Campaign. They used Spear-Phishing Emails to get into these companies they weaponized 4 in adobe reader and flash player including: CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611 Plus 1 Office vulnerability.
- Second Campaign was in May 2011, The Attackers in this Campaign Used Updated Versions of IXESHE and AUMLIB Malware. The Country Targeted in this Attack was Taiwan.
- In Oct 2012, They Targeted the New York Times The Goals of this Attack was Purely Political American New Media at that time was reporting on Chinese leaders and this campaign was basically a cyber espionage activity on the American news media. The Attack Happened after The New York Times Published Named (Billions in Hidden Riches for Family of Chinese Leader) it was talking about Wen Jiabao the Former Premier of the People's Republic of China accumulated a fortune worth several billion dollars through business dealings.
- They Also Done Other Campaigns like RIPTIDE, HIGHTIDE, THREEBYTE, WATERSPOUT, CNACOM These Campaigns were focused on Taiwan and used spear-phishing as an initial access technique. however in January 2016 They Used a derivative of IXESHE was then name IHEATE To Target This Variant of IXESHE was seen in Taiwan since 2009 it has some improvements also they used different c2 servers and encryption methods the malware had capability of profiling the system, process manipulation and connecting to the c2. The Data is Encrypted using a Custom Encryption Algorithm and then sent to the C2 Server Encrypted in RC4 using a RSA-1024 Previously Generated Key that was encrypted using a hardcoded public key in the malware binary.

AX1AL

V. IOCS

MD5 Hashes

eaa6e03d9dae356481215e3a9d2914dc
aa873ed803ca800ce92a39d9a683c644
f6fafb7c30b1114befc93f39d0698560
73f493f6a2b0da23a79b50765c164e88
f9cfda6062a8ac9e332186a7ec0e706a
499bec15ac83f2c8998f03917b63652e
f9cfda6062a8ac9e332186a7ec0e706a
16a9f340c0d353332ba6f525376c93e1
8950bbedf4a7f1d518e859f9800f9347
c61c231d93d3bd690dd04b6de7350abb
100cf902ac31766f7d8a521eeb6f8d68
cb3dcde34fd9ff0e19381d99b02f9692
832f5e01be536da71d5b3f7e41938cfb
cb3dcde34fd9ff0e19381d99b02f9692

C2's

lilywang823@gmail.com
141.108.2.157
icc.ignorelist.com
video.csmcpr.com
documents.myPicture.info
www.documents.myPicture.info
status.acmetoy.com/DD/myScript.js
status.acmetoy.com/DD/css.css

TTP's

DNS Calculation [T1568]
Exploitation for Client Execution [T1203]
Phishing: Spear phishing Attachment [T1566]
User Execution: Malicious File [T1204]
Web Service: Bidirectional Communication [T1102]

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2012%2C%20Numbered%20Panda&n=1

https://attack.mitre.org/groups/G0005/

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all

https://blog.trendmicro.com/trendlabs-security-intelligence/ixeshe-derivative-iheate-targets-users-america/