APT-16

AXIAL

APT- 16

SVCMONDR

CHINA

JAPAN , TAIWAN

SPEAR PHISHING

HAWK BASE

HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-16 ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Apt-16 also known as SVCMONDR is China based apt-group that established attacks between November 26, 2015, and December 1, 2015. Their Goals Was mainly Cyber-Espionage and Data Theft.

II. TARGETS

attacks of this threat group is focused on two countries Taiwan and Japan. They targeted 4 Industries Government, Media, Finance and High-Tech and other critical infra

III. METHODS USED

. APT-16 Made Use of Spear-Phishing and Microsoft Office Word Documents that contains
malicious macro as an initial access technique to get into the victim organization

EPS dict copy use-after-free vulnerability

. CVE-2015-1701 (LPE)

. IRONHALO (Downloader) leverages HTTP for C2 Communications the C2 Commands are Base64 Encoded it had the capa

. ELMER (Backdoor): is an HTTP Backdoor that has capabilities like Retrieving C2 Commands and Profiling the System

IV. CAMPAIGNS

. The Attacks were between November 26, 2015, and December 1, 2015.

. They Targeted Taiwan and Japan their intensions was Espionage and Data Theft they mainly focused on Taiwan's Politics and Journalism's.

. On November 26, 2015, a suspected China-based APT group sent Japanese defense policy-themed spear phishing emails to multiple Japanese financial and high-tech companies (cited from FireEye)

ATTRIBUTION

The activities of the APT-16 are linked to China

[cited from Malpedia]

V. IOCS

Hashes

Hashes (MD5)

6c33223db475f072119fe51a2437a542 (ELMER)
0b176111ef7ec98e651ffbabf9b35a18 (ELMER)
a8ccb2fc5fec1b89f778d93096ff8dd65 (IRONHALO)

C2

121.127.249.74
news.rinpocheinfo.com
rinpocheinfo.com

VI. REFRENCES

https://malpedia.caad.fkie.fraunhofer.de/actor/apt_16

https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2016%2C%20SVCMONDR&n=1