LOTUS BLOSSOM

AXIAL

LOTUS BLOSSOM

CHINA

SOUTHEAST ASIA

SPEAR PHISHING

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

A threat group that has targeted government and military organizations in Southeast Asia and is attributed to China .

Initially, Kaspersky Lab became aware of new activities by an APT actor whom they have been tracking for several years called Spring Dragon (also known as LotusBlossom).Malware experts first spotted the Lotus Bloom hacking group back in 2015. In this early campaign, the Lotus Bloom APT had deployed a hacking tool known as the Elise Malware against its targets.

II. TARGETS

Governments and Military Organizations at Southeast Asia.

III. METHODS USED

- The group is known to have launched 50 seperate attacks . They have mostly targeted through spear-phising emails. The emails would contain a corrupted attachment which upon execution would exploit known vulnerabilities in popular software services . To lure the victim to open the email , they use spicy and tricky headlines are seems to be interesting.
- One of the most used tool used by Lotus Bloom is the Elise Malware . The most important artifact regarding the Elise malware is it is able to avoid sandbox environments , which leverages it to operate in a covert mode.

IV. ATTRIBUTIONS

The Esile targeted attack campaign targeting various countries in the Southeast Asian region has been discussed in the media recently. This campaign – which was referred to by other researchers as Lotus Blossom – is believed to be the work of a nation-state actor due to the nature of the stolen information, which is more valuable to countries than either private companies or cybercriminals."

The information in the screenshot and an analysis of the document’s timestamp suggested that the user was located in China.

The threat actor is running Windows localized for Chinese users, which suggests the actor’s primary language is Chinese. The‘CH’ icon in the Windows tray shows that the built-in Windows input method editor (IME) is currently set to Chinese,” researchers explained.

[Cited from Trend Micro]

VII. IOCS

MD5 : : f12fc711529b48bcef52c5ca0a52335a

C2 server:103.236.150[.]14

Interesting Artifacts :
7g91xhp.envuy3[.]net
•l.hovux.eln9wj7.7gpj[.]org
•w.7sytdjc.wroi.cxy[.]com

V. REFERENCES

1. www.attack.mitre.org
2. wwwe.nigmasoftware.com
3. www.accenture.com