NAIKON

NAIKON

CHINA

AUSTRAALIA , INDONESIA
VIETNAM , THAILAND

INFECTED DOCUMENTS

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Naikon is a threat group based out of China which also goes by the name Lotus Panda .

II. TARGETS

Naikon targets sectors like Defense, Energy, Government, Law enforcement, Media. on multiple countries like Australia , Brunei , India , Myanmar , Nepal , South Korea and the US.

III. METHODS USED

Naikon group used mostly spear-phished documents for the attacks, with CVE-2012-0158 exploits that dropped the group's signature backdoor.

Naikon is known for its custom backdoor, called RARSTONE.

Naikon was also found using Stone Panda Poison Ivy samples delivered with the same CVE-2012-0158 exploits, dropping iph.bat and iExplorer.exe, and running the "iExplorer.exe WMcal" executable filename and parameter.

IV. CAMPAIGNS

- Naikon has been involved with the MsnMM campaigns.
- Naikon has also been involved with the campaign most of the nations involved in the search for MH370. The targets were extremely wide-ranging but included institutions with access to information related to the disappearance of MH370
- Naikon has been involved in the operation CameraShy.

ATTRIBUTION

The APT group Naikon is associated with the People's Liberation Army Chengdu Military Region. The PLA's Chengdu operates primarily out of Kunming, China . analysis of historic command and control (C2) infrastructure used consistently within Naikon malware for espionage operations against Southeast Asian targets has revealed a strong nexus to the city of Kunming, capital of Yunnan Province in southwestern China.

[cited from Threat Connect Reports]

V. IOCS

Hashes

c766e55c48a4b2e7f83bfb8b6004fc51
2ce4d68a120d76e703298f27073e1682
0ed1fa2720cdab23d969e60035f05d92
3516960dd711b668783ada34286507b9

C2's

greensky27.vicp[.]net
checkip.amazonaws[.]com

h

VI. REFRENCES

https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Naikon%2C%20Lotus%20Panda

https://media.kasperskycontenthub.com