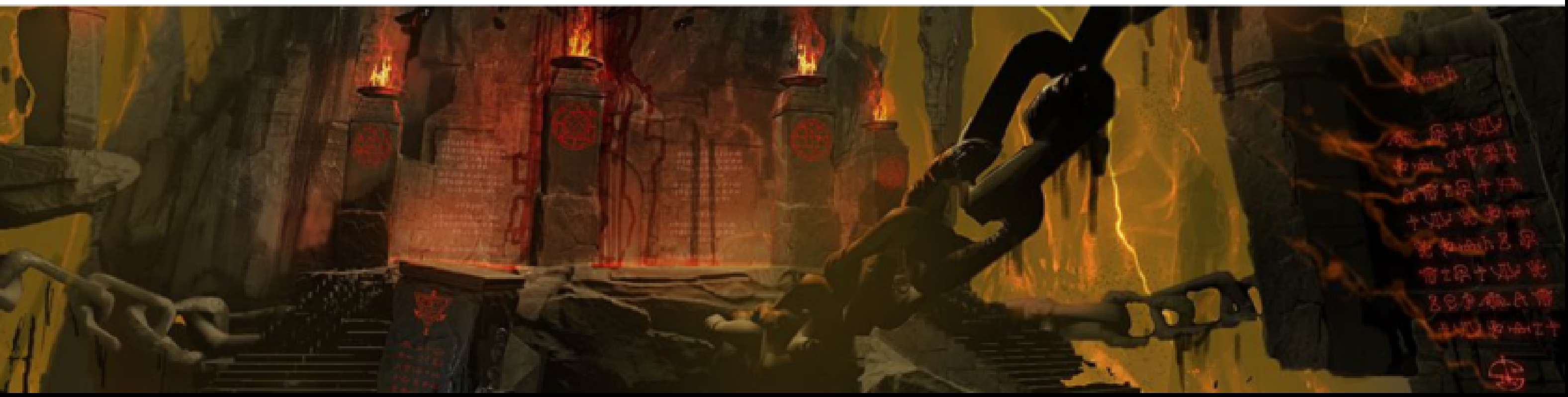
RANCOR

RANCOR

CHINA

SINGAPORE,CAMBODIA THAILAND ,SOUTHEAST ASIA

DDKONG
PLAINTEE



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON RANCOR ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Rancor is a threat group which has been attributed to China whose main motivations are Information theft and espionage, this group is also known as Rancor Group .

II. TARGETS

Attacks of this threat group ranges around government and political entities .

III. METHODS USED

This threat group has been using malware families DDKONG and PLAINTEE among whivh DDKONG is used throughout their campaigns and PLAINTEE has been an addition to the attackers' toolkit .

IV. CAMPAIGNS

During 2017 & 2018 this threat group has been focused onto highly focused in South East Asia .

ATTRIBUTION

Kaspersky found connections between this group and DragonOK which is a chinese attributed threat group .

[cited from ThaiCERT]

V. IOCS

Hashes

863a9199decf36895d5d7d148ce9fd622e825f393d7ebe7591b4d37ef3f5f677
22a5bd54f15f33f4218454e53679d7cfae32c03ddb6ec186fb5e6f8b7f7c098b
c35609822e6239934606a99cb3dbc925f4768f0b0654d6a2adc35eca473c505d
bcd37f1d625772c162350e5383903fe8dbed341ebf0dc38035be5078624c039e
6aad1408a72e7adc88c2e60631a6eee3d77f18a70e4eee868623588612efdd31
9f779d920443d50ef48d4abfa40b43f5cb2c4eb769205b973b115e04f3b978f5

IPs & Domains

www.facebook-apps.com
dlj40s.jdanief.xyz
199.247.6.253
45.76.176.236
103.75.189.74
www.google_ssl.onmypc.org
103.75.191.75
ftp.chinhphu.ddns.ms

VI. REFRENCES

https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Rancor