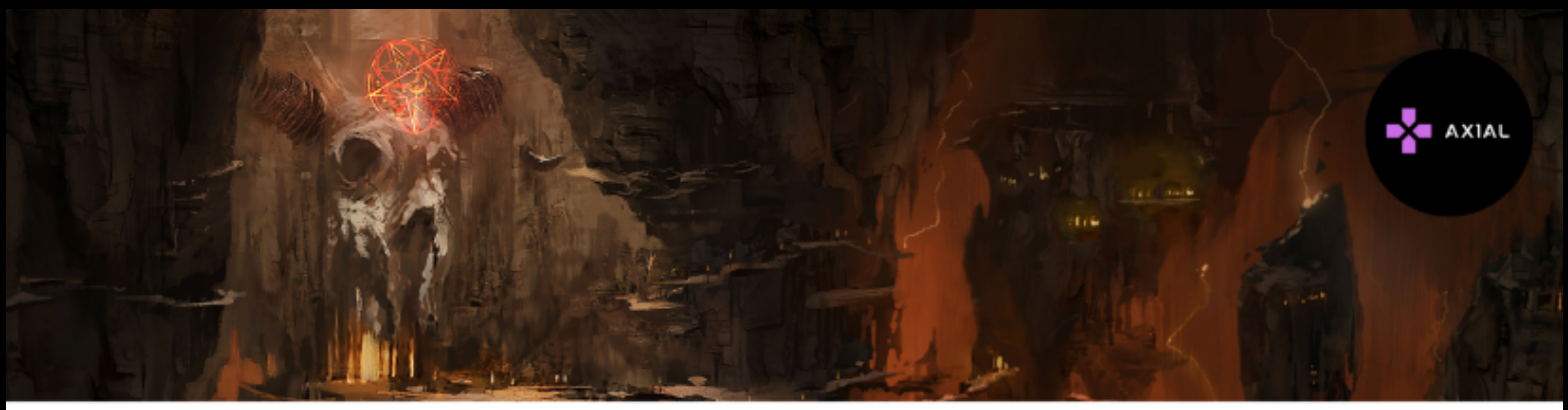
PUTTER PANDA

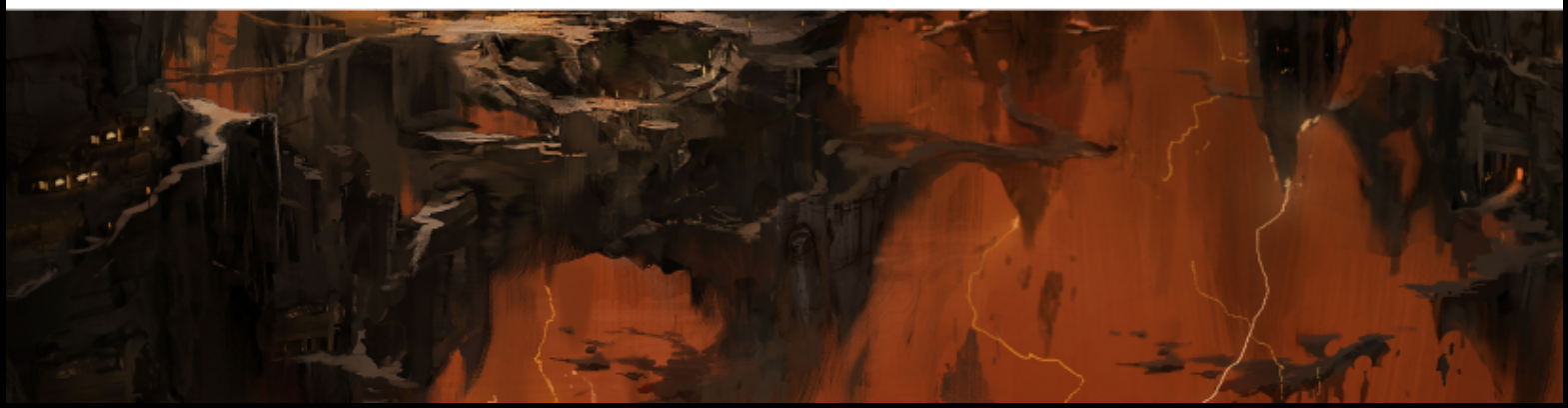


PUTTER PANDA // APT-2

CHINA

U.S. SATELLITE AND AEROSPACE SECTOR

CVE-2012-0158



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON PUTTER PANDA ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Putter Panda is a threat group based out of China , this group also goes by the name APT-2 and Group 36 .

II. TARGETS

Targets of this threat group is attributed to information theft and espionage on sectors like defense , government , research & technology.

III. METHODS USED

This group primarily uses spear phishing techniques .
This group has also been using 3PARA RAT.
This group has been using droppers based on RC4 & XOR .
This group also uses PNGDOWNE.R
This group also focuses on popular exploits against applications such as Adobe Reader and Microsoft Office .

IV. CAMPAIGNS

The campaigns of this threat group includes fake yoga brochure was one of different emails used for a spear-phishing .

This group has also been attributed to conducting large scale cyberespionage campaign targetting government entities , contractors and research companies in parts of Europe , US , Japan .

ATTRIBUTION

Putter Panda / APT-2 has ben linked to it's operation to the activity of the People's Liberation Armyof China , 3rd General Staff Depatment 12th Bereau Unit 61486.

CrowdStrike identified Chen Ping, aka cpyy, a suspected member of the Pla responsible for procurement of the domains associated with operations conducted by Putter Panda.

The threat group has infrastructure overlap with Comment Panda and evidence of interaction between actors ties to both the groups .

[cited from Volexity]

AX1AL

V. IOCS

Hashes
687424F0923dF9049CC3a56C685EB9a5
544FCa6EB8181F163E2768C81F2Ba0B3
8a2a6782e1af29ca8cb691cf0d29a0d
8c7b5501df060ccfc3aa5c8c41b452f

C2

hgcurtain.com
cultivr.com
tensins.net
decipherment.net
konamidata.com
cbssrayli.com
ctable.org

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Putter%20Panda%2C%20APT%202

https://attack.mitre.org/groups/G0024/

https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf