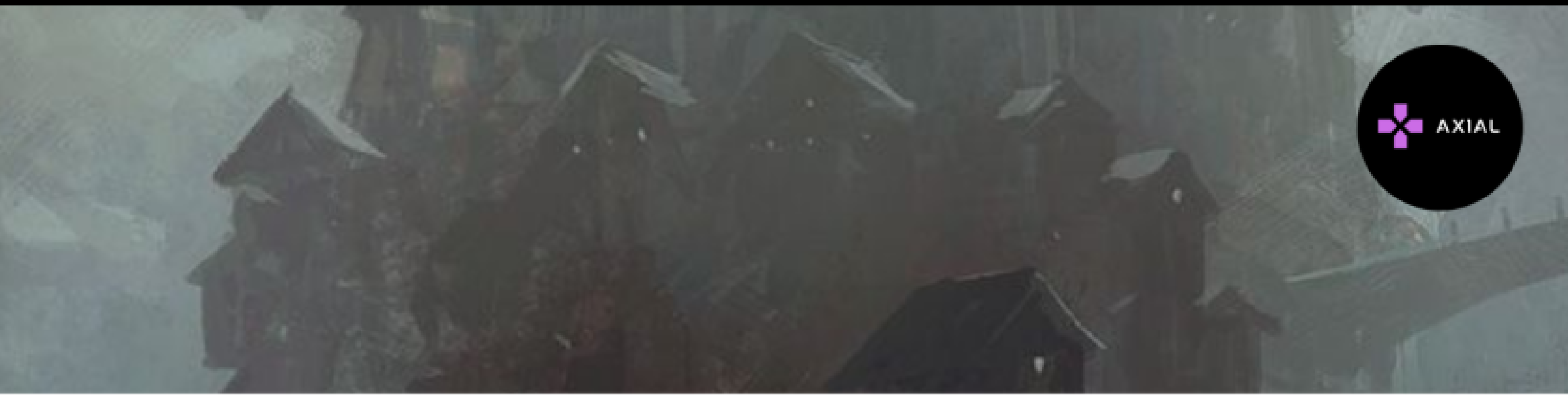
PLATINUM



PLATINUM

-

SOUTHEAST ASIA

EXPLOTING SOL

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Platinum is a threat group based out of China also known as TwoForOne and ATK 33.

II. TARGETS

Defense, Financial, Government,Telecommunications and Intelligenceagencies on multiple countries.

III. METHODS USED

The operators used WMI subscriptions to run an initial Powershelldownloader that, in turn, downloaded another small Powershell backdoor.We collected many initial WMI Powershell scripts and noticed that theyhad different, hardcoded command and control (CnC) addresses, differentencryption keys, salt for encryption (also different between eachinitial loader) and active hours (meaning the malware works only during acertain period of time every day). CnCs were located on free-of-chargehosting services and the attackers also made heavy use of many Dropboxaccounts (for storing the payload and exfiltrated data). The secondbackdoor in this APT killchain can perform a very limited set ofcommands: download or upload a file, run a Powershell script, andundertake the initial fingerprinting of a system.The operators have also been using Spear-Phishing techniques.The operators have also been using Titanium backdoor.

IV. CAMPAIGNS

Platinum is attributed to Operation Eastern Ropples

ATTRIBUTION

Platinum seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia.

[cited from Volexity]

V. IOCS

Hashes , Network & IPs

To be added

VI. REFRENCES

https://www.microsoft.com/security/blog/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/
https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Platinum
https://en.wikipedia.org/wiki/PLATINUM_(cybercrime_group)