

PLATINUM



PLATINUM



SOUTHEAST ASIA



EXPLOTING
SOL



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

- NERDS OF AXIAL

I. INTRODUCTION

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

IV. CAMPAIGNS

Platinum is attributed to Operation Eastern Ropples

II. TARGETS

Defense, Financial, Government, Telecommunications and Intelligence agencies on multiple countries.

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.

III. METHODS USED

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

[cited from Volexity]



V. IOCS

Hashes , Network & IPs

To be added

VI. REFERENCES

<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_\(cybercrime_group\)](https://en.wikipedia.org/wiki/PLATINUM_(cybercrime_group))

