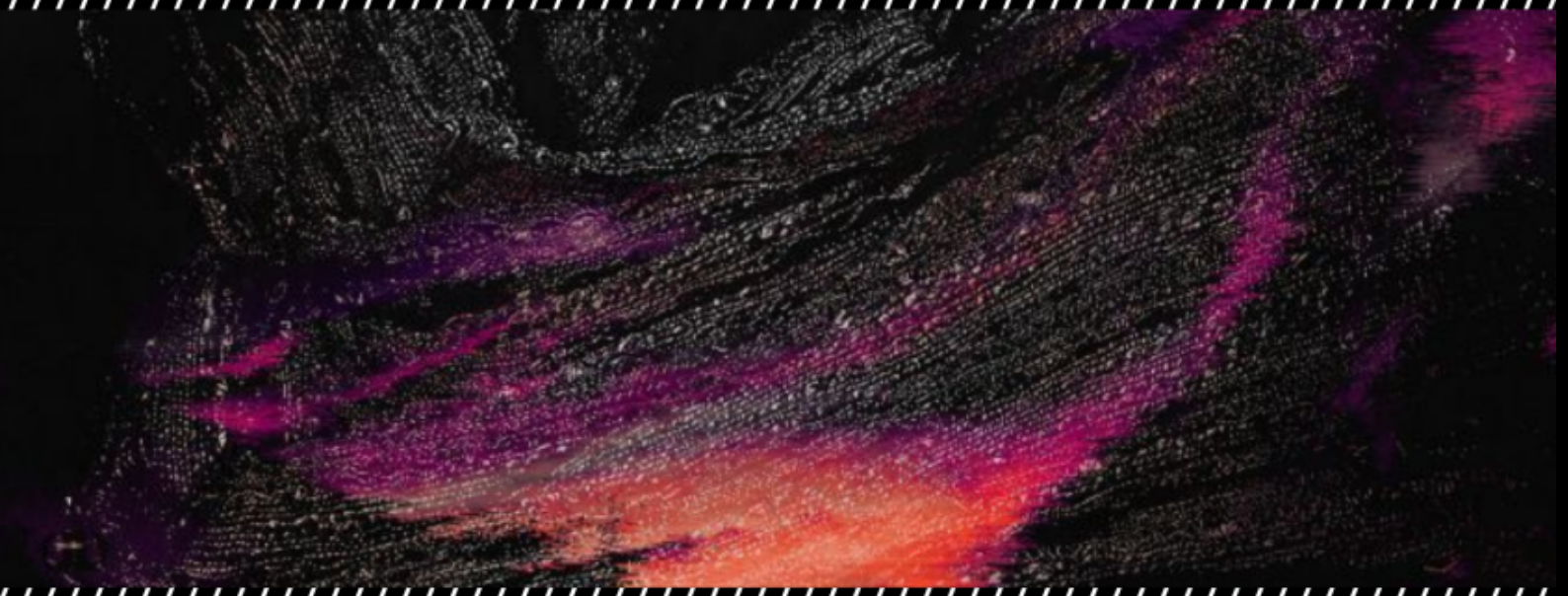
TAIDOOR

AXIAL



TAIDOOR

CHINA

TAIWAN

TAIDOOR BACKDOOR

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Taidoor is a threat group based out of China whose main motivations are information theft and espionage .

II. TARGETS

AGovernment sector , Taiwan.

III. METHODS USED

This group has been using several methods such as exploits , payloads , and decoy documents against their adversaries along with Taidoor Malware which uses ~dfds3.reg, to modify the Windows Registry in order to maintain persistence.

IV. CAMPAIGNS

This threat group has been linked to several campaigns involving Taidoor malware and attacking government sector of Taiwan .

ATTRIBUTION

The Taidoor attackers have been actively engaging in targeted attacks since at least March 4, 2009. Despite some exceptions, the Taidoor campaign often used Taiwanese IP addresses as C&C servers and email addresses to send out socially engineered emails with malware as attachments. One of the primary targets of the Taidoor campaign appeared to be the Taiwanese government. The attackers spoofed Taiwanese government email addresses to send out socially engineered emails in the Chinese language that typically leveraged Taiwan-themed issues. The attackers actively sent out malicious documents and maintained several IP addresses for command and control.

[cited from Trend Micro & ThaiCERT]

AX1AL

V. IOCS

Hashes (MD5)

2d33005a26a9cb2063dde2fa179b453e
85c64f43de8cb83234ee21fb0234f256
5eb86d098a5ab48c7173545829008636
95bfeb4b7b8edb2517ede938bf9791d9
5dd13efe319f0cdfe75346a46c1b791b
1de1a60f51829e5e0d30dfd4b5197a72
608bae3e4a59e4954f9bf43e504e2340
b80da571f2cd7eab4aec12eee8199289
0998743b808b57f6707641be64fa4fcd
265785ccc9503d30465156b90afa252
7488ffd5d9c1751d1ceca88a4231304
ecd97b7cfb4c8715d7800a9808a1646f
d39981092a2f9a4b40413b38917ca57
f43c9cc84fa7c16321241bb3c080276
f43c9cc84fa7c16321241bb3c080276

C&C Server
216.139.109.156
211.35.222.6
60.250.39.73
216.139.109.156
60.249.219.82
61.218.233.51
112.217.74.188

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Taidoor
Trend Micro Reports on Taidoor