

# DRAGONOK

DRAGONOK



CHINA



JAPAN



SPEAR PHISHING

AXIAL



AXIAL

---

# A SURVEY ON DRAGONOK ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

- NERDS OF AXIAL

## I. INTRODUCTION

DragonOk is a threat group based out of China whose main motivations include Information theft and espionage .

This group has been involved in campaign which involved five separate phishing attacks targtting Japanese high-tech variants .

The DragonOK campaign has previously [in 2014] targeted organizations in Taiwan, Japan, Tibet and Russia, and political organizations in Cambodia since at least January, 2017

## II. TARGETS

Attacks of this threat group ranges around high-tech and manufacturing based infrastructure onto multiple countries .

## ATTRIBUTION

As per cybersecurity expert Niklas Fermerstrand and based on his strong indicators the campaigns attributed to this threat group are an operation funded by China .

## III. METHODS USED

This group uses phishing attacks along with a different variant of malware known as Hellobridge a part of sysget malware family .

This group has also been using CVE-2015-1641 to leverage their exploits .

[cited from ThaiCERT]



## V. IOCS

---

### Malicious RTF Documents

020f5692b9989080b328833260e31df7aa4d58c138384262b9d7fb6d221e3673  
0d389a7b7dbdfdfcc9b503d0eaf3699f94d7a3135e46c65a4fa0f79ea263b40  
52985c6369571793bc547fc9443a96166e372d0960267df298221cd841b69545  
785398fedd12935e0ae5ac9c1d188f4868b2dc19fb4c2a13dab0887b8b3e220d  
941bcf18f7e841ea35778c971fc968317bee09f93ed314ce40815356a303a3ec  
ba6f3581c5bcdbe7f23de2d8034aaf2f6dc0e67ff2cfe6e53cfb4d2007547b30  
df9f33892e476458c74a571a9541aebef8d18b16278f594a6723f813a147552  
925880cc833228999ea06bd37dd2073784ab234ea00c5c4d55f130fe43a0940b  
3e4937d06ac86078f96f07117861c734a5fdb5ea307fe7e19ef6458f91c14264  
16204cec5731f64be03ea766b75b8997aad14d4eb61b7248aa35fa6b1873398b  
64f22de7a1e2726a2c649de133fad2c6ad089236db1006ce3d247c39ee40f578  
c3b5503a0a89fd2eae9a77ff92eef69f08d68b963140b0a31721bb4960545e07  
d227cf53b29bf0a286e9c4a1e84a7d70b63a3c0ea81a6483fdabd8fbccd5206  
9190b1d3383c68bd0153c926e0ff3716b714eac81f6d125254054b277e3451fe  
d321c8005be96a13affeb997b881eaba3e70167a7f0aa5d68eeb4d84520cca02  
d38de4250761cb877dfec40344c1642542ca41331af50fa914a9597f8cc0ee9b  
5a94e5736ead7ea46dbc95f11a3ca10ae86c8ae381d813975d71feddf14fc07a  
bbdc9f02e7844817def006b9bdef1698412efb6e66346454307681134046e595

### C2 Domains

www.dppline[.]org  
www.matrens[.]top  
europe.wikaba[.]com  
russiaboy.ssl443[.]org  
cool.skywave[.]top

## VI. REFERENCES

<https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=DragonOK>

<https://attack.mitre.org/groups/G0017/>

<https://unit42.paloaltonetworks.com/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/>

