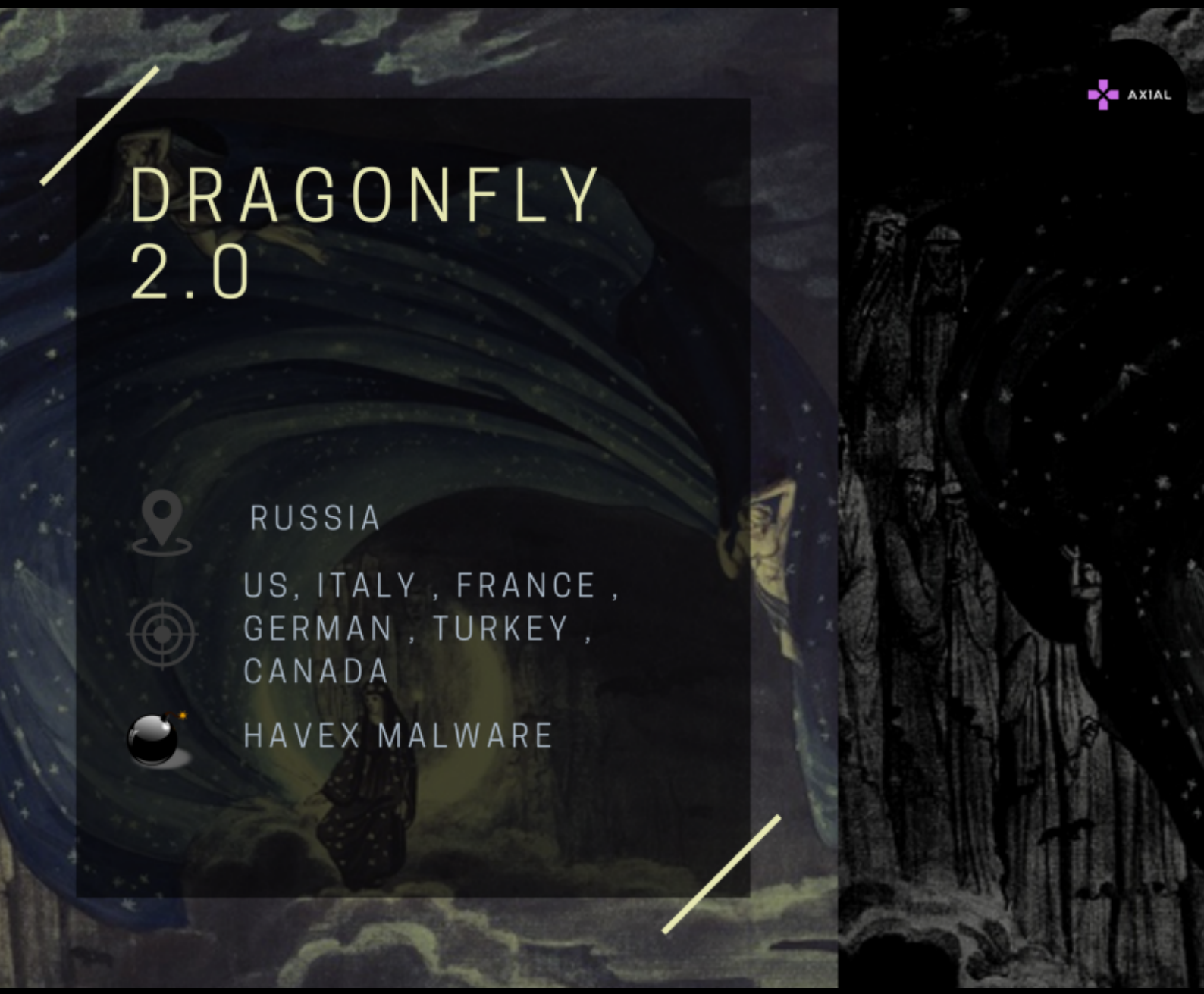
DRAGONFLY 2.0



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON DRAGONFLY 2.0 ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Dragonfly 2.0 also known as Berserk Bear or Dragonfly and other similar names is a Russian threat group .

II. TARGETS

Attacks of this threat group ranges around energy sector onto multiple countries .

III. METHODS USED

This group uses Living Off the land techniques .

This group has been using various types of scripting to perform operations, including Python scripts. The group was observed installing Python 2.7 on a victim .

This group has been using VPNs and Outlook Web Access (OWA) to maintain access to victim networks.

IV. CAMPAIGNS

This group has been involved in attack on nuclear facilities in the US on May 2017.
This group has been involved in attacks on critical infrastructure and energt companies around the world .

ATTRIBUTION

Dragonfly 2.0 is a suspected Russian group that has targeted government entities and multiple U.S. critical infrastructure sectors since at least March 2016. There is debate over the extent of overlap between Dragonfly 2.0 and Energetic Bear, Dragonfly, but there is sufficient evidence to lead to these being tracked as two separate groups.

[cited from ThaiCERT]

AX1AL

V. IOCS

Family	MD5	Command & Control
Backdoor.Dorshel	b3b5d67f5bbf5a043f5bf5d079dbcb56	hxxp://103.41.177.69/A56WY
Trojan.Karagany.B	1560f68403c5a41e96b28d3f882de7f1	hxxp://37.1.202.26/getimage/622622.jpg
Trojan.Heriplor	e02603178c8c47d198f7d34bcf2d68b8	
Trojan.Listrix	da9d8c78efe0c6c8be70e6b857400fb1	
Hacktool.Credrix	a4cf567f27f3b2f8b73ae15e2e487f00	
Backdoor.Goodor	765fcd7588b1d94008975c4627c8feb6	
Trojan.Phisherly	141e78d16456a072c9697454fc6d5f58	184.154.150.66
Screenutil	db07e1740152e09610ea826655d27e8d	

[cited from symantec for Dragonfly threat group] [Dragonfly 2.0 to be added]

VI. REFRENCES

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Berserk%20Bear%2C%20Dragonfly%202%2E0