DRAGONFLY

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Dragonfly also known as Energetic Bear or Dragonfly and other similar names is a russian state sponsored threat group .

II. TARGETS

Attacks of this threat group ranges around various sectors like Aviation, Construction, Defense, Education, Energy, Industrial, IT, Manufacturing, Oil and gas, Pharmaceutical onto multiple countries around the globe .

III. METHODS USED

This group uses spear phishing and emails which contain various malicious PDF attachment.
This group has also has been using waterhole attacks as one of their methods .
This group has been using trozanized software like Hello exploit Kit
This group has also been using Havex Malware.

IV. CAMPAIGNS

This group has been involved at spam campaign against energy sectors.
Thus group has been involved on energy companies in the Ukraine.
This group has been involved in the breach of EirGrid in the UK
This group has been involved with breach of San Francisco airport .
This group has also been involved with watering hole attacks on Turkish critical infrastructure

ATTRIBUTION

This group is attributed being one of the Russian state sponsored threat group as six GRU Officers charged in connection with worldwide deployment of destructive malware and other disruptive actions ,

These GRU hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort.

[cited from DOJ, US]

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]

VI. REFRENCES

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

https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

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