Energetic Bear, Dragonfly - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:54:10 UTC

APT group: Energetic Bear, Dragonfly

Names	Energetic Bear *(CrowdStrike)* Dragonfly *(Symantec)* Crouching Yeti *(Kaspersky)* Group 24 *(Talos)* Koala Team *(iSight)* Iron Liberty *(SecureWorks)* TG-4192 *(SecureWorks)* Electrum *(Dragos)* ATK 6 *(Thales)* ITG15 *(IBM)* Bromine *(Microsoft)* Ghost Blizzard *(Microsoft)* Blue Kraken *(PWC)* G0035 *(MITRE)*	
Country	Russia	
Sponsor	State-sponsored, GRU	
Motivation	Sabotage and destruction	
First seen	2010	
Description	Dragonfly is a cyberespionage group that has been active since at least 2011. They initially targeted defense and aviation comp sector in early 2013. They have also targeted companies related to industrial control systems. According to Kaspersky, Crouching Yeti has been operating since at least 2010 and has infected roughly 2,800 targets in 38 co education and pharmaceuticals. A similar group emerged in 2015 and was identified by Symantec as Berserk Bear, Dragonfly 2.0. There is debate over the ext and Dragonfly 2.0, but there is sufficient evidence to lead to these being tracked as two separate groups.	
Observed	Sectors: Aviation, Construction, Defense, Education, Energy, Industrial, IT, Manufacturing, Oil and gas, Pharmaceutical. Countries: Canada, France, Germany, Greece, Italy, Norway, Poland, Romania, Russia, Serbia, Spain, Turkey, UK, Ukraine, U	
Tools used	Commix, CrackMapExec, Dirsearch, Dorshel, Goodor, Havex RAT, Hello EK, Heriplor, Impacket, Industroyer, Inveigh, Kara PHPMailer, PsExec, SMBTrap, sqlmap, Subbrute, Sublist3r, Sysmain, Wpscan, WSO.	
Operations performed	Feb 2013	Spam campaign The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest met campaign, which saw selected executives and senior employees in target companies receive emails containing a emails had one of two subject lines: “The account” or “Settlement of delivery problem”. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_A
	Jun 2013	Watering Hole Attacks using Lightsout In June 2013, the attackers shifted their focus to watering hole attacks. They compromised a number of energy-r into each of them. This iframe then redirected visitors to another compromised legitimate website hosting the Li exploited either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim’s computer.
	Sep 2013	Watering Hole Attacks using Hello In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a exploit to use based on the information collected.
	2013	Trojanized software The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software pac providers were targeted and malware was inserted into the software bundles they had made available for downlo

	Feb 2014	LightsOut EK Targets Energy Sector Late last year, the story broke that threat actors were targeting the energy sector with Remote Access Tools and I seem that the attackers responsible for this threat are back for more. This particular APT struck late February bet <https://www.zscaler.com/blogs/research/lightsout-ek-targets-energy-sector>
	Dec 2015	Attack on Energy Companies in the Ukraine According to a statement posted this week on the official website of the Ukrainian security service SBU, Russiar malware on the networks of several regional power companies. The malicious software is said to have been disc The SBU said the attackers also flooded the targeted companies' technical support phone lines. The agency remc investigation. Just before Christmas, power outages were reported in the Ivano-Frankivsk Oblast region of Ukraine. The outag remotely tampered with automatic control systems. The power company responsible for the region also reported failure caused by a barrage of calls. <https://ssu.gov.ua/sbu/control/uk/publish/article?art_id=170951&cat_id=39574>
	2016	This report by Kaspersky Lab ICS CERT presents information on identified servers that have been infected and u includes the findings of an analysis of several webservers compromised by the Energetic Bear group during 201(<https://securelist.com/energetic-bear-crouching-yeti/85345/>
	Dec 2016	Power outage at Ukrenergo in the Ukraine Preliminary findings indicate that workstations and Supervisory Control and Data Acquisition (SCADA) system "North", were influenced by external sources outside normal parameters, Ukrenergo said in comments emailed t <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA> <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf> <https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>
	Apr 2017	Breach of EirGrid in the UK The breach of the Vodafone network allowed the hackers to create a type of wiretap known as Generic Routing E EirGrid's Vodafone router located in Shotton. <https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-
	May 2017	Watering Hole Attack on Turkish critical infrastructure Through our web crawling network, we were able to determine that a website belonging to a Turkish energy com attack targeting people associated with Turkish critical infrastructure. Compromised via a supply chain attack, th credential-harvesting malware. <https://www.riskiq.com/blog/labs/energetic-bear/>
	Mar 2020	Breach of San Francisco airport <https://www.zdnet.com/article/russian-state-hackers-behind-san-francisco-airport-hack/>
	Sep 2020	The Russian state-sponsored APT actor has targeted dozens of SLTT government and aviation networks, attempt organizations, successfully compromised network infrastructure, and as of October 1, 2020, exfiltrated data from <https://us-cert.cisa.gov/ncas/alerts/aa20-296a>
Counter operations	Oct 2020	Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Otl <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive
	Mar 2022	US charges 4 Russian govt employees with critical infrastructure hacks <https://www.bleepingcomputer.com/news/security/us-charges-4-russian-govt-employees-with-critical-infrastru
Information	<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks> <https://www.kaspersky.com/resource-center/threats/crouching-yeti-energetic-bear-malware-threat> <https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672> <https://exchange.xforce.ibmcloud.com/threat-group/388909715625410bd48078d0ddbc29c4>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0035/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format