Berserk Bear, Dragonfly 2.0 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:44:55 UTC

APT group: Berserk Bear, Dragonfly 2.0

Names	Berserk Bear *(CrowdStrike)* Dragonfly 2.0 *(Symantec)* Dymalloy *(Dragos)* G0074 *(MITRE)*	
Country	Russia	
Sponsor	State-sponsored, FSB Centre 16L: Radio-Electronic Intelligence on Communications Facilities, Post Number 71330	
Motivation	Sabotage and destruction	
First seen	2015	
Description	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.	
Observed	Sectors: Energy. Countries: Azerbaijan, Belgium, Canada, France, Germany, Italy, Norway, Russia, Singapore, Spain, Switzerland, Turkey, UK, Ukraine, USA.	
Tools used	Goodor, Impacket, Karagany, Phishery, Living off the Land.	
Operations performed	Dec 2015	Symantec has evidence indicating that the Dragonfly 2.0 campaign has been underway since at least December 2015 and has identified a distinct increase in activity in 2017. <https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>
	May 2017	Attack on nuclear facilities in the US Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy

		facilities, as well as manufacturing plants in the United States and other countries. Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week. <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html> <http://fortune.com/2017/09/06/hack-energy-grid-symantec/>
	May 2017	Attacks on critical infrastructure and energy companies around the world Since at least May 2017, Talos has observed attackers targeting critical infrastructure and energy companies around the world, primarily in Europe and the United States. These attacks target both the critical infrastructure providers, and the vendors those providers use to deliver critical services. Attacks on critical infrastructure are not a new concern for security researchers, as adversaries are keen to understand critical infrastructure ICS networks for reasons unknown, but surely nefarious. <https://blog.talosintelligence.com/2017/07/template-injection.html> <https://www.us-cert.gov/ncas/alerts/TA18-074A>
Information	<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0074/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
