EuRepoC

ADVANCED PERSISTENT THREAT profile

Energetic Bear

Associated APT designations

- **Berserk Bear/Energetic Bear** (CrowdStrike)
- **Dragonfly (2.0)** (Symantec)
- **Crouching Yeti** (Kaspersky)
- **G0035** (MITRE ATT&CK)

Sources: [1] [2] [3] [4]

Country of origin

Time period of activity

Since at least 2010

Sources: [8] [3] [9]

Political affiliations

The US and UK governments attribute Energetic Bear to the **Federal Security Service of the Russian Federation** (FSB RF; Russian Федеральная служба безопасности Российской Федерации [ФСБ РФ]), more specifically to **Center 16 (Military Unit 71330)**. Center 16 is believed to be the FSB's main structural unit for signals intelligence (SIGINT).

Sources: [5] [6] [7]

Agency type

State-integrated group (military intelligence service/agency members):
The **United States** Cybersecurity and Infrastructure Security Agency (CISA) and the **US Department of Justice (DoJ)** referred to Energetic Bear as a "**Russian state-sponsored APT actor**" ([10]), citing target selection and aimed intelligence-gathering as strong indicators ([5]). According to **Symantec**, Energetic Bear displays a sufficiently high degree of technical capability which also assumes that the group is able to draw on state resources, both human and material. Additionally, as reported by Crowdstrike, the target selection of the group seems to align very closely with the likely information collection priorities of the Russian foreign, domestic, and military intelligence services; the SVR, FSB and GRU respectively.

Sources: [3] [5] [10] [11] [12]

By Kerstin Zettl-Schabath, Timothy Gschwend and Camille Borrett

November 2022

Most frequent targets:

The main focus of the group appears to be the **Energy Sectors of various countries** and corresponding facilities that rely on *Industrial Control Systems (ICS)*

 **Canada**

 **France**

 **Germany**

 **Italy**

 **Spain**

 **Switzerland**

 **Turkey**

 **Ukraine**

 **US**

Sources: [3] [11] [13] [14]

Group composition/organisational structure

Energetic Bear as a group is likely much larger than the **three (official) members and potential external contractors (see Evgeny Viktorovich Gladkikh) named in the indictments**. Given that Center 16, of which Energetic Bear is a part of, very likely operates as the FSB's main SIGINT group, the total human resources it can deploy are likely substantial. However, since Energetic Bear primarily attracted attention with its reconnaissance tasks, which are technically demanding but not as demanding and elaborate as the tasks of other ATP groups attributed to the FSB, it is plausible that **Energetic Bear is smaller than, for example, the Turla group**.

Source: own assessment based on various sources in this document

Impact type(s)

Direct

- **Intelligence impact**
- **Economic impact**

Indirect

- Possibly ***n*th order physical effects:** attributed to another APT operation (IT industry experts suspect a causal connection to power outages in Ukraine in 2015 and 2016 that were attributed to Sandworm APT), where Energetic Bear may have conducted reconnaissance beforehand and passed on the information
- **Reputational Effects** (in the case of involvement in the **United States Federal Government Data Breach 2020**)

Sources: [8] [3] [15]

Incident type(s)

- **Intelligence gathering** (especially on the energy sector and access possibilities to Industrial Control Systems [ICS]/SCADA
- **Infiltration** via **spearphishing**
- **Watering-Hole-Attacks** or **Drive-by-Compromises**

EuRepoC codes: Hijacking with misuse; data theft

Sources: [8] [3] [5] [10]

Threat Level Index

7/24 moderate threat level

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the **sectorial** and **geographical scope** of the APT's attacks, the **intensity** of the attacks, the **frequency** of attacks and the **use of zero-days**. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here.

Breakdown of the scores for the Energetic Bear group:

Sub-indicator	Score	Explanation
Intensity of attacks	2 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	2 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. In the case of Energetic Bear, on average attacks attributed to the group within the EuRepoC database, targeted only one sector. However, as all attacks were against political systems and/or critical infrastructure, the score was therefore multiplied by 2.
Geographical scope of attacks	2 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of Energetic Bear, on average two countries were targeted per attack attributed to the group within the EuRepoC database.
Frequency of attacks	1 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. In the case of Energetic Bear, the group was responsible for less than 0.3 attacks per year of activity.
Exploitation of Zero days	0 /3	This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero days. The obtained score is then converted to a three-level scale. Energetic Bear did not make use of any zero-days during its period of activity.

→ Overall, the Energetic Bear group obtains a moderate-level threat score compared to other APT groups. The attacks analysed within the EuRepoC framework, had a relatively low intensity in terms of their physical and socio-political effects and were of low frequency, with no exploitation of zero-days.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

Basic attack pattern

According to Symantec, Energetic Bear attacks often follow the same pattern: the attackers install one or more backdoors in the victims' computers to gain remote access and install additional agents if necessary. The group is known for using **brute force** logins and stealthier approaches such as **masquerading operations**. However, Symantec argues that Dragonfly (its designation for activities related to Energetic Bear) – despite being an "accomplished" actor – is **not as technically-sophisticated as other FSB-affiliated groups**. The group is known for using more generally available malware and "living off the land" tools, indicating that they either lack the material/human resources or that they hope to **stay under-the-radar**. However, Symantec argues that, since 2017, Dragonfly may have entered a new phase, "with access to operational systems, access that could be used for more disruptive purposes."

Attack vector(s)

Energetic Bear used at least three infection tactics against targets in the energy sector:

(1) **E-mail campaigns** (*Oldrea or Karagany*)

(2) **Watering Hole Attacks** (*Hello Exploit Kit* in Java)

(3) **Trojanized Software**

Both the Dragonfly and Dragonfly 2.0 campaigns used these attack vectors. F-Secure lists spear **phishing attachment**, **drive-by compromise**, **valid accounts**, and **trusted relationship** as initial access tools.

Zero-Day exploits

Energetic Bear is not known to have used a zero-day exploit.

Malware used (non-exhaustive)

Havex Trojan	Backdoor.Oldrea	Trojan.Karagany (+ Trojan.Karagany.B)
PsExec	CrackMapExec	Trojan.Phisherly

Sources: [8] [3] [11] [14] [16] [17]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access

Drive-by compromise (*including for targeting industrial control systems*)
Exploit public-facing application
External remote services
Phishing
Spearphishing attachment
Supply chain compromise (*including for targeting industrial control systems)*
Valid Accounts

MITRE Persistence

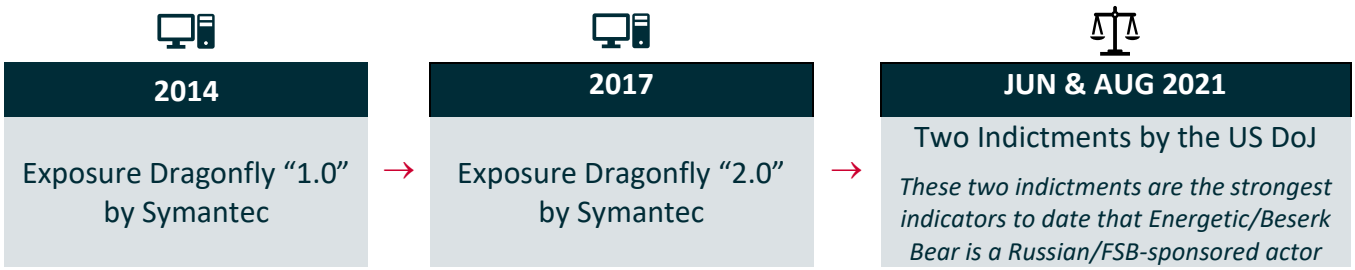
Account Manipulation

MITRE Defense Evasion

Hide Artifacts
Impair Defenses
Masquerading
Modify Registry

ATTRIBUTION

Attribution milestones



Sources: [3] [5] [11]

Attribution controversies

United States Federal Government Data Breach 2020 (unconfirmed):

Energetic Bear is a **prime suspect** in one of the United States' most severe cyberespionage incidents in history. Since the US Federal Government breach is closely connected to the SolarWinds Attack (as one of the **possible attack vectors**), the suspects between SolarWinds and the Federal Government Breach tend to overlap. US Investigators (FBI and CISA) and cybersecurity firms cite several possible perpetrators, among them **Energetic Bear** ([10]), **Cozy Bear** (**ATP29**) ([10.a]) and **Turla** ([10.b]). The FBI attributes SolarWinds to the **SVR**, which would point to APT29 ([10.c]), while not definitively ruling out contributions by other actors.

Sources: [10] [10.a] [10.b] [10.c]

Attribution-/detection sensitivity

Energetic Bear's **use of publicly-available tools** could be an attempt to **thwart attribution** and stay below the radar. Considering Energetic Bear's focus on reconnaissance, a high-priority interest in maintaining cover would fit with this detection evasion strategy. Based on the assumption that the threat actor has most likely been active since 2010 but was only detected in 2014 (after a dwell time of four years), this indicates an ability to evade detection and/or attribution.

Sources: [8] [11] [20]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

Two indictments (a total of four persons charged) – US Department of Justice, June and August 2021 against:

- ***Evgeny Viktorovich Gladkikh*** **(June 2021):** a computer programmer employed by an institute affiliated with the **Russian Ministry of Defence** has been charged for his "*role in a campaign to hack industrial control systems (ICS) and operational technology (OT) of global energy facilities using techniques designed to enable future physical damage with potentially catastrophic effects*". [5]
- ***Pavel Aleksandrovich Akulov Mikhail Mikhailovich Gavrilov, and Marat Valeryevich Tyukov*** **(August 2021):** three computer hackers, all of whom were residents and nationals of the Russian Federation (Russia) and officers in **Military Unit 71330 or "Centre 16" of the FSB,** charged with *"violating U.S. laws related to computer fraud and abuse, wire fraud, aggravated identity theft and causing damage to the property of an energy facility."* [5]

Arrest warrant – Federal Prosecutor General's Office of Germany, September 2021:

- **Pawel A. (September 2021):** In September 2021, the Federal Prosecutor General's Office in Germany (Karlsruhe) obtained an arrest warrant for **Pawel A.** The arrest warrant is not publicly available. Pawel A. is accused of compromising the infrastructure of the company NetcomBW in 2017. The APT group Berserk Bear, to which Pawel A. allegedly belongs, is also accused of attacking the company E.ON, one of the largest German electricity companies. It seems likely that **Pawel A. is the same individual** identified in the August 2021 DoJ indictment against **Pavel Akulov**. [5] [21]

Indicted individuals / sanctioned (associated) entities

- **Pavel Aleksandrovich Akulov (Павел Александрович Акулов),** 36 (Center 16) (Possibly same person as Pawel A., see above)
- **Mikhail Mikhailovich Gavrilov (Михаил Михайлович Гаврилов),** 42 (Center 16)
- **Marat Valeryevich Tyukov (Марат Валерьевич Тюков),** 39 (Center 16)
- **Evgeny Viktorovich Gladkikh,** 36 (private company; private contractor)

Sources: [5] [21]

Landmark incidents

Dragonfly Campaign 2010 – 2014:
Targeting of Western States' Energy Sectors.

Dragonfly-2.0 Campaign 2015 – 2019:
Targeting of Western States' Energy Sectors, especially in the United States, Switzerland, and Turkey.

United States Federal Government Data Breach 2020 (unconfirmed):
Energetic Bear is a **prime suspect** in one of the United States' most severe cyberespionage incidents in history. The 2020 attack (in the **context of SolarWinds**) infiltrated multiple US federal government institutions, including the US Treasury Department, the National Telecommunications and Information Administration, and the US Department of Commerce. Apart from entities in the United States, the group carried out operations aimed at NATO, the UK government, the European Parliament, and at least 200 more foreign organizations, stealing several gigabytes of data. The attackers most likely used multiple entry points, and US investigators estimate the group was active on the networks for eight to nine months before being detected. US investigators cite **Energetic Bear, Turla, and Cozy Bear** as possible perpetrators (see **Attribution Controversies**).

Sources: [3] [10] [14] [18] [19] [20]

SOURCES

[1] Crowd Strike (2013), *Global Threat Report, 2013 Year in review*. Available at: https://scadahacker.com/library/Documents/Threat_Intelligence/CrowdStrike%20-%20Global%20Threat%20Report%202013.pdf [Last accessed: 20.10.2022]

[2] Malpedia, *Energetic Bear*. Available at: https://malpedia.caad.fkie.fraunhofer.de/actor/energetic_bear [Last accessed: 02.11.2022]

[3] Symantec (2017), *Dragonfly: Western energy sector targeted by sophisticated attack group*. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks [Last accessed: 20.10.2022]

[4] Kaspersky, *Crouching Yeti (Energetic Bear) Malware*. Available at: https://www.kaspersky.com/resource-center/threats/crouching-yeti-energetic-bear-malware-threat [Last accessed: 02.11.2022]

[5] US Department of Justice (2022), *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide*. Available at: https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical [Last accessed: 02.11.2022]

[6] US Congressional Research Service (2022), *Russian Cyber Units*, In Focus. Available at: https://crsreports.congress.gov/product/pdf/IF/IF11718 [Last accessed: 02.11.2022]

[7] UK Foreign, Commonwealth and Development Office (2022), *Russia's FSB malign activity: factsheet*. Available at: https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet [Last accessed: 02.11.2022]

[8] MITRE (2022), *Dragonfly*. Available at: https://attack.mitre.org/groups/G0035/ [Last accessed: 02.11.2022]

[9] Cybersecurity Help (2022), *The story of the four bears: Brief analysis of APT groups linked to the Russian government (Part 4)*. Available at: https://www.cybersecurity-help.cz/blog/2512.html [Last accessed: 02.11.2022]

[10] US Cybersecurity and Infrastructure Security Agency (2020), *Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets*. Available at: https://www.cisa.gov/uscert/ncas/alerts/aa20-296a [Last accessed: 02.11.2022]

[10a] Ellen Nakashima (2020), *Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm*, Washington Post. Available at: https://web.archive.org/web/20201213220635/https:/www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html [Last accessed: 02.11.2022]

[10b] Kaspersky (2021), *Sunburst backdoor – code overlaps with Kazuar*. Available at: https://securelist.com/sunburst-backdoor-kazuar/99981/ [Last accessed: 02.11.2022]

[10c] FBI Director Christopher Wray (2021), *Statement Before the House Judiciary Committee*. Available at: https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-061021 [Last accessed: 02.11.2022]

[11] A L Johnson (2014), *Dragonfly: Western Energy Companies Under Sabotage Threat*. Available at: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments [Last accessed: 02.11.2022]

[12] Crowd Strike (2015), *Falcon Intelligence Datasheet May 2015*. Available at: https://www.crowdstrike.com/wp-content/brochures/falcon-intel/FalconIntelDatasheetMay2016.pdf [Last accessed: 02.11.2022]

[13] Cyware (2020), *Berserk Bear APT Penetrates German Infrastructure via Supply Chain Attacks*. Available at: https://cyware.com/news/berserk-bear-apt-penetrates-german-infrastructure-via-supply-chain-attacks-f790a4d5 [Last accessed: 02.11.2022]

[14] F-Secure (2019), *The State of the Station: A report on attackers in the energy industry*. Available at: https://blog-assets.f-secure.com/wp-content/uploads/2019/04/15105531/F-Secure_energy_report.pdf [Last accessed: 02.11.2022]

[15] Pierluigi Paganini (2017), *Dragonfly 2.0: the sophisticated attack group is back with destructive purposes*. Available at: https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html [Last accessed: 02.11.2022]

[16] Kaspersky Lab (2018), *Energetic Bear — Crouching Yeti*. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf [Last accessed: 02.11.2022]

[17] Joe Slowik (2021), *The Baffling Berserk Bear: A decade's activity targeting critical infrastructure*. Available at: https://vblocalhost.com/uploads/VB2021-Slowik.pdf [Last accessed: 02.11.2022]

[18] Mara Hvistendahl, Micah Lee, Jordan Smith (2020), *Russian Hackers Have Been in Austin City Networks for Months, The Intercept*. Available at: https://theintercept.com/2020/12/17/russia-hack-austin-texas/ [Last accessed: 02.11.2022]

[19] US Cybersecurity and Infrastructure Security Agency (2020), *Emergency Directive 21-01- Mitigate SolarWinds Orion Code Compromise*. Available at: https://www.cisa.gov/emergency-directive-21-01 [Last accessed: 02.11.2022]

[20] Kaspersky (2018), *Energetic Bear/Crouching Yeti: attacks on servers*. Available at: https://securelist.com/energetic-bear-crouching-yeti/85345/ [Last accessed: 02.11.2022]

[21] Hakan Tanriverdi, Florian Flade (2022), *Spionage im Stromnetz: "Russland ist in unseren Netzen"*, Tagesschau. Available at: https://www.tagesschau.de/investigativ/br-recherche/stromnetz-hacker-russland-101.html [Last accessed: 02.11.2022]

Calculations for the Threat Level Index Indicator are based on version 1.0 of the EuRepoC Database downloadable here: https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Global_Database_1_0_22d4a4aee7.xlsx

Last updated: 05.12.2022