



ENERGETIC BEAR

THREAT ACTOR

PROFILE

SEP 11ND, 2025

TLP:GREEN Free Version

Stay updated: subscribe to our intelligence feeds for real-time updates on APT activity and emerging cyber threats. Reach out to our team at commercial@malwarepatrol.net or visit our website: <https://malwarepatrol.net/>

STATUS

Active. Energetic Bear continues to operate and adapt its tactics.

KNOWN ALIASES

ALLANITE, ATK6, BERSERK BEAR, Blue Kraken, BROMINE, CASTLE, Crouching Yeti, Dragonfly, DYMALLOY, G0035, Ghost Blizzard, Group 24, Havex, IRON LIBERTY, ITG15, Koala Team, TG-4192, or ENERGETIC BEAR.

ATTRIBUTION AND ASSOCIATIONS

- **Russian Federation:** Strong evidence linking Energetic Bear to the Russian Federation and its intelligence agencies (SVR, FSB).

OPERATIONAL MODEL

- **State-Sponsored Espionage:** Energetic Bear operates as a state-sponsored group with a focus on intelligence gathering, not financial gain.
- **Long-Term Persistence:** Demonstrates a commitment to maintaining long-term access to target systems.



Energetic Bear (also known by numerous aliases) is a sophisticated, state-sponsored cyber espionage group primarily focused on intelligence gathering. They are consistently linked to the Russian Federation and have demonstrated capabilities in targeting critical infrastructure sectors. Their operations are characterized by long-term persistence, stealth, and a focus on exfiltrating sensitive information rather than causing widespread disruption, though disruption has occurred as a side effect.



TARGETING AND VICTIMS

- **Energy Sector:** Primary target, including power plants, wind farms, and oil & gas facilities.
- **Critical Infrastructure:** Targets extending to transportation, defense, and manufacturing industries.
- **Geographic Locations:** Primarily United States, Europe (Germany, Ukraine, UK, France), and Ukraine.
- **Market Sectors:** Critical Manufacturing, Energy, Government.



HISTORICAL CONTEXT

- **2012:** Initial discovery of the Dragonfly malware, marking the start of their known operations.
- **2014-2015:** Targeted European energy companies with the Dragonfly/Havex malware, seeking to gain access to industrial control systems (ICS).
- **2015:** Discovery of the Kostovox/DYMALLOY malware, a sophisticated ICS malware targeting wind farms.
- **2017:** Continued targeting of energy and industrial sectors in Europe and the US.
- **2018:** Continued operations and attribution to Russian state actors.
- **2019:** Increased focus on critical infrastructure, including US critical infrastructure.
- **2021:** Continued targeting of critical infrastructure sectors, demonstrating persistence and adaptability.
- **2022:** Focused on supply chain attacks targeting industrial control system vendors.
- **2023-Present:** Recent activities demonstrate a focus on gaining access to information related to critical infrastructure, demonstrating continued activity.



TECHNICAL PROFILE

Malware and Tools

- **Dragonfly/Havex:** An early ICS malware platform used to compromise industrial control systems. Used for reconnaissance and data exfiltration.
- **Various Custom Tools:** Energetic Bear utilizes a variety of custom-built tools for reconnaissance, privilege escalation, and lateral movement, often tailored to specific targets.
- **Binary Padding:** Techniques to evade detection, by padding malware binaries.

Infrastructure

- **Compromised Servers:** Command-and-control (C2) servers are often hosted on compromised servers located in various countries, making attribution challenging.
- **Spearphishing:** Email campaigns utilizing malicious attachments or links to deliver initial malware payloads.
- **Supply Chain Compromise:** Targeting software vendors and integrating malicious code into legitimate software updates.
- **Dynamic Resolution:** Malware dynamically resolves C2 infrastructure to avoid static IP addresses and domain names.

RECENT DEVELOPMENTS

- **2023:** Continued focus on ICS vendors and supply chain attacks.
- **2023:** Adaptation of malware to evade detection by updated security solutions.
- **2023:** Observed use of more sophisticated obfuscation techniques.

INTELLIGENCE GAPS

- The specific Russian intelligence agencies responsible for directing and funding Energetic Bear remain somewhat unclear.
- The full extent of Energetic Bear's global targeting remains unknown.
- The specific vulnerabilities exploited by Energetic Bear and their methods for discovering them require more research.

Tactics, Techniques, and Procedures (TTPs)

- **T1566 - Phishing: Spearphishing campaigns** to gain initial access.
- **T1082 - System Information Discovery:** Gathering information about the target system. (MITRE ATT&CK ID: T1082)
- **T1016 - System Network Configuration Discovery:** Discovering network configurations. (MITRE ATT&CK ID: T1016)
- **T1059.001 - Command and Scripting Interpreter:** Leveraging scripting interpreters like PowerShell for reconnaissance and execution. (MITRE ATT&CK ID: T1059.001)
- **T1071.001 - Application Layer Protocol:** Using common application layer protocols (e.g., HTTP, HTTPS) for C2 communication. (MITRE ATT&CK ID: T1071.001)
- **T1574 - Hijack Execution Flow:** Employing techniques to redirect the execution flow of legitimate processes to execute malicious code.
- **T1027 - Obfuscated Files or Information:** Obfuscating files or information to avoid detection.
- **T1218.011 - Signed Binary Proxy Execution:** Using signed binaries to proxy execution and evade detection.

DEFENSE AND MITIGATION GUIDANCE

- **Network Segmentation:** Segment critical infrastructure networks to limit the impact of potential breaches.
- **Multi-Factor Authentication (MFA):** Implement MFA for all user accounts.
- **Patch Management:** Maintain rigorous patch management processes to address known vulnerabilities.
- **Endpoint Detection and Response (EDR):** Deploy EDR solutions to detect and respond to suspicious activity.
- **Regular Security Audits:** Conduct regular security audits to identify and remediate vulnerabilities.

DETECTION GUIDANCE

- **Monitor Network Traffic:** Monitor network traffic for unusual activity, such as connections to known malicious IP addresses or domains.
- **Analyze System Logs:** Analyze system logs for suspicious events, such as unauthorized access attempts or unusual process executions.
- **Implement Intrusion Detection Systems (IDS):** Deploy IDS to detect and alert on known attack patterns.
- **Scan Endpoint for Anomalous Processes:** Scan endpoints for the presence of malicious processes and files.

IOCS - INDICATORS OF COMPROMISE

FULL LIST OF IOCS AVAILABLE TO
MALWARE PATROL CUSTOMERS ONLY

IOCS - INDICATORS OF COMPROMISE

FULL LIST OF IOCS AVAILABLE TO
MALWARE PATROL CUSTOMERS ONLY

IOCS - INDICATORS OF COMPROMISE

FULL LIST OF IOCS AVAILABLE TO
MALWARE PATROL CUSTOMERS ONLY

IOCS - INDICATORS OF COMPROMISE

FULL LIST OF IOCS AVAILABLE TO
MALWARE PATROL CUSTOMERS ONLY

Although the information provided in this report has been produced and processed from sources believed to be reliable, no warranty expressed or implied is made regarding its accuracy, adequacy, completeness, legality, reliability or usefulness. This disclaimer applies to both isolated and aggregate uses of the information. Malware Patrol provides this information on an "AS IS" basis. All warranties of any kind, express or implied, including but not limited to the IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, freedom from contamination by computer viruses and non-infringement of proprietary rights ARE DISCLAIMED. Changes may be periodically added to the information herein; these changes may or may not be incorporated in any new version of the publication. If the user has obtained information from Malware Patrol from a source other than Malware Patrol, the user must be aware that electronic data can be altered subsequent to original distribution. Data can also quickly become out-of-date. It is recommended that the user pay careful attention to the contents of any metadata associated with a file, and that the originator of the data or information be contacted with any questions regarding appropriate use. If the user finds any errors or omissions, we encourage the user to report them to Malware Patrol



 [MALWAREPATROL.NET](https://malwarepatrol.net)

 +1 813 321 0987