Dragonfly APT Group

Name: Dragonfly
Also known as: Berserk Bear, Blue Kraken, Koala Team, Energetic Bear, Crouching Yeti, TG-4192
Type: Advanced Persistent Threat (APT)
Origin: Russian Federation
Period of activity: Approximately 2010–2011 to present day

Energetic Bear/Crouching Yeti is a well-known APT group that has been active since at least 2010. The group primarily targets organizations in the energy and industrial sectors. Victims of Energetic Bear/Crouching Yeti operations have been identified worldwide, with a notable concentration in Europe and the United States. During 2016–2017, the number of attacks targeting companies in Turkey increased significantly.

The group’s primary tactics include phishing campaigns using malicious documents, as well as the compromise of various servers. Some compromised servers are used as supporting infrastructure to host tools and store operational logs. Others are specifically compromised to facilitate watering hole attacks and serve as an entry point to reach intended targets.

Although documented attacks did not result in direct disruption of operational technology (OT) systems, their structure, target selection, and technical execution suggest potential preparation for operations capable of affecting the economic activities of other countries. The scale and sophistication of these tactics demonstrate a high level of operational maturity and align with the profile of a state-sponsored APT actor.

Available evidence, including criminal indictments issued by the U.S. Department of Justice and the nature of the group’s target selection, indicates links between Dragonfly and Russian state entities. Taken together, these factors support the assessment that the group’s activities form part of a broader strategy of cyber intelligence gathering and preparation for potential operations against critical infrastructure.

Activities

Compromise and Infection of Servers Worldwide (2014 – Early 2017)

An analysis by Kaspersky Lab[1] provides information on servers infected and used by the group, as well as the results of an investigation into web servers compromised by Energetic Bear.

Victims:

- Turkey (industrial enterprises, an oil holding company, and hospitality sector resources);
- Ukraine (a bank and an energy company were compromised);
- United Kingdom (malware was deployed within an aerospace company);
- Germany (a software developer and systems integrator was targeted);
- Greece (a university server was attacked);
- United States (an oil and gas company was targeted).

Compromise of watering hole servers followed a consistent pattern: a reference such as file://IP/filename.png was embedded into a web page or JavaScript file. This reference triggered a request for an image, causing the user to connect to a remote SMB server. The objective of this attack was to collect information from the session, including the victim's IP address, username, domain, and NTLM password hash. The image referenced in the request did not actually exist on the remote server.

In some cases, compromised servers were subsequently used to attack other resources. During the investigation of infected systems, numerous websites and servers were identified as having been scanned by the attackers using tools such as Nmap, Dirsearch, SQLMap, and others. These targets did not share a common theme, and the criteria used to select them were not immediately apparent. It is most likely that the majority of these scans were conducted to identify potential footholds for hosting attacker infrastructure and facilitating future operations.

Dragonfly Attacks on the U.S. Energy Sector (2014–2017)

The names of the affected companies have been intentionally replaced with generic designations (e.g., Company "One", Company "Three", etc.), as the identities of the victims are not essential for understanding the technical aspects of the attacks. The primary focus is on the tactics and techniques employed rather than on specific organizations.

This approach is also consistent with responsible disclosure practices and helps avoid unnecessary reputational risks for the affected entities. (Source)

List of Victims:

1. Nuclear Regulatory Commission (NRC) – a U.S. government agency responsible for regulating organizations that use nuclear materials, including nuclear power plants;

2. Wolf Creek Nuclear Operating Corporation (Wolf Creek) – a company based in Burlington, Kansas, that operates the Wolf Creek Generating Station nuclear power plant;

3. Westar Energy Inc. – a Kansas-based company that was one of the owners of Wolf Creek during the conspiracy;

4. Kansas Electric Power Cooperative (KEPCO) – a member-owned, non-profit electric generation and transmission cooperative based in Kansas that was also one of the owners of Wolf Creek during the conspiracy;

5. Company “One” – a data storage company located in the U.S. Midwest;

6. Company “Three” – a commercial construction company located in Michigan;

7. Company “Four” – a renewable energy company based in New York;

8. Company “Five” – a renewable energy company based in New England;

9. Company “Six” – an Illinois-based media company that publishes magazines and websites focused on manufacturing, oil and gas, and industrial control systems engineering;

10. Company “Seven” – a Pennsylvania-based company providing digital high-definition cable television and high-speed internet services;

11. Company “Eight” – an energy company located in Illinois;

12. Company “Nine” – an energy company located in Ohio;

13. Company “Ten” – a U.S. company specializing in consulting services for nuclear energy providers;

14. One of the victim organizations located outside the United States was Company “Two”, a global SCADA and industrial automation company.

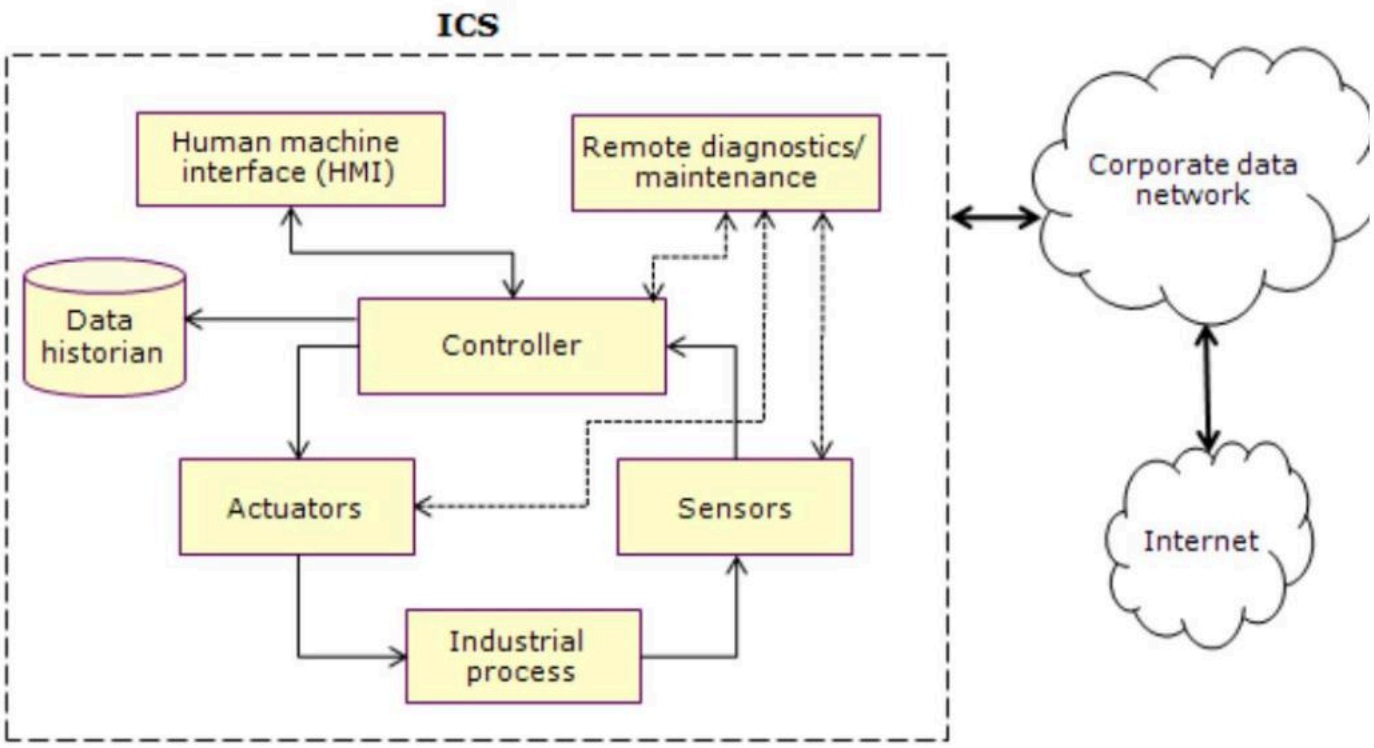
During both phases of the campaign, the primary targets were Industrial Control Systems (ICS) and their SCADA components, which are used to collect data, monitor operations, and control equipment within energy sector facilities.

Havex Phase

During the first phase, the attackers focused on compromising software vendors and suppliers serving the ICS/SCADA sector. They embedded the Havex malware into legitimate software updates, causing malicious code to be distributed alongside official installation packages. Havex enabled the creation of backdoors and provided remote access to compromised systems, allowing the attackers to collect information about networks, devices, and users.

SCADA (Supervisory Control and Data Acquisition) is a subsystem within ICS that:

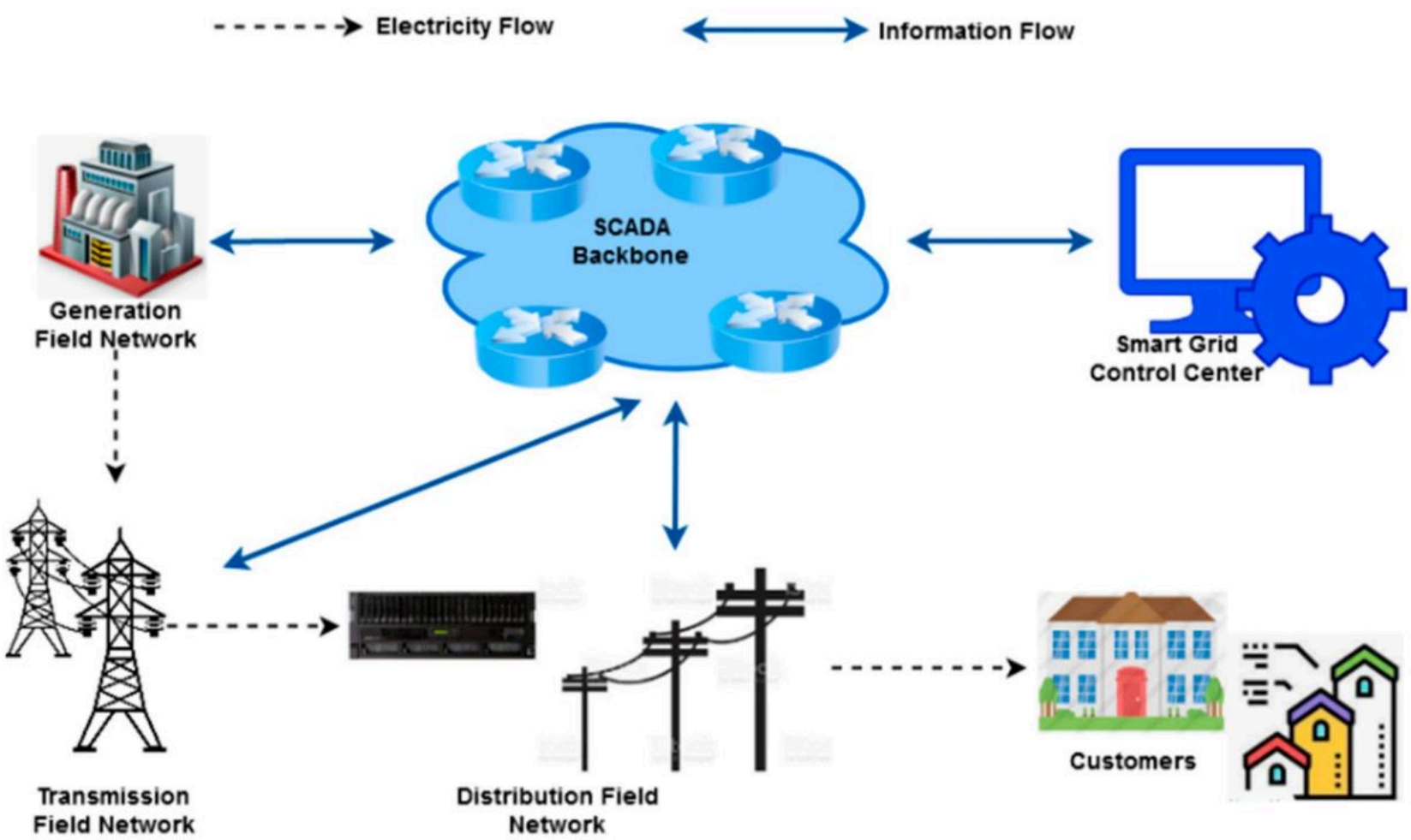
- collects data from equipment;
- presents that data to operators;
- enables operators to monitor and control industrial processes.



To manage their infrastructure, the attackers used compromised servers as proxies. For example, a server belonging to Company “One” was used between 2012 and 2013 to route traffic and support command-and-control (C2) infrastructure. Numerous domains hosting Havex administration panels were created and managed through this server.

The group also conducted active reconnaissance of its targets. Attackers investigated web resources belonging to organizations in the energy sector, including those associated with the nuclear industry. To gain access to information, they used SQL injection attacks, which allowed them to read and modify database contents and execute administrative commands.

In a separate operation, the attackers compromised a SCADA software vendor (Company “Two”). They gained access to internal data, server configurations, and administrator accounts. Following the compromise, they downloaded BIOS files and drivers, which were later used in malware deployment activities.



Between 2013 and 2014, Havex was embedded into drivers produced by this vendor and made available for public download. Once installed, these drivers automatically connected to attacker-controlled command-and-control (C2) servers. One such case was identified on the SCADA system of a power generation facility.

Dragonfly 2.0 Phase

During the second phase, the attacks became significantly more targeted. The primary focus shifted to specific energy sector companies and engineers working with ICS/SCADA systems.

The attackers employed:

- phishing campaigns;
- compromise of servers and their use as operational footholds;
- compromise of websites frequently visited by engineers;
- exploitation of vulnerabilities enabling remote code execution.

After gaining access to networks (for example, that of Company “Three”), the attackers created administrator accounts with names resembling legitimate system accounts (such as MS_AutoUP, SYSTEM_USER, and similar) in order to remain undetected. These accounts were then used to establish RDP access and create corporate email accounts.

Phishing emails were then sent from these accounts, disguised as job applications. Documents such as “Controls Engineer.docx” contained malicious code:

From: Kevin North [redacted]
To: [redacted]
Date: 5/5/2017 8:58:01 AM
Subject: CV Kevin North
Attachments CV Controls Engineer.docx

Hello

Over 10 years Controls/Software Experience

Software development for PLC based control systems:
SIEMENS S5, S7-200, S7-300, S7-400 series,
Rockwell 5000, 500 series.
SCADA, HMI configuration.

Various Conveyor system experiences
Networking with PLC's: Ethernet, PROFIBUS-DP, PROFINET MPI, ASI, DeviceNet, DH+
EPLAN

Multi – skilled controls engineer with experience in hands-on project based work. Experience ranges from budget estimate and man engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,

Kevin North

After opening the document, the file initiated a connection to an attacker-controlled server via SMB and transmitted credential hashes. If the network did not block such connections, the attackers could recover passwords through brute-force attacks and use them to gain access to systems.

At the same time, the group compromised websites belonging to energy companies and injected malicious JavaScript designed to steal visitors’ credentials. Once access to victim networks was obtained, the attackers deployed tools to maintain control. Among them was the Goodor backdoor, which provided persistent access and communication with command-and-control (C2) servers.

This enabled the attackers to:

- move laterally across the network (between computers);
- escalate privileges (vertical movement);
- gain access to critical systems and sensitive information.

To collect credentials, the attackers extensively used SMB-based attacks, including specially crafted shortcuts and scripts that transmitted password hashes without requiring a file to be opened—simply viewing the folder was sufficient.

Attack on Wolf Creek[4]

In 2017, the attackers conducted an operation against Wolf Creek. Initial access was obtained through a phishing campaign. After compromising an account, they repeatedly logged into the environment, established persistence, and uploaded malicious files.

The following were deployed within the network:

- backdoors;
- credential-harvesting scripts;
- tools designed to facilitate further propagation.

The attackers also used SMB-based attacks to obtain additional credentials. They successfully compromised more accounts and expanded their presence within the network. In addition, they compromised websites belonging to energy companies, injecting malicious code through phishing techniques and CMS vulnerabilities, enabling them to harvest credentials from other users within the sector.

Conclusion

Overall, Dragonfly’s operation against U.S. energy companies did not achieve its primary objective of gaining control over ICS/SCADA systems and carrying out sabotage. The attackers were able to compromise corporate IT networks through phishing campaigns and credential harvesting, which allowed them to conduct reconnaissance of internal infrastructure. However, critical control systems remained isolated through network segmentation, preventing movement into the operational technology (OT) environment.

The attack was detected in a timely manner, and U.S. cybersecurity authorities responded, limiting the attackers’ ability to advance further within the targeted networks. As a result, no physical damage or operational disruption was reported.

This incident is widely regarded as an example of the preparatory phase of a sophisticated APT operation aimed at enabling future influence over critical infrastructure. While the attackers achieved partial success in gathering intelligence and expanding access within corporate networks, they failed to accomplish their strategic objective.

Primary Targets:

- Energy sector (power grids, nuclear power plants, oil and gas infrastructure)
- Industrial control systems (ICS/SCADA)
- Defense and aerospace industries
- Government organizations

Motivation:

- Cyber espionage and intelligence collection
- Gaining access to critical systems
- Potential sabotage of critical infrastructure

Key Individuals

Marat Tyukov, Mikhail Gavrilov, Pavel Akulov, and Yevgeny Viktorovich Gladkikh were officers of the FSB’s Center 16. According to the U.S. Department of Justice, they participated in a campaign conducted between 2012 and 2017 targeting government entities, including the U.S. Nuclear Regulatory Commission (NRC), as well as Wolf Creek Nuclear Operating Corporation, the operator of a nuclear power plant in Kansas.

SHUM

Yevgeny Viktorovich Gladkikh
Євгеній Вікторович Гладких

Place of Birth: Russia
Hair: Brown
Eyes: Brown
Height: Approximately 185 cm (6 ft 1 in)
Weight: Approximately 84 kg (185 lbs)
Sex: Male
Race: White
Citizenship: Russian

From at least August 2014 through July 2018, Yevgeny Viktorovich Gladkikh allegedly conspired with, among others, the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), the Center for Applied Developments, and other co-conspirators to conduct computer intrusions targeting energy facilities and oil refineries in the United States and abroad and to cause damage to those facilities.

Gladkikh and his co-conspirators allegedly agreed to and did infiltrate operational technology (OT) networks and safety systems in order to deploy malware designed to disable physical safety systems or cause them to operate in an unsafe manner.

In June 2021, a federal arrest warrant for Gladkikh was issued by a U.S. District Court after he was charged with conspiracy to damage an energy facility, attempted damage to an energy facility, conspiracy to access protected computers and obtain information, and intentional damage to protected computers through the knowing transmission of data.

Pavel Aleksandrovich Akulov
Павло Олександрович Акулов / Павел Александрович Акулов

Place of Birth: Russia
Hair Color: Blonde
Eye Color: Blue
Sex: Male
Race: White
Citizenship: Russian
Date of Birth: July 2, 1985

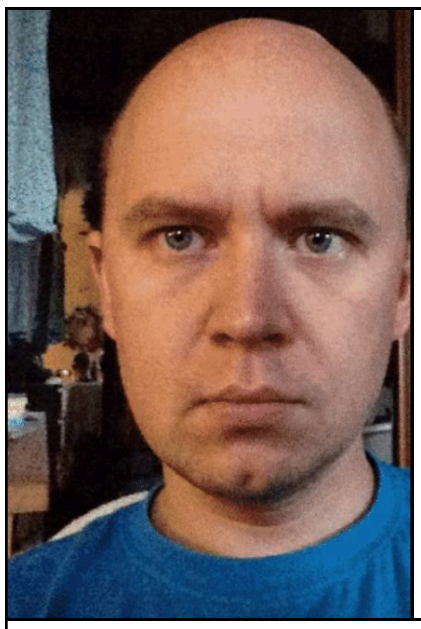
Akulov is an officer of the Russian Federal Security Service (FSB) who conspired with others to obtain and maintain unauthorized persistent access to hundreds of U.S. and international energy companies, thereby enabling the Russian government to disrupt and damage such facilities.Akulov is a member of an FSB unit known as Center 16 and, as of 2013, held the rank of lieutenant and worked in an operational group known as Military Unit 71330.

U.S. authorities charged him with computer intrusion, wire fraud, and aggravated identity theft.

Akulov conducted online reconnaissance in support of customer phishing campaigns, including reconnaissance supporting the customers' targeted attacks against and unauthorized access to the Wolf Creek computer network.

Support the organization's activities: https://donate.shum-ng.org/

SHUM

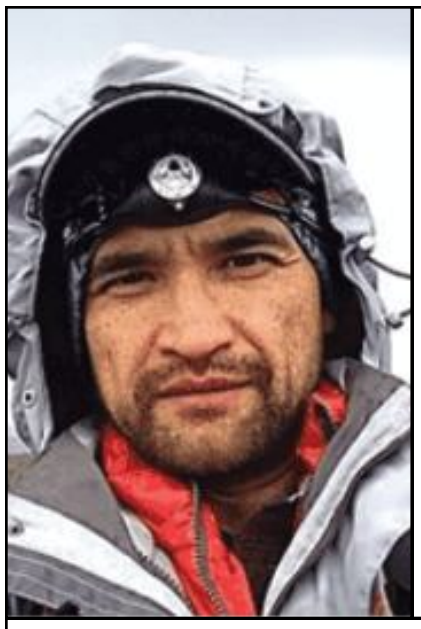


Marat Valeryevich Tyukov
Марат Валерьевич Тюков

Place of Birth: Russia
Eye Color: Gray
Sex: Male
Race: White
Citizenship: Russian
Date of Birth: November 17, 1982

Marat Valerievich Tyukov is an officer of the Russian Federal Security Service (FSB) who conspired with others to obtain and maintain unauthorized persistent access to hundreds of U.S. and international energy companies, thereby enabling the Russian government to disrupt and damage such facilities. Tyukov is a member of an FSB unit known as Center 16, where he works in an operational group known as Military Unit 71330.

He gained unauthorized access to a server belonging to Company “One”, where he used a C2 espionage tool. Tyukov also carried out an intrusion into the computer network of Company “Two”. The group subsequently trojanized updates for Company “Two” industrial control software, making them available for download by energy companies around the world, including in the United States (part of the Dragonfly/Havex campaign).



Mikhail Mikhailovich Gavrilov
Михаил Михайлович Гаврилов / Михайло Михайлович Гаврилов

Place of Birth: Russia
Eye Color: Brown
Sex: Male
Race: White
Citizenship: Russian
Date of Birth: November 7, 1979

Mikhail Mikhailovich Gavrilov is an FSB officer who conspired with others to obtain and maintain unauthorized persistent access to hundreds of U.S. and international energy companies, thereby enabling the Russian government to disrupt and damage such facilities. Gavrilov is a member of an FSB unit known as Center 16, where he works in an operational group known as Military Unit 71330. During his service in this unit, Gavrilov held the rank of captain and was later promoted to major.

Gavrilov conducted attacks against the Wolf Creek network, as well as against Company “Seven”, which the hackers used to access various webmail login pages belonging to energy, utility, and critical infrastructure companies (as part of Dragonfly 2.0).

Support the organization’s activities: https://donate.shum-ng.org/

After the compromise of Carmoney, a secured loan provider reportedly linked to Putin’s former wife, Lyudmila, the Ukrainian Cyber Alliance discovered personal information relating to several additional employees of the FSB’s Center 16[10]. Screenshots of the obtained data are provided below:

Приказом ООО МФК «КарМани»/
№ КМ-45/24 от 27.02.2024

ЗАЯВЛЕНИЕ-АНКЕТА
№25010422937739 от 04.01.2025
о предоставлении потребительского микрозайма

Сведения о Заёмщике – физическом лице				
Фамилия	СОЛОВЬЕВ			
Имя	ДМИТРИЙ			
Отчество	АЛЕКСЕЕВИЧ			
Предыдущая фамилия				
Предыдущее имя				
Предыдущее отчество				
Дата рождения	25.07.2003 г.			
Место рождения	ЧЕЛЯБИНСКАЯ ОБЛАСТЬ СЕЛО ЧЕСМА			
ИНН				
СНИЛС	200-960-210 09			
Паспорт гражданина (действующий)	Серия	4524	Номер	108296
Кем выдан	ГУ МВД РОССИИ ПО Г. МОСКВЕ			
Дата выдачи	30.05.2024 г.		Код подразделения	770086
Паспорт гражданина (предыдущий)	Серия		Номер	
Место регистрации	РОССИЯ, 457220, ЧЕЛЯБИНСКАЯ ОБЛ, ЧЕСМЕНСКИЙ Р-Н, ЧЕСМА С, КОЛХОЗНАЯ УЛ, Д 54			
Место пребывания	РОССИЯ, 457220, ЧЕЛЯБИНСКАЯ ОБЛ, ЧЕСМЕНСКИЙ Р-Н, ЧЕСМА С, КОЛХОЗНАЯ УЛ, Д 54			
Контактный телефон (Зарегистрированный номер)	9000847013		E-mail (Зарегистрированный электронный почтовый адрес)	

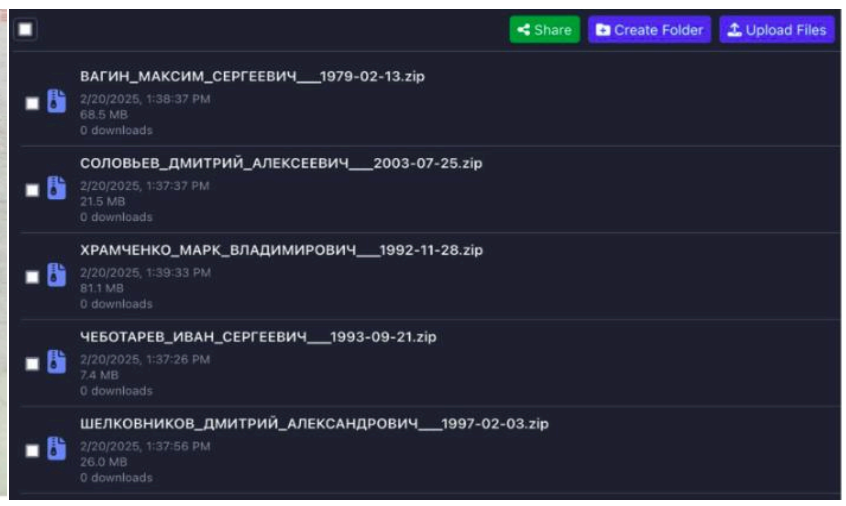
Продукт	Всё Про100 2.0	Сумма Микрозайма	9 900
Срок пользования микрозаймом дней		До 14 дней	
Место работы	ФГКУ "В/Ч 71330"		
Адрес организации	РОССИЯ, 108840, МОСКВА Г, ТРОИЦК Г, КАЛУЖСКОЕ Ш, Д 2		
Рабочий телефон	4959146666		
Ежемесячные доходы, руб.	150 000		
Способ получения микрозайма			
Система Быстрых Платежей (СБП)	79000847013		
Наименование Банка	Sberbank		
Номер банковской карты Заёмщика			
Имя владельца карты			

УТВЕРЖДЕНО
Приказом ООО МФК «КарМани»
№ КМ-14/24 от 18.01.2024

ЗАЯВЛЕНИЕ-АНКЕТА
№ 25011202973320 от 12.01.2025
о предоставлении потребительского микрозайма

Сведения о Заёмщике – физическом лице				
Фамилия	ВАГИН			
Имя	МАКСИМ			
Отчество	СЕРГЕЕВИЧ			
Дата рождения	13.02.1979 г.			
Место рождения	С. ТОРБЕЕВО СТУПИНСКИЙ РАЙОН МОСКОВСКАЯ ОБЛАСТЬ			
Паспорт гражданина	Серия	0523	Номер	148267
Кем выдан	УМВД РОССИИ ПО ПРИМОРСКОМУ КРАЮ			
Дата выдачи	22.02.2024 г.		Код подразделения	250011
Место регистрации	РОССИЯ,690911,ПРИМОРСКИЙ КРАЙ,ВЛАДИВОСТОК Г,АННЫ ЩЕТИНИНОЙ УЛ,Д 7,КВ 120			
Место пребывания	РОССИЯ, 690911, ПРИМОРСКИЙ КРАЙ, ВЛАДИВОСТОК Г, АННЫ ЩЕТИНИНОЙ УЛ, Д 7, КВ. 120			
Контактный телефон (Зарегистрированный номер)	9990400916		E-mail (Зарегистрированный электронный почтовый адрес)	mak-vagin@yandex.ru

Заёмщик	ВАГИН МАКСИМ СЕРГЕЕВИЧ		
Кредитору – Обществу с ограниченной ответственностью Микрофинансовая компания «КарМани» (ООО МФК «КарМани»)			
Продукт	Заём под залог транспортного средства	Сумма Микрозайма	337 079
Срок пользования Микрозаймом, мес.		48	
Место работы	МИНОБОРОНЫ РОССИИ (В/Ч 40083)		
Адрес организации	РОССИЯ,690088,ПРИМОРСКИЙ КРАЙ,ВЛАДИВОСТОК Г,СНЕГОВАЯ УЛ,Д 3А		
Рабочий телефон	9289301626		
Ежемесячные доходы, руб.	130 000		
Предмет залога			
Марка	МЕРСЕДЕС BENZ	Модель	G500
Идентификационный номер (VIN, Рамы, Номер кузова)		**WDB4632481X123946**	
Способ получения микрозайма			
Номер банковской карты Заёмщика	220039XXXXXX8423		
Имя владельца карты	VAGIN MAKSIM		

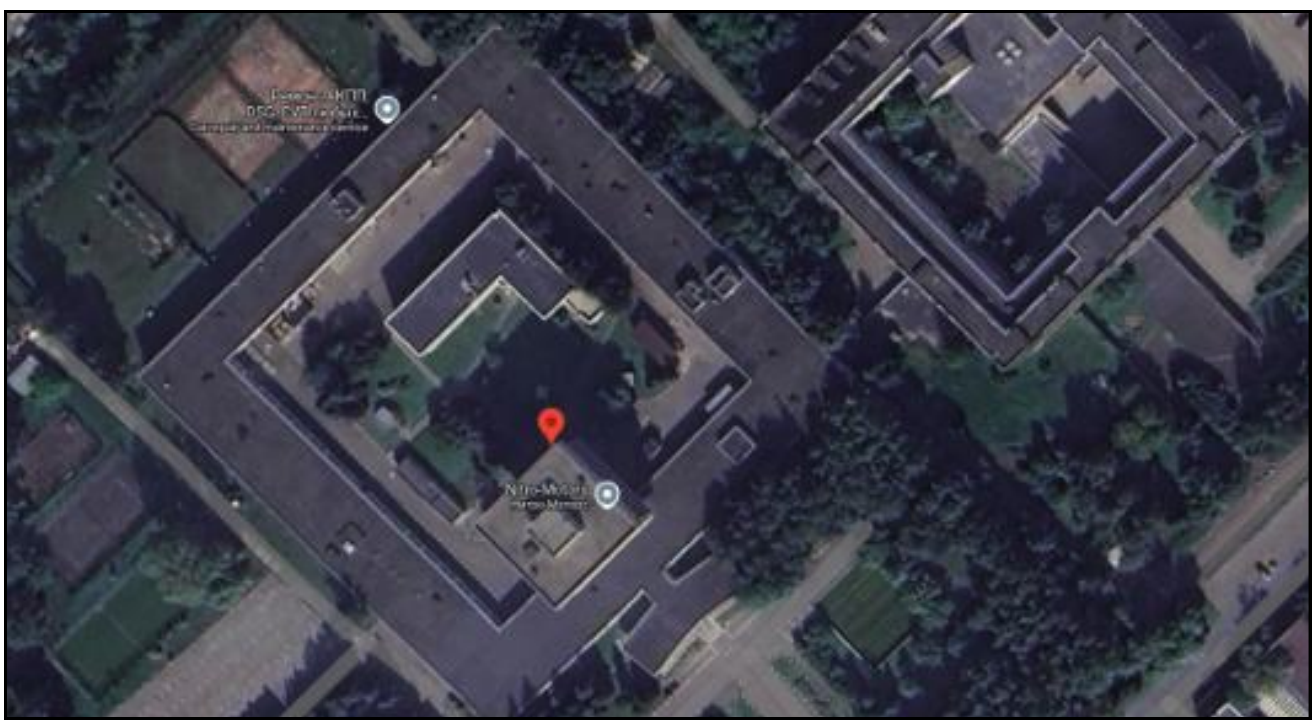


Support the organization’s activities: https://donate.shum-ng.org/

SHUM

Location

FSB Center 16 is located at: 2 Vernadskogo Avenue, Moscow, Russia, 119331.



Support the organization’s activities: https://donate.shum-ng.org/

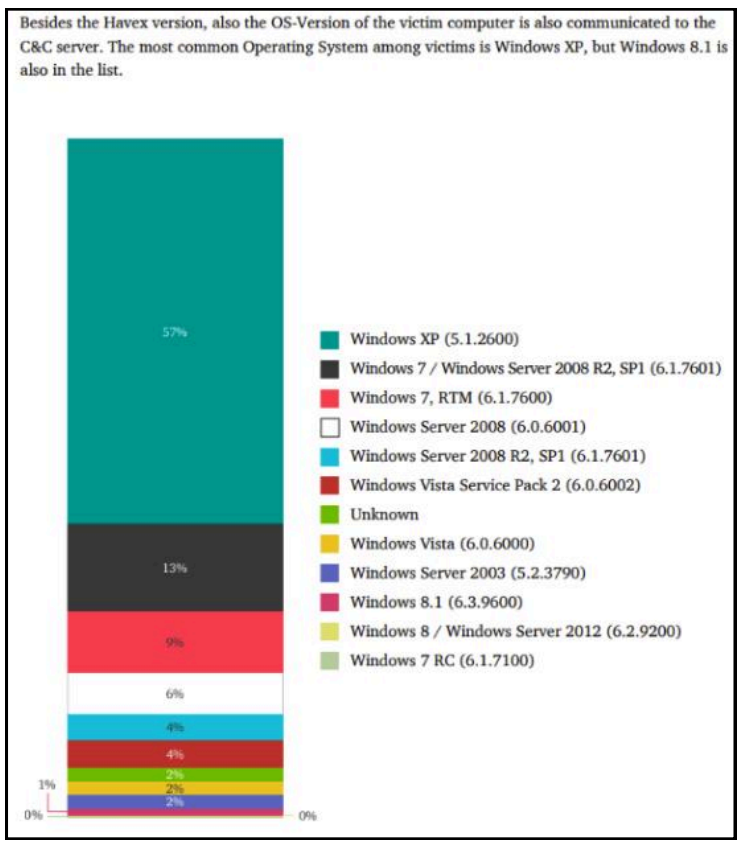
Tactics, Techniques, and Procedures (TTPs)

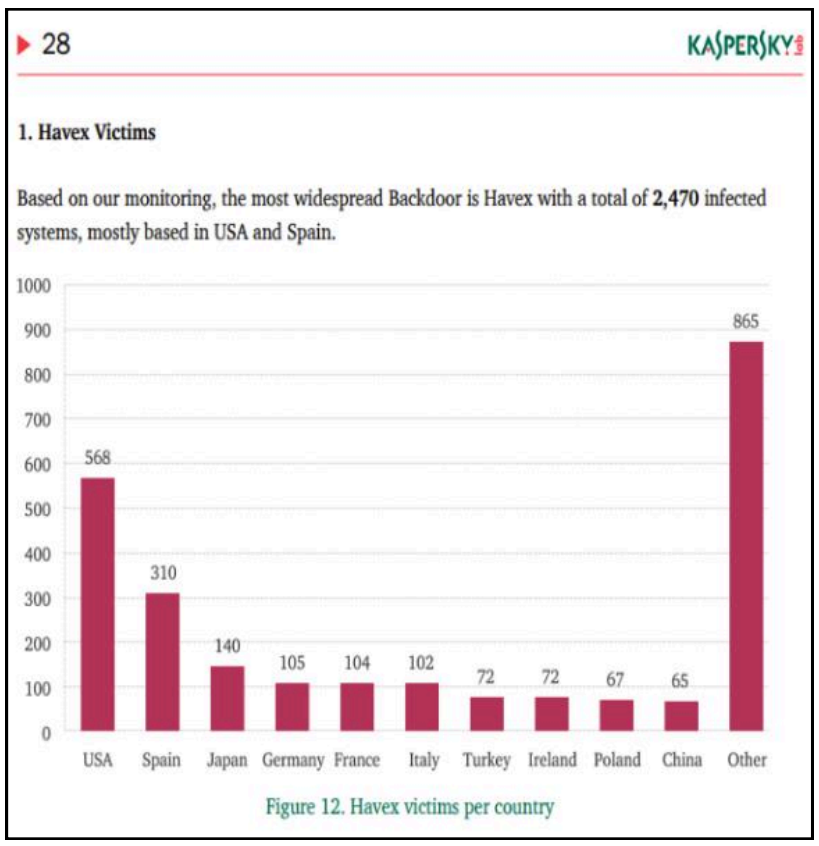
Tools

Feature	Dragonfly (2013-2014)	Dragonfly 2.0 (2015-2017)	Link strength
Backdoor.Oldrea	Yes	No	None
Trojan.Heriplor (Oldrea stage II)	Yes	Yes	Strong
Trojan.Karagany	Yes	Yes (Trojan.Karagany.B)	Medium-Strong
Trojan.Listrix (Karagany stage II)	Yes	Yes	Medium-Strong
"Western" energy sector targeted	Yes	Yes	Medium
Strategic website compromises	Yes	Yes	Weak
Phishing emails	Yes	Yes	Weak
Trojanized applications	Yes	Yes	Weak

Dragonfly's preferred remote access tool is Backdoor.Oldrea, also known as Havex or Energetic Bear. Oldrea opens a backdoor on the victim's computer, allowing the attackers to steal data and install additional malicious software.

Once installed on a victim system, Oldrea collects system information and creates inventories of files, installed applications, and available hard drives. In addition, it gathers data from the Outlook address book and VPN configuration files.





Звіт лабораторії Касперського за 2018 р. щодо зараженності пристроїв Havex або Energetic Bear.[11]

The second most frequently used Dragonfly tool is Trojan.Karagany. Karagany supports the exfiltration of stolen data, the download of additional files, and the execution of files on compromised systems. In addition, Karagany allows the deployment of additional modules, including tools for password collection, screenshot capture, document cataloging on infected computers, and other functions.

The group’s toolkit also includes command-and-control (C2) traffic mechanisms, DNS-based C2 communication, malicious executable files (PE/.exe), malicious documents (RTF, PDF, Office), watering hole payloads, and drive-by download exploit kits.

MITRE ATT&CK Analysis of the Dragonfly Attack Against the U.S. Energy Sector:

Classifying the attackers’ activities according to the MITRE ATT&CK framework allows us to translate disparate facts into a structured model of adversary behavior.

Initial access to victim infrastructure was achieved through several vectors, the primary one being phishing (T1566 Phishing), particularly through the delivery of malicious attachments (T1566.001 Spearphishing Attachment). Execution of the malicious code depended on user interaction (T1204 User Execution), with victims opening infected files (T1204.002 Malicious File).

At the same time, the attackers employed watering hole attacks (T1189 Drive-by Compromise), enabling the compromise of users through trusted web resources. In more sophisticated scenarios, the threat actors leveraged supply chain compromise (T1195 Supply Chain Compromise) by embedding malicious code into legitimate software, significantly expanding the scale of initial access. Additionally, they may have exploited vulnerabilities in public-facing services (T1190 Exploit Public-Facing Application) and conducted infrastructure scanning (T1595.002 Active Scanning: Vulnerability Scanning) to identify potential entry points.

In addition to executing malicious files, the attackers were observed using command and scripting interpreters (T1059), including operation through network device command-line interfaces or Unix shells (T1059.004 Unix Shell), which provided flexible control over the environment. To remain undetected, the threat actors relied on both stolen credentials (T1078 Valid Accounts), including default or weakly protected accounts (T1078.001 Default Accounts, T1552 Unsecured Credentials), and the creation of new accounts (T1136 Create Account). They also employed autostart mechanisms (T1547.001 Registry Run Keys / Startup Folder) and scheduled tasks (T1053.005 Scheduled Task), enabling them to maintain access even after system reboots.

Once established within the network, the attackers conducted an active discovery phase (TA0007 Discovery), including analysis of the file system (T1083 File and Directory Discovery), user accounts (T1087.001 Account Discovery: Local Account), and the overall network structure. At the same time, they employed network sniffing (T1040 Network Sniffing) to collect additional information and credentials. The intelligence gathered was then used to facilitate further movement throughout the environment.

Lateral movement was carried out through remote services (T1021 Remote Services), particularly RDP (T1021.001 Remote Desktop Protocol), which, when combined with valid accounts, allowed the attackers to operate within normal user activity patterns. This approach minimized behavioral anomalies and made detection more difficult. Additionally, the attackers may have leveraged server software components (T1505 Server Software Component) to expand their control over the infrastructure.

To manage compromised systems, the group relied on command-and-control infrastructure (TA0011 Command and Control). Traffic was often concealed through the use of commonly used ports (T1043 Commonly Used Port), proxies (T1090 Proxy), and obfuscated files or information (T1027 Obfuscated Files or Information). These techniques reduced the likelihood of detection and complicated analysis of the C2 infrastructure.

The attackers also placed significant emphasis on defense evasion (TA0005 Defense Evasion). This included masquerading (T1036 Masquerading), particularly T1036.005 Match Legitimate Resource Name, hiding artifacts (T1564 Hide Artifacts), and impairing or modifying security tools (T1562.001 Impair Defenses). They may also have employed indicator blocking (T1562.006 Indicator Blocking) to hinder detection and response efforts by defensive systems.

In the final stages of the operation, the attackers conducted data collection and exfiltration (TA0010 Exfiltration). Prior to transmission, data was staged locally (T1074.001 Data Staged) and then transferred through command-and-control channels (T1041 Exfiltration Over C2 Channel).

Taken together, these techniques form a complete, multi-layered attack lifecycle. The coordination and depth of the operations indicate a high degree of organization and support the assessment that Dragonfly fits the profile of a sophisticated APT actor focused on long-term persistence, intelligence collection, and preparation for potential future operations.

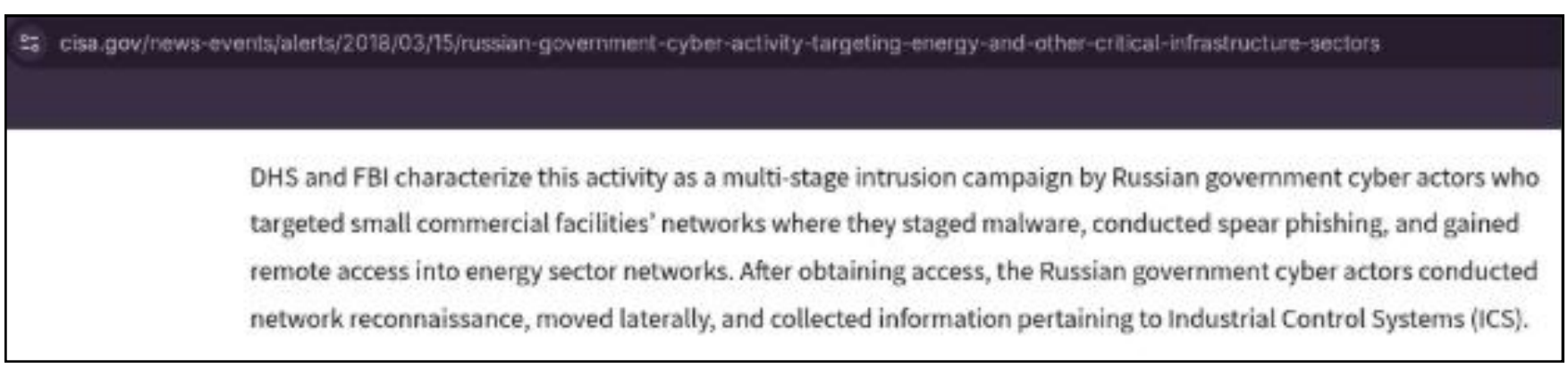
Conclusion

Taken together, these techniques form a complete, multi-layered attack lifecycle. The consistency and depth of the operations demonstrate a high level of organization and support the assessment that Dragonfly fits the profile of a sophisticated APT actor focused on long-term persistence, intelligence collection, and preparation for potential future activities.

Attribution of Dragonfly to the Russian Federation

1. The list of victims closely aligns with Russian strategic interests, including U.S. and European energy companies, power grid operators, and oil and gas infrastructure. Independent hackers typically do not target energy infrastructure, as such operations are more characteristic of state-sponsored APT groups than conventional cybercriminal activity. In addition, the group's technical capabilities significantly exceed what would normally be expected from unaffiliated individuals or small independent actors.

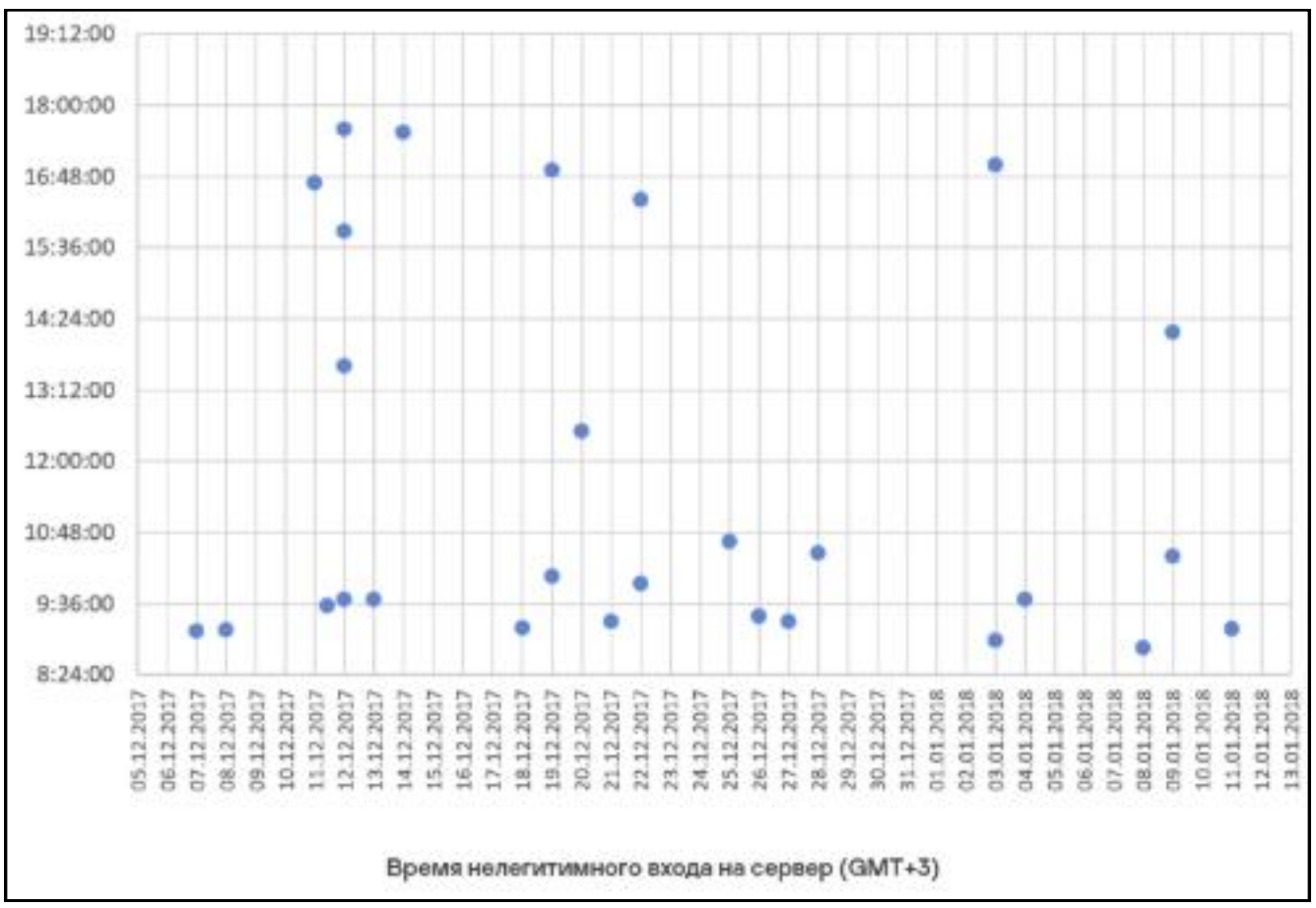
2. Attribution is directly reflected in materials published by the U.S. Department of Justice and U.S. government agencies: https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors



3. Analysis indicates that the group's activity aligns with Eastern European working hours:

Symantec: 09:00–18:00 (UTC+4)

Kaspersky Lab: UTC+3 [2]



Support the organization's activities: https://donate.shum-ng.org/

4. There is overlap with other Russian APT groups. Dragonfly’s methods and infrastructure intersect with those used by Sandworm Team and APT28, both of which have been officially attributed to the Russian Federation, including the GRU.

Dragonfly’s activities demonstrate a systematic and long-term approach to compromising critical infrastructure that goes beyond traditional cybercrime and aligns with the characteristics of state-sponsored cyber operations. The group’s focus on the energy sector, ICS/SCADA systems, and related software suppliers indicates a strategic interest in gaining access to environments that have a direct impact on economic and industrial processes.

Conventional cybercriminal operations are typically focused on rapid monetization through large-scale phishing campaigns, ransomware deployment, or payment card theft, where the primary objective is to generate profit as quickly as possible while minimizing resource expenditure. As a result, such actors generally do not invest significant time in extensive reconnaissance or complex multi-stage intrusions. In contrast, attacks against the energy sector and other economically significant targets, which are characteristic of APT groups, are driven by long-term objectives, including covert access, intelligence collection, and preparation for potential operations against critical infrastructure. These operations are substantially more complex, longer in duration, and aimed at achieving strategic rather than financial outcomes.

The use of supply chain compromise enables attackers to obtain initial access to a large number of targets with relatively limited effort, while subsequent phases focus on identifying the most valuable victims and achieving deep integration within their infrastructure. This approach reflects a clear prioritization of targets and resources, which is characteristic of actors operating in support of state interests.

Analysis of the Wolf Creek incident and related operations indicates that the primary objective at the observed stage was not immediate disruption, but rather reconnaissance, credential collection, and the study of network architecture. The attack was ultimately contained within the IT environment due to effective network segmentation; however, this does not exclude the possibility that the attackers intended to move into operational technology environments at a later stage.

The overlap between Dragonfly’s infrastructure, tactics, and operational approaches and those of other known Russian APT groups, combined with the alignment of target selection with the geopolitical interests of the Russian Federation, strengthens the assessment of state attribution. In this context, the group’s activities can be viewed as part of a broader strategy aimed at preparing for potential cyber operations intended to influence or disrupt energy infrastructure.

Sources

1. https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors

2. https://ics-cert.kaspersky.ru/publications/reports/2018/04/23/energetic-bear-crouching-yeti-attacks-on-servers/

3. https://dailystorm.ru/obschestvo/rossiyskie-hakery-iz-energetic-bear-vzlamyvayut-elektrostancii-ssha-chto-o-nih-izvestno

4. https://www.justice.gov/d9/press-releases/attachments/2022/03/24/ks_akulov_gavrilov_tyukov_0.pdf

5. https://www.security.com/threat-intelligence/dragonfly-energy-sector-cyber-attacks

6. https://www.justice.gov/archives/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

7. https://hackyourmom.com/novyny/ssha-ogolosyly-vynagorodu-10-miljoniv-za-infu-pro-hakeriv-fsb/

8. https://www.fbi.gov/image-repository/four-russians.jpg/view

9. https://www.paloaltonetworks.com/blog/2014/07/palo-alto-networks-offers-threat-mitigation-havex-dragonfly-variants/

10. https://t.me/UCAgroup/44

11. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf