Analytical Report: APT44 Sandworm

19.01.2026

APT44, also known as Sandworm, is a cyber threat group affiliated with GRU Unit 74455, a cyber warfare division of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation. The group has been active since 2009.

Sandworm’s hacking campaigns include both espionage and credential theft, as well as large-scale destructive operations targeting critical infrastructure worldwide.

Name: Sandworm, APT44

Other known aliases: ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Seashell Blizzard, FROZENBARENTS, BE2 APT, Hades (according to Kaspersky Lab), Blue Echidna, UAC-0002 (as listed by CERT-UA), SANDFISH, Sunglow Blizzard, DEV-0665.

APT44 has repeatedly targeted Ukraine and NATO member states. Its operations have focused on critical infrastructure, government institutions, local authorities, media, telecommunications, electoral processes, and the broader political sphere.

Sandworm’s campaigns are characterized by advanced technical capabilities, multi-stage attack chains, and significant damage to targeted countries. The group plays an active role in geopolitical conflicts. Since 2014, its activities have steadily expanded and remain a significant factor in the Russia–Ukraine war.

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

Early APT44 operations involved the exploitation of zero-day vulnerabilities in Microsoft Office and phishing campaigns targeting Ukrainian and NATO-affiliated organizations. In 2015, Sandworm was responsible for the first known power outage caused by malware, using BlackEnergy3 to attack Ukraine’s power grid.

Another well-known development attributed to APT44 is the NotPetya malware, released in 2017 via a compromised software supply chain, which caused billions of dollars in damages worldwide.

Sandworm also expanded its operations beyond Ukraine, including the Olympic Destroyer attack on the 2018 Winter Olympics in PyeongChang, interference related to the French elections, and a large-scale website defacement operation targeting Georgian government and media organizations in 2019.

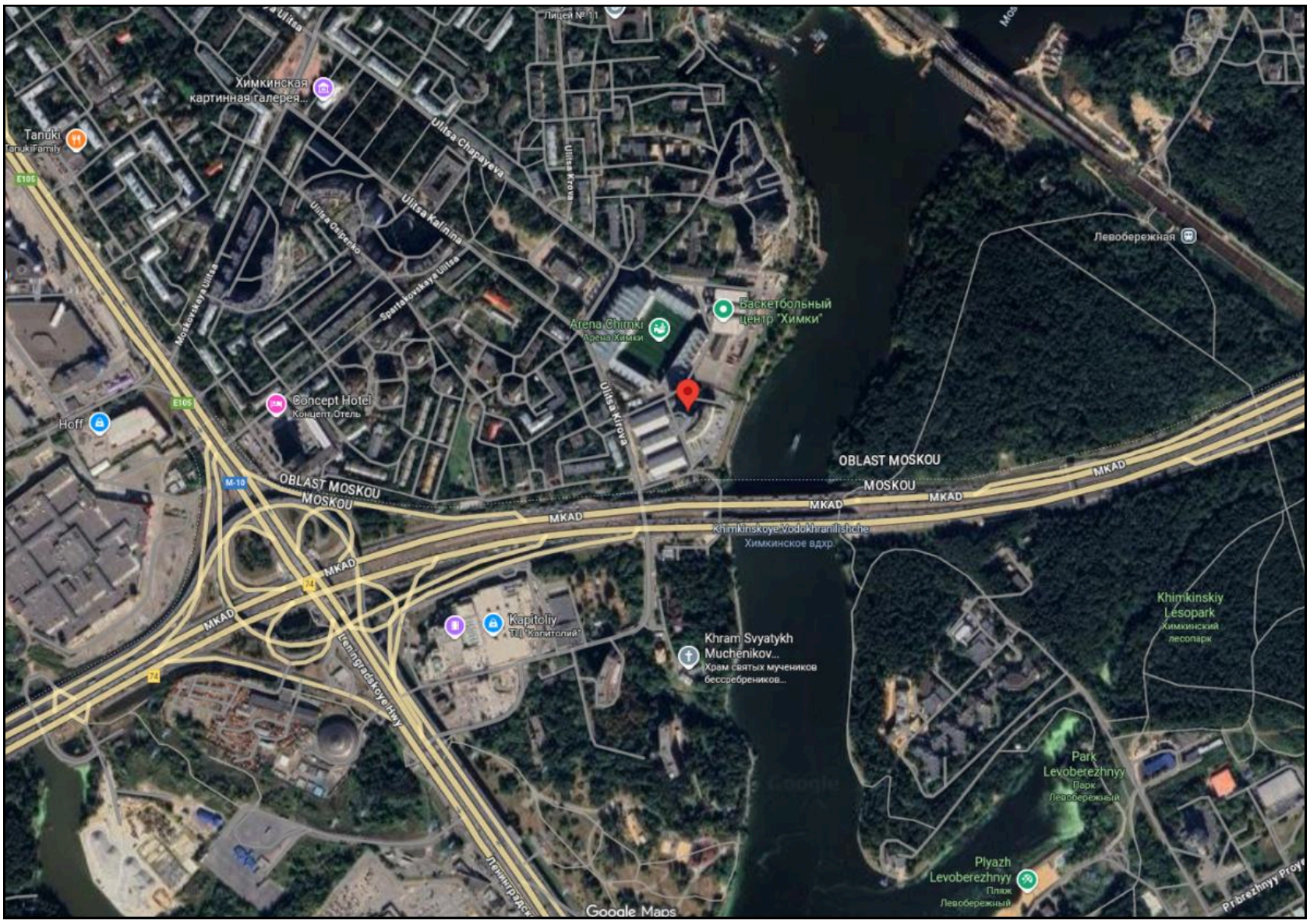
However, throughout its existence, Ukraine has remained the primary target of APT44.

LOCATION

There are several most likely addresses associated with APT44 and its subclusters.

1. **“Bashnya” / “Rota-Tower” / Novator Business Center**
   Address: 22a Kirova Street, Khimki, Moscow Oblast, Russia, 125445
   Entrance coordinates:55°53'02.4"N 37°27'20.5"E

This address is referenced in the U.S. government’s indictment against 12 Russian hackers as the location from which the attacks were conducted. Six of the indicted individuals are officers of Unit 74455, which, according to the indictment, is based at this address.



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

Key Individuals

Six individuals have currently been confirmed as GRU officers of Unit 74455 who coordinated and carried out cyberattacks against Ukraine and other countries as part of APT44.

On 19 October 2020, the U.S. Department of Justice indicted six Russian officers serving in the Main Center for Special Technologies (Unit 74455) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation. They were charged with conducting global cyberattacks against the United States, Ukraine, France, Georgia, South Korea, the United Kingdom, and other countries, as well as deploying destructive malware that caused billions of dollars in damages worldwide.

The indictment names the following Russian military officers: Yuriy Andriyenko, Sergey Detistov, Pavel Frolov, Artem Ochichenko, Petr Pliskin, and Anatoliy Kovalyov.

2. Unit 40904 and the 28th Central Communications Center “Aurora”

Address: Military Compound No. 48/1, 21/2 Svobody Street, Moscow, Russia

Координати входу: 55°49'59.6"N 37°27'09.1"E

An investigation by Radio Liberty dated 17 July 2018 identifies this address as one of the possible locations associated with Unit 74455, APT44, or its subclusters:

3. GRU Headquarters Complex

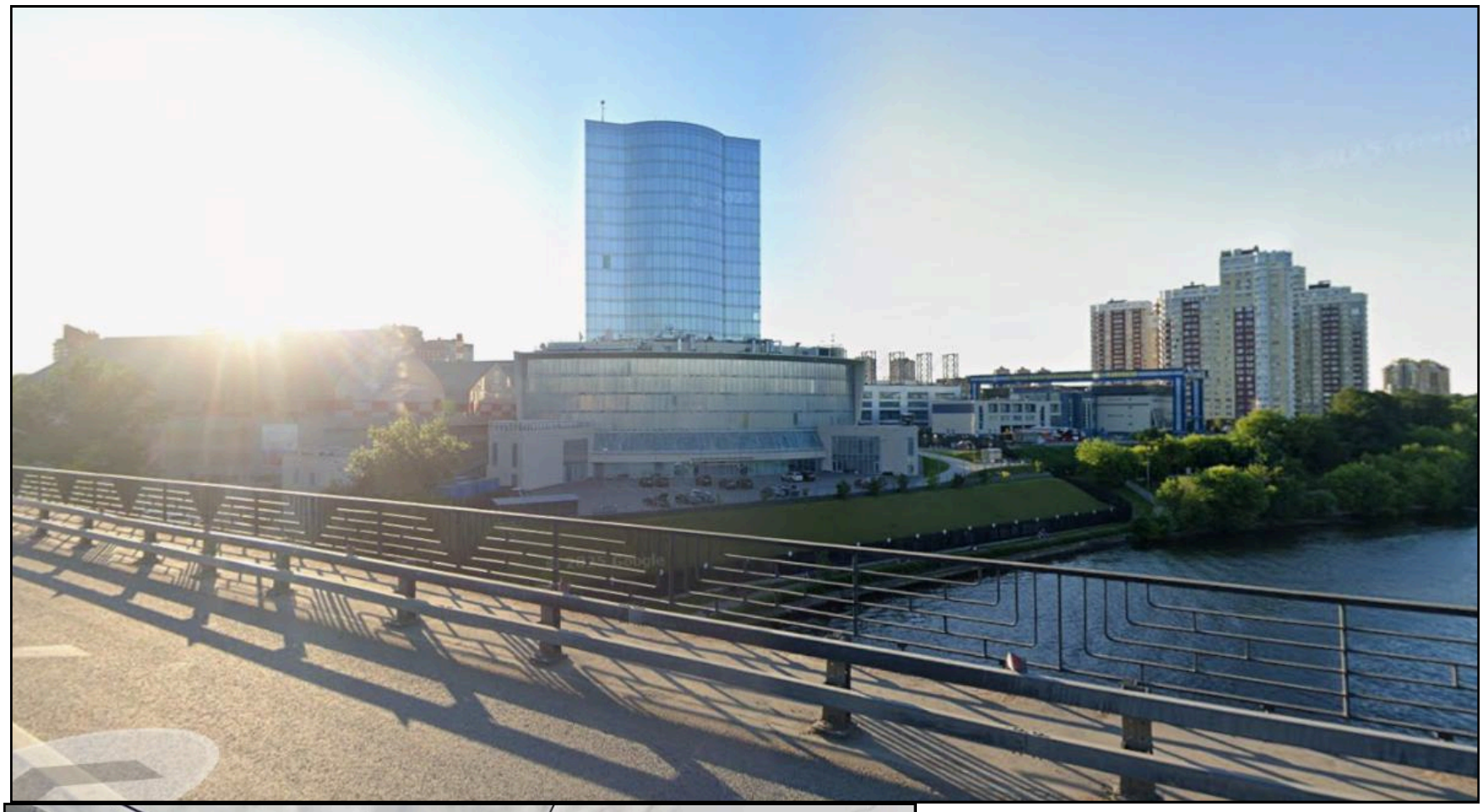
Address: 76 Khoroshevskoye Shosse, Building B, Moscow, Russia

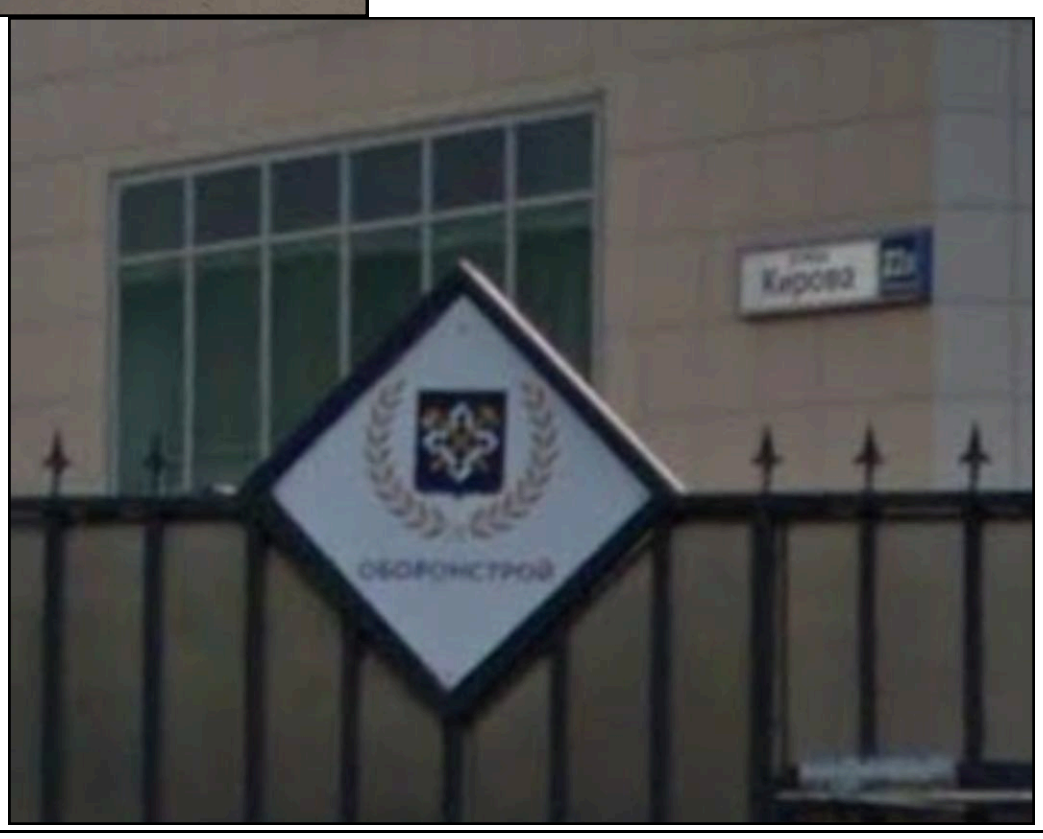
Building coordinates:55°46'58.8"N 37°31'19.6"E

The same Radio Liberty investigation identifies this address as one of the potential locations associated with Unit 74455.

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

SHUM

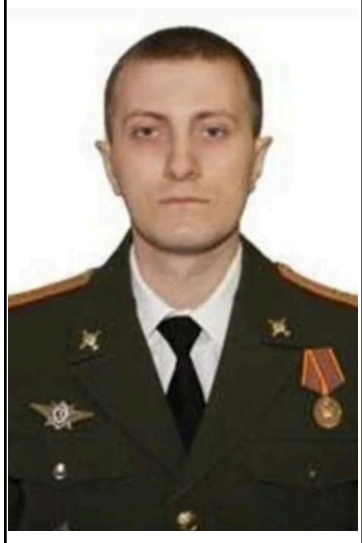
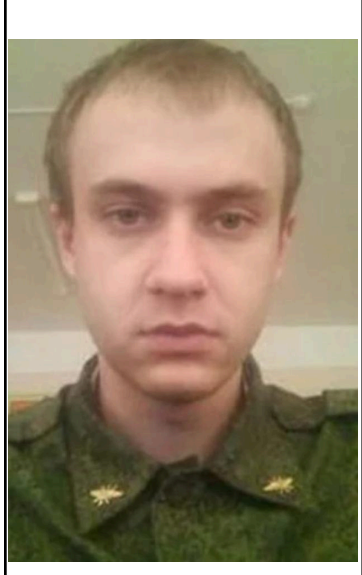
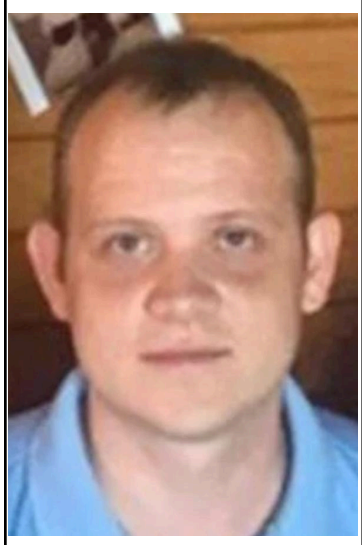


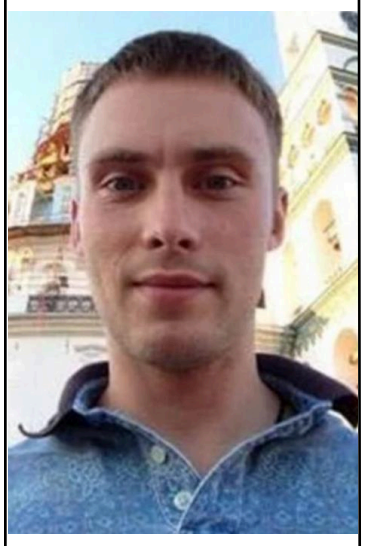


Support the organization’s activities: https://donate.shum-ng.org/

SHUM

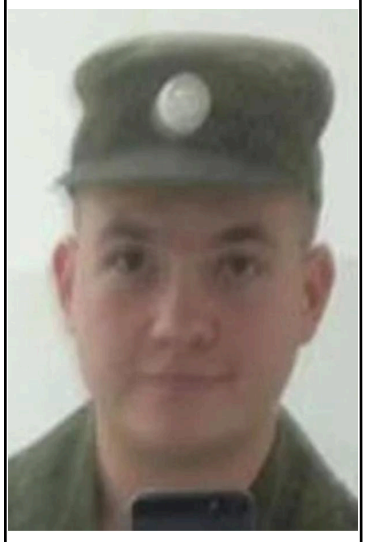
Key Individuals

	**Sergey Vladimirovich Detistov** • Date and place of birth: 1985.07.21, Rostov-on-Don • Place of residence: Moscow, 7 Fomichevoy St., Bldg. 2, Apt. 177 / Moscow Oblast, Vatutinki, Bldg. 53, Apt. 243 • Passport: (RU) 6005448327 • Contacts: markelovsv@alfa-lnk.ru, hab@ya.ru, sergo.voronkin@mail.ru, sergovoronkin@mail.ru, 79165745468@ya.ru, sergeokhripkov@gmail.com, sdetistov@gmail.com, alligero@mail.ru+79772882928,+79199961314, +79164548675,+79852028077,+79165745468, TG: 67894811 • Additional information: timezone: Europe/Moscow,ip: 185.52.31.163 • Position: Officer of Unit 74455, Main Directorate of the General Staff of the Russian Federation • Activity within APT44: Developed components of the NotPetya malware; prepared phishing campaigns targeting the 2018 Winter Olympic Games in PyeongChang.
	**Pavel Valeriyovych Frolov** • Date and place of birth: 07.06.1992, Kaluga • Place of residence: Moscow, 21/2 Svobody Street (one of the possible locations of Unit 74455); Kaluga Oblast, Kaluga, 5 Kaluzhskogo Opolcheniya Street, Apt. 137; Kaluga Oblast, Kaluga, 1 Tramplinnaya Street, Building V; Kaluga Oblast, Kaluga, 16 Akademika Koroleva Street. • Passport (RU) 2912547750, TIN 402914808123, SNILS 13043246508 • Contacts: +79105984581, +79916244342, HAN-92@mail.ru, han-92@mail.ru, Han-92@mail.ru, agueroam@rambler.ru, vk.com: Серхио Кун Агуеро (Sergio Kun Aguero) • Additional information: • Position: Officer of Unit 74455, Main Directorate of the General Staff of the Russian Federation • Activity within APT44: Developed components of the KillDisk and NotPetya malware.
	**Yuriy Serhiyovych Andriyenko** • Date and place of birth: 30.05.1988, Minsk, Belarus • Place of residence: 12 Meshcherino-1 Territory, Apt. 23, Meshcherino village, Stupino District, Moscow Oblast, 142855, Russia; 14A Krupskoy Street, Apt. 18, Lobnya, Moscow Oblast, Russia. • Passport: (RU) 4608230478, TIN 504506704482, SNILS 11278100218 • Contacts: +79250784526; +79197222438, Janetm@list.ru, janetm@list.ru, alexey_452@list.ru; janettravel@mail.ru • Additional information: vehicle X527AA199 • Position: Officer of Unit 74455, Main Directorate of the General Staff of the Russian Federation. • Activity within APT44: Developed components of the NotPetya and Olympic Destroyer malware.



Anatoliy Serhiyovych Kovalyov

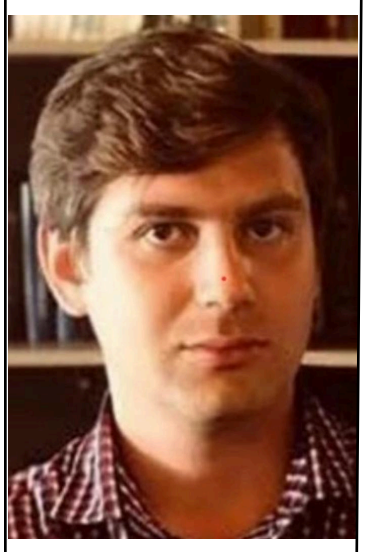
- Date and place of birth: 02.08.1991, Totma, Vologda Oblast, Russia
- Place of residence: Oryol Oblast, Oryol, 4 Kromskoye Highway, Room 20606; Oryol Oblast, Oryol, 4 Kromskoye Highway, Room 132; Krasnodar Krai, Anapa District, Anapa, 34 Pionerskiy Avenue; Oryol Oblast, Oryol, 4 Kromskoye Highway; Moscow, 20 Nagornaya Street, Building 3, Apt. 44; Oryol Oblast, Oryol, 4 Kromskoye Highway, Room 11010; Moscow, 21 Svobody Street, Building 2, Unit Room (one of the possible locations of Unit 74455); Bryansk Oblast, Suzemsky District, Suzemka settlement, 6 Sovetskaya Street; Bryansk Oblast, Suzemsky District, Suzemka settlement, 9 Lenina Square, Building 3, Apt. 13; Moscow, внутpicity territory, Desenovskoye settlement, 1 Novovatutinskiy Avenue; Moscow, внутpicity territory, Desenovskoye settlement, 2 Novovatutinskiy Avenue.
- Passport (RU) 1511951536, TIN 322800244201, SNILS 19849671556
- Contacts: +79150556650, +79150556850 ask.homemail@gmail.com
- Additional information: Registration of residence in Anapa (34 Pionerskiy Avenue) may indicate possible affiliation with FGAU VIT “ERA” (TIN 2539025440), an entity involved in the development of drones, communications equipment, and cryptographic systems, located nearby at 41 Pionerskiy Avenue.
- Position: Officer of Unit 74455, Main Directorate of the General Staff of the Russian Federation.
- Activity within APT44: Developed techniques and messaging for targeted phishing campaigns used in attacks against officials of En Marche!; staff of DSTL; members of the International Olympic Committee (IOC) and Olympic athletes; and employees of Georgian media outlets.



Артем Валерійович Очиченко

- Date and place of birth: 8.11.1992., Sosnovka, Russia
- Place of residence: Krasnodar Krai, Gelendzhik, 9 Mayachnaya Street; Moscow, 21 Svobody Street, Building 2, Unit Apartment (one of the possible locations of Unit 74455); Moscow Oblast, Odintsovsky District, Kubinka, 80 Sosnovka Street, Apt. 2.
- Passport (RU) 4612867190, international: 460779249, SNILS 13966746517
- Contacts: +79999870195, +79778814491, nataly.gonn79@gmail.com, mulen07@rambler.ru, NATALY.GONN79@gmail.com
- Additional information: Also appears in databases under the name Goncharov Artem Valeryevich; date and place of birth, SNILS as well as place of registration, reportedly match, PASSPORT: (RU) 4607792497 — This is also the number of Ochichenko’s old, invalidated passport issued in 2006.
- Position: Officer of Unit 74455, Main Directorate of the General Staff of the Russian Federation.
- Activity within APT44: Participated in spearphishing campaigns targeting partners of the 2018 Winter Olympic Games in PyeongChang; conducted technical reconnaissance of the official domain of the Parliament of Georgia and attempted to gain unauthorized access to its network.

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

	**Petro Mykolayovych Pliskin** • Date and place of birth: 26.08.1988, Khabarovsk, Russia • Place of residence: Moscow, 21 Svobody Street, Building 2, Unit Apartment (one of the possible locations of Unit 74455). • Passport (RU) 0808773870, TIN 773391089500, SNILS 20127219101 • Contacts: +79164357059, +79818006135; +79118485441; +79151389409, P.N.PLISKIN@gmail.ru, zemeloev@yandex.ru, p.n.pliskin@gmail.ru • Additional information: Associated with several registered vehicles, including a 2011 Nissan X-Trai H696ME197, vehicle O410CT799, vehicle H211OT77, vehicle A425PH197, vehicle T353OK197 • Position: Officer of Unit 74455, Main Directorate of the General Staff of the Russian Federation. • Activity within APT44: Developed components of the NotPetya and Olympic Destroyer malware.

NOTE

At the address Moscow, 21 Svobody Street, Building 2, Unit Apartment (also written as 212 Svobody Street, Moscow), which is likely associated with Unit 74455, the following individuals are registered:

- Yevhen Anatoliyovych Krestyaninov – 25 May 1984
- Kyrylo Serhiyovych Tyshin – 6 August 1995
- Mykhailo Volodymyrovych Zhukovskyi – 21 November 1990 (also registered in Anapa, 41 Pionerskiy Avenue — the official registration address of FGAU VIT “ERA” (TIN 2539025440), a developer of communications and cryptographic systems)
- Yuriy Leonidovych Uraskov – 12 April 1990
- Dmytro Yevhenovych Bekhmetyev – 28 April 1993 (also registered in Anapa, 41 Pionerskiy Avenue)
- Pavlo Vyacheslavovych Andreyev – 19 March 1986

Although a confirmed link between these individuals and APT44 hacking activities has not been established, it is considered necessary to include their names in the report due to a possible connection with a developer of cryptographic systems and their registration at a location likely associated with Unit 74455.

Associated Structures and Groups

APT44 (Sandworm) is closely linked to another cyber threat group, APT28 (Fancy Bear), which is attributed to Unit 26165 (the 85th Main Special Service Center of the GRU). Both groups operate under the Main Directorate of the General Staff of the Armed Forces of the Russian Federation.

APT44, alongside APT28, was involved in the 2016 cyberattack against the Democratic National Committee (DNC) aimed at influencing the U.S. elections. One member of APT44, Anatoliy Sergeyevich Kovalyov, is referenced in the U.S. government indictment against 12 Russian hackers.

According to the UK’s National Cyber Security Centre (NCSC), Fancy Bear and Sandworm jointly participated in the cyberattacks against Ukrainian energy companies on 23 December 2015. Officers from Unit 26165 and Unit 74455 were also jointly charged with interference in the 2017 French presidential election.

In addition to other APT groups operating in related domains, Sandworm maintains its own subclusters dedicated to specific attack vectors, intelligence collection, data leak publication, and hacktivism. These groups are largely composed of volunteers and less experienced actors recruited via Telegram channels affiliated with or coordinated by Sandworm.
Such groups include:

- **Cyber Army of Russia Reborn**
  According to America's Cyber Defense Agency, Cyber Army of Russia Reborn (CARR) was created by Unit 74455 in late February 2022. In April 2022, the group began using a new Telegram channel called "CyberArmyofRussia_Reborn" to organize and coordinate collective actions. The channel's administrators recruited participants to conduct cyber activities below the operational level of APT groups. CARR actors have claimed responsibility for DDoS attacks against the United States and European countries in response to their support for Ukraine. Mandiant assesses that CARR coordinates its activities with APT44 and APT28 and uses some of their tools. The CARR Telegram channel is also used to publish information obtained through wiper malware operations.

- **Solntsepyok**
  A Russian hacktivist group established in 2023, primarily targeting Ukrainian media outlets. Solntsepyok has claimed responsibility for the cyberattack against the Kyivstar telecommunications company on 12 December 2023; however, it has not provided convincing evidence to substantiate this claim.The group's generally low technical sophistication suggests that it may function as a front for more advanced APT activity. The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and CERT-UA assess that APT44 (Sandworm) is likely behind the group's operations, using Solntsepyok to leak data and obscure direct attribution for its attacks.

- **XakNet**
  A Russian hacktivist group primarily operating via Telegram and most likely leveraged by Sandworm to publish data obtained through wiper malware operations. In addition, the group conducts DDoS attacks and website defacements targeting Ukrainian media outlets. The group is also known for attempting to distribute a deepfake video of Volodymyr Zelenskyy in March 2022, falsely portraying him as calling for capitulation. Mandiant assesses that this hacktivist group is linked to APT44, as the leaked data contained unique technical artifacts associated with the CADDYWIPER malware, which has been exclusively attributed to APT44, indicating a common source of origin.

- **Infoccentr**
  A Telegram-based hacktivist group likely coordinated by APT44. Its primary targets include the social media accounts of Ukrainian media outlets, with activities focused on spreading disinformation, publishing leaked data, and conducting information-psychological influence operations.The group was established on 4 March 2022. Together with XakNet and CARR, it has published data stolen by APT44 on at least 16 occasions, four of which occurred within less than 24 hours of the respective cyberattacks.

Timeline of APT44 / Sandworm Activity (2009–2026)

Date	Target	Tool / Method	Actor / Subgroup	Sources
~2009	Governments, military entities, and critical infrastructure (multiple countries)	Phishing, backdoors, living-off-the-land techniques	Sandworm / APT44	MITRE, Mandiant
2014-09-03	Ukrainian government agencies, NATO, and affiliated entities	Office 0-day (CVE-2014-4114), spear-phishing	Sandworm	MITRE, ESET
2015-12-23	Ukraine’s energy sector	BlackEnergy-3, SCADA intrusion	Sandworm	ESET, CERT-UA
2016-12-17	Kyiv power grid	Industroyer / CrashOverride (ICS)	Sandworm	ESET
2017-06-27	Ukraine, globally	NotPetya (supply-chain M.E.Doc, wiper)	Sandworm	US/UK Gov, Mandiant
2018-02-09	Olympics, PyeongChang (South Korea)	Olympic Destroyer (wiper)	Sandworm	US Gov, Cisco
2019-10-28	Georgia (government, media)	Mass defacement	Sandworm	US/UK Gov
2022-02	Ukrainian public sector, critical infrastructure (CIKR)	Large-scale wiper attacks, use of bot networks, and fake statements distributed via Telegram.	APT44 + XakNet / CARR / Solntsepyok	Mandiant
2022-03-15	Ukrainian organizations	CaddyWiper	Sandworm	ESET
2022-04-12	Ukraine’s energy sector	Industroyer2 + wipers	Sandworm	ESET, CERT-UA
2022-03	Ukrainian government websites and media outlets	DDoS (DDoSia)	NoName057	SentinelOne

Date	Target	Tool / Method	Actor / Subgroup	Sources
2022-10	Ukrainian and Polish logistics infrastructure, including military aid supply chains	Prestige (disruptive, pseudo-ransomware)	Sandworm	Mandiant
2023-01	Ukraine (multiple sectors)	SwiftSlicer (wipers)	Sandworm	ESET
2023-12-13	Kyivstar	Destructive attack on the telecommunications sector	Solntsepyok (Sandworm)	Reuters, Gov UA
2024-01	OT incidents (claimed)	HMI manipulation (video evidence)	CARR (claims)	Mandiant
2024-03	Ukraine’s telecommunications network	AcidPour (wiper lineage AcidRain)	Sandworm	SentinelOne
2024-10 →	OT/ICS (internationally)	Hack-and-leak operations, defacements, OT access	Z-Pentest + союзники	CISA
2025-01 →	OT/ICS (internationally)	Opportunistic OT attacks	Sector16 (+ Z-Pentest)	Orange Cyberdefense
2025-12-18	OT internet-facing (internationally)	VNC/edge-device abuse	CARR / NoName057(16) / Z-Pentest	CISA

Details of Selected Attacks

23 December 2015 — Attack on Ukrainian Energy Companies

- Target: Critical infrastructure — Ukrainian power grids (Ivano-Frankivsk and region / Kyiv).
- Tool / Method: BlackEnergy-3 and supporting modules used to access SCADA systems, disconnect substations, and cause temporary power outages.
- Impact: Approximately 230,000 consumers were left without electricity for 1–6 hours.

17 December 2016 — Attack on the Kyiv Power Grid

- Target: Energy infrastructure — “Pivnichna” substation.
- Tool / Method: Industroyer (CrashOverride) — malware designed for industrial control systems.
- Impact: Power supply was disrupted for approximately 20% of consumers in Kyiv.

27 June 2017 — «NotPetya”

• Target: IT systems of government, financial, transportation, and other organizations and institutions (Ukraine, Europe, United States).
• Tool / Method: NotPetya wiper malware, a variant of Petya, distributed through compromised M.E.Doc software updates.
• Impact: The United States estimated global damages from NotPetya at approximately $10 billion, calling it one of the most destructive cyberattacks in history. The malware caused widespread disruption not only in Ukraine, but also to logistics companies in Europe and postal services in North America.

9 February 2018 — “Olympic Destroyer” (PyeongChang, South Korea)

• Target: IT infrastructure of the Winter Olympic Games (Wi-Fi, broadcasting systems, ticketing services).
• Tool / Method: Olympic Destroyer wiper, which disrupted domains and services supporting the event.
• Impact: Broadcast disruptions during the Olympics and blocked ticketing systems.

28 October 2019 — Attack on Georgia (web resources)

• Target: Georgian government, media, and business websites.
• Tool / Method: Website defacement, malicious scripts, and DDoS attacks.
• Impact: Compromise of major media websites.

Timeline of Cyberattacks Against Ukraine Since 2022

2022

- 2022-02-24 — Ukrainian public sector and critical infrastructure — multiple wiper attacks, DDoS campaigns; operation referred to as Cyclops Blink.
- 2022-03-15 — Ukrainian organizations (multiple sectors) — CaddyWiper wiper malware (ESET identified this as a distinct wave of data destruction in 2022).
- 2022-04-12 — Ukraine’s energy sector (high-voltage substations) — ICS malware Industroyer2 + accompanying wipers (according to CERT-UA, the attacks were attributed to Sandworm).
- 2022-10 — Logistics infrastructure in Ukraine and Poland — PRESSTEA / Prestige (disguised as ransomware / disruptive malware) (according to Mandiant).
- 2022-03 → ongoing (regularly) — Ukrainian government, media, and public web resources — DDoS campaigns (NoName057, tool: DDoSia) (NoName057 active since March 2022, according to Mandiant).

2023

- 2023-01-28 (cyberattacks in January 2023) — Ukraine — SwiftSlicer wiper malware (according to ESET).
- 2023-12-13 — Kyivstar company (mass service degradation, disabling of communication towers, damage to base stations) — cyberattack against telecommunications infrastructure** (the attack was claimed by the Solntsepyok group; CERT-UA and Mandiant link the group to the APT44 cluster).

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

2024

- 2024-01-17—2024-01-18 — attack targeting the Signal messenger used by military personnel, including Ukrainian forces, aimed at extracting sensitive data — phishing and abuse of the linked device feature (according to Mandiant).
- 2024-03-22 — Ukrainian telecom operators — AcidPour wiper (an evolution of AcidRain)** (according to SentinelOne).

Latest Known Activity

Attack on Polish energy companies (25–29 December 2025)

The attack on Polish energy infrastructure in late December 2025 using the DynoWiper and LazyWiper wipers is currently considered by some analysts to be the latest activity potentially linked to APT44.

Between 25–29 December 2025, several Polish combined heat and power plants (CHPs), as well as approximately 30 wind and solar facilities, were targeted with DynoWiper and LazyWiper through compromised FortiGate devices and exploitation of vulnerability CVE-2024-2617. According to a CERT Polska report, the wipers partially destroyed data on computers within internal networks. Modules providing access to SCADA and OT systems were also targeted; however, damage to power generation was avoided. Distribution networks were affected, and coordination between substations was disrupted due to the compromise of Hitachi RTU560 controllers, resulting in approximately 230,000 customers losing power for 1–6 hours. Overall, the attack was described as “unsuccessful.”

Although the overall pattern of the attack resembles previous Sandworm activity (targeting the energy sector and use of wipers), CERT Polska attributed responsibility to a different group — BerserkBear, linked to the FSB. Analysts from Cisco and the FBI, cited in the report, share this assessment. However, ESET specialists assess with “medium confidence” that APT44 may be behind the attack, citing similarities between DynoWiper and ZOV Wiper, which targeted a Ukrainian financial institution in summer 2025. ESET attributes ZOV Wiper to APT44 with “high confidence.”

Sources

1: https://attack.mitre.org/groups/G0034/

2: https://www.pwc.de/de/energiewirtschaft/under-the-lens-the-energy-sector.pdf

3: https://github.com/blackorbird/APT_REPORT/blob/master/summary/2024/threat%20actor%20list%20from%20cs.csv

4: https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf

5: https://www.svoboda.org/a/29372280.html

6: https://informnapalm.org/ua/ssha-ofitsiino-vysunuly-zvynuvachennia/

7: https://www.justice.gov/archives/opa/press-release/file/1328521/dl?inline=

8: https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

9: https://www.gchq.gov.uk/news/reckless-campaign-of-cyber-attacks-by-russian-military-intelligence-service-exposed

10: https://www.thedailybeast.com/mueller-finally-solves-mysteries-about-russias-fancy-bear-hackers/

11:https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a

12: https://dev.ua/ru/news/atakovali-suspilne-provaiderov-i-minrazvitiya-obschin-kto-stoit-za-rossiiskoi-gruppirovkoi-solntsepek-kotoraya-aktivizirovala-napadeniya-na-ukrainskie-struktury

13: https://www.bbc.com/ukrainian/articles/c51z82rdppxo

14: https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions/

15: https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

16: https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/russia-cyber-threat-operations/russia-apt44

17: https://www.hackthebox.com/blog/apt-44-sandworm-attack-anatomy-mitre-techniques#:~:text=Explore%20Sandworm%20(APT44)%2C%20the,to%20defend%20against%20their%20tactics.&text=Sandworm%20is%20an%20advanced%20persistent,Technologies%20(GTsST)%20Unit%2074455.&text=to%20Frank%20Herbert's%20Dune.,data%20theft%20or%20financial%20gain.&text=The%20focus%20in%20this%20Attack,related%20Hack%20The%20Box%20resources.

18: https://www.euronews.com/2026/01/15/polands-pm-praises-cyber-defences-after-attempted-attack-on-energy-infrastructure-foiled

19: https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf

20: https://www.eset.com/us/about/newsroom/research/eset-research-russian-sandwormapt-attacks-energy-company-poland-with-dynowiper/