THREAT ANALYSIS: APT28 (BLUEDELTA / FANCY BEAR)

APT28, also known as Fancy Bear and BlueDelta, is one of the most active and well-known Russian cyber espionage groups, attributed to the Main Directorate of the General Staff of the **Armed Forces of the Russian Federation (GRU),** specifically Military Unit 26165 (85th Main Special Service Center, 20 Komsomolsky Avenue, Moscow, Russia).

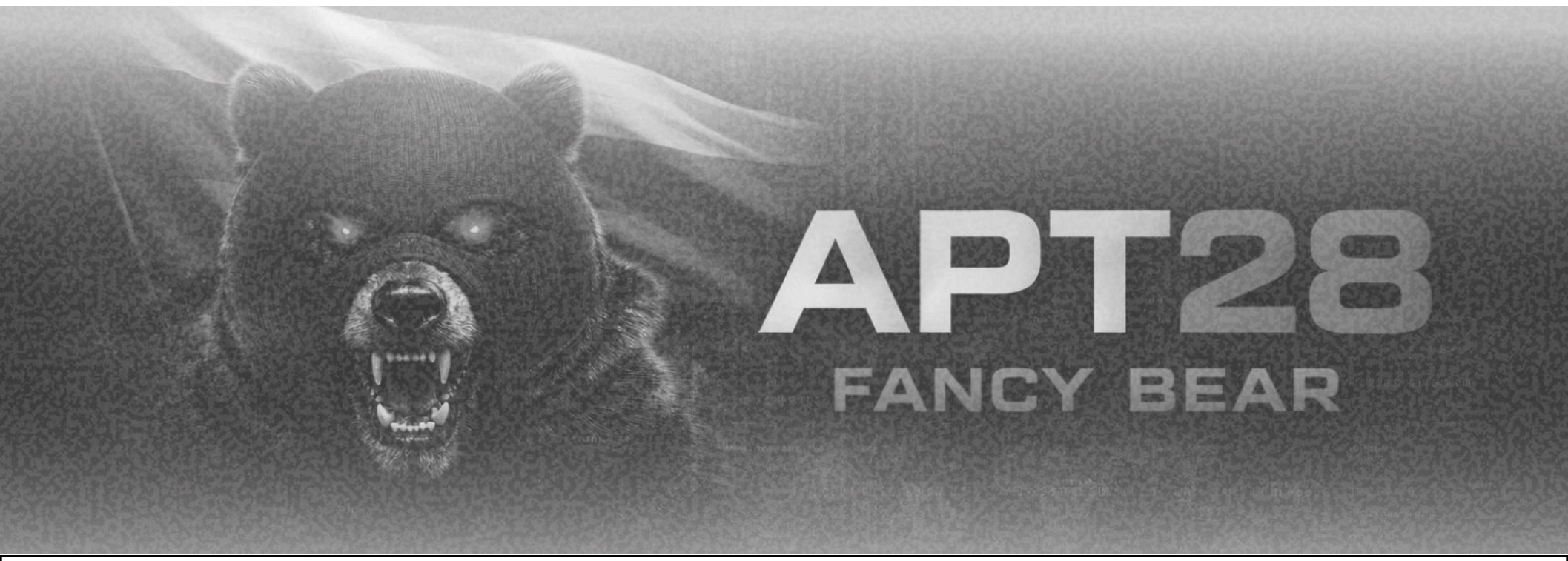
The group has been active since 2004 and specializes in cyber espionage, interference in political processes, data collection, and influence operations.

APT28 has been linked to numerous significant geopolitical attacks aligned with the interests of the Russian Federation:

- Early attacks against **Georgia, Ukraine, Eastern European countries, and NATO, w**ith a focus on military and government networks (2008–2014).
- The theft of data from the **German Bundestag.**
- The attack on the **French television network TV5Monde.**
- The most well-known campaign was interference **in the U.S. presidential elections. Compromise of the Democratic National Committee (DNC), H**illary Clinton’s campaign, and the DCCC, including email theft, leaks, etc.
- Attacks on anti-doping organizations **(WADA, USADA, OPCW, Spiez Laboratory).** Theft of data to discredit investigations into doping in the Russian Federation.
- Exploitation of **XSS vulnerabilities in webmail systems** to steal emails and contacts.

In 2025, APT28 continues to refine its methods.

From February to September, an expanded data collection campaign was observed, involving fake login pages **(Microsoft OWA, Google, Sophos VPN),** the use of Turkish-language PDF lures, and free web services.



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

OPERATIONAL STYLE

APT28 adheres to a low-cost, high-return tactic: phishing, spear-phishing, zero-day exploits, and data collection. They often use publicly available tools or services such as ngrok, webhook.site, infinityfree, RemcosRAT, and Kardon Loader.

Among their proprietary software: X-Agent (RAT), X-Tunnel (used to create an encrypted tunnel between the infected PC and C2), Zebrocy (a simplified version of X-Agent), CORESHELL (a loader and data exfiltration tool), and GameFish (a rootkit).

> Identifiers: T1566, T1110, T1669, T1059, T1071, T1567; use of free domains to host fake pages; domain registration shortly before campaigns; overlap with information operations and the following:

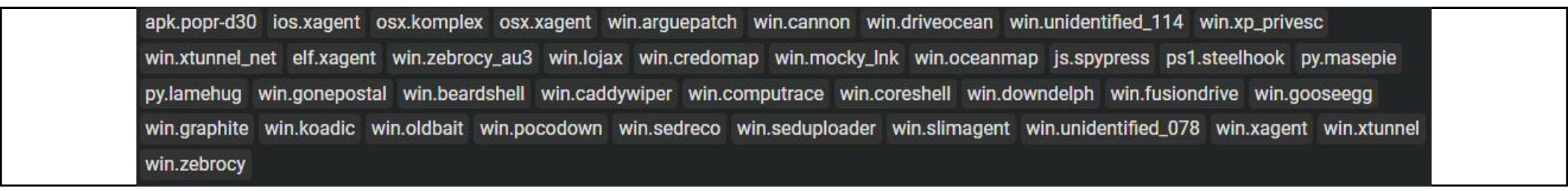


Fig. 1.1. APT28 Identifiers

KEY EVENTS

Year	Event	Description
2004	Attacks on the Ministries of Foreign Affairs, Ministries of Defense, and state media in Poland, the Czech Republic, Georgia, Ukraine, and the Baltic states	Mass phishing campaigns themed around regionally relevant topics to collect intelligence in support of Russian geopolitical interests, using primitive versions of Sofacy and X-Agent that exploited known vulnerabilities in Microsoft Office and Internet Explorer.
2008	Cyberattacks on Georgia	DDoS attacks that paralyzed the country’s infrastructure, including government, financial, and media websites in Georgia. The cyber operations were synchronized with the war.
2014-2015	Attack on the German Bundestag	Targeted phishing against staff members, followed by the use of a zero-day exploit, installation of the X-Agent backdoor, and theft of 16 GB of data.
2015	Attack on TV5Monde	DDoS and defacement attack featuring pro-Russian symbols and “letters” from the “Cyber Caliphate,” using BlackEnergy malware.
2016	Interference in the U.S. elections (GRIZZLY STEPPE)	Phishing against staff members, use of exploits, deployment of X-Agent and X-Tunnel, and data leaks through DCLeaks, WikiLeaks, and under the pseudonym Guccifer 2.0.

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

2016-2018	Attacks on WADA/OPCW/USADA	Phishing using fake domains, theft of athletes' medical data
2017	Attack on Macron's campaign	Spear-phishing targeting Emmanuel Macron's campaign to steal data and interfere in the French elections
2022–2024	"Nearest Neighbor" campaign and attacks on Ukraine	Use of compromised office Wi-Fi routers in Europe as proxy nodes for access, brute-force attacks on cloud services. Attacks on Ukrainian government and military networks, European organizations supporting Ukraine, and the use of Ngrok.
2023-2024	Attacks on Turkey, Europe, North Macedonia, and Uzbekistan	Data collection in support of Russia's geopolitical interests; attacks targeting TENMAK (Turkey), ECFR (Europe), North Macedonia, and Uzbekistan.
2025	Attacks on tech companies in Western Europe and the United States	New tactic: scanning for publicly accessible or weakly secured Kubernetes API servers and dashboards; brute-force attacks on API endpoints to steal advanced AI algorithms, cybersecurity code, and data processing technologies for military applications; compromise of software supply chains.

PLAYBOOK APT28

Based on APT28's activities, it can be determined that the group's primary mission is to conduct influence operations targeting geopolitical events and to shape the information environment in order to advance the objectives of the Russian government.

Phase 0: reconnaissance and target selection. Target selection by APT28 is politically motivated; therefore, attacks are carried out against organizations connected to current geopolitical interests of the Russian Federation.

Phase 1: initial access. APT28 may gain initial access through spear-phishing, using documents with malicious macros, exploiting software vulnerabilities, and compromising legitimate websites.

Phase 2: access expansion. APT28 uses both proprietary malware and publicly available tools to steal credentials and execute commands while blending in with legitimate traffic. To evade antivirus detection, they may employ "Living off the Land" tactics, which involve the use of built-in utilities on the victim's system.

Phase 3: data exfiltration. Data is gradually transmitted in limited volumes to external servers via encrypted connections.

Phase 4: influence operations. The cyberattack serves merely as a tool for an information operation, in which stolen data is passed to platforms such as DCLeaks (recognized by the U.S. as operating as a cover for Russian intelligence — GRU Unit 26165, Unit 74455) and others, and subsequently amplified through controlled media outlets or the propaganda network associated with Prigozhin (2016).

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

CYBER ESPIONAGE, DISINFORMATION, AND HYBRID INFLUENCE

Based on reports, analytical findings, and indictments, it can be concluded that APT28 (GRU Unit 26165) may operate within coordinated tasking frameworks alongside Sandworm (GRU Unit 74455). For example, the attacks on the OPCW were conducted with support from Sandworm; however, the exact nature of this partnership remains open to interpretation, as current evidence suggests coordination at a higher command level rather than a fully integrated operational structure.

In 2022, Mandiant attributed several hacktivist Telegram channels (XakNet, Infoccentr, CyberArmyofRussia_Reborn) to APT28. However, in April 2024, following reassessment, this activity was reattributed to APT44. This indicates that different GRU-linked groups may share network access or operational infrastructure, enabling one group to conduct reconnaissance while another carries out disruptive attacks or data leaks via so-called “hacktivist” fronts. Such an approach allows Russian military intelligence to avoid direct attribution, create an illusion of grassroots activism, and obscure state involvement through proxy channels that are difficult to trace.

I**n its report of 13 June 2023, the Global Disinformation Lab** stated that “A*PT28 is one of the most prolific APT groups involved in interference in Western elections. APT28 conducted the 2016 phishing attacks against the Democratic National Committee, aimed at discrediting former Secretary of State Hillary Clinton and undermining public trust in the security of U.S. elections. Additionally, APT28 was responsible for cyberattacks against the German Bundestag in 2015 and 2016 and against the campaign of French President Emmanuel Macron in 2017. The group sought to steal sensitive information that could be leveraged to influence electoral outcomes in both countries.*”

The report further notes that “*the GRU may be the most powerful information actor in Russia due to its extensive resources and its links to the Internet Research Agency.*” The Internet Research Agency (IRA) is **a Russian company founded in 2013 by oligarch Yevgeny Prigozhin,** specializing in large-scale disinformation operations. IRA-generated content reportedly reached **over 126 million Americans ahead of the 2016 U.S. elections. Prior to the 2022 U.S. midterm elections,** Prigozhin publicly claimed that his organization “interfered… is interfering… and will continue to interfere… [in U.S. elections].”

While the operational roles of IRA and APT28 differ, their activities illustrate a coordinated operational model: APT28 conducts technical intrusion and cyber intelligence activities, while IRA executes information operations that leverage the results of those intrusions. This division of roles is reflected **in the 2019 Mueller Report.** Volume I details the GRU’s (APT28) hacking and theft of Democratic Party emails, while Volume II outlines the IRA’s parallel social media disinformation campaign.

Taken together, the available evidence suggests a close working relationship between I**RA and APT28.** The shared strategic direction and operational logic indicate participation in aligned campaigns, where each entity performs a distinct but complementary function within broader influence operations.

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

PERSONNEL

Based on indictments issued by the U.S. Department of Justice, members of APT28 have been identified:

	**Dmitry Sergeyevich Badin 15.11.1990, Kursk, RF** GRU officer, Unit 26165, Assistant Head of Department. Phone: +79852936987 // E-mail: smithmailbox@yandex.ru Passport (RU): 4010155154 Vehicles: KIA SOUL 2018, B574CO750, VIN: XWEJP811BJ0011261 // EXEED LX 2022, B443AO977, VIN: LVTDB21B3ND307586 Allegedly involved in coordination of cyber operations and development/use of malware.
	**Artem Andriyovych Malyshev 02.02.1988, Bologoye 4, Kalinin Oblast, RF** Phone: +79685152243 // E-mail: imanixman@gmail.com Passport (RU): 4519193476 // Tax Identification Number (TIN): 2718605901 // СНИЛС: 19940774023 Operated the X-Agent malware and sent phishing emails.
	**Oleksiy Valeriyovych Minin 27.05.1972 Perm Krai, RF** GRU officer Passport (RU, international): 120017582
	**Oleksiy Serhiyovych Morenets 31.07.1977 Murmansk Oblast, RF** GRU officer, Unit 26165 Address: Moscow, 4/18 Livoberezhnaya St., Apt. 40 Phone: +79160607896, +79154761498, 79161409545 // E-mail: koldyr@mail.ru Vehicles: БМВ F800R, 2013, 7240AT77 VIN:WB1021706DZ432659 SNILS: 15325806656 // Tax Identification Number: 770475638952 // Passport (RU): 100128330 (international), 100135556 (international), 4500295359 Son: Erik Oleksiyovych Morenets, 01.08.2012

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

SHUM

Yevhen Mykhailovych Serebryakov 26.07.1981 Kursk, RF

GRU officer Unit 26165, обіймав посаду заступника начальника управління.

Passport (RU): 3802614492

Phone: +79629637937, +79055302405

Likely spouse: Oksana Serebryakova E-Mail: aksiniushka@mail.ru

Oleh Mykhailovych Sotnikov 24.08.1972 Ulyanovsk, RF

GRU officer, Unit 26165

Phone: +79264325095, +79299715940, +79299098751 //
E-mail: sotnikova.info@gmail.com, sotstroy2@mail.ru

Passport (RU): 4617725623 // SNILS: 13469255074

Ivan Serhiyovych Yermakov 10.04.1986 Chelyabinsk Oblast, RF

GRU officer Unit 26165

Phone: +79152651636, +79157900085, +79167900085 //
E-Mail: i.s.ermakow@yandex.ru

Passport (RU): 7505775444 // SNILS: 09027701351

Vehicle: VOLVO XC90, 2017, K635BA799, VIN: УV1LC68ACJ1341649

Conducted technical and online reconnaissance of victim organizations, their employees, and computer networks; sent phishing emails.

Serhiy Oleksandrovych Morgachov 22.05.1977 м. Kyiv, Ukraine

GRU officer, Lieutenant Colonel, curator of APT28, Unit 26165.

Passport (RU): 4622608349 // IHH: 505016492079 // SNILS: 14560900148 //
Phone: +79295518624

Involved in the creation of the Telegram channels Legitimnyy («Легитимный»), Rezident («Резидент»), Kartel («Картель»), Spletnitsa («Сплетница»), Chornyy kvartal («Чорний квартал»), Politicheskiy rasklad («Политический расклад»), Netipichnoye Zaporozhye («Нетипичное Запорожье»), Trempel Kharkov («Тремпель Харьков»), Odesskiy fraer («Одесский фраер»), Dnepr Live («Днепр live»), Nikolaev Live («Николаев live»), and Kherson Live («Херсон live»). The channels were reportedly managed by former participants of the so-called “Russkaya Vesna” (2014) and were based in occupied Transnistria.

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

Viktor Borysovych Netiksho 08.09.1966 Chita, RF

GRU officer, Commander of Unit 26165.

Phone: +79169348027, +74954229059, +74956963350, +74957289700

Passport (RU): 4506095450 // SNILS: 12354621128

Borys Oleksiyovych Antonov 19.12.1980 RF

GRU officer, Major, Unit 26165

Passport (RU): 4602584079 // TIN: 500603554972 // SNILS: 19443972209

Phone: +79265594226 // E-Mail: zerbob@yandex.ru

Involved in the creation of the Telegram channels Legitimnyy («Легитимный»), Rezident («Резидент»), Kartel («Картель»), Spletnitsa («Сплетница»), Chornyy kvartal («Чорний квартал»), Politicheskiy rasklad («Политический расклад»), Netipichnoye Zaporozhye («Нетипичное Запорожье»), Trempel Kharkov («Тремпель Харьков»), Odesskiy fraer («Одесский фраер»), Dnepr Live («Днепр live»), Nikolaev Live («Николаев live»), and Kherson Live («Херсон live»). The channels were reportedly managed by former participants of the so-called “Russkaya Vesna” (2014) and were based in occupied Transnistria.

Oleksiy Viktorovych Lukashev 07.11.1990 Murmansk Oblast, RF

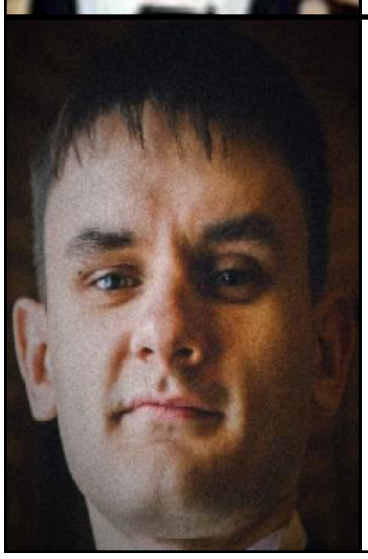
GRU officer, Lieutenant, Unit 26165

Phone: +79164991216

Passport (RU): 401015493 (international), 4010154937

Involved in the creation of the Telegram channels Legitimnyy («Легитимный»), Rezident («Резидент»), Kartel («Картель»), Spletnitsa («Сплетница»), Chornyy kvartal («Чорний квартал»), Politicheskiy rasklad («Политический расклад»), Netipichnoye Zaporozhye («Нетипичное Запорожье»), Trempel Kharkov («Тремпель Харьков»), Odesskiy fraer («Одесский фраер»), Dnepr Live («Днепр live»), Nikolaev Live («Николаев live»), and Kherson Live («Херсон live»).мThe channels were reportedly managed by former participants of the so-called “Russkaya Vesna” (2014) and were based in occupied Transnistria.

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

	**Mykola Yuriyovych Kozachok 29.07.1989 Stavropol Krai, RF** GRU officer, Unit 26165 Passport (RU): 4009816680 // IHH: 260806559800 // SNILS: 16737701997 Phone: +79684564887, +79014224179 // E-Mail: kazak666666@yandex.ru
	**Pavlo Vyacheslavovych Yershov14.12.1990 м. Tver, RF** GRU officer, Unit 26165 Passport (RU): 2810084084 // TIN: 695006053516 // SNILS: 14725434564 Phone: +79969226471, +79261761464

According to the Security Service of Ukraine, 50 clients were identified who transferred funds for the publication of materials in the above-mentioned Telegram channels. Two members of the agent network were detained on suspicion of high treason.

CONCLUSIONS

APT28 remains one of the most active Russian state-sponsored cyber groups. The group is affiliated with the GRU (Unit 26165) and cooperates with other Russian military units. In 2025, APT28 focused on data collection, operational speed, scalability, and cost reduction, as evidenced by its use of free or disposable services to minimize operational expenses.

In 2024–2025, the group intensified attacks against technology companies, AI algorithms, cybersecurity solutions, and Kubernetes infrastructure, indicating an effort to gain access to advanced technologies for intelligence purposes.

According to Recorded Future, APT28 remains a persistent threat and is expected to continue data collection activities in 2026. The group appears to be shifting from high-profile operations (such as the 2016 election interference) toward low-cost, stealth-oriented methods supported by automated and freely available infrastructure. This trend highlights the continued growth of Russian cyber activity in 2025.

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