АНАЛІЗ ЗАГРОЗИ APT28 (BLUEDELTA / FANCY BEAR)

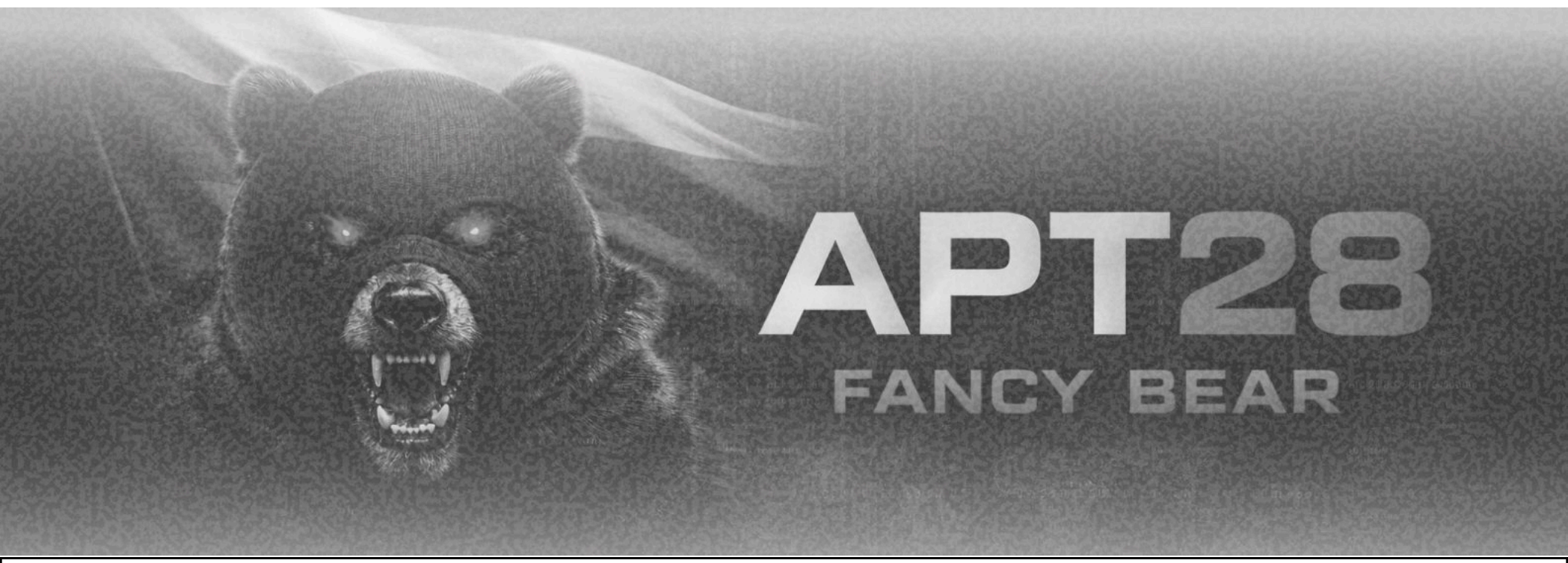
APT28, також відома як Fancy Bear, BlueDelta —
одна з найактивніших та найвідоміших російських кібершпигунських груп, яка атрибується **Головному управлінню Генерального штабу Збройних сил РФ** (ГРУ), зокрема військовій частині 26165 (85-й Головний центр спеціальної служби, Комсомольський проспект, 20, Москва, Росія).

Група активна з 2004 року та спеціалізується на кібершпигунстві, втручанні в політичні процеси, зборі даних та операціях впливу.

APT28 була пов’язана з багатьма значущими геополітичними атаками, синхронізованими з інтересами РФ:

- **Ранні атаки на Грузію, Україну, країни східної Європи, НАТО**, фокус на військових та урядових мережах (2008-2014 рр.)
- Крадіжка даних **німецького Бундестагу**
- Атака на **французьку телекомпанію TV5Monde**
- Найвідомішою кампанією є втручання у **президентські вибори США**. Компрометація Демократичного національного комітету (DNC), кампанії Гілларі Клінтон та DCCC, крадіжка E-Mail, витоки і т.д.
- Атаки на **антидопінгові організації** (WADA, USADA, OPCW, Spiez Lab). Крадіжка даних для дискредитації розслідувань допінгу в РФ
- Експлуатація **XSS-вразливостей у webmail для крадіжки E-Mail та контактів**

У 2025 р. APT28 продовжує вдосконалення своїх методів.
З лютого по вересень зафіксовано розширену кампанію збору даних з фейковими сторінками входу **(Microsoft OWA, Google, Sophos VPN),** використанням турецькомовних PDF-приманок та безкоштовних сервісів.



Підтримати діяльність організації: https://donate.shum-ng.org/

СТИЛЬ ОПЕРАЦІЙ

APT28 дотримується тактики низьких витрат та більшого профіту: фішинг, спір-фішинг, експлойти нульового дня, збір даних, часто використовують загальнодоступні інструменти або сервіси: ngrok, webhook.site, infinityfree, RemcosRAT, Kardon Loader.

Серед власного програмного забезпечення: X-Agent (RAT), X-Tunnel (для створення зашифрованого тунелю між інфікованим ПК та C2), Zebrocy (спрощена версія X-Agent), CORESHELL (завантажувач та засіб для викрадення даних), GameFish (руткіт).

> Ідентифікатори: T1566, T1110, T1669, T1059, T1071, T1567, безкоштовні домени для хостингу фейкових сторінок, реєстрація доменів незадовго до кампаній, перетин з інформаційними операціями та наступні:

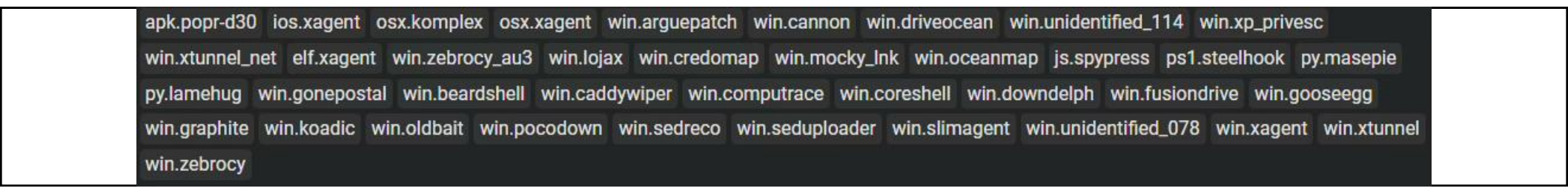


Рис. 1.1. Ідентифікатори APT28

КЛЮЧОВІ ПОДІЇ

Рік	Подія	Опис
2004	Атаки на МЗС, МО, держ. ЗМІ у Польщі, Чехії, Грузії, Україні, країнах Балтії	Килимовий фішинг з тематикою, актуальною для регіону для збору розвіданних для підтримки російських геополітичних інтересів з використанням примітивних версій Sofacy, X-Agent, які експлуатували відомі вразливості в Microsoft Office, Internet Explorer.
2008	Кібератаки на Грузію	DdoS атаки, що паралізували інфраструктуру країни: урядові, фінансові та медіа-сайти Грузії. Кібероперації синхронізувались із війною.
2014-2015	Атака на німецький Бундестаг	Цільовий фішинг проти співробітників з подальшим використанням експлойту нульового дня, встановлення бекдора X-Agent, викрадено 16ГБ даних.
2015	Атака на TV5Monde	DdoS та дефейс атака з проросійськими символами та «листами» від «кіберхаліфату», використовували ПЗ BlackEnergy.
2016	Втручання в вибори США (GRIZZLY STEPPE)	Фішинг проти співробітників, використання експлойтів, встановлення X-Agent та X-Tunnel, витоки даних через DCLeaks, WikiLeaks та під псевдонімом Guccifer 2.0

2016-2018	Атаки на WADA/OPCW/USADA	Фішинг з використанням фейкових доменів, викрадення медичних даних спортсменів
2017	Атака на кампанію Макрона	Спір-фішинг на кампанію Емманюеля Макрона для крадіжки даних та втручання у французькі вибори
2022–2024	Кампанія "Nearest Neighbor" та атаки на Україну	Використання скомпрометованих офісних Wi-Fi-роутерів в Європі як проксі-ланок для доступу, brute force на cloud. Атака на українські урядові та військові мережі, європейські організації підтримки України, використання Ngrok
2023-2024	Атаки на Туреччину, Європу, Північну Македонію, Узбекистан	Збір даних для геополітичних інтересів РФ, атаки на TENMAK (Туреччина), ECFR (Європа), Північну Македонію, Узбекистан
2025	Атаки на tech-компанії в Західній Європі, США	Нова тактика: сканування на публічно доступні або слабко захищені Kubernetes API-сервери, Dashboards, brute force атаки на ендпоінти API для викрадення передових алгоритмів ШІ, кодів для кіберзахисту та технологій обробки даних для військового застосування, компрометація ланцюгів постачання ПЗ

PLAYBOOK APT28

На основі діяльності APT28 можна визначити, що основною місією APT28 є проведення операцій впливу на геополітичні події та підготовка інформаційного середовища для досягнення цілей російського уряду.

Фаза 0: розвідка та вибір цілі. Вибір цілей у APT28 є політично мотивованим, тому атаки відбуваються на організації, що мають відношення до актуальних геополітичних інтересів РФ.

Фаза 1: початковий доступ. Початковий доступ APT28 може здійснювати через спір-фішинг, де використовуються документи із шкідливими макросами, експлойти для вразливостей програм та компрометація легальних сайтів.

Фаза 2: розширення доступу. APT28 використовує як власне ПЗ, так і загальнодоступні інструменти для крадіжки паролів та виконання команд, щоб злитися з легальним трафіком. Для уникнення виявлення антивірусами можуть використовувати тактику «Living off the Land», що передбачає використання вбудованих утиліт в системі жертви.

Фаза 3: викрадення даних. Дані поступово, обмеженою кількістю, передаються на зовнішні сервери через зашифровані з’єднання.

Фаза 4: операції впливу. Кібератака є лише засобом для інформаційної операції, де викрадені дані передаються створеним платформам DCLeaks (визнаний США як той, що діяв для прикриття російської розвідки — ГРУ Unit26165, Unit74455) та іншим, а згодом активно розкручуються через підконтрольні ЗМІ або пропагандистську мережу Пригожина (2016).

КІБЕРШПИГУНСТВО, ДЕЗІНФОРМАЦІЯ ТА ГІБРИДНИЙ ВПЛИВ

На основі звітів, аналізу та обвинувальних актів можна визначити, що APT28 (в/ч 26165 ГРУ) можуть діяти в рамках спільних завдань з Sandworm (в/ч 74455 ГРУ). Наприклад, атаки на OPCW проводилися за підтримки Sandworm, проте питання партнерства залишається відкритим, оскільки на сьогоднішній час взаємодія виглядає як координація на вищому рівні. **У 2022 році Mandiant приписували діяльність хактивістських Telegram-каналів (XakNet, Infoccentr, CyberArmyofRussia_Reborn)** APT28, однак у квітні 2024 року, після повторного аналізу, діяльність переатрибували APT44. Це свідчить про те, що групи можуть ділитися доступом до мереж, дозволяючи одній групі проводити розвідку, а іншій деструктивні атаки чи витоки даних через «хактивістські» фронти, що дозволяє ГРУ РФ уникати прямих атрибуцій, створювати відчуття масовості та «народної ініціативи», де проксі-канали може бути важко відстежити та прив’язати до державного актора.

The Global Disinformation Lab у звіті від 13 червня 2023 року зазначили, що *«APT28 є однією з найпродуктивніших APT у втручанні у вибори західних країн.* ***APT28 здійснювала фішингові атаки 2016 року на Національний комітет Демократичної партії,*** *метою яких було очорнити колишню державну секретарку Гілларі Клінтон та створити недовіру серед громадськості щодо безпеки американських виборів. Крім того, APT28 відповідала за кібератаки на німецький парламент у 2015 та 2016 роках та на кампанію президента Франції Емманюеля Макрона у 2017 році. Вони прагнули викрасти конфіденційну інформацію, яка могла бути використана для впливу на вибори в обох країнах».*

«ГРУ, можливо, є найпотужнішим інформаційним агентом росії через його великі ресурси та зв’язки з Агенством інтернет-досліджень». Агентство інтернет-досліджень (Internet Research Agency, IRA) — це російська компанія, ***заснована у 2013 році олігархом Євгеном Пригожиним****, яка займається масштабними дезінформаційними операціями. IRA генерувала контент, який був доступний* ***понад 126 мільйонам американців****, напередодні виборів 2016 року.* ***Також Пригожин вихвалявся перед проміжними виборами в США 2022 року****, що його організація «втручалася… втручається… і продовжуватиме втручатися… [у вибори США]»*.

Функції IRA та APT28 при проведенні атак відрізняються, проте це дозволяє описати модель операції, де роль APT28 була у технічних заходах та кіберрозвідці, тоді як IRA працювали над інформаційними операціями, реалізовуючи результати APT28. Це підтверджує **звіт спецпрокурора Мюллера (2019),** де у першому томі звіту детально описуються дії ГРУ (APT28) щодо зломів та викрадення листів демократичної партії, а в другому описуються паралельні дії IRA щодо ведення «*операції з дезінформації в соціальних медіа*».

Вищезазначене дозволяє заявити про те, що **IRA та APT28 мають тісні робочі стосунки.** Спільний стратегічний напрямок та логіка злочинів свідчать про залученість угруповань до одних і тих самих операцій, де кожне угруповання виконує свою функцію.

ПЕРСОНАЛІЇ

На підставі обвинувальних актів Міністерства Юстиції США було ідентифіковано учасників APT28:

	**БАДІН ДМИТРО СЕРГІЙОВИЧ 15.11.1990 Курськ, РФ** Офіцер ГРУ РФ, в/ч 26165, помічник начальника відділу Телефон: +79852936987 // E-mail: smithmailbox@yandex.ru Паспорт (RU): 4010155154 Авто: KIA SOUL 2018, B574CO750, VIN: XWEJP811BJ0011261 // EXEED LX 2022, B443AO977, VIN: LVTDB21B3ND307586 Контролював злочинну діяльність, збирав та використовував шкідливе ПЗ.
	**МАЛИШЕВ АРТЕМ АНДРІЙОВИЧ 02.02.1988, Бологе 4, Калінінська обл., РФ** Офіцер ГРУ РФ, старший лейтенант (2018) в/ч 26165. Телефон: +79685152243 // E-mail: imanixman@gmail.com Паспорт (RU): 4519193476 // ІНН: 2718605901 // СНИЛС: 19940774023 Керував ПЗ X-Agent, надсилав фішингові електронні листи.
	**МІНІН ОЛЕКСІЙ ВАЛЕРІЙОВИЧ 27.05.1972 Пермський край, РФ** Офіцер ГРУ РФ Паспорт (RU, закордонний): 120017582
	**МОРЄНЄЦ ОЛЕКСІЙ СЕРГІЙОВИЧ 31.07.1977 Мурманська обл., РФ** Офіцер ГРУ РФ, в/ч 26165 Адреса: м. Москва, вул. Лівобережна, 4/18, кв.40 Телефон: +79160607896, +79154761498, 79161409545 // E-mail: koldyr@mail.ru Авто: БМВ F800R, 2013, 7240AT77 VIN:WB1021706DZ432659 СНИЛС: 15325806656 // ІНН: 770475638952 // Паспорти (RU): 100128330 (закордонний), 100135556 (закордонний), 4500295359 Син: МОРЄНЄЦ ЕРІК ОЛЕКСІЙОВИЧ, 01.08.2012

SHUM

СЕРЕБРЯКОВ ЄВГЕН МИХАЙЛОВИЧ 26.07.1981 м. Курськ, РФ

Офіцер ГРУ РФ, в/ч 26165, обіймав посаду заступника начальника управління.

Паспорт (RU): 3802614492

Телефон: +79629637937, +79055302405

Ймовірно дружина: Серебрякова Оксана, E-Mail: aksiniushka@mail.ru

СОТНІКОВ ОЛЕГ МИХАЙЛОВИЧ 24.08.1972 м. Ульяновськ, РФ

Офіцер ГРУ РФ, в/ч 26165

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

Паспорт (RU): 4617725623 // СНИЛС: 13469255074

ЄРМАКОВ ІВАН СЕРГІЙОВИЧ 10.04.1986 Челябінська обл., РФ

Офіцер ГРУ РФ, в/ч 26165

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

Паспорт (RU): 7505775444 // СНИЛС: 09027701351

Авто: VOLVO XC90, 2017, K635BA799, VIN: YV1LC68ACJ1341649

Проводив технічну та онлайн-розвідку організацій-жертв, їхніх співробітників та комп'ютерних мереж, надсилав фішингові електронні листи.

МОРГАЧОВ СЕРГІЙ ОЛЕКСАНДРОВИЧ 22.05.1977 м. Київ, Україна

Офіцер ГРУ РФ, підполковник, куратор APT28, в/ч 26165.

Паспорт (RU): 4622608349 // ІНН: 505016492079 // СНИЛС: 14560900148 // Номер: +79295518624

Причетний до створення телеграм-каналів «Легитимный», «Резидент», «Картель», «Сплетница», «Чорний квартал», «Политический расклад», «Нетипичное Запорожье», «Трампель Харьков», «Одесский фраер», «Днепр live», «Николаев live», «Херсон live». Канали вели колишні учасники т.з. «русской весны», 2014р., знаходилися в окупованому Придністров'ї.

Підтримати діяльність організації: https://donate.shum-ng.org/

SHUM

НЕТИКШО ВІКТОР БОРИСОВИЧ 08.09.1966 м. Чита, РФ

Офіцер ГРУ РФ, начальник в/ч 26165

Телефон: +79169348027, +74954229059, +74956963350, +74957289700

Паспорт (RU): 4506095450 // СНИЛС: 12354621128

АНТОНОВ БОРИС ОЛЕКСІЙОВИЧ 19.12.1980 РФ

Офіцер ГРУ РФ, майор, в/ч 26165

Паспорт (RU): 4602584079 // ІНН: 500603554972 // СНИЛС: 19443972209

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

Причетний до створення телеграм-каналів «Легитимный», «Резидент», «Картель», «Сплетница», «Чорний квартал», «Политический расклад», «Нетипичное Запорожье», «Тремпель Харьков», «Одесский фраер», «Днепр live», «Николаев live», «Херсон live». Канали вели колишні учасники т.з. «русской весны», 2014р., знаходилися в окупованому Придністров'ї.

ЛУКАШЕВ ОЛЕКСІЙ ВІКТОРОВИЧ 07.11.1990 Мурманська обл., РФ

Офіцер ГРУ РФ, лейтенант, в/ч 26165

Телефон: +79164991216

Паспорт (RU): 401015493 (закордонний), 4010154937

Причетний до створення телеграм-каналів «Легитимный», «Резидент», «Картель», «Сплетница», «Чорний квартал», «Политический расклад», «Нетипичное Запорожье», «Тремпель Харьков», «Одесский фраер», «Днепр live», «Николаев live», «Херсон live». Канали вели колишні учасники т.з. «русской весны», 2014р., знаходилися в окупованому Придністров'ї.

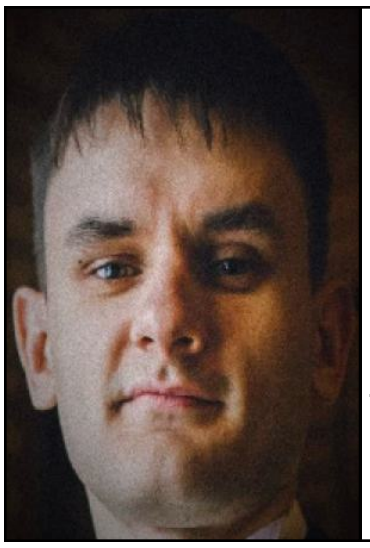
КОЗАЧОК МИКОЛА ЮРІЙОВИЧ 29.07.1989 Ставропольський край, РФ

Офіцер ГРУ РФ, в/ч 26165

Паспорт (RU): 4009816680 // ІНН: 260806559800 // СНИЛС: 16737701997

Телефон: +79684564887, +79014224179 // E-Mail: kazak666666@yandex.ru

Підтримати діяльність організації: https://donate.shum-ng.org/



ЄРШОВ ПАВЛО В’ЯЧЕСЛАВОВИЧ 14.12.1990 м. Твер, РФ

Офіцер ГРУ РФ, в/ч 26165

Паспорт (RU): 2810084084 // ІНН: 695006053516 // СНИЛС: 14725434564

Телефон: +79969226471, +79261761464

За даними Служби Безпеки України, було встановлено 50 замовників, які перераховували гроші за публікації матеріалів в вищезгаданих телеграм-каналах, затримано двох учасниць агентурної мережі з підозрою про державну зраду

ВИСНОВКИ

APT28 залишається однією з найактивніших російських державних кібергруп. Група належить до ГРУ (в/ч 26165) та співпрацює з іншими російськими військовими частинами. У 2025 р. APT28 була зосереджена на зборі даних, швидкості, обсязі операцій та здешевленні, про що свідчить використання безкоштовних або одноразових сервісів для здешевлення операцій.

У 2024–2025 роках угруповання активізувало атаки на технологічні компанії, ШІ-алгоритми, кібербезпекові рішення та інфраструктуру Kubernetes, що свідчить про прагнення отримати доступ до передових технологій для розвідувального використання.

За прогнозом Recorded Future, APT28 — стійка загроза, яка продовжить збір даних і в 2026 році. Група зміщує фокус від гучних операцій (виборів 2016 р.) до дешевих та стелс-методів з безкоштовною, автоматизованою структурою. Це підкреслює зростання російської кіберактивності у 2025 роц