ТИПОВІ ТАКТИКИ ТА СЦЕНАРІЇ ДІЯЛЬНОСТІ APT-ГРУП ГРУ РФ

У цьому звіті досліджено типовий сценарій кіберзагроз APT-груп у складі Головного управління Генерального штабу Збройних Сил Російської федерації (ГУ ГШ ЗС РФ), проте для зручності у звіті буде використовуватися також і колишня назва – Головне розвідувальне управління (ГРУ). Цей звіт базується на основі наших попередніх звітів про APT44 та APT28, та доповнюється матеріалами про них, що стали відомими у ході аналізу. Також було проаналізовано структуру ГУ ГШ ЗС РФ.

У контексті цього звіту термін «APT» виступає аналітичним ярликом, що при зазначенні номеру APT-групи, атрибується певному підрозділу ГУ ГШ ЗС РФ. Атрибуції базуються на відкритих джерелах. Ми не стверджуємо існування «єдиної концепції», а моделюємо можливі патерни, тому «гіпотетична модель» в контексті цього звіту – це припущення про те, як військові частини розподіляють функції в єдиній екосистемі. Термін «APT» є лише аналітичною абстракцією, тоді як реальними операційними одиницями виступають конкретні військові частини з власною інфраструктурою, символікою та ієрархією. З точки зору російського законодавства, ці структури мають статус легітимного інструменту державної політики, що діє в межах системи військового командування. Метою дослідження є систематизація відомих тактик, технік і процедур, що застосовуються російськими APT-групами зі складу ГУ ГШ ЗС РФ. Особливу увагу у звіті приділено виявленню кореляцій між різними угрупованнями та їхніми активностями, що допомагає побудувати цілісну картину організаційної та операційної структури ГРУ.

Організації сприймають APT-групи через призму власних даних та класифікації. Перші згадки про інциденти, пов’язані з APT-групами почались приблизно з 2000-х років, коли команди реагування на комп’ютерні інциденти США та Великої Британії опублікували повідомлення зі сповіщеннями, в яких описувалися цільові, соціально спроектовані електронні листи, що містили трояни для викрадення конфіденційної інформації. Організації досліджують APT-групи понад 20 років, тому сьогоднішній результат та висновки – це здобутки довгої та кропіткої праці.

Представлені у звіті дані базуються на відкритих джерелах, опублікованих у період з 2014 року по теперішній час. Динамічний характер розвідувальної інформації, зміна тактик супротивника та постійне оновлення таких баз знань, як MITRE ATT&CK (що спирається на публічні звіти), обумовлюють необхідність розглядати наведені TTP як актуальні на момент підготовки матеріалу, та такі, що можуть зазнавати змін у майбутньому.

ОРГАНІЗАЦІЙНА МОДЕЛЬ ПІДРОЗДІЛІВ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ГУ ГШ ВС РФ

Після розпаду радянського союзу, підрозділи інформаційних операцій були інтегровані до новостворених структур у складі Головного розвідувального управління РФ в листопаді 1991 року, сформувавши основу для майбутніх Військ Інформаційних Операцій ГУ ГШ ЗС РФ, що зазначається у звіті від CheckFirst 2026 року, де було проаналізовано підрозділи військових інформаційних операцій ГУ ГШ. У своєму звіті вони допускають, що ці підрозділи інтегровані в спеціальне управління, яке об’єднує три основні сфери компетенції під єдиним командуванням: психологічні операції, шифрування та криптоаналіз, операції в комп’ютерних мережах.[1]

Головне управління Генерального штабу ЗС РФ є центральним органом управління військовою розвідкою. У системі управління війська інформаційних операцій (ВІО) займають особливе місце, будучи інструментом для реалізації стратегії «інформаційного протиборства», де кібератаки та пропаганда розглядаються як одне ціле. Також у російській військовій доктрині технічні заходи в рамках концепції «інформаційного протиборства» також включать і комп’ютерні мережеві операції. У цій моделі система військ інформаційних операцій визначає напрям діяльності тоді як військова частина виконує визначені фукнкції, де «APT-група» виступає у ролі аналітичного відображення спостережуваної діяльності, тобто, є сталим поведінковим профілем діяльності підрозділу у кіберпросторі.

Рис. 1.1 – Структура «Військ інформаційих операцій» ГРУ РФ. ©CheckFirst 2026

ВІЙСЬКОВА ЧАСТИНА	ПІДРОЗДІЛ	РОЗТАШУВАННЯ	НАПРЯМ ДІЯЛЬНОСТІ
ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ			
54777	72-й Центр спеціальної служби	м. Сенєж	Головний центр управління інформаційних операцій
03126	2148-й підрозділ	м. Сертолово-2	Європа, НАТО, Балтія
03127	2156-й підрозділ	м. Твер	Невідомо
03128	2140-й підрозділ	м. Батайськ	Україна, Кавказ
03132	2047-й підрозділ	м. Чита	Азія
03134	2040-й підрозділ	м. Хабаровськ	Східна Азія
03138	2059-й підрозділ	м. Єкатеринбург	Центральна Азія
20697		м. Санкт-Петербург	Україна, Балтія
ДЕШИФРУВАННЯ ТА КРИПТОАНАЛІЗ			
20766		м. Хабаровськ	
26165 (APT28)		м. Москва	Європа, Америка
48707		м. Курськ	
78430		м. Єкатеринбург	
КОМП’ЮТЕРНІ МЕРЕЖЕВІ ОПЕРАЦІЇ			
20978		м. Москва	
74455 (APT44)		м. Хімки	Європа, Америка

Таблиця 1.1 – Структура, відтворена на основі відкритих джерел (може відрізнятися від фактичної)[2][3][4][5][6][7]

Варто зазначити, що в розслідуванні від CheckFirst в/ч 20697 входить до складу департаменту дешифрування та криптоаналізу, проте, OSINT-розслідування «Телебачення Торонто» описало діяльність в/ч 20697 як таку, що відповідальна за проведення інформаційно-психологічних операцій.[8] Це підтверджується діяльністю співробітників, які спеціалізуються на політології, комунікаціях, психології, тощо.

За даними з відкритих джерел, також існують декілька підрозділів, що підпорядковуються в/ч 55111 та виконують роль центрів у кожному військовому окрузі:

- в/ч 76836 (706 Центр інформаційного протиборства Західний воєнний округ);
- в/ч 76853 (711 Центр інформаційного протиборства Південний воєнний округ);
- в/ч 76854 (Центр інформаційного протиборства Центральний воєнний округ);
- в/ч 76862 (738 Центр інформаційного протиборства Східний воєнний округ).

Центральним органом управління є 72-й Центр спеціальної служби в м. Сенєж, якому підпорядковані регіональні підрозділи ІПсО з географічним розподілом відповідальності (Європа, НАТО, Україна, Кавказ, Азія, тощо). Підрозділи інформаційно-психологічних операцій ГУ ГШ, ймовірно, виконують функцію перетворення отриманих даних іншими підрозділами на психологічний вплив, координуючи інформаційні кампанії проти конкретних цілей. Як зазначає CheckFirst у своєму звіті: «У сукупності ці висновки свідчать про те, що підрозділ психологічних операцій керує значним і структурованим апаратом, призначеним для проведення психологічних операцій не тільки проти іноземної цільової аудиторії, але й проти російської внутрішньої аудиторії.»

Дешифрування та криптоаналіз є другим ключовим компонентом у системі ВІО. Як зазначено у звіті CheckFirst, аналіз нагородної символіки дозволив ідентифікувати ці підрозділи як окремий напрям у структурі ГУ ГШ. Формально ці підрозділи відповідають за захист зв’язку, але фактично є основою кібероперацій РФ. Пояснюється це пострадянською трансформацією, де серед нових методів, замість перехоплення радіосигналів вони почали перехоплювати саме цифрові комунікації, а для цього потрібно не лише дешифрувати, але й проникати в системи, щоб отримати доступ до зашифрованих даних.

На основі публічних звітів, сучасна роль підрозділів комп’ютерно мережевих операцій розкривається через функції кіберсаботажу, збору розвідувальної інформації через компрометацію мережевих пристроїв, інформаційні операції через проксі структури або підконтрольні засоби.

Гіпотетично, ми можемо висунути декілька моделей діяльності для окреслення ролей, яку виконують всі підрозділи у взаємодії з APT-групами, проте для цього необхідно дослідити інші підрозділи як окрему складову загальної екосистеми. Отже, питання щодо конкретної ролі, яку виконують інші військові частини у цій структурі, залишається відкритим для дослідження.

Кадрові індикатори інституціоналізації кіберпідрозділів

Окрему увагу слід приділити кадровим змінам у системі державного управління РФ. Показовим прикладом стала відставка Коновальчика Павла Михайловича з посади помічника секретаря ради безпеки РФ (помічник Сергія Шойгу), який займав цю посаду з липня 2024 року. «Павел Михайлович Коновальчик является высококвалифицированным управленцем стратегического уровня, он в плановом порядке переходит на другую работу с повышением в сфере информационно-аналитического направления по обеспечению национальной безопасности государства».

Павло Коновальчик – офіцер воєнної розвідки технічного профілю. В розслідуванні CNA зазначається, що він був пов’язаний з в/ч 26165, та очолював війська інформаційних операцій.

Відповідно до коментаря ради безпеки РФ, можна припустити, що його професійна діяльність буде пов’язана з напрямком розвідки та інформаційних операцій. Переведення його на вищу посаду може свідчити про посилення ролі інформаційно-аналітичного та кіберкомпоненту в системі стратегічного планування національної безпеки РФ. На нашу думку, це може вказувати на подальшу інституціоналізацію інформаційних та кібероперацій у системі державної безпеки РФ, де технічні підрозділи діють у межах ширшої системи стратегічного планування, координація якої здійснюється на рівні Ради безпеки або інших надвідомчих структур. Також у 2021 році фіксувався схожий випадок, де офіцер ГРУ Олександр Старунський, причетний до підрозділів психологічних операцій, зайняв посаду наукового радника тієї ж Ради безпеки.[9] Повторюваність подібних переміщень дозволяє розглядати їх як патерн цілеспрямованого просування технічних і оперативних кадрів кібер-напрямку у вищий ешелон стратегічного планування.

Ймовірно, інтеграція профільних кадрів на рівень Ради безпеки може свідчити про поступову зміну функціонального статусу кібер- та інформаційних операцій у системі державного управління РФ – від інструменту виконання стратегічних рішень до компоненту їхнього формування. Якщо ця тенденція є стійкою, це матиме наслідки не лише для операційної активності підрозділів ГУ ГШ, але й для логіки, в межах якої ці операції плануються та виконуються.

РОЗВІДУВАЛЬНО-ОРІЄНТОВАНИЙ ПІДРОЗДІЛ 26165 (APT28)

Раніше ми писали, що діяльність цього підрозділу була помічена у 2004 році, проте його витоки були сформовані ще за часів холодної війни, де він виконував роль підрозділу зв'язку, яке працювало в напрямку військової розвідки та шифрування. Підрозділ був відомий як «Служба дешифрування» так і «85-й головний центр спеціальної служби ЗЗ». Історично підрозділ 26165 займався розшифровкою перехоплених тактичних військових повідомлень у СРСР або за кордоном. Для цього підрозділ, використовував систему «Булат», розроблену в 1970-х роках дослідницьким центром «Квант» для потреб 16-го управління КДБ – попередника 16-го центру ФСБ. «Квант» досі звинувачують у розробці технологій на користь технічних підрозділів російських розвідувальних служб.

Рис. 1.2 – Знаки розрізнення підрозділу 26165.

Діяльність APT28 завжди була обґрунтована геополітичними інтересами Росії. В 2000-х ми могли спостерігати атаки на Кавказькі регіони, де під час нестабільної ситуації Росія намагалася зберегти свій геополітичний вплив. Особливе значення мала Грузія, яка за президенства Саакашвілі взяла курс на зближення з Заходом і вступ до НАТО. В кремлі це сприймалося як загроза його інтересам, кульмінацією чого стала російсько-грузинська війна в серпні 2008 року.

З 2011 року, APT28 надсилала журналістам та особам, пов’язаним з урядовими установами, електронні листи з інформацією, що цікавить одержувача, одночасно реєструючи веб-сайти, що імітують легітимні новинні сайти. Сьогодні ця тенденція не просто зберігається, а набула тотального характеру, де APT28 діє у всьому світі, націлюючись на декілька країн одночасно.

Якщо раніше це були переважно країни пострадянського простору, то тепер географія атак охоплює всю Європу, Північну Америку та Близький Схід. Ключовим пріоритетом залишається Україна, де центральні органи влади постійно перебувають під прицілом хакерів, про що свідчить нещодавня атака (січень 2026 року) з використанням вразливості Microsoft Office CVE-2026-21509, яку дослідники Zscaler Threat Labz пов’язали з APT28 через значний збіг інструментів, методів та процедур (TTP). Були атаковані користувачі у Центральній та Східній Європі, включаючи Україну, Словаччину та Румунію, де приманки соціальної інженерії були створені як англійською, так і локалізованими мовами, щоб орієнтуватися на споживачів у відповідних країнах.[10][11][12]

Рис. 1.3 – Вимпел «ВИО ГУ ГШ» - військові інформаційні операції. Червоним виділено символіку в/ч 26165.

Підрозділ складається з кількох команд, що зосереджені на різних аспектах кібер- та гібридних операцій ГРУ. Три відповідні команди включають операційну групу (Ops), групу розвитку операцій (DevOps), та групу операційної інфраструктури. Станом на грудень 2025 року, Борис Антонов обіймає старшу керівну посаду в підрозділі 26165, де він керує діяльністю операційної команди. Вперше його викрили ФБР та Міністерство юстиції США в 2018 році. Олексій Лукашев, Іван Єрмаков, Андрій Баранов були членами цієї команди.

Сергій Моргачов відповідав за керівництво розробників у підрозділі. Ця команда відповідає за розробку та управління шкідливим ПЗ підрозділу 26165, включаючи X-Agent та інструмент для витоку даних, відомий як X-Tunnel. Микола Козачок, Артем Малишев, Павло Єршов були членами цієї команди.

Анатолій Істомін відповідав за керівництво оперативною групою з питань інфраструктури. Підлеглими були: Ігор Бочка, Олексій Умець, Сергій Васюк, та інші. Ця група та її члени проводять низку оперативних заходів, включаючи закупівлю інфраструктури, тестування та налаштування, вилучення даних, дослідження відкритих джерел та розвідувальну підтримку операцій підрозділу, зосереджених на Україні.

Хоча й підрозділ 26165 переважно зосереджується на кібератаках, також він може діяти і у фізичному просторі. У 2018 році, уряд Нідерландів заявив, що у квітні в Гаазі затримали чотирьох агентів ГРУ, коли вони намагалися зламати Wi-Fi мережу організації із заборони хімічної зброї. ОЗХЗ розслідувала хімічну атаку на Сирію та атаку з використанням нервово-паралітичної речовини на Сергія Скрипаля – колишнього російського шпигуна у Великій Британії. Також, за словами Голландців, один із чотирьох агентів перебував у Малайзії, де займався розслідуванням авіакатастрофи, яка увійшла до десятки найбільших у історії людства – справи про літак «Boeing 777, MH17», збитим на сході України в 2014 році.

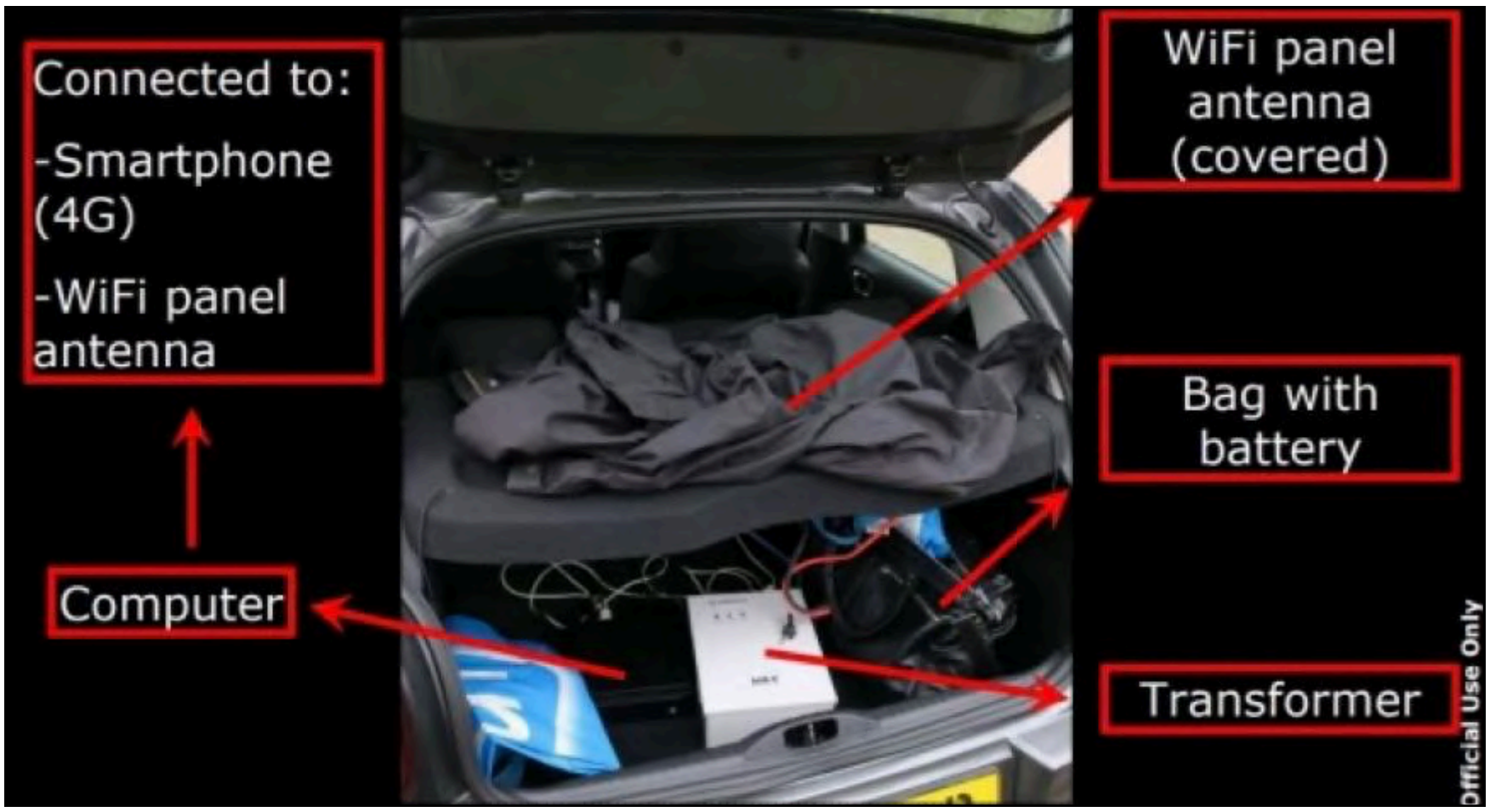

Рис. 1.4 – Обладнання, використовуване військовослужбовцями 26165 для атаки на Організацію заборони хімічної зброї в Гаазі (2018).

На порталі уряду Великої Британії підкреслено роль підрозділу 26165 у проведенні онлайн-розвідки цивільних укриттів у Маріуполі та Харкові 15 березня 2022 року.

16 березня 2022 року, ЗС РФ цілenаправлено завдали артилерійських ударів по Маріупольському драмтеатру, що призвело до загибелі мирних жителів та дітей, які там переховувалися.[14]

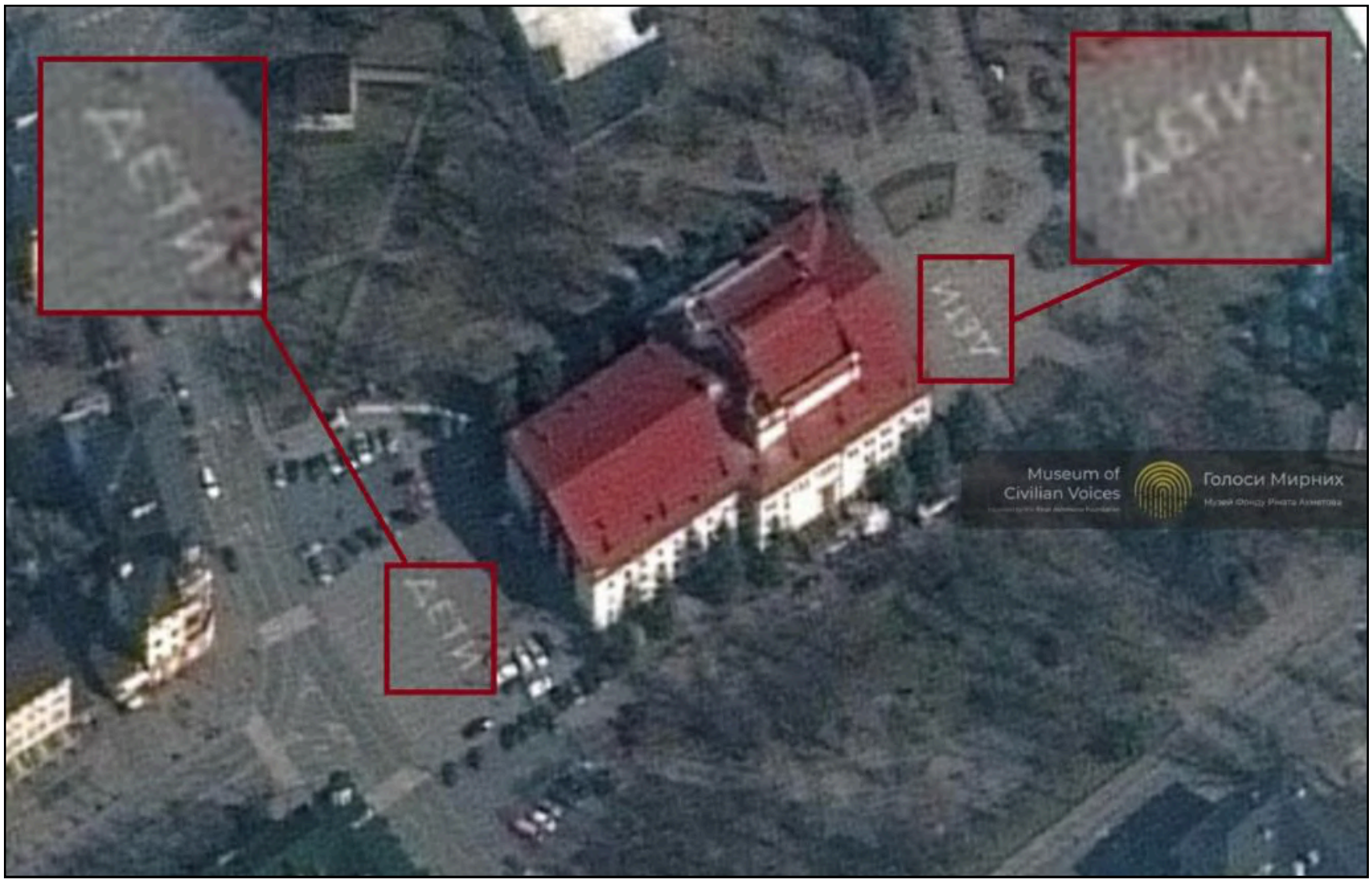

Рис. 1.5 – Напис «ДЕТИ» біля драмтеатру в м. Маріуполь

У силу того що російські збройні сили не досягли своїх військових цілей, а західні країни нарощували допомогу для підтримки оборони України, підрозділ 26165 розширив таргетинг на логістичні структури та технологічні компанії, залучені до доставки іноземної допомоги. Ця кампанія тривала понад два роки та була задокументована у спільному адвайзорі CISA/ NSA/FBI та партнерських агентств одинадцяти країн від 21 травня 2025 року. Підрозділ 26165 таргетував широке коло логістичних і технологічних провайдерів, компрометуючи організації практично в усіх видах транспортування – повітряному, морському та залізничному – у країнах НАТО, Україні та міжнародних організаціях. Окремим вектором розвідки стало використання камер відеоспостереження.

Починаючи з березня 2022 року, підрозділ 26165 проводив масштабні кампанії з компрометації IP-камер. Понад 80% скомпрометованих камер розташовані в Україні, помірно концентровані у Румунії та Польщі. Таким чином, інфраструктура цивільного відеоспостереження – муніципальні камери дорожнього руху, системи моніторингу портів, залізничних станцій і прикордонних переходів – перетворилася на інструмент стратегічної розвідки.

Для аналізу технічних методів та особливостей використання технік APT28, ми звернулися до MITRE ATT&CK. Реальна кількість атак та ідентифікаторів є значно більшою, ніж ті, що згадано у Додатку А, про технічні особливості APT-груп. Зазвичай техніки використовуються в логічній послідовності, яка залежить від мети та тактики атаки. Також, кількісне домінування (згадки) тактик у відкритих джерелах може бути наслідком кращого виявлення конкретних інструментів, а не об'єктивною оцінкою застосування.

Аналіз використовуваного програмного забезпечення показав, що APT28 використовує ПЗ власної розробки, з відкритих джерел та системні утиліти або інструменти (Living off the Land – LotL), вбудовані у операційні системи (Windows, Linux). Деякі назви програмного забезпечення були дані дослідниками, та можуть не відповідати оригінальній назві інструменту.

Цікавим фактом є те, що значна частина програмного забезпечення розроблена безпосередньо операторами APT28 або пов'язаними з ними розробниками. APT28 підтримує власні сімейства шкідливого ПЗ, прикладом цього є сімейство «Zebrocy», що відповідає за початковий доступ. «Sofacy», що відповідальне за основні бекдори та шпигунство, «X-Agent» – мобільне та кросплатформене шпигунство. Крім того, APT28 комбінує кастомне ПЗ із open-source інструментами та утилітами LotL. Варто виділити, що більшість ідентифікаторів (IoC) мають обмежений термін актуальності, оскільки APT28 регулярно змінює інфраструктуру, домени та файли, зберігаючи при цьому сталі поведінкові патерни.

Команда виявлення та реагування на кіберзагрози Sekoia проаналізувала заражені файли, що були задіяні у одній з атак APT28 та передавались українським військовим через месенджер Signal. Sekoia відзначає, що поширеність документації, пов'язаної з пораненими, також може свідчити про потенційний інтерес до поранених військовослужбовців, їхнього командування та підрозділів, що може бути взято до уваги для оцінки виснаження, оперативної готовності або психологічної стійкості в межах конкретних підрозділів. Схожа ситуація і з логістичними документами-приманками, які використовуються для легітимізації серед військового адміністративного персоналу, щоб зібрати розвідувальні дані про комбатантів на передовій.[13]

ПІДРОЗДІЛ ДЕСТРУКТИВНИХ ОПЕРАЦІЙ У КІБЕРПРОСТОРІ 74455 (APT44)

Діяльність підрозділу 74455 простежується з 2000-х років, проте публічно відомою група стала з 2009 року. 3 вересня 2014 року iSIGHT Partners виявила кампанію з фішингу, яка використовувала вразливість нульового дня CVE-2014-4114. Ця атака збіглася з самітом НАТО щодо України в Уельсі, та стала першою задукоментованою операцією APT44.

У звіті від 19.01.2026 року, ми описали діяльність групи, де APT44 є класичним прикладом «domain-oriented» підрозділу, існування якого визначається сферою компетенції: деструктивні операції та кіберсаботаж. На відміну від APT28 (шпигунство), APT44 зосереджується на руйнівних атаках, де часто метою виступає знищення інформації або пошкодження систем.

Однією з ключових особливостей та важливим «слідом» APT44 є створення та управління проксі-структурами, які видають себе за «народних хактивістів». Дослідження Mandiant (2022) встановило, що модератори Telegram-каналів «XakNet Team», «Infoccentr» та «CyberArmyofRussia_Reborn» координують свої операції з APT44. The Insider також описали випадок, коли канал «CyberArmyofRussia» опублікував інформацію про успішну атаку на півгодини раніше, ніж вона реально відбулася. Канал «Солцнепек», спочатку створений для публікації персональних даних українських військовослужбовців, за словами Mandiant, після ребрендингу у 2023 році, також став каналом, через який ГРУ «зливає» дані, отримані під час своїх зламів.[15][16]

Рис. 1.6 – Пам’ятний знак 10 років в/ч 74455

Підрозділ 74455, який є основою групи психологічної війни ГРУ, тісно співпрацює з «технічними» підрозділами та здійснює кібератаки на організації щонайменше з 2014 року. Цьому підрозділу приписують створення та розповсюдження шкідливого програмного забезпечення, що використовувалося для спуфінгу під час президентських виборів у США 2016 року, шкідливого програмного забезпечення NotPetya та атак на енергетичну інфраструктуру України.[17] Російські спецслужби конкурують одна з одною та часто проводять схожі операції проти тих самих цілей. Тому, іноді важко робити конкретні оцінки атрибуцій. Однак всередині ГРУ атаки можуть здійснюватися спільно, наприклад, згідно з обвинуваченням Мюллера, в/ч 74455 використовувала в інтересах Росії інформацію, викрадену в/ч 26165.

У червні 2016 року, посеред президентської виборчої кампанії в США, був створений блог на WordPress під ім’ям Guccifer 2.0. Представляючись румунським хакером-одинаком, він опублікував перший допис із викраденими документами DNC (Democratic National Commitet). Майже одночасно з цим, інтернет-платформа DCLeaks, яка позиціонувала себе як ініціатива американських «хактивістів», почала оприлюднювати особисте листування високопосадовців США та військових. Згодом були опубліковані 300 листів республіканців та персональні номери телефонів понад 200 законодавців. 15 серпня 2016 року було опубліковано файли Фонду Джорджа Сороса із внутрішніми робочими планами та інформацією про діяльність фонду по всьому світу.

У серпні 2016 року, кандидат у Конгрес від Флориди, зв’язався з Guccifer 2.0 із запитом отримати інформацію про свого опонента. Guccifer 2.0 надіслав запитувані викрадені дані. Республіканський стратег Аарон Невінс також зв’язався з Guccifer 2.0. Він створив Dropbox акаунт, куди Guccifer 2.0 завантажив 2.5 гігабайти даних. Невінс проаналізував дані, опублікував результати у своєму блозі і надіслав посилання Guccifer 2.0, той переслав посилання раднику Трампа – Роджеру Стоуну. Обвинувальний акт Міністерства юстиції США (2018) вказує, що:

- Guccifer 2.0 і DCLeaks контролювалися офіцерами ГРУ;
- в/ч 26165 здійснювала злом;
- в/ч 74455 брала участь у поширенні та інформаційній частині.

Інфраструктура та облікові записи в соціальних мережах, які адмініструвалися відділом Олексія Потьомкіна (офіцер в/ч 74455), використовувалися для сприяння оприлюдненню викрадених документів через DCLeaks та Guccifer 2.0. Військовослужбовці в/ч 74455 орендували сервер в Малайзії для хостингу сайту, управляли ним та створювали фальшивий образ «американських хактивістів». Створили WordPress блог, вели Twitter акаунт – Guccifer_2, комунікували з журналістами Vice та The Hill. За даними слідства, метою операції був вплив на президентські вибори та дискредитація демократичної партії.

За даними Mandiant, атака на енергетичний об’єкт в жовтні 2022 року, яку приписують «Sandworm» – підрозділу ГРУ 74455, є рідкісним прикладом кіберінциденту, що порушує фізичну роботу цільового об’єкта. За словами дослідників, вторгнення також включало раніше невідому техніку порушення промислових систем управління та операційних технологій. Це не лише перший публічний випадок відключення електроенергії внаслідок кібератаки з початку війни, але й перший випадок, коли такий інцидент збігся з ракетним ударом. В свою чергу, дослідники Ради економічної безпеки України та незалежного комунікаційного агенства «Truman», заявили, що Росія координувала цю діяльність з психологічними операціями, щоб заплутати свої цілі. Дослідники заявили, що Росія здійснила серію кібератак на енергетичну інфраструктуру наприкінці 2022 року, перш ніж завдати масованих ракетних ударів. Водночас, Москва розпочала пропагандистську кампанію, спрямовану на перекладання відповідальності за відключення електроенергії, спричинені цими атаками, на український уряд, державну владу та приватні енергетичні компанії.[18][19]

Кампанія з використанням «Infamous Chisel» була атрибутована APT44 спільним технічним звітом агентств Five Eyes (NCSC, CISA, NSA, FBI, ASD, CCCS, NCSC-NZ) від 31 серпня 2023 року, який містить детальний аналіз шкідливого ПЗ, розгорнутого проти Android-пристроїв українських військовослужбовців. Паралельно Служба Безпеки України опублікувала власний звіт, у якому приписала кампанію «військовій розвідці Росії та її хакерам». За словами начальника департаменту кібербезпеки СБУ Іллі Вітюка, відповідальність за кібератаки лежить безпосередньо на підконтрольній ГРУ групі Sandworm (APT44).

Принципово важливим є встановлений СБУ механізм первинного зараження. За висновком кіберекспертів відомства, противник захопив українські планшети на полі бою з метою поширення шкідливого програмного забезпечення та зловживання наявним доступом для проникнення у військові мережі. Таким чином, фізичне захоплення пристрою в ході бойових дій стало вектором подальшого кіберпроникнення – що є задокументованим прикладом поєднання кінетичних і кіберметодів на тактичному рівні. СБУ також зазначила, що оперативне реагування дозволило заблокувати спроби отримати доступ до конфіденційної інформації щодо діяльності ЗСУ, розгортання Сил оборони та їхнього технічного забезпечення.[20]

ОПЕРАЦІЙНО-ЦІЛЬОВИЙ ПІДРОЗДІЛ 29155 (CADET BLIZZARD)

Підрозділ 29155 – це гібридна військова частина, яка зосереджується як на фізичних так і на кібердиверсіях. Цей підрозділ не схожий на APT28 та APT44 за своїм призначенням, та не входить в систему військ інформаційних операцій, проте для демонстрації його впливу на кіберпростір ми вирішили розглянути цей випадок, адже Microsoft ідентифікує кіберкрило цього підрозділу як «threat group». Також, на урядовому порталі Великої Британії розміщена інформація щодо накладання санкцій на підрозділ 29155 (Cadet Blizzard) «в одному рядку» з 26165 та 74455. Підрозділ, що складається переважно з молодих новобранців, які працюють під керівництвом досвідчених керівників, має низку можливостей, але є погано дисциплінованим та хаотичним у проведенні своїх операцій.[14][21][22]

Cadet Blizzard – це кіберкрило військової частини 29155, що підтверджується оцінками CISA та ФБР. На відміну від APT-груп, підрозділ 29155 є «task-oriented» підрозділом, який діє в різних сферах, до яких можуть додаватися кіберкомпоненти. Діяльність підрозділу, можна описати як проектну роботу, де від цілі операції залежить застосування ресурсів військової частини, прикладом чого є «Отруєння Скрипалів у Солсбері», «Вибухи у Врбетиці» та в січні 2022 року, за місяць до повномасштабного вторгнення, Cadet Blizzard розгорнув вірус-винищувач WhisperGate проти IT-систем українських урядових установ. Також, Microsoft зазначає, що «...принаймні одна російська організація приватного сектору надала матеріальну підтримку «Cadet Blizzard» під час руйнівної атаки WhisperGate». За оцінками Microsoft, Cadet Blizzard діє щонайменше з 2020 року, з початковими компрометаціями східноєвропейських урядових та технологічних секторів з квітня 2021 року.[23]

«У серпні 2021 року, за п'ять місяців до повномасштабного вторгнення Росії, хакери військової частини 29155 спробували загострити конфлікт між українськими націоналістичними підрозділами та адміністрацією Володимира Зеленського… … Дотримуючись звичної схеми операцій під чужим прапором, Стігал залучив десятки дрібних інформаторів, щоб ті видавали себе за членів полку «Азов» – одного з найкращих воєнізованих формувань України, яке, привертало увагу на Заході через праві погляди своїх представників.

Він пішов далі й вийшов на зв'язок щонайменше з двома вищими командирами «Азова», видаючи себе за лідера чеченської дисидентської організації Ічкерія, яка виступає проти глави Чечні Рамзана Кадирова, і запропонував їм союз проти Зеленського. Введений в оману Стігалом, принаймні один із командирів «Азова» погодився на пропозицію допомоги.». The Insider не розкрив ім'я співрозмовника, який нині служить у Збройних силах України, оскільки, він не знав, що співпрацює з російською розвідкою (Стігал виступав від імені проукраїнського голови Чеченської республіки Ічкерія за кордоном Ахмета Закаєва).

Стігал завербував десятки агентів «малого калібру», які мали видавати себе за членів батальйону «Азов» і організовувати провокації. Серед файлів на сервері хакерів було знайдено папку «Графіті в містах», яка містить зображення образливих написів на адресу Зеленського, намальованих провокаторами на стінах українських міст (за що вони отримали від одного до п'яти доларів). До цієї операції була підключена завербована ГРУ болгарська журналістка Діляна Гайтанджиева. В 2022 році вона опублікувала, а потім видалила матеріал, в якому розповідалось про «конфлікт» Азова з ГРУ, при тому інтерпретація була така, що Азовці нібито отримували гроші від кадирівців.[24]

Рис 1.7 – Приклад графіті, оплаченого ГРУ РФ. ©The Insider

Як зазначив Пол Чічестер, директор операцій NCSC: «Викриття підрозділу 29155 як спроможного кібергравця ілюструє важливість, яку російська військова розвідка надає використанню кіберпростору для ведення своєї незаконної війни в Україні та інших державних пріоритетів».

ТАКТИКА ЗАСТОСУВАННЯ APT-ГРУП

Цей playbook є аналітичною реконструкцією операційної логіки APT-груп ГУ ГШ ЗС РФ, які діють у кіберпросторі. Його мета – пояснити, як стратегічні завдання військово-політичного керівництва трансформуються в конкретні дії військових частин, яким атрибується APT-профіль.

Початок кібероперацій підрозділів ГУ ГШ не є випадковим і пов’язаний з певними подіями. До стратегічних тригерів належать політичні або військові події, що створюють підвищену потребу у розвідувальній інформації або інформаційно-психологічному впливі, наприклад: міжнародні політичні кризи, військові конфлікти, виборчі кампанії в іноземних державах, дипломатичні конфлікти, запровадження міжнародних санкцій, ресурсні кризи, прориви у військовій сфері, протести або політичні кризи всередині держави, міжетнічні або міжрелігійні конфлікти, міжнародні скандали, тощо. У таких умовах кібероперації можуть використовуватися для збору розвідувальної інформації, впливу на інформаційний простір або створення додаткового тиску на цільові держави.

Операційні тригери зазвичай пов’язані з конкретними можливостями або умовами, що відкривають нові або спрощують можливості для здійснення атаки. У таких випадках рішення про проведення операції може прийматися на основі наявності сприятливих технічних умов. Також, окремі операції можуть запускатися на основі випадково отриманих можливостей. У подібних випадках операція може мати експериментальний або розвідувальний характер і використовуватися для подальшого розвитку доступу (доступ до компрометованих серверів або мереж, витоки облікових даних, тощо).

Аналіз операційної діяльності цих APT-груп демонструє, що застосовувані тактики не є фіксованим набором. Вони варіюються в залежності від типу цільової організації та залежить від багатьох факторів, а не тільки від бажання застосувати той чи інший інструмент. Часто сигнатурний підхід унеможливлює ефективну протидію і вимагає контекстно-орієнтованого моделювання загроз.

Розглянемо узагальнену модель playbook:

1) Стратегічне завдання.
Застосування проаналізованих у звіті підрозділів ГУ ГШ (APT-груп) починається з формування стратегічного завдання на рівні військово-політичного керівництва або відповідних структур військової розвідки (наприклад, ВІО). Цей етап передбачає визначення загальної мети операції, яка може включати збір розвідувальної інформації, саботажі, отримання компроматів, дестабілізацію інфраструктури, тощо.

2) Визначення цілі.
На цьому етапі здійснюється процес конкретизації цілей, де стратегічні задачі в межах «департаменту кіберпідрозділів» трансформуються у перелік конкретних установ, мереж або інфраструктурних об’єктів, які можуть містити необхідну інформацію або мати критичне значення для політичного впливу, функціонування держави, установи, сфери діяльності, тощо. Цей процес є ітеративним, оскільки, інформація, отримана на пізніших етапах може призвести до перевизначення або розширення початкового списку цілей.

3) Розвідка.

На етапі розвідки проводиться систематичний збір інформації про обрані цілі та їхню інфраструктуру. Значна частина цієї діяльності базується на використанні відкритих джерел. Також здійснюється технічна розвідка, що включає аналіз доменної інфраструктури, поштових серверів, мережевих сервісів та інших елементів IT та OT середовищ. Метою цього етапу є визначення потенційних точок входу до інформаційних систем, supply chain – вивчення підрядників та партнерів організації як потенційного вектора атаки та встановлення персональних зв'язків особистостей, що теж може бути потенційним вектором атаки.

4) Етап підготовки.

Цей етап передбачає створення технічних засобів, які будуть використані для проникнення в систему жертви. Зазвичай він включає реєстрацію доменів, що імітують легітимні ресурси, підготовку фішингових сторінок, налаштування серверів або модифікацію шкідливого ПЗ. Часто інфраструктура будується з використанням проксі-серверів, зламаних сайтів або легітимних хмарних сервісів, щоб ускладнити відстеження та блокування.

Одночасно можуть готуватися документи або повідомлення, які використовуються для соціальної інженерії.

5) Початковий доступ.

Початковий доступ до системи досягається шляхом використання методів соціальної інженерії або технічних вразливостей. Часто застосовується цільовий фішинг, спрямований на конкретних людей, які мають доступ до внутрішніх сервісів організації або є мішенню атаки. Також можуть використовуватися вразливості мережевих сервісів або корпоративних систем доступу.

6) Закріплення в системі.

Після проникнення до системи, атакуючі намагаються забезпечити довготривалий доступ до компрометованого середовища. Для цього можуть використовуватися різні механізми закріплення, які дозволяють відновлювати доступ після перевстановлення операційних систем або часткового усунення наслідків атаки, наприклад: використання буткітів для закріплення рівні ядра ОС, UEFI-руткітів, тощо. Контроль каналу доступу є критично важливим для подальших етапів операції, адже дозволяє поступово розширювати контроль над мережею. Важливою трансформацією сучасних кібероперацій є перехід від одноразових атак до довгострокового стратегічного закріплення у мережах противника. У ранніх моделях кібероперацій основною метою було виконання конкретного завдання, а після виконання операції доступ міг втрачатися або свідомо не підтримуватися. Сьогодні доступ до інформаційної системи дедалі частіше розглядається як довгостроковий стратегічний актив, який може використовуватися протягом тривалого часу. Саме така модель відстежується у діяльності підрозділу 26165, який у багатьох випадках виконує функцію підготовки доступу та довгострокового збору розвідувальної інформації. Отримані доступи можуть зберігатися протягом тривалого часу та використовуватися іншими підрозділами, зокрема 74455, для реалізації деструктивних або інформаційних операцій.

7) Доступ до облікових даних.

Після закріплення в системі, атакуючі прагнуть отримати облікові дані користувачів та адміністраторів, оскільки це дозволяє значно розширити їхні можливості всередині мережі та отримати доступ до більшої кількості інформації. Використовуючи певні інструменти та техніки, вони можуть перехоплювати паролі, отримувати токени автентифікації або використовувати вже наявні облікові записи для подальших дій.

8) Розповсюдження по мережі.

Легітимні протоколи та наявність привілеїв адміністратора дозволяють переміщатися всередині мережі організації компрометуючи інші системи та сервери. Таким чином, атакуючі розширяють зону контролю та отримують доступ до більш захищених сегментів мережі, де може зберігатися більш чутлива інформація.

9) Внутрішня розвідка.

Паралельно з переміщенням мережею проводиться внутрішня розвідка. Її метою є виявлення ключових інформаційних ресурсів, серверів та систем управління. Особливу увагу приділяють файловим сховищам, системам електронної пошти, базам даних та іншим компонентам, які можуть містити важливу інформацію. У випадку атак на інфраструктуру, додатково аналізуються системи промислового управління та технологічні мережі.

10) Збір даних.

Після ідентифікації необхідних ресурсів починається етап збору інформації. Залежно від характеру операції (розвідувальна або деструктивна) визначаються її основні цілі. Попри те, що такі операції фокусуються на різних технічних аспектах, між ними часто існує перетин. Під час деструктивної атаки, отримання доступу до інформації, яка має цінність, може виступати стратегічною складовою на рівні окремої операції або кампанії.

11) Command & Control

Для координації подальших дій встановлюється канал зв’язку між компрометованою системою та інфраструктурою операторів. Через цей канал передаються команди, оновлення шкідливого ПЗ та результати виконаних дій. Використання зашифрованого або маскованого трафіку дозволяє приховувати цей зв’язок серед легітимної мережевої активності.

12) Ексфільтрація.

Передача за межі мережі об’єкту атаки може відбуватися різними методами, які дозволяють уникнути виявлення системами моніторингу. Передача даних може здійснюватися поступово, невеликими обсягами, щоб замаскувати активність під звичайний мережевий трафік.

13) Вплив операції.

Фінальний етап, в більшості, але не завжди, залежить від початкової мети операції. Зазвичай результатом стає отримання інформації, яка використовується для подальшого аналізу або впливу, порушення роботи систем, знищення даних або виведення з ладу елементів інфраструктури.

14) Інформаційні операції.

У деяких випадках результати кібероперації використовуються в інформаційних кампаніях. Отримані матеріали можуть публікуватися у відкритому доступі або передаватися через посередницькі ресурси для створення інформаційно-психологічного ефекту. Таким чином кібероперація стає частиною інформаційно-психологічної діяльності, спрямованої на формування вигідного для ініціатора операції наративу або інтерпретації. Прикладом цього є підконтрольні APT44 проксі-канали, про які згадувалось у розділі про підрозділ 74455.

Реконструйований playbook демонструє, що кібероперації не здійснюються ізольовано окремими APT-групами, а є частиною більш широкого операційного процесу, у межах якого різні підрозділи виконують визначені функції на різних етапах операції. У цій моделі підрозділ 26165 зосереджений на довготривалому зборі інформації, підготовці доступу та формуванні технічних можливостей для подальших дій. Підрозділ 74455 спеціалізується на реалізації кібернетичних ефектів, включаючи деструктивні операції та атаки на критичну інфраструктуру.

Відповідно до реконструйованого плейбуку, типовий операційний цикл включає послідовні етапи стратегічного завдання, в окремих випадках – подальшу інформаційну або психологічну експлуатацію результатів атаки. Водночас, аналіз свідчить, що цей операційний цикл не завжди реалізується повністю. У багатьох випадках підрозділи діють автономно, виконуючи лише окремі етапи. Це дозволяє припустити, що система кібероперацій ГУ ГШ ЗС РФ поєднує централізоване стратегічне планування з відносною тактичною автономією виконавчих підрозділів.

Цей плейбук свідчить про наявність структурованої моделі ведення кібероперацій, у якій розвідувальні, деструктивні та гібридні компоненти можуть комбінуватися для досягнення різних ефектів у кібернетичному, інформаційному та політичному вимірах.

Аналіз діяльності підрозділів ГУ ГШ демонструє, що сучасні кібероперації дедалі більше інтегруються у ширшу систему стратегічного протиборства між державами. У цьому контексті діяльність проаналізованих APT-груп розглядається як частина довгострокової моделі операцій, спрямованих на формування стратегічних переваг у цифровому середовищі.

Реконструйований playbook демонструє відносно стабільну логіку дій. Особливу роль у цій моделі відіграє етап довгострокового збереження доступу, який дозволяє операторам не лише отримувати інформацію, але й формувати потенціал для майбутніх операцій впливу.

Важливою тенденцією є те, що доступ до мережі дедалі частіше розглядається як стратегічний ресурс, який може використовуватися протягом тривалого часу. Це змінює характер кібероперацій з одноразових атак до формування стійкої присутності у цифровій інфраструктурі противника.

Аналіз задокументованих операцій виявляє певну закономірність, де у ряді випадків кібератаки передували кінетичним ударам, та були скоординовані з ними за часом та цільовою аудиторією. Ця тенденція змінює модель загрози для операторів критичної інфраструктури, де кіберінцидент у таких умовах може бути не самостійною подією, а індикатором підготовки або початку кінетичного впливу на той самий об'єкт. Це свідчить про те, що модель скоординованих кібер-кінетичних операцій потенційно може набути більш широкого стратегічного застосування.

ДОДАТКИ

ДОДАТОК А. ТЕХНІЧНІ ХАРАКТЕРИСТИКИ APT-ГРУП НАЙПРИТАМАННІШІ ТЕХНІКИ APT28

Ми створили список із найпритаманніших технік для APT-груп за допомогою MITRE ATT&CK.

ID		НАЗВА	ЗАСТОСУВАННЯ
T1566	.001	Phishing: Spearphishing Attachment	APT28 sent spearphishing emails containing malicious Microsoft Office and RAR attachments.[37][10][11][3][22][17][21][16]
T1204	.001	User Execution: Malicious Link	APT28 has tricked unwitting recipients into clicking on malicious hyperlinks within emails crafted to resemble trustworthy senders.[14][16]
T1204	.002	User Execution: Malicious File	APT28 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts.[37][17][16]
T1078		Valid Accounts	APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has specifically used credentials stolen through a spearphishing email to login to the DCCC network. The group has also leveraged default manufacturer's passwords to gain initial access to corporate networks via IoT devices such as a VOIP phone, printer, and video decoder.[52][3][23][2]
T1078	.004	Cloud Accounts	APT28 has used compromised Office 365 service accounts with Global Administrator privileges to collect email from user inboxes.[2]
T1003		OS Credential Dumping	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[47][3][14]
T1003	.001	LSASS Memory	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[47][3] They have also dumped the LSASS process memory using the MiniDump function.[2]
T1003	.002	Security Account Manager	During APT28 Nearest Neighbor Campaign, APT28 used the following commands to dump SAM, SYSTEM, and SECURITY hives: reg save hklm\sam, reg save hklm\system, and reg save hklm\security.[27]

ID		НАЗВА	ЗАСТОСУВАННЯ
T1003	.003	NTDS	APT28 has used the ntdsutil.exe utility to export the Active Directory database for credential access.[2] During APT28 Nearest Neighbor Campaign, APT28 dumped NTDS.dit through creating volume shadow copies via vssadmin.[27]
T1210		Exploitation of Remote Services	APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[6][40][41]
T1114	.002	Email Collection: Remote Email Collection	APT28 has collected emails from victim Microsoft Exchange servers.[3][2]
T1567		Exfiltration Over Web Service	APT28 can exfiltrate data over Google Drive.[21] During APT28 Nearest Neighbor Campaign, APT28 exfiltrated data over public-facing webservers – such as Google Drive.[27]
T1070	.001	Indicator Removal: Clear Windows Event Logs	APT28 has cleared event logs, including by using the commands wevtutil cl System and wevtutil cl Security.[5][3]
T1070	.004	Indicator Removal: File Deletion	APT28 has intentionally deleted computer files to cover their tracks, including with use of the program CCleaner.[3]
T1070	.006	Indicator Removal: Timestomp	APT28 has performed timestomping on victim files.[5]

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТОВУВАНЕ APT28

ID	НАЗВА	ТИП	ОПИС
S0045	ADVSTORESHELL	Custom	C2 backdoor with data archiving and keylogging
S0351	Cannon	Custom	Email-based C2 backdoor. Screen capture and file discovery
S0023	CHOPSTICK	Custom	Modular C2 framework. Keylogging and file search
S0137	CORESHELL	Custom	C2 backdoor for persistence and local reconnaissance
S0243	DealersChoice	Custom	Exploitation framework for browser/document exploitation and payload delivery
S0134	Downdelph	Custom	Bootkit providing kernel-lvl persistence and stealthy DLL injection

S0502	Drovorub	Custom	Linux malware toolkit with kernel rootkit and C2 agent
S0410	Fysbis	Custom	Linux backdoor providing remote shell and persistence
S0135	HIDEDRV	Custom	Stealth driver for file hiding and DLL injection
S0044	JHUHUGIT	Custom	C2 implant using COM hijacking for persistence
S0162	Komplex	Custom	macOS backdoor with C2 communication and hidden file exfiltration
S0397	LoJax	Custom	UEFI rootkit providing firmware-lvl persistence
S0138	OLDBAIT	Custom	Targeted credential harvesting
S0136	USBStealer	Custom	Data exfiltration for air-gapped systems via USB.
S0314	X-Agent (Android)	Custom	Android spyware with surveillance and data exfiltration
S0161	XAgentOSX	Custom	macOS spyware with keylogging and screen capturing
S0117	XTunnel	Custom	C2 tunneling tool providing traffic proxying and remote shell access
S0251	Zebrocy	Custom	Multi-language initial access backdoor
S0250	Koadic	Open Source	Post-exploitation framework with JScript/ VBScript RAT capabilities
S0002	Mimikatz	Open Source	Credential dumping tool targeting LSASS and SAM
S1187	reGeorg	Open Source	SOCKS proxy tool for internal network pivoting
S0174	Responder	Open Source	LLMNR/NBT-NS poisoning for NTLM credential interception
S0183	Tor	Open Source	Anonymization network used for C2 traffic concealment
S0191	Winexe	Open Source	Remote command execution for Windows systems
S0160	Certutil	LotL	Payload download and Base64 encoding/ decoding
S1205	cipher.exe	LotL	Secure file wiping
S0193	Forfiles	LotL	Indirect command execution
S0039	Net	LotL	Network discovery and account management

S0108	netsh	LotL	Firewall modification and port forwarding
S0645	Wevtutil	LotL	Event log management and log clearing

НАЙПРИТАМАННІШІ ТЕХНІКИ APT44

ID		НАЗВА	ЗАСТОСУВАННЯ
T1566	.001	Phishing: Spearphishing Attachment	Sandworm Team has delivered malicious Microsoft Office and ZIP file attachments via spearphishing emails.[31][30][22][1][37][14] During the 2015 Ukraine Electric Power Attack, Sandworm Team obtained their initial foothold into many IT systems using Microsoft Office attachments delivered through phishing emails. [35]
T1566	.002	Phishing: Spearphishing Link	Sandworm Team has crafted phishing emails containing malicious hyperlinks.[1]
T1190		Exploit Public-Facing Application	Sandworm Team exploits public-facing applications for initial access and to acquire infrastructure, such as exploitation of the EXIM mail transfer agent in Linux systems.[27][13]
T1003	.001	OS Credential Dumping: LSASS Memory	Sandworm Team has used its plainpwd tool, a modified version of Mimikatz, and comsvcs.dll to dump Windows credentials from system memory. [22][26][11] During the 2016 Ukraine Electric Power Attack, Sandworm Team used Mimikatz to capture and use legitimate credentials.[18]
T1003	.003	OS Credential Dumping: NTDS	Sandworm Team has used ntdsutil.exe to back up the Active Directory database, likely for credential access.[11]
T1021	.002	Remote Services: SMB/ Windows Admin Shares	Sandworm Team has copied payloads to the ADMIN$ share of remote systems and run net use to connect to network shares.[18][11] During the 2016 Ukraine Electric Power Attack, Sandworm Team utilized net use to connect to network shares.[18]

T0855		Unauthorized Command Message	During the 2015 Ukraine Electric Power Attack, Sandworm Team issued unauthorized commands to substation breaks after gaining control of operator workstations and accessing a distribution management system (DMS) application. [35] During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[20]
T0846		Remote System Discovery	During the 2015 Ukraine Electric Power Attack, Sandworm Team remotely discovered operational assets once on the OT network.[36][15]
T1561	.002	Disk Wipe: Disk Structure Wipe	Sandworm Team has used the BlackEnergy KillDisk component to corrupt the infected system's master boot record.[30][26]
T1486		Data Encrypted for Impact	Sandworm Team has used Prestige ransomware to encrypt data at targeted organizations in transportation and related logistics industries in Ukraine and Poland.[11]

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТОВУВАНЕ APT44

ID	НАЗВА ПЗ	ТИП	ОПИС
S1167	AcidPour	Custom	Wiper for Linux
S1125	AcidRain	Custom	Wiper for modems/routers
S0606	Bad Rabbit	Custom	Ransomware
S0089	Black Energy	Custom	DDoS and espionage framework
S0693	CaddyWiper	Custom	Wiper
S0555	CHEMISTGAMES	Custom	Espionage malware
S0154	Cobalt Strike	Open Source	PenTest tool (abused)
S0687	Cyclops Blink	Custom	Backdoor for network devices
S0363	Empire	Open Source	Post-exploitation framework
S0401	Exaramel Linux	Custom	Backdoor for Linux
S0343	Exaramel Windows	Custom	Backdoor for Windows

S0342	GreyEnergy	Custom	Successor to BlackEnergy
S0357	Impacket	Open Source	Toolkit for working with network protocols
S0604	Industroyer	Custom	Attack on industrial systems
S1072	Industroyer2	Custom	Variant targeting substations
S0231	Invoke-PSImage	Open Source	Hiding PowerShell in .png
S1190	Kapeka	Custom	Backdoor
S0607	KillDisk	Custom	Wiper
S0002	Mimikatz	Open Source	Password stealing
S0039	Net	LotL	Disks mounting, stopping services
S0368	NotPetya	Custom	Pseudo-ransomware / effectively a wiper
S0365	OlympicDestroyer	Custom	Wiper
S0598	P.A.S. Webshell	Custom	Web backdoor
S0378	PoshC2	Open Source	Powershell C2 framework
S1058	Prestige	Custom	Wiper
S0029	PsExec	LotL	Remote command execution
S0195	SDelete	LotL	Secure file deletion tool
S1010	VPNFilter	Custom	Malware for routers

ДЖЕРЕЛА

1. OSINT & Phaleristics: Unveiling GRU’s Information Operations Troops (VIO) © CheckFirst 2026

2. Безєк А. 攻心为上：揭秘俄罗斯GRU的心理战“前线部队” [Психологічні операції як зброя: розкриття "фронтових підрозділів" психологічної війни ГРУ РФ]. Бєзєк Лаб / SecurityLab, 4 березня 2021

3. Мачульський Є. Російські інформаційно-психологічні війська: одкровення полоненого підполковника. Цензор.НЕТ, 28.07.2022

4. Головне управління розвідки Міністерства оборони України. Ідентифіковано кадрових військовослужбовців ЗС РФ, які воюють на сході України. 27 жовтня 2016

5. shoygu-secretar. Серые мыши в Центральном и Восточном военных округах. LiveJournal, 2020

6. shoygu-secretar. Как тупой солдат может спалить деятельность секретной части ГРУ? LiveJournal, 2020

7. OSINT-бджоли. Хто на росії займається ІПСО. 24 травня 2024

8. «Телебачення Торонто». Журналісти «Телебачення Торонто» викрили секретний російський підрозділ ГРУ. Media Sapiens, 4 травня 2023

9. Meduza. Psy-ops in high places: Putin’s new science adviser to Russia’s National Security Council is a military intelligence agent accused of spreading disinformation about the coronavirus. 17 травня 2021

10. Paoli C. Russian Hackers Continue Exploiting Microsoft Office Zero-Day After Emergency Patch. 4 лютого 2026

11. ThreatLabz. APT28 Leverages CVE-2026-21509 in Operation Neusploit. Zscaler, 3 лютого 2026

12. Trellix. APT28’s Stealthy Multi-Stage Campaign Leveraging CVE202621509 and Cloud C2 Infrastructure

13. Amairy G., Charles M., Sekoia TDR. APT28 Operation Phantom Net Voxel. Sekoia, 16 вересня 2025

14. UK Government. Profile: GRU cyber and hybrid threat operations. 4 грудня 2025

15. The Insider. Google доказал причастность ГРУ к новым атакам на электростанции США и взломам российских журналистов. 18 квітня 2024

16. Mandiant. Hacktivists Collaborate with GRU-sponsored APT28. Google Cloud Blog, 26 березня 2024

17. Proska K. та ін. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Mandiant / Google Cloud Blog, 9 листопада 2023

18. Національний координаційний центр кібербезпеки (NCSCC). Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії. 17 січня 2023

19. Доброхотов Р. «Песчаный червь». Как хакеры ГРУ отключали электростанции в Украине, взламывали избирком США и создали самый разрушительный вирус в мире. The Insider, 22 жовтня 2020

20. Security Service of Ukraine (SBU). SBU exposes russian intelligence attempts to penetrate Armed Forces' planning operations system. 08.08.2023

21. Доброхотов Р., Швецова К. Мошенники, убийцы, студенты. Из кого ГРУ собрало команду хакеров-провокаторов и почему она провалилась. The Insider, 2 червня 2025

22. Microsoft Threat Intelligence. Cadet Blizzard. Microsoft Security Insider

23. National Cyber Security Centre (NCSC). UK and allies uncover Russian military unit carrying out cyber attacks and digital sabotage for the first time. 5 вересня 2024

24. Dobrokhotov R., Shvetsova K. Hidden Bear: The GRU hackers of Russia’s most notorious kill squad. The Insider, 31 травня 2025

25. CISA, NSA, FBI, NCSC-UK, BND, BSI, BfV, VZ, NÚKIB, BIS, ABW, SKW, DC3, USCYBERCOM, ASD’s ACSC, CCCS, DDIS, EFIS, NCSC-EE, ANSSI, MIVD. Russian GRU Targeting Western Logistics Entities and Technology Companies. 20 травня 2025

26. Brandefense CTI Analyst Team. SandWorm APT Group Cyber Intelligence Report (Summary). 19 жовтня 2022

27. Rewards for Justice (U.S. Department of State). Сотрудники ГРУ — Воинская часть 29155

28. Council of the European Union. Council Decision (CFSP) 2025/171 of 27 January 2025 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, 27 січня 2025

29. Council of the European Union. Council Decision (CFSP) 2024/3174 of 16 December 2024 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia’s destabilising activities. Official Journal of the European Union, 16 грудня 2024

30. Cheravitch J. The Role of Russia's Military in Information Confrontation. CNA, червень 2021