Аналітичний звіт APT44 Sandworm

19.01.2026

APT44, також відома як Sandworm, — це група кіберзлочинців, що належить до військової частини ГРУ 74455, підрозділ кібервійни ГУ ГШ ЗС РФ. Група існує з 2009 року. Хакерські кампанії Sandworm охоплюють як шпигунство та крадіжку облікових даних, так і масштабні руйнівні атаки, що впливають на критичну інфраструктуру в усьому світі.

Назва: Sandworm, APT44

Інші відомі назви: ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Seashell Blizzard, FROZENBARENTS, BE2 APT, Hades (за даними Kaspersky Lab), Blue Echidna, UAC-0002 (в переліку загроз CERT-UA), SANDFISH, Sunglow Blizzard, DEV-0665

APT44 неодноразово атакували Україну та країни НАТО. Атаки були спрямовані на критичну інфраструктуру, державні органи та органи місцевого врядування, медіа, телекомунікації, виборчий процес та політичну сферу країн. Операції Sandworm характеризуються розвинутою технічною складовою, багатоетапними процесами атак, значними збитками для атакованих країн, та участю Sandworm в геополітичних конфліктах. З 2014 року діяльність групи постійно розширюється і є значимим фактором в російсько-українській війні.

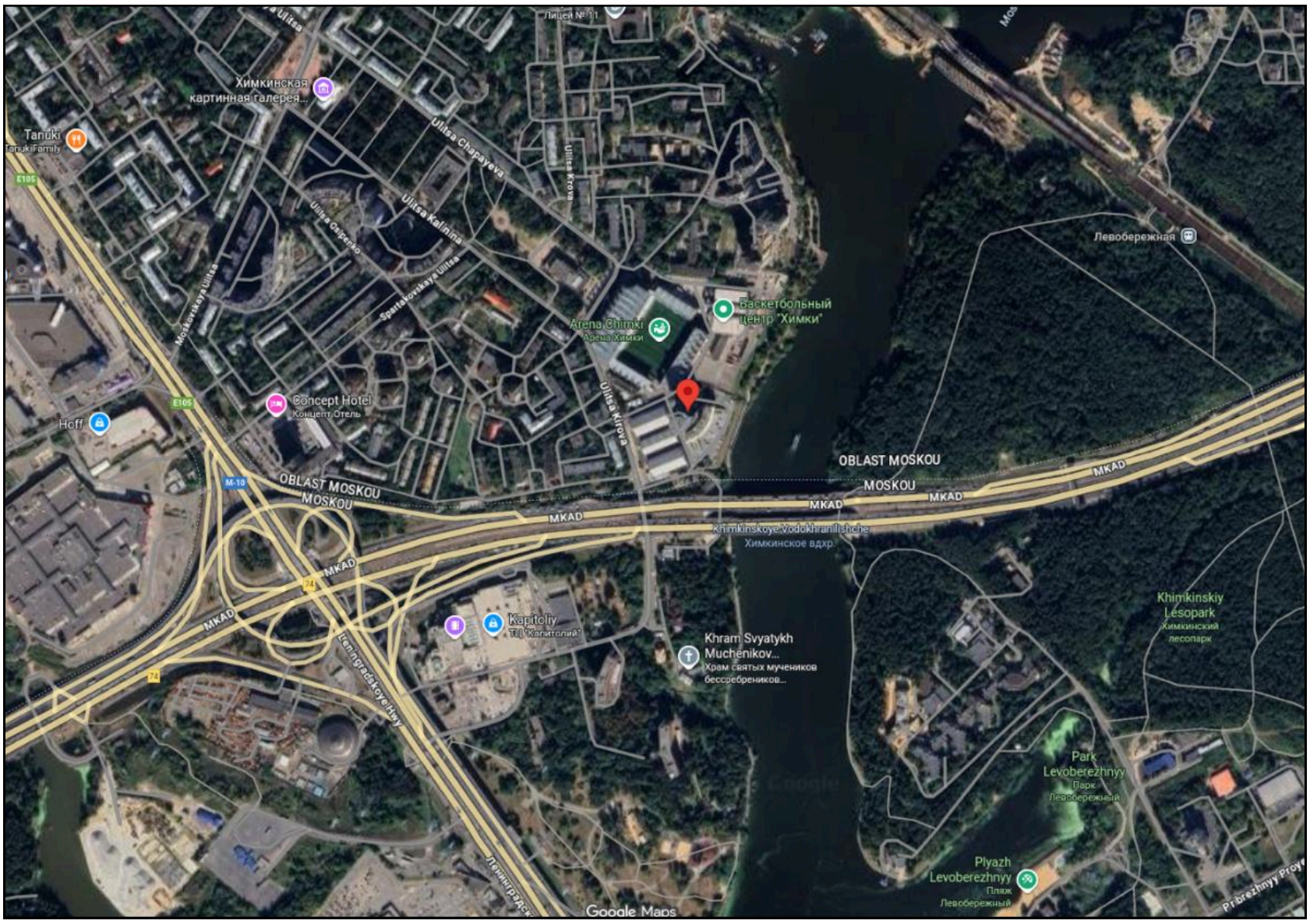
Ранні операції APT44 полягали у використанні уразливостей нульового дня в Microsoft Office, фішингових кампаніях проти українських та пов'язаних з НАТО організацій. У 2015 році Sandworm спричинила перше відоме відключення електроенергії, викликане шкідливим програмним забезпеченням, використавши BlackEnergy3 для атаки на українські електромережі. Ще однією відомою розробкою APT44 є вірус NotPetya, випущений у 2017 році через скомпрометований ланцюжок постачання програмного забезпечення, що завдав збитків на мільярди доларів у всьому світі. Sandworm також розширив свої кампанії за межі України, включаючи атаку Olympic Destroyer на Зимові Олімпійські ігри 2018 року в Пхьончхані, вибори у Франції та операцію з масового зламу веб-сайтів урядових і медійних організацій Грузії у 2019 році. Проте головною ціллю протягом усього періоду існування групи APT44 залишається Україна.

Місцезнаходження

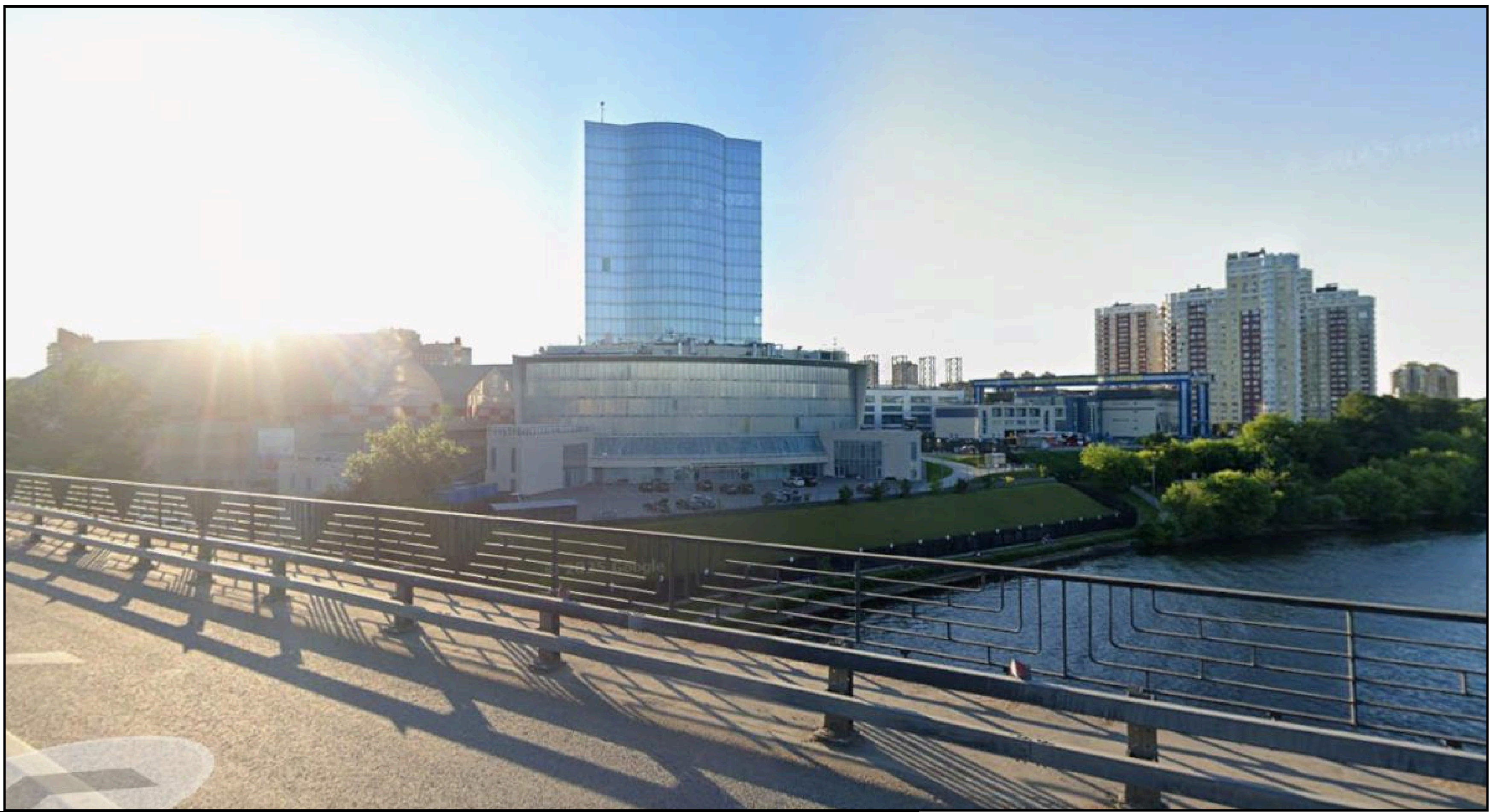
Існує декілька найбільш вірогідних адрес, за якими працює APT44 та її субкластери.

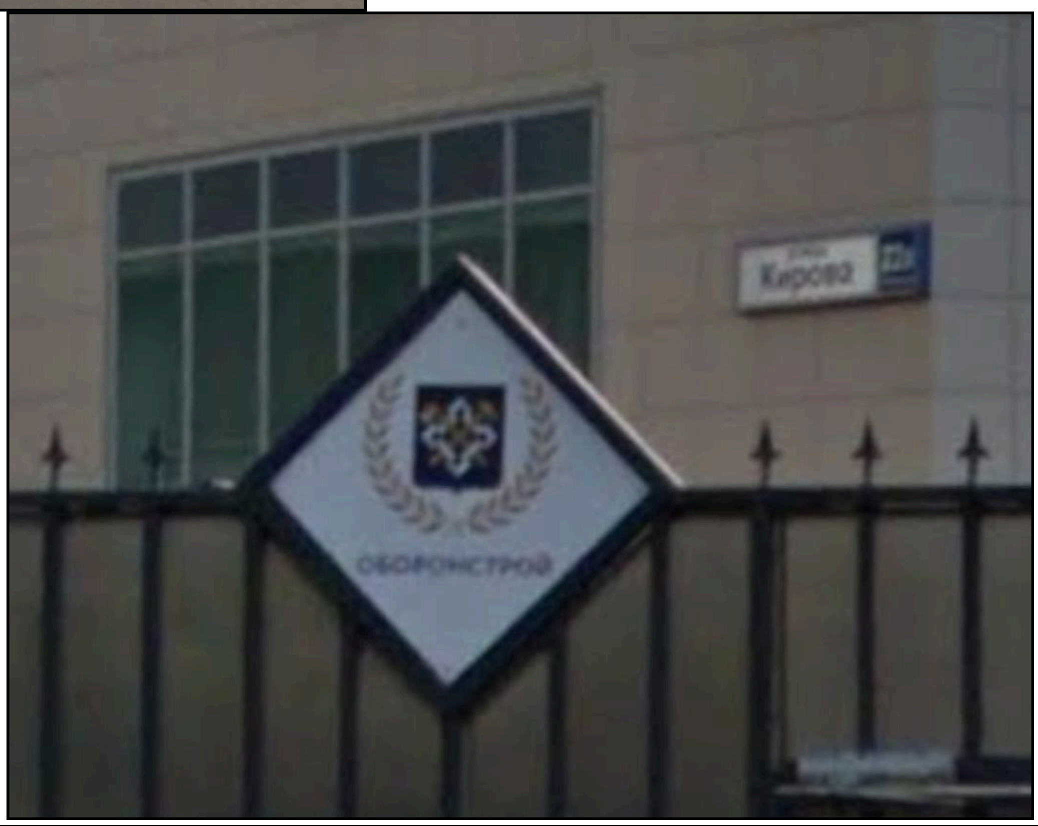
1. **«Башня»/«Рота-Тауэр»/бізнес-центр «Новатор»**
   Адреса: Вулиця Кірова, 22а, Хімки, Московська область, Росія, 125445
   Координати входу: 55°53'02.4"N 37°27'20.5"E

Ця адреса згадується у звинуваченні уряду США проти 12 російських хакерів як місце, звідки здійснювалися атаки. Шестеро із звинувачених — співробітники в/ч 74455, яка, як вказано у звинуваченні, знаходиться за даною адресою.



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




Кирова
ОБОРОНСТРОЙ

2. в/ч 40904 і 28-й ЦУС «Аврора»

Адреса: військове містечко №48/1, м. Москва, вул. Свободи, буд. 21/2

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

Розслідування Радіо Свобода від 17.07.2018 вказує на дану адресу як одне з можливих місць дислокації в/ч 744557 або APT44 чи їх субкластерів:

3. Комплекс будівель штаб-квартири ГРУ

Адреса: Москва, Хорошевське шосе, будинок 76, корпус Б

Координати будівлі: 55°46'58.8"N 37°31'19.6"E

Те саме розслідування Радіо Свобода вказує на цю адресу як одну з потенційних адрес в/ч 744557

Ключові особи

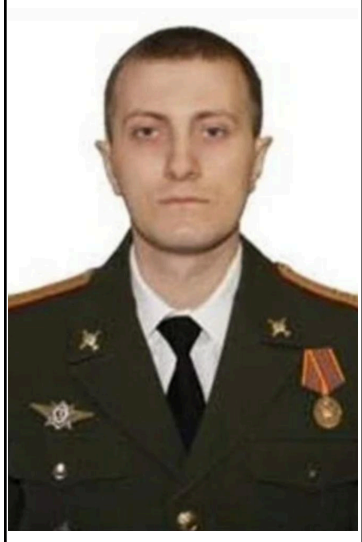
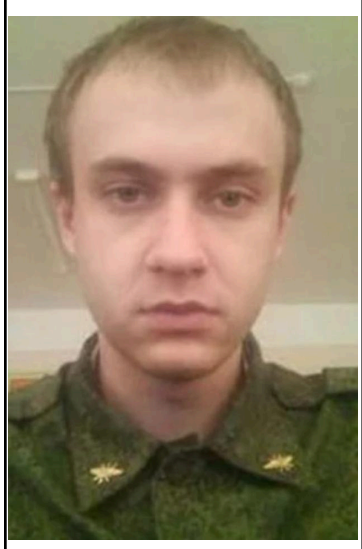
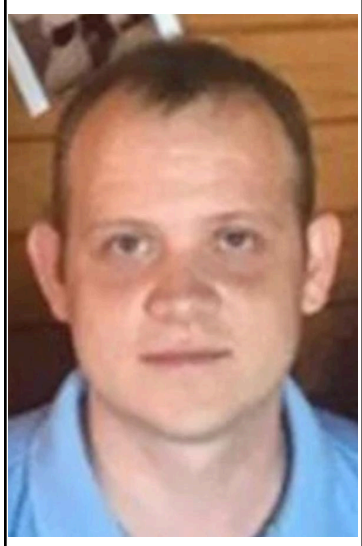
Наразі підтверджено шестеро осіб, що є офіцерами ГРУ в/ч 74455, які координували і здійснювали хакерські кібератаки проти України та інших країн в складі APT44.

19 жовтня 2020 Департамент юстиції США висунув звинувачення 6 російським офіцерам, які проходять службу у складі Головного центру спеціальних технологій (в/ч 74455) ГУ ГШ ЗС Російської Федерації, звинувативши їх у скоєнні глобальних кібератак проти США, України, Франції, Грузії, Південної Кореї, Великої Британії та інших країн, а також за поширення небезпечних вірусних програм у світі, які спричинили мільярдні збитки.

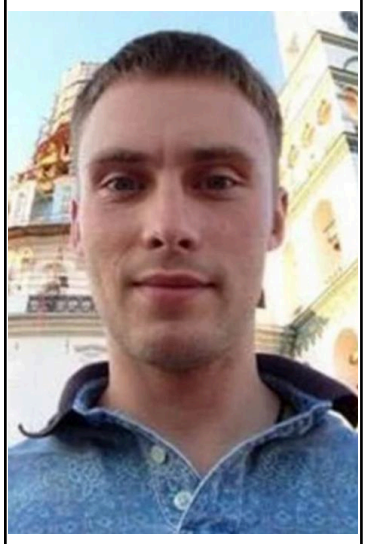
У обвинувальному акті фігурують російські військові Юрій Андрієнко, Сергій Детистов, Павел Фролов, Артем Очиченко, Петро Пліскін, Анатолій Ковальов.

SHUM

Ключові особи

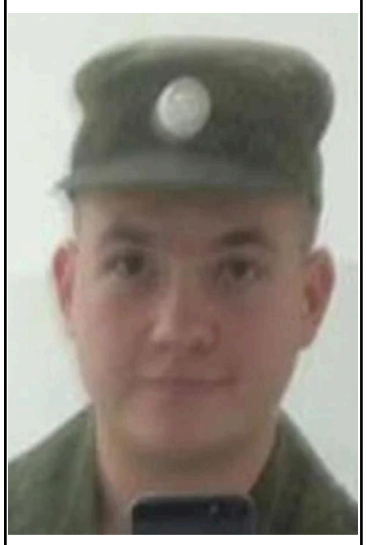
	**Сергій Володимирович Детистов** • Дата і місце народження: 1985.07.21, Ростов-на-Дону • Місце проживання: м. Москва, вул. Фомичевой, б. 7, стр. 2, кв. 177 / Московська обл., м. Ватутінки, б.53, кв.243 • Паспортні дані: (RU) 6005448327 • Контакти: markelovsv@alfa-lnk.ru, hab@ya.ru, sergo.voronkin@mail.ru, sergovoronkin@mail.ru, 79165745468@ya.ru, sergeokhripkov@gmail.com, sdetistov@gmail.com, alligero@mail.ru+79772882928,+79199961314, +79164548675,+79852028077,+79165745468, TG: 67894811 • Додаткова інформація: timezone: Europe/Moscow,ip: 185.52.31.163 • Посада: офіцер в/ч 74455 ГУ ГШ РФ • Діяльність в APT44: Розробив компоненти шкідливого програмного забезпечення NotPetya; підготував фішингові кампанії, спрямовані на Зимові Олімпійські ігри 2018 року в Пхьончхані
	**Павел Валерійович Фролов** • Дата і місце народження: 07.06.1992, м. Калуга • Місце проживання: м. Москва, вул. Свободи, б. 21/2 (одне з можливих місцезнаходжень в/ч 74455); обл. Калузька, м. Калуга, вул. Калужского Ополченія, б. 5, Квартира 137; обл. Калузька, м. Калуга вул. Трамплінная, б. 1, Корпус В; обл. Калузька, м. Калуга, вул. Академіка Королева, б. 16. • Паспортні дані: (RU) 2912547750, ІНН 402914808123, СНИЛС 13043246508 • Контакти: +79105984581, +79916244342, HAN-92@mail.ru, han-92@mail.ru, Han-92@mail.ru, agueroam@rambler.ru, vk.com: Серхио Кун Агуеро • Додаткова інформація: - • Посада: офіцер в/ч 74455 ГУ ГШ РФ • Діяльність в APT44: розробляв компоненти шкідливих програм KillDisk і NotPetya.
	**Юрій Сергійович Андрієнко** • Дата і місце народження: 30.05.1988, Мінськ, Білорусь • Місце проживання: 142855 Росія, Московська обл., Ступінський р-н, с. Мещеріно, тер. Мещеріно-1, б. 12, кв. 23; Московська область, Лобня Крупской 14 А, кв. 18 • Паспортні дані: (RU) 4608230478, ІНН 504506704482, СНИЛС 11278100218 • Контакти: +79250784526; +79197222438, Janetm@list.ru, janetm@list.ru, alexey_452@list.ru; janettravel@mail.ru • Додаткова інформація: автомобіль X527AA199 • Посада: офіцер в/ч 74455 ГУ ГШ РФ • Діяльність в APT44: Розробляв компоненти шкідливого програмного забезпечення NotPetya та Olympic Destroyer

SHUM



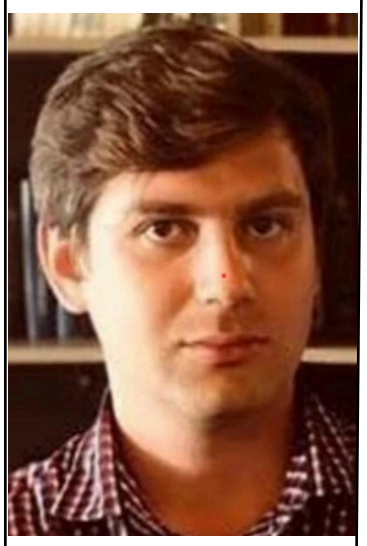
Анатолій Сергійович Ковальов

- Дата і місце народження: 02.08.1991, Тотьма, Вологодська область, Росія
- Місце проживання: обл. Орловська, м. Орел, ш. Кромское, б. 4, Комната 20606; обл. Орловська, м. Орел, ш. Кромское, б. 4, Комната 132; край Краснодарський, р-н Анапський, м. Анапа, пр-кт Піонерский б. 34; обл. Орловська, м. Орел, ш. Кромское, б. 4; м. Москва, вул. Нагорная, б. 20, Корпус 3, Квартира 44; обл. Орловська, м. Орел, ш. Кромское, б. 4, Комната 11010; м. Москва, вул. Свободи, б. 21, Корпус 2, Комната ВЧ (одне з можливих місцезнаходжень в/ч 74455); обл. Брянська, р-н Суземський, п. Суземка, вул. Советская. б. 6; обл. Брянська, р-н Суземський, п. Суземка, пл. Леніна, б. 9, Корпус 3, Квартира 13; м. Москва, внутрішньоміська територія, поселення Десенівське, Нововатутінський проспект, буд. 1; м. Москва, внутрішньоміська територія, поселення Десенівське, Нововатутінський проспект, б. 2.
- Паспортні дані: (RU) 1511951536, ІНН 322800244201, СНИЛС 19849671556
- Контакти: +79150556650, +79150556850 ask.homemail@gmail.com
- Додаткова інформація: реєстрація проживання в м. Анапа, пр-кт Піонерський, б. 34 можливо вказує на причетність до роботи у ФГАУ ВИТ «ЭРА» (2539025440, розробка дронів, засобів зв'язку і криптографічних систем), що розташована поруч за адресою пр-кт Піонерський, б. 41.
- Посада: офіцер в/ч 74455 ГУ ГШ РФ
- Діяльність в APT44: розробляв техніки та повідомлення для цільового фішингу, які використовуються для атак на посадових осіб En Marche!; співробітників DSTL; членів МОК та олімпійських спортсменів; співробітників грузинського ЗМІ.ських спортсменів; співробітників грузинського ЗМІ.



Артем Валерійович Очиченко

- Дата і місце народження: 8.11.1992., Сосновка, Росія
- Місце проживання: край Краснодарський, м. Геленджик, вул. Маячная, б. 9; м. Москва, вул. Свободи, б. 21, Корпус 2, Квартира ВЧ (одне з можливих місцезнаходжень в/ч 74455); обл. Московська, р-н Одинцовський, м. Кубінка, вул. Сосновка, б. 80, Квартира 2;
- Паспортні дані: (RU) 4612867190, міжнародний: 460779249, СНИЛС 13966746517
- Контакти: +79999870195, +79778814491, nataly.gonn79@gmail.com, mulen07@rambler.ru, NATALY.GONN79@gmail.com
- Додаткова інформація: також знаходиться в базах за іменем Гончаров Артем Валерьевич, дата, місце народження, місце реєстрації і СНИЛС співпадають, номер паспорта: (RU) 4607792497 — це також номер старого недійсного паспорта Очиченко, виданого у 2006 р.
- Посада: офіцер в/ч 74455 ГУ ГШ РФ
- Діяльність в APT44: Брав участь у кампаніях спіфішингу, спрямованих проти партнерів Зимових Олімпійських ігор 2018 року в Пхьончхані; проводив технічну розвідку офіційного домену парламенту Грузії та спробував отримати несанкціонований доступ до його мережі.

	**Петро Миколайович Пліскін** • Дата і місце народження: 26.08.1988, м. Хабаровськ, Росія • Місце проживання: м. Москва, вул. Свободи, б. 21, Корпус 2, Квартира ВЧ (одне з можливих місцезнаходжень в/ч 74455) • Паспортні дані: (RU) 0808773870, ІНН 773391089500, СНИЛС 20127219101 • Контакти: +79164357059, +79818006135; +79118485441; +79151389409, P.N.PLISKIN@gmail.ru, zemeloev@yandex.ru, p.n.pliskin@gmail.ru • Додаткова інформація: автомобіль Nissan X-Trail 2011р, реєстраційний номер Н696МЕ197, автомобіль О410СТ799, автомобіль Н211ОТ77, автомобіль А425РН197, автомобіль Т353ОК197 • Посада: офіцер в/ч 74455 ГУ ГШ РФ • Діяльність в APT44: Розробляв компоненти шкідливого програмного забезпечення NotPetya та Olympic Destroyer

Примітка

За адресою м. Москва, вул. Свободи, б. 21, Корпус 2, Квартира ВЧ (також варіант написання м. Москва, вул. Свободи, б. 212), де вірогідно знаходиться в/ч 74455, зареєстровано:

- Крестьянинов Євген Анатолійович 25.05.1984
- Тишин Кирило Сергійович 06.08.1995
- Жуковський Михайло Володимирович 21.11.1990 (зареєстрований також в м. Анапа пр-кт Пионерский б. 41 — місце офіційної реєстрації розробника засобів зв'язку і криптографічних систем ФГАУ ВИТ «ЭРА” 2539025440)
- Урасков Юрій Леонідович 12.04.1990
- Бехметьєв Дмитро Євгенович 28.04.1993 (зареєстрований також в м. Анапа пр-кт Пионерский б. 41)
- Андреєв Павло В’ячеславович 19.03.1986

Хоча достовірний зв'язок цих осіб з хакерською діяльністю APT44 не було встановлено, вважаю необхідним надати імена в звіті через можливий зв'язок із розробником криптографічних систем і приписку до вірогідної дислокації в/ч 74455.

Пов’язані структури і групи

APT44 Sandworm тісно пов'язані з іншою кіберзагрозою: APT28 Fancy Bear, яку приписують до в/ч № 26165 (85-й Головний центр спеціальної служби ГРУ). Обидві групи спільно підпорядковані ГУ ГШ ЗС РФ. APT44, як і APT28, також здійснювали кібератаку на Національний комітет Демократичної партії США у 2016 році з метою впливу на вибори. Один із членів APT44 (Анатолій Сергійович Ковальов) згадується у звинуваченні уряду США проти 12 російських хакерів. За даними британського центру інформаційної безпеки NCSC, Fancy Bear та Sandworm спільно приймали участь в кібератаках на енергетичні компанії України 23 грудня 2015 року. Російським військовослужбовцям з в/ч 26165 та в/ч 74455 було також висунуте спільне обвинувачення у втручанні в президентські вибори у Франції у 2017р.

Окрім інших APT що діють за суміжними напрямками, Sandworm також має власні субкластери для окремих напрямків атак, збору інформації, публікації витоків та хактивізму. Ці групи переважно складаються з волонтерів і початківців, яких вербують через телеграм-канали, що належать або координуються Sandworm. До таких груп відносять:

- **Cyber Army of Russia Reborn**
  За даними America's Cyber Defence Agency, Cyber Army of Russia Reborn (або CARR) була створена військовою частиною 74455 наприкінці лютого 2022 року.
  У квітні 2022 року група почала використовувати новий канал Telegram під назвою «CyberArmyofRussia_Reborn" для організації та планування групових дій. Творці каналу вербували учасників для використання CARR, для проведення кібердіяльності нижче рівня APT. Зловмисники CARR взяли відповідальність за DDoS-атаки проти США та Європи за підтримку України. Mandiant вважає, що CARR координує свою діяльність із APT44 та APT28, використовує деякі з їх інструментів. Телеграм-канал CARR використовуються для публікації інформації, добутої через програми-вайпери.

- **Солнцепьок**
  Група російських хактивістів, що була створена у 2023 році, атакують переважно українські медіа. Солнцепьок заявляють, що стоять за кібератакою на компанію Київстар 12 грудня 2023р., однак не надали переконливих доказів. Загалом низький технічний рівень групи дозволяє припустити, що вона слугує прикриттям для дій APT.
  Держспецзв'язку та CERT-UA вважають, що за діями групи стоїть APT44 Sandworm, яка використовує Солнцепьок для зливу даних та приховування своєї участі в атаках.

- **XakNet**
  Група російських хактивістів, що базується в основному в Telegram і найімовірніше використовується Sandworm для зливу даних, отриманих нею через вайпери. Окрім цього, група також займається DDoS-атаками та зламами сайтів українських медіа. Відомі тим, що намагались розповсюджувати діпфейк із Володимиром Зеленським у березні 2022 року, на якому він нібито закликав до капітуляції. Mandiant вважає, що ця група хактивістів також відноситься до APT44, оскільки в злитих ними даних були знайдені унікальні технічні артефакти вайпера CADDYWIPER, що використовувався лише APT44, і які свідчать про єдине джерело походження.

- **Infoccentr**
  Група телеграм-хактивістів, що також вірогідно координуються APT44. Головна ціль — соціальні мережі українських медіа, поширення фейків, злив інформації, інформаційно-психологічний вплив. Створені 4 березня 2022 р. Разом із XakNet та CARR публікували викрадені APT44 дані щонайменше 16 разів, 4 із них — менше ніж за 24 години від атаки.

Таймлайн активності APT44 / Sandworm (2009–2026)

Дата	Ціль	Засіб / Метод	Актор / підгрупа	Джерела
~2009	Уряди, військові, критична інфраструктура (різні країни)	Фішинг, бекдори, living-off-the-land	Sandworm / APT44	MITRE, Mandiant
2014-09-03	Держоргани України, НАТО і пов’язані структури	Office 0-day (CVE-2014-4114), spear-phishing	Sandworm	MITRE, ESET
2015-12-23	Енергетика України	BlackEnergy-3, SCADA втручання	Sandworm	ESET, CERT-UA
2016-12-17	Енергомережі Києва	Industroyer / CrashOverride (ICS)	Sandworm	ESET
2017-06-27	Україна, глобально	NotPetya (supply-chain M.E.Doc, wiper)	Sandworm	US/UK Gov, Mandiant
2018-02-09	Олімпіада, Пхьончхан (Південна Корея)	Olympic Destroyer (вайпер)	Sandworm	US Gov, Cisco
2019-10-28	Грузія (уряд, медіа)	Масовий дефейс	Sandworm	US/UK Gov
2022-02	Держсектор, CIKR України	Масована атака вайперами, використання ботів, фейкові заяви в телеграмі Telegram	APT44 + XakNet / CARR / Solntsepyok	Mandiant
2022-03-15	Українські організації	CaddyWiper	Sandworm	ESET
2022-04-12	Енергетика України	Industroyer2 + вайпери	Sandworm	ESET, CERT-UA
2022-03	Держсайти, медіа України	DDoS (DDoSia)	NoName057	SentinelOne

Дата	Ціль	Засіб / Метод	Актор / підгрупа	Джерела
2022-10	Логістика України / Польщі, постачання військової допомоги	Prestige (disruptive, pseudo-ransomware)	Sandworm	Mandiant
2023-01	Україна (різні сектори)	SwiftSlicer (вайпер)	Sandworm	ESET
2023-12-13	Київстар	Деструктивна атака на телеком	Solntsepyok (Sandworm)	Reuters, Gov UA
2024-01	OT-інциденти (claims)	Маніпуляції HMI (відео-докази)	CARR (claims)	Mandiant
2024-03	Телекомунікаційна мережа України	AcidPour (вайпер lineage AcidRain)	Sandworm	SentinelOne
2024-10 →	OT/ICS (міжнародно)	Hack-and-leak, дефейси, OT-доступ	Z-Pentest + союзники	CISA
2025-01 →	OT/ICS (міжнародно)	Opportunistic OT атаки	Sector16 (+ Z-Pentest)	Orange Cyberdefense
2025-12-18	OT internet-facing (міжнародно)	VNC/edge-device abuse	CARR / NoName057(16) / Z-Pentest	CISA

Деталі щодо деяких атак

23 грудня 2015 — Атака на енергетичні компанії України

• Ціль: критична інфраструктура — електричні мережі України (Івано-Франківськ та область/ Київ)
• Засіб: BlackEnergy-3 та супровідні модулі для доступу до SCADA, відключення підстанцій, тимчасових відключень електрики.
• Результат: близько 230 000 споживачів опинилися без електрики на 1–6 годин.

17 грудня 2016 — Атака на електромережу Києва

• Ціль: енергетична інфраструктура — підстанція «Північна»
• Засіб: Industroyer (CrashOverride) — шкідливе ПЗ для промислових контролерів
• Результат: вимкнення електропостачання для близько 20% абонентів у Києві.

27 червня 2017 — «NotPetya”

Ціль: IT-системи урядових, фінансових, транспортних та інших організацій та установ (Україна, Європа, США)
• Засіб: програма-вайпер NotPetya, варіант Petya, розповсюджений через оновлення M.E.Doc.
• Результат: США оцінили збитки від NotPetya у близько 10млрд. дол. у всьому світі, назвавши її однією з найбільш руйнівних кібератак за всю історію. NotPetya викликав масштабні збої не лише в Україні, а й логістичних компаній в Європі і поштових сервісів в Північній Америці.

9 лютого 2018 — «Olympic Destroyer” (Пхьончхан, Південна Корея)

• Ціль: IT-інфраструктура Зимових Олімпійських ігор (Wi-Fi, трансляції, квиткові системи)
• Засіб: вайпер Olympic Destroyer, який пошкодив домени та сервіси, що підтримували проведення заходу.
• Результат: збої під час трансляції Олімпіади, заблоковані сервіси продажу квитків.

28 жовтня 2019 — Атака на Грузію (веб-ресурси)

• Ціль: уряд, медіа та бізнес-сайти Грузії
• Засіб: дефейс сайтів, шкідливі скрипти, DDoS-атаки
• Результат: зламані сайти основних медіа.

Таймлайн кібератак по Україні з 2022 року

2022

- 2022-02-24 — держсектор і критична інфраструктура України — численні атаки вайперами, DDoS-атаки, операція мала назву CyclopBlink
- 2022-03-15 — українські організації (різні сектори) — вайпер CaddyWiper (ESET фіксує як окрему хвилю знищення даних у 2022)
- 2022-04-12 — енергетика України (високовольтні підстанції) — ICS-malware Industroyer2 + супровідні вайпери (за даними CERT-UA, за атаками стояв Sandworm)
- 2022-10 — логістика в Україні та Польщі — PRESSTEA/Prestige (маскування під ransomware/ disruptive) (за даними Mandiant)
- 2022-03 → далі (регулярно) — українські державні, медіа, публічні веб-ресурси — DDoS кампанії (NoName057, інструмент — DDoSia) (NoName057 активна з березня 2022, за даними Mandiant)

2023

- 2023-01-28 (кібератаки в січні 2023) — Україна — вайпер SwiftSlicer (за даними ESET)
- 2023-12-13 — компанія Київстар (масова деградація сервісів, виведення з ладу вишок зв'язку, пошкодження базових станцій) — кібератака проти телеком-інфраструктури** (про атаку заявила група Солнцепьок, CERT-UA та Mandiant пов'язують групу з кластером APT44)

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

2024

- 2024-01-17—2024-01-18 — атака на меседжер Signal, яким користуються військові, в т.ч українські, з метою екстракції чутливих даних — фішинг, використання функції linked device (за даними Mandiant)
- 2024-03-22 — українські телеком-оператори — вайпер AcidPour (еволюція AcidRain)** (за даними SentinelOne)

Остання відома активність

Атака на польські енергетичні компанії 25-29.12.25

Атака на польську енергетику в кінці грудня 2025 року за допомогою вайперів DynoWiper LazyWiper вважається наразі останньою атакою, яку деякі аналітики пов'язують із APT44. 25-29 грудня 2025 року ряд польських ТЕЦ, близько 30 вітрових та сонячних станцій зазнали атаки вайперами DynoWiper та LazyWiper через скомпроментовані пристрої FortiGate та вразливість CVE-2024-2617. Згідно з звітом CERT Polska, вайпери частково знищили дані з комп'ютерів у внутрішній мережі. Ціллю також були модулі доступу до SCADA та OT, однак пошкоджень генерації вдалося уникнути. Шкоди зазнали розподільчі мережі. Між підстанціями була втрачена координація через злам контролерів Hitachi RTU560, внаслідок чого 230 000 абонентів залишились без світла на 1–6 годин. Атаку загалом було названо «невдалою".

Хоча загальний патерн атаки схожий на патерн Sandworm (атака на енергетику, використання вайперів), CERT Polska у своєму звіті покладає відповідальність на іншу групу — BerserkBear, що належить до структури ФСБ. Спільної думки дотримуються також аналітики компанії Cisco та ФБР, на чиї слова посилається звіт. Однак спеціалісти з ESET вважають, що за атакою може стояти APT44 «із середньою імовірністю», оскільки, за їх словами, було знайдено подібні елементи коду в DynoWiper та в ZOV Wiper, що атакував одну з фінансових установ в Україні влітку 2025 року. ESET атрибує ZOV Wiper до APT44 «з високою імовірністю".

Джерела

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/