Cadet Blizzard
(Ember Bear, DEV-0586, UAC-0056)

161-й Центр спеціального призначення ГРУ РФ (в/ч 29155)

Назва угруповання	Cadet Blizzard
Альтернативні назви	Ember Bear, DEV-0586, UAC-0056, UNC2589
Країна походження	Російська Федерація
Афіліація	ГРУ ГШ ЗС РФ
Пов'язаний підрозділ	В/ч 29155, 161-й Центр спеціального призначення
Тип загрози	Advanced Persistent Threat (APT)
Основна мотивація	Кіберрозвідка, диверсії, інформаційно-психологічні операції
Період активності	2020 р. – дотепер
Основні цілі	Україна, країни НАТО, державний сектор, критична інфраструктура

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

Аналітичне резюме

Cadet Blizzard (також відома як Ember Bear, DEV-0586 та UAC-0056) є російським кіберугрупованням, яке пов'язують із Головним управлінням Генерального штабу Збройних сил Російської Федерації (ГРУ). За оцінками Microsoft, CERT-UA, Mandiant та інших дослідницьких центрів, діяльність групи координується структурами, пов'язаними з військовою частиною 29155 та так званою «бригадою Авер'янова».

Основною спеціалізацією угруповання є проведення кібершпигунських, деструктивних та інформаційно-психологічних операцій проти України, держав-членів НАТО та країн Європейського Союзу.

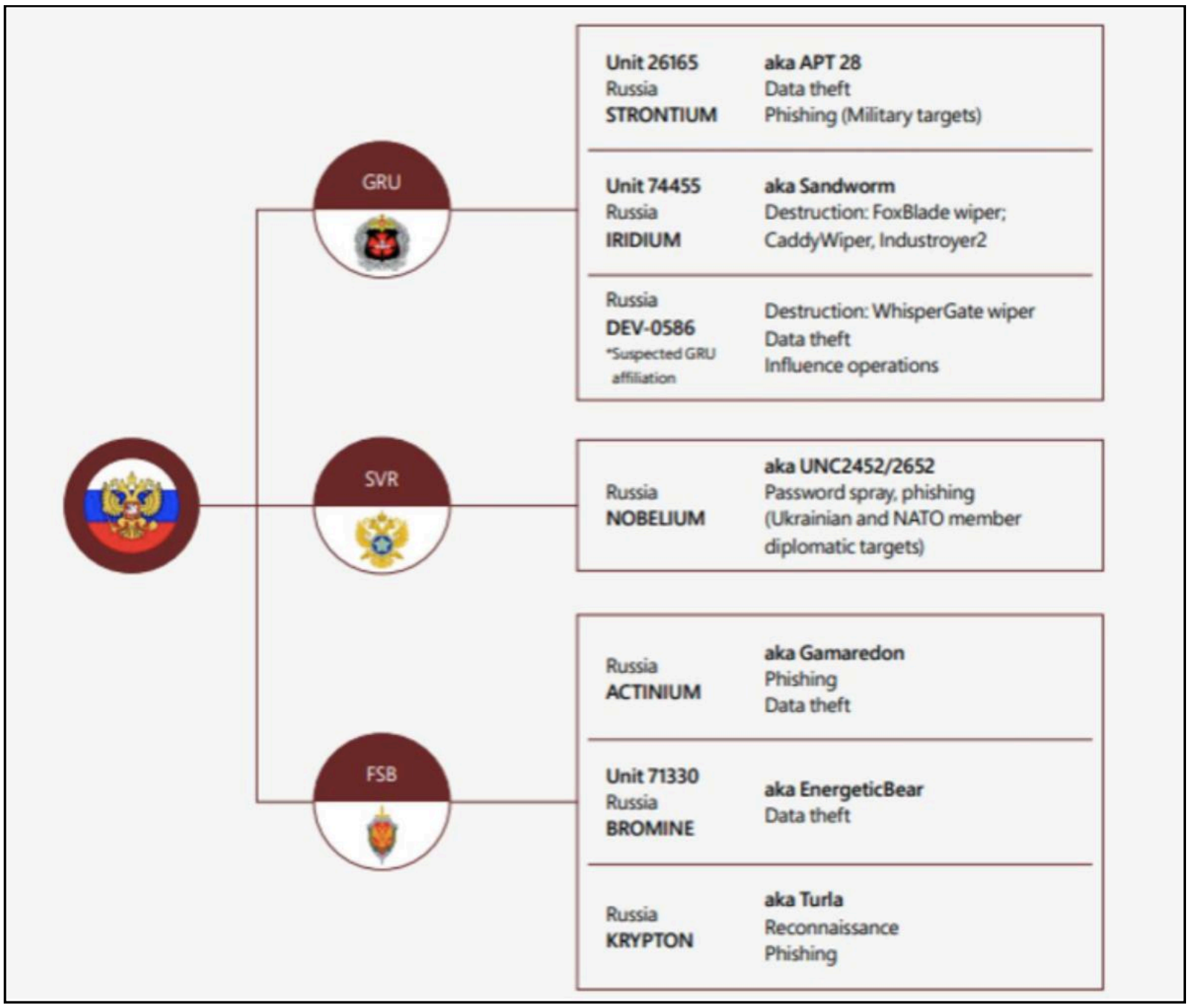
Широку міжнародну увагу Cadet Blizzard привернула після використання шкідливого програмного забезпечення WhisperGate напередодні повномасштабного вторгнення РФ в Україну у січні 2022 року. Надалі угруповання неодноразово брало участь у кампаніях зі збору розвідувальної інформації, компрометації державних інформаційних ресурсів та атаках на критичну інфраструктуру.

На відміну від багатьох інших APT-груп, Cadet Blizzard поєднує традиційні методи соціальної інженерії, фішингові кампанії та використання легітимних адміністративних інструментів, що значно ускладнює виявлення їхньої присутності в мережах жертв.

Станом на 2026 рік угруповання залишається однією з найбільш активних російських кіберзагроз, спрямованих проти України та її міжнародних партнерів.

СТРУКТУРНА СХЕМА КЛАСТЕРУ ЗАГРОЗ

Структурна схема кластеру загроз Cadet Blizzard (Ember Bear, DEV-0586, UAC-0056), пов'язаного з підрозділом 29155 ГРУ РФ



Структура кіберпідрозділів ГРУ РФ Unit 29155
Основні напрямки діяльності та відомі кампані

Ключові аналітичні висновки

Після 2022 року активність, пов’язана з цим кластером, помітно змістилася в бік більш агресивних і руйнівних операцій проти України. Основний акцент став робитися не на приховану розвідку, а на пряме порушення роботи систем і інфраструктури

Серед ключових типів активності виділяються масштабні деструктивні атаки проти української інфраструктури використання шкідливого програмного забезпечення типу вайперів включно з WhisperGate та подібними інструментами масові дефейси державних веб ресурсів розвідувальні операції проти структур НАТО та країн союзників атаки на організації які прямо або опосередковано підтримують Україну

Деструктивні атаки проти України 2022

У 2022 році активність яку дослідники пов’язують з цим кластером стала значно більш руйнівною Основний фокус змістився з класичної кіберрозвідки на пряме виведення з ладу державних і критичних систем

Це проявлялося у наступному знищення або пошкодження даних на серверах державних установ порушення роботи державних онлайн сервісів атаки на системи зв’язку та адміністративну інфраструктуру синхронізація кібератак з подіями на фізичному рівні

У цілому такі кампанії розглядаються як приклад державних APT операцій де кібердії використовуються як частина ширшої стратегії впливу

Ланцюг атаки WhisperGate від компрометації інфраструктури до знищення даних

Операції з використанням wiper шкідливого програмного забезпечення, зокрема WhisperGate, слід розглядати як цілеспрямовану деструктивну кампанію, в якій основний акцент зроблено не на приховане викрадення даних, а на їх повне та швидке знищення з подальшим виведенням інфраструктури з ладу.

У технічному плані WhisperGate демонстрував багатоступеневу архітектуру: початковий компонент імітував поведінку ransomware, однак фактично не передбачав механізмів відновлення, тоді як наступні стадії забезпечували перезапис і руйнування критичних даних та завантажувальних структур, що призводило до фактичної незворотної втрати працездатності систем. Основними цілями виступали державні та критичні інформаційні системи України, що дозволяє класифікувати дану активність як кібератаку саботажного характеру.

Паралельно фіксувалися масові дефейс-операції проти державних вебресурсів, які супроводжувалися компрометацією урядових порталів, заміною контенту на пропагандистські повідомлення, короткочасним блокуванням доступу до сервісів та формуванням ефекту інформаційного хаосу. У сукупності ці дії виконували не лише технічну, але й виражену інформаційно-психологічну функцію, а в окремих випадках могли використовуватися як елемент прикриття для більш глибокого проникнення в інфраструктуру.

Окремий напрямок активності становили розвідувальні операції проти структур НАТО та держав-союзників України, що включали збір інформації щодо військово-політичної підтримки, аналіз логістичних і оборонних ланцюгів постачання, а також спроби компрометації урядових, дипломатичних і аналітичних структур. Основною метою цих дій було формування стратегічної розвідувальної картини для подальшого використання у військово-політичному плануванні.

Додатково відзначається системна активність проти організацій, залучених до підтримки України, включно з IT-компаніями, хмарними провайдерами, гуманітарними структурами та оборонними підрядниками. Типовий вектор атак включав фішингові кампанії, компрометацію облікових даних, проникнення у внутрішні мережі та використання скомпрометованих вузлів як точок подальшого розширення доступу в партнерські екосистеми.

У цілому дана сукупність операцій характеризується як багатовекторна деструктивно-розвідувальна кампанія державного рівня, в якій кіберзасоби застосовуються як інструмент одночасного руйнування інфраструктури, інформаційного впливу та стратегічного збору розвідувальних даних.

Повідомлення про викуп, яке відображалося після компрометації системи WhisperGate

```
.text:00403B93          mov     [esp+14h+hTemplateFile], 0 ; hTemplateFile
.text:00403B9B          mov     dword ptr [esp+14h], 0 ; dwFlagsAndAttributes
.text:00403BA3          mov     [esp+14h+dwCreationDisposition], 3 ; dwCreationDisposition
.text:00403BAB          mov     [esp+14h+lpSecurityAttributes], 0 ; lpSecurityAttributes
.text:00403BB3          mov     [esp+14h+dwShareMode], 3 ; dwShareMode
.text:00403BBB          mov     [esp+14h+dwDesiredAccess], 10000000h ; dwDesiredAccess
.text:00403BC3          mov     [esp+14h+lpFileName], offset FileName ; "\\\\.\\PhysicalDrive0"
.text:00403BCA          call    CreateFileW
.text:00403BCF          mov     esi, eax
.text:00403BD1          lea     eax, [ebp-2018h]
.text:00403BD7          sub     esp, 1Ch
.text:00403BDA          mov     [esp+14h+lpFileName], esi ; hFile
.text:00403BDD          mov     [esp+14h+dwCreationDisposition], 0 ; lpOverlapped
.text:00403BE5          mov     [esp+14h+lpSecurityAttributes], 0 ; lpNumberOfBytesWritten
.text:00403BED          mov     [esp+14h+dwShareMode], 200h ; nNumberOfBytesToWrite
.text:00403BF5          mov     [esp+14h+dwDesiredAccess], eax ; lpBuffer
.text:00403BF9          call    WriteFile
.text:00403BFE          sub     esp, 14h
.text:00403C01          mov     [esp+14h+lpFileName], esi ; hObject
.text:00403C04          call    CloseHandle
```

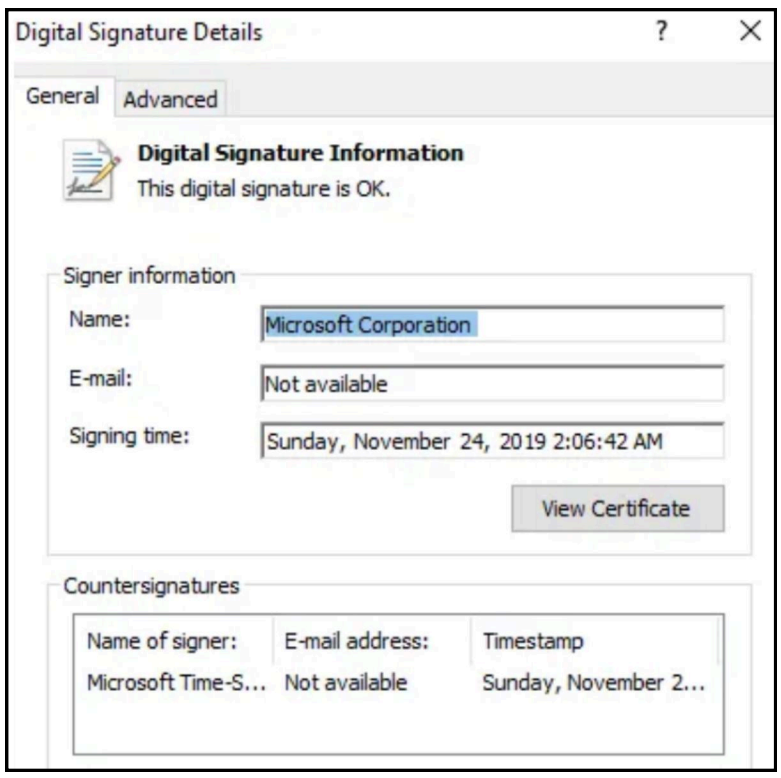
Механізм пошкодження головного завантажувального запису (MBR) у WhisperGate

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

WhisperGate використовує набір інструментів Impacket для переміщення мережею та запуску шкідливих програм. Основний файл (stage1.exe) — це виконуваний PE-файл, який може приховано розміщуватися в різних системних папках, наприклад C:\Temp або C:\ProgramData.

Після запуску шкідливе ПЗ отримує доступ до фізичного диска комп’ютера (PhysicalDrive0), де знаходиться головний завантажувальний запис (MBR). Далі воно перезаписує MBR шкідливим кодом із повідомленням про вимогу викупу.

У результаті після перезавантаження система більше не завантажується нормально, а користувач бачить повідомлення про «пошкодження диска» та вимогу заплатити викуп.

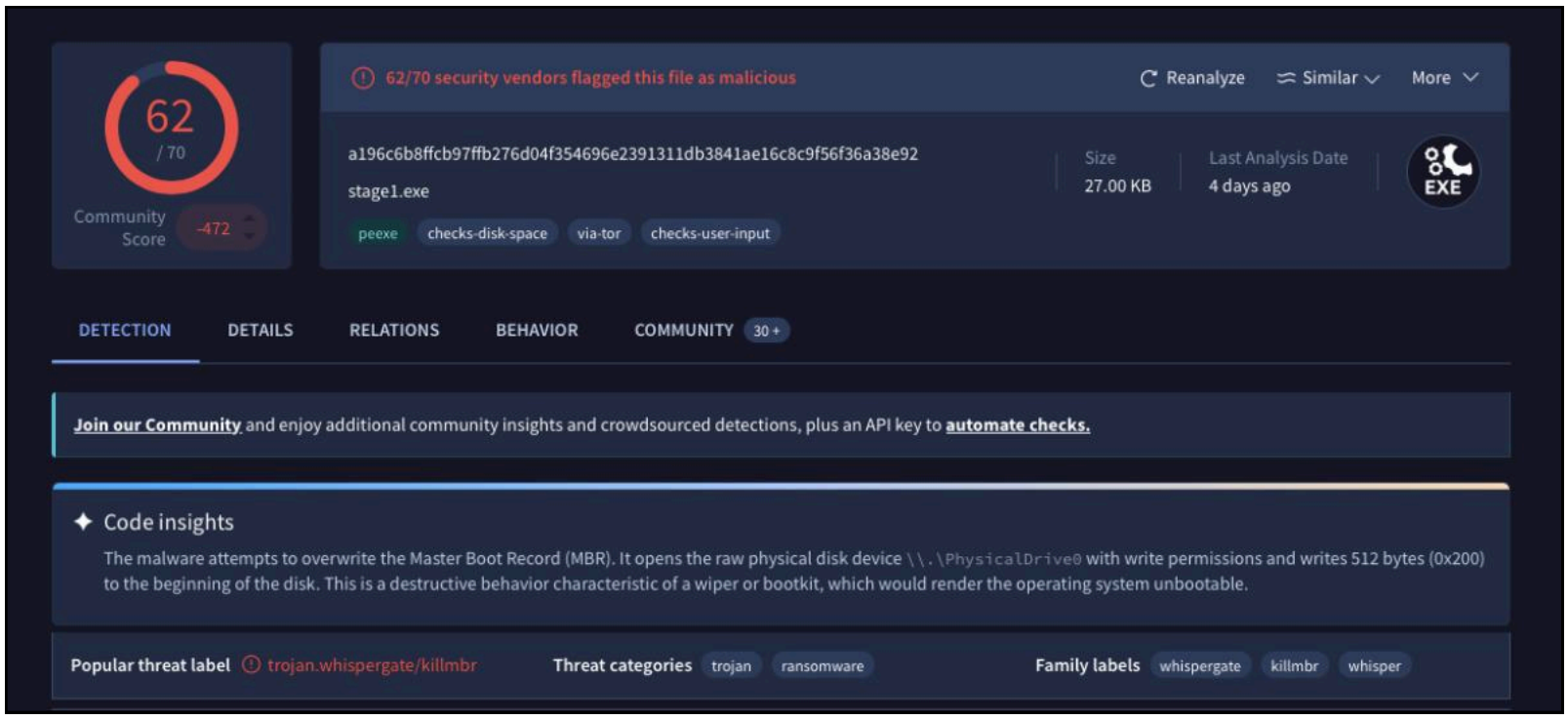


Під час виконання ця програма записує 22,53 ГБ даних на диск комп’ютера. Оригінальна програма не містить жодного підозрілого коду, тому можна припустити, що WhisperGate впроваджує шкідливий код у цей процес для пошкодження файлу.

15 січня 2022 року Microsoft повідомила про виявлення складної шкідливої операції проти кількох організацій в Україні. Шкідливе ПЗ WhisperGate має дві стадії: воно пошкоджує головний завантажувальний запис (MBR), показує підроблене повідомлення про вимогу викупу та шифрує/псує файли з певними розширеннями.

Рівень впевненості атрибуції

Атрибуція Cadet Blizzard до ГРУ РФ оцінюється як висока впевненість (High confidence) на основі сукупності технічних індикаторів, інфраструктурних перетинів, TTP-патернів та аналітичних звітів Microsoft MSTIC, CISA та інших дослідницьких організацій. Пряма офіційна державна верифікація відсутня, однак консенсус у кіберрозвідувальній спільноті є стійким.



Виявлення зразка WhisperGate та пов'язані індикатори компрометації (IOC)

Хронологія активності

- 2020–2021 — рання активність, кібершпигунські операції та підготовчі інфраструктурні кампанії.
- Січень 2022 — WhisperGate деструктивна кампанія проти українських державних систем.
- 2022 — масштабні атаки на критичну інфраструктуру України та оборонний сектор.
- 2023–2024 — розширення цілей на НАТО, ЄС та організації підтримки України, включаючи supply-chain операції.
- 2025–2026 — продовження розвідувально-деструктивної активності з фокусом на довготривалі операції доступу (persistent access).

1. Критична інфраструктура України у 2022 році

У 2022 році критична інфраструктура України стала однією з ключових цілей деструктивних кібероперацій, пов’язаних із кластером активності, який дослідники асоціюють із GRU та DEV-0586. Йдеться не про одиничні інциденти, а про системну кампанію, спрямовану на порушення стійкості базових державних і цивільних сервісів.

Основні сектори впливу включали енергетичну інфраструктуру, телекомунікаційних операторів, транспортні системи, а також державні IT-центри та дата-центри, які забезпечують функціонування цифрових сервісів держави.

З точки зору тактики, атаки поєднували кілька рівнів впливу: отримання несанкціонованого доступу до внутрішніх мереж, закріплення в інфраструктурі, подальше порушення роботи систем і в окремих випадках — деструктивні дії, спрямовані на пошкодження або знищення даних і сервісів.

Операційний ефект полягав у створенні перебоїв у роботі критично важливих систем, зниженні доступності цифрових державних послуг та загальному навантаженні на інфраструктуру в умовах кризового періоду.

2. Організації оборонного та безпекового сектору України

Атаки на оборонний та безпековий сектор України у 2022 році мали цільовий і багатоступеневий характер та були спрямовані на військові інформаційні системи, структури Міністерства оборони України, СБУ та інші силові відомства з метою отримання доступу до внутрішніх мереж, збору розвідданих і підготовки потенційних деструктивних дій, при цьому типовий сценарій включав фішинг, компрометацію облікових даних, закріплення в інфраструктурі, розвідку всередині мережі та в окремих випадках використання шкідливого ПЗ для подальшого саботажу або знищення даних.

Таблиця: атаки на оборонний сектор

Таблиця: атаки на оборонний сектор	Тип атаки	Дії зловмисників	Наслідки
Військові інформаційні системи	Фішинг, компрометація акаунтів	Отримання логінів, доступ до пошти та внутрішніх сервісів	Розвідка, потенційний доступ до внутрішніх даних
Міністерство оборони України	Spear-phishing, malware	Встановлення шкідливого ПЗ, закріплення в мережі	Перехоплення інформації, підготовка до саботажу
СБУ та пов’язані підрозділи	Фішинг + credential theft	Викрадення облікових даних, спроби lateral movement	Компрометація окремих акаунтів, витік даних

Силові відомства (загалом)	Розвідувальні атаки	Збір інформації, сканування інфраструктури	Підготовка до подальших кібероперацій
Оборонні IT-системи	Malware / web-shells	Отримання віддаленого доступу до серверів	Потенційне порушення роботи систем

Висновок: Атаки мали комбінований характер — спочатку фішинг і отримання доступу, далі закріплення в мережі, розвідка і в окремих випадках підготовка до деструктивних дій (wiper-активність).

3. Міжнародні та НАТО пов’язані цілі 2022–2024

У період 2022–2024 років фіксувалася розширена розвідувальна та supply chain активність проти міжнародних організацій, пов’язаних із НАТО та ЄС, з акцентом на урядові мережі країн Альянсу, державні установи Європейського Союзу, оборонних підрядників, логістичні компанії, що забезпечують постачання в Україну, а також IT та cloud провайдерів, які обслуговують державні та оборонні системи.

Основний характер операцій включав цільовий фішинг співробітників, викрадення облікових даних, компрометацію поштових і корпоративних акаунтів, проникнення в інфраструктуру через постачальників та довготривале приховане перебування в скомпрометованих мережах.

Метою цих дій було отримання розвідувальної інформації про військову та логістичну підтримку України, відстеження ланцюгів постачання, а також створення потенційних передумов для майбутніх кібероперацій і компрометації критичних елементів інфраструктури союзників.

4. Організації, пов’язані з підтримкою України 2023–2024

У 2023–2024 роках спостерігалася цілеспрямована розвідувальна активність проти організацій, залучених до військової, гуманітарної та логістичної підтримки України, з фокусом на гуманітарні структури, західні IT компанії, що працюють з українським державним сектором, логістичних операторів постачання допомоги та оборонні компанії Європи.

Основний вектор атак включав цільовий фішинг співробітників, компрометацію електронної пошти та корпоративних акаунтів, викрадення облікових даних, а також встановлення стійкого прихованого доступу до внутрішніх мереж із подальшим збором розвідувальної інформації.

Метою цих операцій було отримання доступу до внутрішніх комунікацій, відстеження військової та гуманітарної допомоги Україні, а також підготовка потенційних майбутніх кібероперацій у межах ширшої розвідувально диверсійної діяльності.

Сектор	TTP	Приклади	Наслідки
Критична інфраструктура	Wiper, sabotage, intrusion	WhisperGate, MBR overwrite	Знищення даних, зупинка сервісів
Оборонний сектор України	Phishing, credential theft	MFA bypass, email compromise	Розвіддані, доступ до мереж
НАТО / ЄС	Espionage, supply-chain	Компрометація підрядників	Стратегічна розвідка
Підтримка України	Persistence, phishing	Доступ до IT/ логістики	Моніторинг допомоги
Держ. інфраструктура	Defacement, malware	Заміна сайтів, web-shells	Дестабілізація сервісів

MITRE ATT&CK mapping

Фаза	Техніка MITRE	Приклад
Initial Access	T1566 Phishing	фішингові листи
Execution	T1059 Command & Scripting	запуск payload
Persistence	T1505.003 Web Shells	закріплення на серверах
Privilege Escalation	T1068 Exploitation	використання вразливостей
Defense Evasion	T1027 Obfuscation	приховані payload
Credential Access	T1003 OS Credential Dumping	крадіжка паролів
Lateral Movement	T1021 Remote Services	рух у мережі
Impact	T1485 Data Destruction	WhisperGate wiper
Impact	T1491 Defacement	заміна вебсторінок

Інфраструктура, C2 та інструментарій

Активність Cadet Blizzard характеризується використанням динамічної інфраструктури з короткоживучими доменами, компрометованими серверами та легітимними сервісами для прихованої комунікації.

Основні техніки включають використання фішингових інфраструктур, скомпрометованих облікових записів, PowerShell-скриптів, Windows-native інструментів та кастомних wiper-компонентів. У випадку WhisperGate спостерігалося використання багатоступеневої архітектури з окремими payload-компонентами для знищення даних та пошкодження завантажувальних структур систем.

Також фіксується використання легітимних адміністративних інструментів для прихованого переміщення в мережах жертв (Living-off-the-Land Techniques), що ускладнює виявлення активності та знижує ефективність традиційних засобів захисту.

Аналітична оцінка загрози

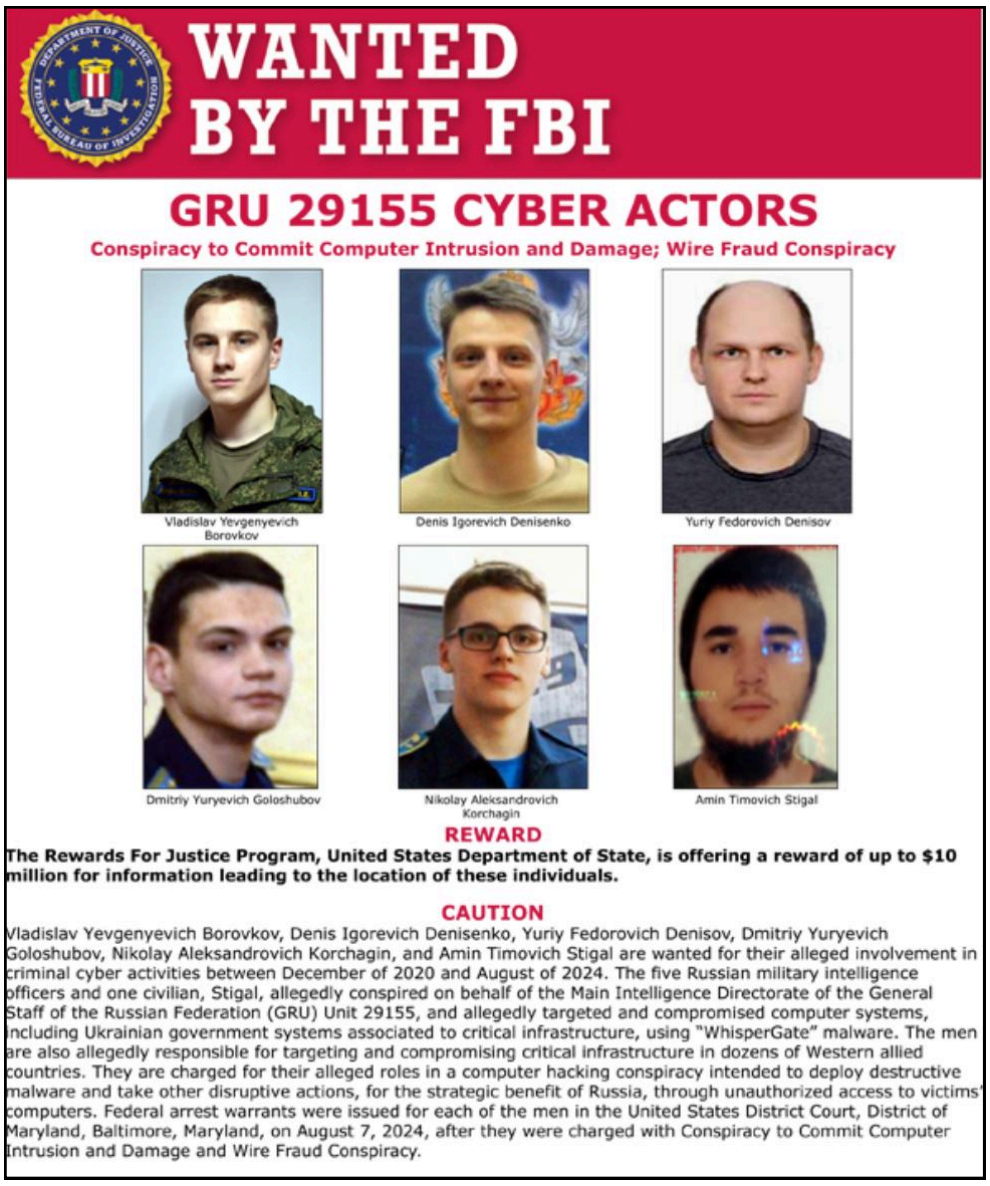
Група демонструє комплексну та гібридну модель APT-активності, що поєднує розвідувальні, інформаційно-психологічні та деструктивні кібероперації. Типовий сценарій передбачає отримання первинного доступу через фішинг або компрометацію облікових даних, подальше закріплення в інфраструктурі жертви, внутрішню розвідку та розширення контролю над мережею.

Окремою особливістю діяльності є використання supply-chain атак, які дозволяють отримувати доступ не лише до безпосередніх цілей, але й до організацій-партнерів та підрядників. Такий підхід суттєво розширює потенційний масштаб компрометації та ускладнює виявлення джерела атаки.

Важливим елементом операцій є застосування деструктивних інструментів типу wiper, спрямованих на знищення даних і порушення роботи інформаційних систем. На відміну від класичних кіберзлочинних кампаній, основною метою таких атак є не отримання фінансової вигоди, а досягнення стратегічного та операційного ефекту.

Діяльність Cadet Blizzard охоплює державний сектор, оборонні структури, критичну інфраструктуру та міжнародні організації. Особливий фокус спрямований на Україну, а також на країни НАТО та організації, залучені до військової, гуманітарної й технологічної підтримки України.

Ключові особи



WANTED BY THE FBI

GRU 29155 CYBER ACTORS

Conspiracy to Commit Computer Intrusion and Damage; Wire Fraud Conspiracy

Vladislav Yevgenyevich Borovkov

Denis Igorevich Denisenko

Yuriy Fedorovich Denisov

Dmitriy Yuryevich Goloshubov

Nikolay Aleksandrovich Korchagin

Amin Timovich Stigal

REWARD

The Rewards For Justice Program, United States Department of State, is offering a reward of up to $10 million for information leading to the location of these individuals.

CAUTION

Vladislav Yevgenyevich Borovkov, Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Aleksandrovich Korchagin, and Amin Timovich Stigal are wanted for their alleged involvement in criminal cyber activities between December of 2020 and August of 2024. The five Russian military intelligence officers and one civilian, Stigal, allegedly conspired on behalf of the Main Intelligence Directorate of the General Staff of the Russian Federation (GRU) Unit 29155, and allegedly targeted and compromised computer systems, including Ukrainian government systems associated to critical infrastructure, using "WhisperGate" malware. The men are also allegedly responsible for targeting and compromising critical infrastructure in dozens of Western allied countries. They are charged for their alleged roles in a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victims' computers. Federal arrest warrants were issued for each of the men in the United States District Court, District of Maryland, Baltimore, Maryland, on August 7, 2024, after they were charged with Conspiracy to Commit Computer Intrusion and Damage and Wire Fraud Conspiracy.

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

Пропонується винагорода до 10 млн доларів за інформацію про осіб, які здійснювали кібератаки на критичну інфраструктуру США за вказівкою іноземного уряду.

Йдеться про п’ять російських військових розвідників ГРУ (підрозділ 29155), які пов’язані з атакою шкідливим ПЗ WhisperGate проти України перед вторгненням 2022 року, а також із кібершпигунством і атаками на інфраструктуру України, США та інших країн (енергетика, урядові та аерокосмічні системи).

Юрій Федорович Денисов (Yuriy Fyodorovich Denisov)
офіцер підрозділу 29155 ГРУ РФ

Стать чоловіча.
Тип зовнішності європеоїдний.
Волосся коротке, темне.
Очі: голубі
Громадянство: Російська Федерація
Дата народження: 17 июня 1980 г.

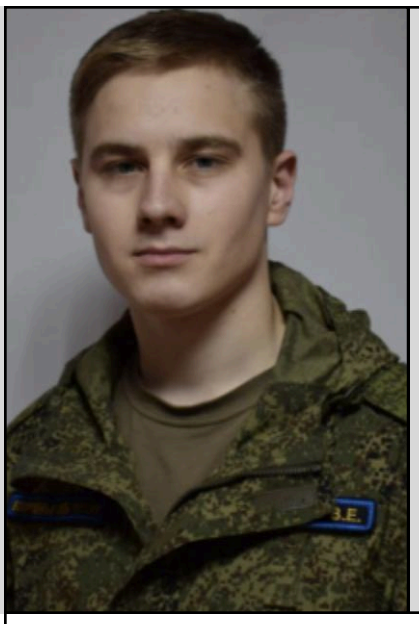
У відкритих матеріалах він з’являється в цивільному одязі та під легендованими прикриттями, що відповідає практиці роботи спецпідрозділів ГРУ.

Юрій Федорович Денисов (Yuriy Fyodorovich Denisov) у відкритих розслідуваннях описується як офіцер ГРУ Росії, пов’язаний із підрозділом 29155. Його діяльність не виглядає як робота хакера-одинака, а як участь у командній структурі, яка займалася підготовкою та технічним супроводом кібератак.

Йому приписують участь у плануванні та технічній підготовці атак проти України, зокрема тих, що використовували шкідливе програмне забезпечення типу WhisperGate. Такі атаки були спрямовані не на крадіжку даних, а на руйнування або виведення з ладу державних і інфраструктурних систем. У цьому контексті він фігурує як учасник робіт, пов’язаних із підготовкою зараження систем і запуском шкідливого коду через інфраструктуру атакуючих груп.

Також його пов’язують із розвідувальною частиною кібероперацій. Це включає аналіз мереж цілей, пошук слабких місць у державних і критичних системах, а також підготовку доступу для подальших атак. Окремо вказується, що подібні дії стосувалися не лише України, а й об’єктів у країнах НАТО, де здійснювалися спроби розвідки та сканування інфраструктури.

У структурі 29155 він розглядається як технічний виконавець середньої ланки, який забезпечував кіберкомпонент операцій. Його роль описується як підготовча і підтримуюча, тобто він працював із даними, інструментами та мережами до моменту проведення атак, а не керував усією операцією.



Владислав Євгенович Боровков (Vladislav Yevgenyevich Borovkov)
офіцер підрозділу 29155 ГРУ РФ

Відомий під іменем: Влад Боровков
Дата народження:: 7 жовтня 1997 року
Стать: чоловіча
Громадянство: Російська Федерація
Раса: білий
Тип зовнішності: європеоїдний
Волосся: каштанове / темно-русяве
Очі: карі
Мови: російська, англійська

Владислав Євгенович Боровков описується як офіцер російської військової розвідки, пов’язаний із кібернапрямом підрозділу 29155 ГРУ. Він належить до молодшої офіцерської ланки та виконує функції технічного виконавця в операціях, пов’язаних із проникненням у комп’ютерні мережі та використанням шкідливого програмного забезпечення.

Його діяльність у структурі розглядається як участь у практичному етапі кібероперацій. Це включає підготовку інфраструктури для атак, роботу з цільовими мережами, сканування систем, виявлення уразливостей та технічну підтримку розгортання шкідливого коду. Такі дії є частиною більш широкого процесу, який передує безпосередньому запуску кібератак і забезпечує доступ до цільових систем.

У межах операцій, пов’язаних із підрозділом 29155, його ім’я пов’язують із кампаніями проти України та держав НАТО, де застосовувалися руйнівні кіберінструменти, спрямовані на порушення роботи державних сервісів та критичної інфраструктури. Йдеться про дестабілізаційні атаки, що мали не лише розвідувальний, а й руйнівний характер.

У структурі він розглядається як тактичний виконавець середнього або молодшого рівня, який не здійснює стратегічного планування, але відповідає за технічну реалізацію окремих етапів кібероперацій. Його роль полягає у забезпеченні роботи інструментів, підготовці середовища атаки та супроводі процесів проникнення в системи.

Денис Ігорович Денисенко (Denis Igorevich Denisenko)
офіцер підрозділу 29155 ГРУ РФ

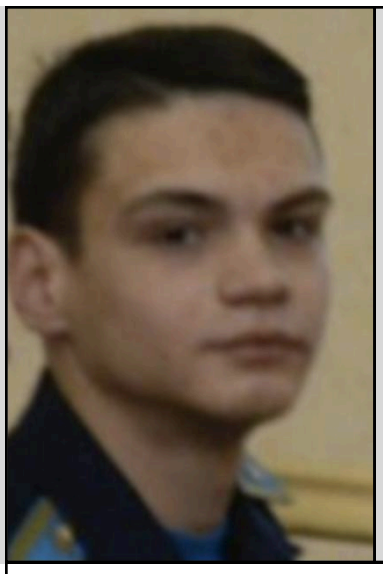
Стать: чоловіча
Громадянство: Російська Федерація
Раса: білий
Тип зовнішності: європеоїдний
Волосся: каштанове / русяве
Очі: блакитні
Дата народження: 14 травня 1997 року
Мови: російська, англійська

Денис Ігорович Денисенко описується як офіцер, пов’язаний із кібернапрямом у структурі російської військової розвідки. У рамках цієї діяльності його роль визначається як технічна та операційна, пов’язана з розробкою та застосуванням інструментів для атак на комп’ютерні мережі.

Його діяльність охоплює участь у створенні та налаштуванні шкідливого програмного забезпечення, а також у проведенні атак на державні та критичні інфраструктурні системи. У таких операціях він розглядається як виконавець, який працює з технічною частиною проникнення в мережі, включаючи підготовку середовища атаки, використання експлойтів та забезпечення доступу до цільових систем.

Також його пов’язують із участю в операціях проти України та інших держав, де кібердіяльність використовувалася як елемент ширшої гібридної стратегії впливу, що включає розвідку, дестабілізацію та порушення роботи інфраструктури.

У структурі він розглядається як технічний офіцер середнього рівня, який забезпечує реалізацію атак на практичному рівні, а не стратегічне планування операцій.



Дмитро Юрійович Голошубов (Dmitriy Yuryevich Goloshubov)
офіцер підрозділу 29155 ГРУ РФ

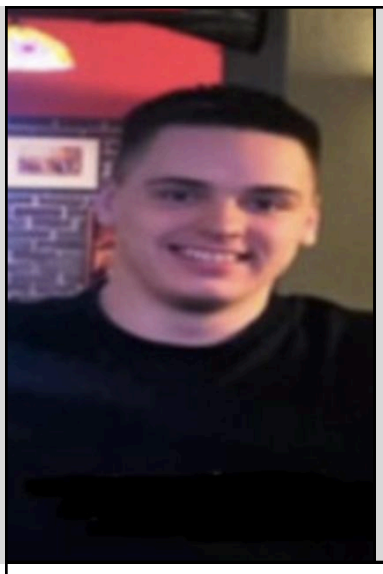
Стать: чоловіча
Громадянство: Російська Федерація
Раса: білий
Тип зовнішності: європеоїдний
Волосся: каштанове / русяве
Очі: карі
Дата народження: 10 жовтня 1998 року
Мови: російська, англійська

Дмитро Юрійович Голошубов описується як офіцер, пов’язаний із кібернапрямом російської військової розвідки. У межах структури, з якою його пов’язують, він виконує роль технічного спеціаліста, відповідального за практичну реалізацію мережевих атак.

Його діяльність охоплює участь у підготовці та проведенні вторгнень у комп’ютерні системи, включаючи технічне налаштування інструментів атаки, забезпечення доступу до цільових мереж та супровід процесів проникнення. Він розглядається як виконавець, який працює з інфраструктурною частиною кібероперацій, а не як стратегічний планувальник.

У рамках операцій, пов’язаних із групою, його діяльність описується як участь у кампаніях проти державних і критичних систем України та інших країн, де застосовувалися методи прихованого доступу, компрометації мереж та подальшого використання отриманих точок входу для розгортання атакуючих інструментів.

Його роль визначається як технічна реалізація мережевих вторгнень, що включає підтримку кібероперацій на рівні інфраструктури та забезпечення функціонування атакуючих механізмів у цільових системах.



Микола Олександрович Корчагін (Nikolay Aleksandrovich Korchagin)
офіцер підрозділу 29155 ГРУ РФ

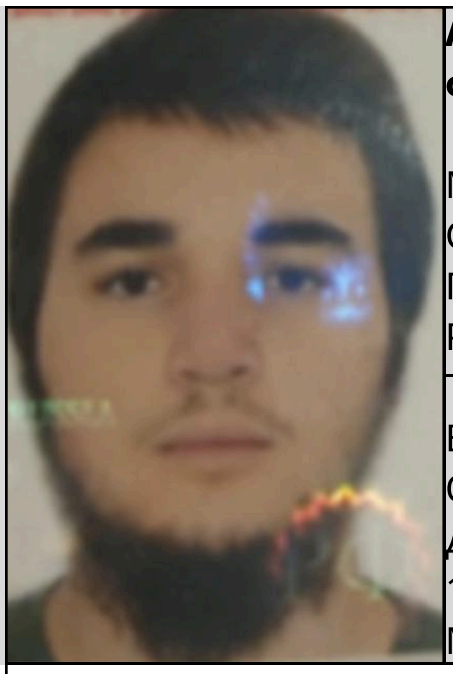
Стать: чоловіча
Громадянство: Російська Федерація
Раса: білий
Тип зовнішності: європеоїдний
Волосся: каштанове / русяве
Очі: не зафіксовані у стабільних підтверджених даних
Дата народження: 16 вересня 1997 року
Мови: російська, англійська

Микола Олександрович Корчагін описується як офіцер, пов’язаний із кібернапрямом російської військової розвідки. У структурі, з якою його пов’язують, він виконує роль технічного виконавця в операціях, що включають проникнення в комп’ютерні системи та закріплення доступу в скомпрометованих мережах.

Його діяльність пов’язується з етапами кібероперацій, які починаються з отримання первинного доступу до цільових систем і продовжуються утриманням цього доступу. Це включає роботу з інфраструктурою компрометації, підтримку стабільного контролю над зламаними мережами та допомогу в розгортанні інструментів для подальших дій у системі.

У межах операцій, пов’язаних із підрозділом 29155, його роль описується як участь у кампаніях проти державних і критичних систем України та інших країн, де кібердіяльність використовується як інструмент дестабілізації та довготривалого прихованого доступу до інфраструктури.

Його функція в структурі визначається як тактична: він забезпечує технічну стійкість уже скомпрометованих систем і підтримує роботу атакуючої інфраструктури на етапі після первинного проникнення.



Амін Тимович Стігал (Amin Timovich Stigal)
фігурант розслідувань щодо операції WhisperGate

Місце народження: Грозний, Чечня, Росія
Стать: чоловіча
Громадянство: Російська Федерація
Раса: білий
Тип зовнішності: європеоїдний
Волосся: каштанове / коричневе
Очі: карі
Дата народження: 1 жовтня 2002 року (ймовірно основна), 1 серпня 1996 року (використовувана легенда)
Мови: російська, англійська, арабська

Амін Стігал описується як цивільна особа, пов’язана у звинуваченнях США з участю в кібероперaціях проти України, зокрема з атакою на базі шкідливого програмного забезпечення WhisperGate у січні 2022 року. За версією американського обвинувачення, він діяв у взаємодії з людьми, пов’язаними з російською військовою розвідкою ГРУ, та брав участь у діяльності, спрямованій на компрометацію державних і критичних систем України.

У межах цієї справи Стігал фігурує як один із виконавців кібероперацій, які включали злам державних ресурсів, публікацію викрадених даних, розміщення деструктивних повідомлень на українських урядових платформах, а також спроби поширення викраденої інформації через даркнет. Окремо йому приписується участь у кампанії, де використовувалося шкідливе програмне забезпечення, що знищувало дані на уражених системах, створюючи ефект руйнування інфраструктури.

Справу Стігала розглядають у контексті ширшої моделі залучення Росією цивільних хакерів і молодих спеціалістів до операцій, які можуть виконувати роль допоміжної або проміжної ланки між спецслужбами та кіберзлочинним середовищем. У цій моделі підкреслюється можливість використання таких осіб як інструментів із частковим або непрямим зв’язком із державними структурами, що дозволяє приховувати реальних організаторів атак.

Також у матеріалах справи зазначається, що паралельно з кіберзвинуваченнями щодо Аміна Стігала існують окремі кримінальні провадження проти його батька, пов’язані з фінансовими кіберзлочинами, однак вони не вважаються частиною тієї ж операційної лінії.

Загальна картина, яку формують слідчі та аналітики, описує Стігала як молодого учасника кіберсередовища, який міг бути залучений до складних операцій або свідомо, або через посередницькі структури, де межа між злочинною діяльністю та державними кібероперaціями розмивається.

Амін Тимович Стігал (праворуч) та його батько Тімур Стігал (ліворуч)

Модель багатоступеневої кібероперації WhisperGate: проникнення, поширення та деструктивний вплив

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

Подана схема відображає багаторівневу структуру кібероперації типу wiper-атаки, характерної для WhisperGate. Операція будується за принципом послідовного проходження етапів: від первинного доступу до інфраструктури до повного знищення даних і систем.

На першому етапі здійснюється проникнення в мережу через компрометацію користувацьких або адміністративних точок доступу. Далі йде фаза внутрішньої розвідки, під час якої атакувальники вивчають структуру мережі, виявляють ключові сервери, бази даних та елементи управління інфраструктурою.

Після цього відбувається горизонтальне переміщення всередині мережі з метою розширення контролю та отримання доступу до критичних вузлів. На етапі підготовки атаки розміщуються шкідливі компоненти та налаштовується синхронний запуск руйнівного коду.

Фінальна фаза характеризується активацією wiper-механізму, який призводить до знищення даних, порушення роботи операційних систем і виведення з ладу серверної інфраструктури. Паралельно реалізується інформаційний компонент, спрямований на психологічний тиск і дестабілізацію, включно з публікацією повідомлень і поширенням викрадених даних.

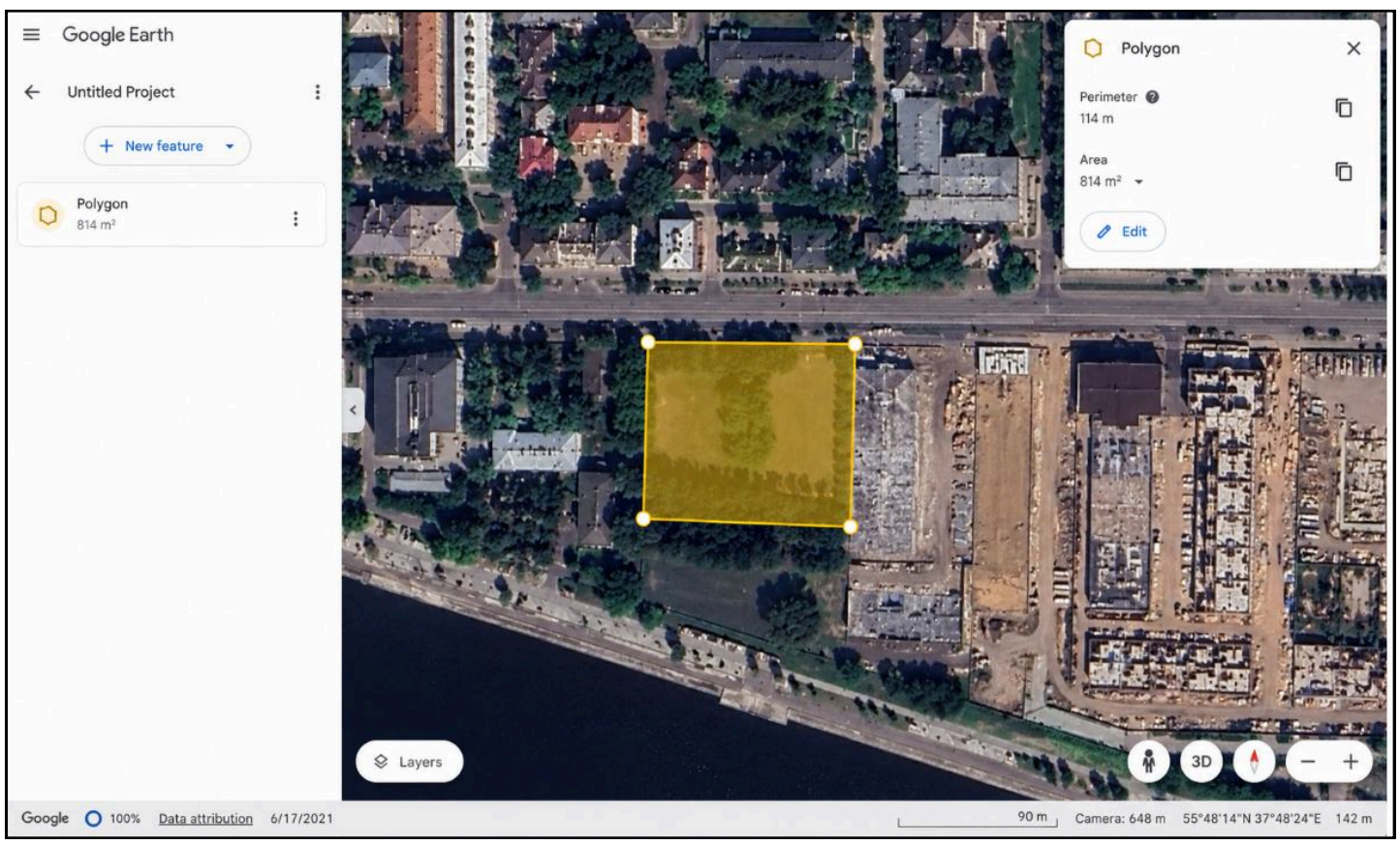
У результаті атака призводить не лише до технічного руйнування систем, а й до зниження довіри до державних цифрових сервісів, що підсилює загальний дестабілізаційний ефект.

Місцезнаходження

в/ч 29155 (161-й центр ГРУ) і пов’язані кіберкластерні групи

м. Москва, вул. 11-я Паркова, буд. 38А

Координати: 55.801–55.803 N, 37.805–37.808 E



Контур досліджуваної ділянки за координатами 55.801–55.803 N, 37.805–37.808 E

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

Контур досліджуваної зони за координатами 55.801–55.803 N, 37.805–37.808 E (Москва)

Виділена область представляє собою прямокутну ділянку міської забудови, визначену за координатами 55.801–55.803 N, 37.805–37.808 E. Контур використовується для аналізу супутникових знімків та структури міського середовища.

TTP таблиця:
Ember Bear (DEV-0586 / Cadet Blizzard) — WhisperGate

Фаза (Tactic)	Техніка (MITRE ATT&CK)	Опис поведінки (конкретно для групи)
🟢 **Початковий доступ**	Phishing (T1566)	Використання фішингових листів із шкідливими вкладеннями або посиланнями для первинного проникнення
🟢 **Початковий доступ**	Exploit Public-Facing Application (T1190)	Використання вразливостей у публічних сервісах (сервери, веб-додатки)
🟡 **Виконання**	PowerShell (T1059.001)	Запуск шкідливих скриптів для завантаження та виконання payload
🟡 **Виконання**	Windows Command Shell (T1059.003)	Використання cmd.exe для запуску команд і сценаріїв
🔵 **Розвідка**	System/Network Discovery (T1018, T1046)	Сканування мережі, виявлення серверів, доменів і критичних систем
🔵 **Розвідка**	Account Discovery (T1087)	Збір інформації про користувачів та адміністративні облікові записи
🟠 **Закріплення / рух**	Remote Services (T1021)	Використання RDP/SMB для переміщення мережею
🟠 **Закріплення / рух**	Valid Accounts (T1078)	Використання викрадених або легітимних облікових даних
🟠 **Lateral Movement**	Pass-the-Hash (T1550.002)	Використання хешів паролів для доступу до інших систем
🟣 **Підготовка атаки**	Scheduled Task (T1053)	Створення задач для запуску шкідливого коду у визначений час
🟣 **Підготовка атаки**	Obfuscated/Encoded Files (T1027)	Маскування шкідливих компонентів перед активацією
🔴 **Деструкція (Impact)**	Disk Wipe (T1561.002)	Знищення структури диску (MBR/boot)
🔴 **Деструкція (Impact)**	Data Destruction (T1485)	Масове знищення файлів і даних на системах
🔴 **Деструкція (Impact)**	System Shutdown/ Reboot (T1529)	Примусові перезавантаження та виведення систем із ладу
⚫ **Приховування слідів**	Indicator Removal (T1070)	Видалення файлів і логів після виконання атаки
🟤 **Психологічний вплив**	Defacement (T1491)	Повідомлення/екрани-вимоги та демонстративні повідомлення жертвам

WhisperGate варто розглядати як показовий приклад сучасної руйнівної кібероперації, де технічна складність поєднується з чітко вираженою деструктивною метою. Це не була класична кібершпигунська кампанія чи спроба фінансової вигоди — основний акцент робився на максимальному порушенні працездатності систем і створенні ефекту раптової цифрової дезорганізації.

Особливо важливо, що така атака демонструє багатоступеневу модель впливу: від початкового проникнення і закріплення в інфраструктурі до фінальної фази знищення даних і виведення систем з ладу. Це свідчить про високий рівень планування та координації, характерний для організованих кібероперацій державного рівня.

Водночас WhisperGate підкреслює, що сучасні кіберзагрози виходять за межі суто технічної площини. Окрім фізичного руйнування даних, важливу роль відіграє психологічний і інформаційний ефект, спрямований на дестабілізацію та підрив довіри до цифрової інфраструктури.

Таким чином, ця операція є яскравим прикладом того, як кіберпростір використовується як інструмент гібридного впливу, де технічні атаки стають частиною ширших стратегічних і політичних цілей.

ДЖЕРЕЛА

1. https://attack.mitre.org/groups/G1003/
2. https://www.microsoft.com/security/blog/2024/01/25/cadet-blizzard-emerges-as-a-novel-threat-actor/
3. https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf
4. https://www.crowdstrike.com/blog/who-is-ember-bear/
5. https://www.paloaltonetworks.com/blog/security-operations/whispergate-malware-analysis/
6. https://unit42.paloaltonetworks.com/ukraine-cyber-attacks/
7. https://www.mandiant.com/resources/blog/ukraine-cyber-threat-activity
8. https://www.s2w.inc/blog/whispergate-analysis
9. https://arxiv.org/abs/2510.18484
10. https://war-sanctions.gur.gov.ua/ru/sanctions/persons/36234
11. https://thehackernews.com/2024/09/us-offers-10-million-for-info-on.html
12. https://www.opensanctions.org/entities/NK-eeazQVNhtHhNCisAvwakVv/
13. https://rewardsforjustice.net/rewards/gru-officers-unit-29155/
14. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/?ocid=magicti_ta_blog
15. https://www.golosameriki.com/a/russia-father-son-accused-cybercrimes-gru/7701912.html