OSINT-звіт: APT-угрупування Killnet

KillNet — проросійське хакерське активістське угруповання, яке активізувалося після початку повномасштабного вторгнення РФ в Україну у 2022 році. До війни група функціонувала як сервіс DDoS-for-hire, однак згодом переорієнтувалася на політично мотивовані атаки проти державних установ, приватних компаній та об’єктів критичної інфраструктури країн, що підтримують Україну. Основною діяльністю KillNet залишаються DDoS-атаки, інформаційно-психологічні операції та кампанії залякування, які активно супроводжуються медійною активністю в Telegram та інших соціальних платформах.

Група позиціонує себе як «захисник інтересів Росії» та систематично використовує проросійську риторику. Навколо KillNet сформувалася широка мережа афілійованих хактивістських груп, серед яких Anonymous Sudan, Infinity Team та інші проросійські кіберспільноти.

KillNet неодноразово брала на себе відповідальність за атаки на урядові ресурси країн НАТО, медичні установи, оборонні компанії та фінансовий сектор. Частина заяв групи має ознаки перебільшення або інформаційних маніпуляцій, однак угруповання залишається одним із найбільш публічних та впізнаваних проросійських хактивістських брендів. KillNet часто співпрацює із проросійськими кіберкримінальними спільнотами, що підвищує ризик комбінованих атак із використанням DDoS, шифрувальників та витоків даних.

Попри переважно низький або середній технічний рівень окремих операцій, KillNet становить загрозу через здатність швидко мобілізувати велику кількість прихильників для проведення масових кампаній та створення інформаційного резонансу. Основними цілями угруповання залишаються державні структури, критична інфраструктура та організації країн, які підтримують Україну у війні проти РФ.

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

Ідеологія та мотивація

KillNet від початку свого існування дотримується вираженої проросійської позиції. Після початку повномасштабного вторгнення РФ в Україну акцент діяльності групи змістився на підтримку російської військової кампанії та протидію Україні й державам, які її підтримують. Така позиція сприяла зближенню KillNet з іншими проросійськими хактивістськими угрупованнями, зокрема білоруською групою Infinity Hackers. Група демонструє виражену антизахідну та антиамериканську риторику, розглядаючи США як одного з ключових опонентів Росії в кіберпросторі.

Основною мотивацією KillNet є не фінансовий прибуток, а підтримка власної ідеології та дестабілізація діяльності противників, про це свідчить відсутність вимагання грошей у багатьох кейсах, а також ідеологічне обгрунтування самих атак хакерами з killnet. Водночас група регулярно збирає пожертви для підтримки своєї мережі хактивістів.

В багатьох статтях присвячених KillNet, часто вказують що: “Хоча прямий зв’язок KillNet із російськими спецслужбами офіційно не підтверджений, діяльність угруповання часто збігається з геополітичними інтересами РФ”. Однак, якщо проаналізувати діяльність KillNet, то про співпрацю з ФСБ або іншими державними органами можна зробити наступні припущення:

1. Цілі KillNet співпадають з цілями Кремля, бо незважаючи на повідомлення про ксенофобські погляди окремих представників Killnet, вибір цілей угруповання демонструє послідовну орієнтацію на держави, які підтримували Україну або займали позиції, несприятливі для зовнішньополітичних інтересів РФ. Це дозволяє припустити, що оперативне планування кампаній здійснювалося в рамках пріоритетів, ширших за особисті ідеологічні переконання окремих учасників групи.

2. Відсутність реакції російських правоохоронних органів та позитивне висвітлення діяльності угруповання. KillNet весь час відкрито здійснювало вербування учасників, публічно заявляло про проведення кібератак та підтримувало активну присутність у соціальних мережах і месенджерах. Попри це, інформація про системні заходи з боку російських правоохоронних органів щодо припинення його діяльності відсутня. Натомість окремі операції та заяви KillNet отримували позитивне або нейтральне висвітлення в російських державних медіа.
   Джерело: https://www.rbc.ru/rbcfreenews/6a27f7299a794768a9e67668

3. Можливість використання моделі plausible deniability («правдоподібного заперечення»). Такий підхід передбачає використання формально незалежних хактивістських або кримінальних угруповань для досягнення державних цілей із збереженням можливості офіційно заперечувати будь-який зв'язок із ними. Подібна практика неодноразово описувалася дослідниками кібербезпеки як характерний елемент російської кіберстратегії, що дозволяє поєднувати політичні вигоди від діяльності проксі-структур із мінімізацією репутаційних та юридичних ризиків для держави.

3. Відсутність у KillNet складних кіберрозвідувальних операцій не є достатньою підставою для заперечення його можливої ролі у реалізації російських державних інтересів. На відміну від APT-угруповань, орієнтованих на приховану розвідку та довготривалий доступ до мереж, KillNet спеціалізувався на DDoS-атаках та інформаційно-психологічних кампаніях. Це може свідчити не про відсутність зв'язків із державою, а про іншу функціональну роль угруповання в межах ширшої системи проросійських кібероперацій.

4. Попри те що Killmilk намагається розвіяти уявлення, що Killnet є російською проксі-групою, Killnet дотримується російських хакерських норм і вимагає від членів групи засвідчити, що вони ніколи не працюватимуть у російському сегменті Інтернету або не атакуватимуть російські цілі чи ініціативи. Зрештою, Killmilk утримує діяльність груп у межах того, що російський уряд вважає прийнятною поведінкою, щоб уникнути будь-якого негативного опору з боку держави.

Ключові події

Дата / рік	Подія	Короткий опис атаки
29.04.2022 – 01.05.2022	Атаки на урядові сайти Румунії	KillNet здійснила DDoS-атаки на веб-ресурси урядових установ Румунії.
Квітень 2022	Кібератаки на Молдову після подій у Придністров'ї	Проросійська група, пов'язана з KillNet, атакувала сайти державних органів та установ Молдови. Атаки проводилися з-за кордону, переважно методом DDoS.
Квітень 2022	Атаки на державні установи Чехії	KillNet заявила про відповідальність за атаки на вебсайти державних установ Чехії. Основним методом були DDoS-атаки для перевантаження ресурсів.
14.05.2022	Атака на державні ресурси Італії	Під атаку потрапили сайти Istituto Superiore di Sanità, Automobile Club of Italy та Сенату Італії. Атаки були спрямовані на тимчасове блокування доступу до ресурсів через DDoS.
29–30.05.2022	Масована кібератака на Італію	KillNet анонсувала «руйнівну» атаку на Італію. Було атаковано низку державних сайтів, однак більшість атак була успішно відбита CSIRT Італії.
Травень 2022	Спроба атаки на Eurovision 2022	Імовірна DDoS-атака на сайт Eurovision Song Contest під час виступу України. Атаку заблокувала поліція Італії. Після цього KillNet атакувала сайт італійської поліції.

Дата / рік	Подія	Короткий опис атаки
Червень 2022	Кібератаки на Литву	KillNet заявила про атаки на мережеву інфраструктуру Литви у відповідь на обмеження транзиту до Калінінграда. Використовувалися DDoS-атаки проти державних та мережевих ресурсів.
28.06.2022	Атаки на організації Норвегії	Норвезькі організації зазнали серії DDoS-атак. За даними влади Норвегії, витоку приватних даних зафіксовано не було.
2022	Найбільша кібератака на мовника Латвії	KillNet атакувала державного мовника Латвії. Атака вважається однією з найбільших в історії країни, однак була успішно відбита.
01.08.2022	Атака на Lockheed Martin (США)	KillNet заявила про кібератаку на оборонну компанію Lockheed Martin у відповідь на постачання HIMARS Україні. Заявлялось про спроби атак на виробничі системи та дані співробітників.
10.10.2022	Атаки на сайти аеропортів США	Було атаковано низку вебсайтів американських аеропортів. Основним методом були DDoS-атаки, спрямовані на тимчасове порушення роботи ресурсів.
6–7.09.2022	Атаки на державні ресурси Японії	KillNet заявила про атаки на сайти міністерств, e-Gov, eLTAX та платформу Mixi. Також були заяви про атаки на Tokyo Metro та Osaka Metro. Ознак витоку даних не виявлено.
2022	Погрози кібератак уряду Грузії	KillNet та її лідер Killmilk публічно погрожували атаками на уряд Грузії через антиросійську позицію країни.
26.01.2023	Масові DDoS-атаки на Німеччину	Федеральне відомство інформаційної безпеки Німеччини (BSI) повідомило про масштабні DDoS-атаки на аеропорти, фінансовий сектор та державні установи. Атаки пов’язували з рішенням Німеччини передати Україні танки Leopard 2.
28.01.2023 - 23.04.2023	DDoS-атаки, спрямовані на організації HPH у США	Понад 90 відомих DDoS-атак було спланновано і здійснено на системи охорони здоров'я, окремі лікарні та медичні центри. Оскільки це зазвичай великі заклади зі значним обсягом даних пацієнтів, ці типи організацій охорони здоров'я є ідеальними цілями для KillNet та її афілійованих осіб. 17 березня 2023 року Microsoft Security опублікувала свої спостереження про те, що KillNet атакував медичні програми, використовуючи інфраструктуру Microsoft Azure, протягом понад трьох місяців. Атаки пов’язують з наданням допомоги Україні, у вигляді танків.

Висновок: Описи атак свідчать про реактивний характер діяльності KillNet. Група не демонструє власної стратегічної програми вибору цілей, а переважно реагує на політичні рішення держав, що суперечать інтересам РФ.

Організаційна структура та зв'язки

4 січня 2022 року було створено Telegram-канал «We are KillNet», через який просувалися послуги DDoS/Stressor-атак на довільні вебресурси. Засновником угруповання вважається особа під псевдонімом KillMilk. З моменту початку повномасштабного вторгнення РФ в Україну KillNet перетворилася з сервісу DDoS-for-hire на одну з найбільш відомих проросійських хактивістських спільнот. Група активно використовує Telegram для координації діяльності, поширення пропагандистських повідомлень та залучення нових прихильників. Навколо KillNet сформувалася широка мережа афілійованих угруповань, які підтримують спільні цілі та здійснюють скоординовані кібероперації.

Представники KillNet неодноразово наголошували, що організація не має жорсткої централізованої структури. **У березні 2023 року** в офіційних повідомленнях група позиціонувала себе як децентралізовану спільноту, яка об'єднує так званих «кіберпатріотів Росії», та заперечувала будь-яку державну підтримку. Водночас діяльність її лідера KillMilk свідчить про спроби формалізації окремих напрямків роботи. Зокрема, у березні 2023 року ним було оголошено про створення структури Black Skills PMHC («Приватна військова хакерська компанія»), яка передбачала наявність понад двадцяти функціональних підрозділів, відповідальних за розвідку, інформаційний супровід, фінанси, інвестиції та інші напрямки діяльності.

У липні 2022 року KillMilk заявив про свій вихід із KillNet, мотивуючи це необхідністю захистити учасників групи від потенційних ризиків. Незважаючи на формальний вихід із керівництва, подальша активність у Telegram свідчила про збереження взаємодії між KillMilk та KillNet. Після його відходу керівництво групою, за наявними даними, перейшло до хакера під псевдонімом BlackSide, якого пов'язують із діяльністю у сферах програм-вимагачів (ransomware), фішингових кампаній та викрадення криптовалютних активів.

Серед найбільш відомих партнерських та афілійованих угруповань KillNet фігурують Anonymous Russia, Infinity Hackers, National Hackers Russia, NETSIDE Group, Passion Botnet та Phoenix. Аналіз інформаційних кампаній групи свідчить про значний вплив KillNet на ширше середовище проросійських хактивістів. На відміну від професійних кіберугруповань, пов'язаних із російськими спецслужбами, таких як Fancy Bear або Sandworm, діяльність KillNet характеризується більш реактивним та ідеологічно мотивованим характером. Основними об'єктами її атак стають державні установи, організації та компанії, які група вважає такими, що підтримують Україну або займають антиросійську позицію. Саме поєднання значної медійної присутності, широкої мережі прихильників та здатності швидко мобілізовувати учасників для проведення масових кампаній робить KillNet одним із найвпливовіших проросійських хактивістських брендів. (5)

У березні 2023 року лідер KillNet, Ніколай Серафімов, оголосив про створення структури під назвою Black Skills, яку позиціонував як «Приватну військову хакерську компанію» (Private Military Hacking Company). Сам термін є очевидною відсилкою до концепції приватних військових компаній, що набули значної популярності в Росії після активного використання таких структур, як Wagner Group.

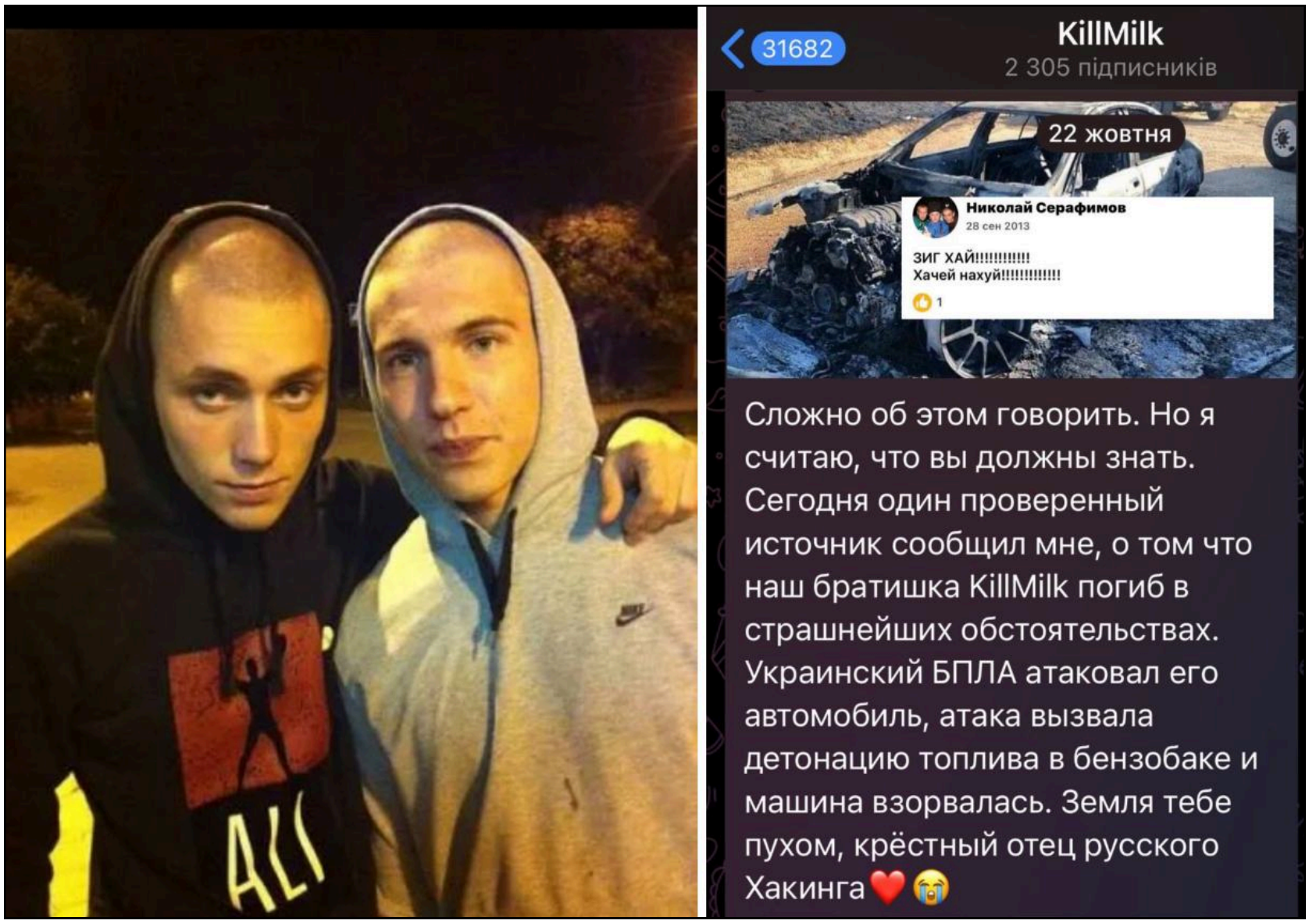
На відміну від попередньої моделі функціонування KillNet як відносно децентралізованого хактивістського об'єднання, проєкт Black Skills передбачав створення більш формалізованої організаційної структури. Згідно із заявами учасників угруповання, нова модель мала включати окремі функціональні підрозділи, відповідальні за кадрове забезпечення, фінансове адміністрування, зв'язки з громадськістю, технічну підтримку, проведення пентестів, збір та аналіз інформації, інформаційно-психологічні операції, а також здійснення атак проти визначених цілей. Такий підхід свідчить про прагнення перейти від спільноти добровольців до структури з чітким розподілом функцій та внутрішньою ієрархією.

Додатковим елементом формалізації стала процедура відбору нових учасників. Кандидати повинні були заповнювати анкети із зазначенням професійних навичок, досвіду роботи, проходження військової служби та державної служби. Це відрізнялося від попередньої практики відкритого залучення учасників через Telegram-канали та свідчило про спробу створення системи внутрішньої перевірки й розподілу ролей залежно від компетенцій.

Поява Black Skills також може розглядатися як реакція на невдачі попередніх ініціатив KillNet щодо масштабування своєї діяльності. Зокрема, створений наприкінці 2022 року форум Infinity, який мав стати майданчиком для співпраці між хактивістами та кіберзлочинцями, не зміг залучити достатню кількість активних учасників, а проєкт так званої «школи хакерів» не отримав значного розвитку. У цих умовах Black Skills стала спробою перейти від неформальної мережевої моделі до більш керованої організації із власними адміністративними, операційними та фінансовими механізмами.

Водночас відсутні підтвердження того, що всі заявлені структурні підрозділи фактично функціонували на практиці. Частина оголошених «департаментів» могла мати декларативний характер і використовуватися насамперед для створення образу професійної кіберструктури. Це можна пояснити тим, що створити хакера з звичайного інтернет-активіста доволі складно, складні операції потребують дуже тривалої підготовки і навичок, а не тільки бажання. Проте сама спроба побудови організації за принципом корпоративної або військової моделі свідчить про прагнення керівництва KillNet підвищити керованість угруповання, монетизувати наявні ресурси та створити стійку інфраструктуру для подальшого розвитку своїх операцій.[6]

Лідер KillNet



Nick — KillMilk
ПІБ - Серафимов Николай Николаевич
Дата народження - 16.05.1993
Відбував покарання в Республіці Башкортостан, місто Салават (ВК-2).

Стаття — 228.1 частина 5. Строк — 8 років. Був звільнений умовно-достроково (УДО), пізніше був завербований ФСБ і направлений до Краснодара нібито на ПТР (примусові трудові роботи).
Основний Telegram — t.me/sooosoosos
Джерело: https://telegra.ph/Lichnost-KillMilk-11-03

Висновок:

На відміну від класичних APT-угруповань із чіткою організаційною структурою та спеціалізованими підрозділами, KillNet функціонує за моделлю децентралізованої хактивістської мережі. Центральну роль у формуванні стратегічних наративів та координації діяльності тривалий час відігравав засновник угруповання KillMilk. Навколо нього сформувалося ядро координаторів, яке взаємодіяло з афілійованими проросійськими групами та широкою мережею прихильників у Telegram. Відсутність підтверджених витоків внутрішніх комунікацій та достовірної інформації про склад учасників не дозволяє точно визначити чисельність і структуру KillNet. Наявні дані свідчать, що головною перевагою угруповання є не централізоване управління, а здатність швидко мобілізувати зовнішніх учасників для проведення скоординованих кібер- та інформаційних кампаній.

Тактики та методи атак

Від початку російсько-української війни група успішно виводила з ладу веб-ресурси та порушувала роботу організацій у різних країнах НАТО. Хоча подібні атаки зазвичай не становлять загрози, вони можуть спричиняти суттєві перебої в роботі організацій та значні фінансові збитки через простої сервісів і втрату доходів. Окрім економічних наслідків, діяльність KillNet свідчить про прагнення порушувати комунікації та тестувати потенційні цілі для більш серйозних операцій. Наприклад, атака на виборчий веб-ресурс у штаті Кентуккі та заяви про отримання персональних даних співробітників компанії Lockheed Martin, які потенційно могли використовуватися для подальшого переслідування або таргетування окремих осіб. Це свідчить про поступову ескалацію кібероперацій, коли об’єктами атак стають не лише безпосередні учасники військових дій, а й представники оборонно-промислового комплексу та цивільної інфраструктури. (4)

Крім того, KillNet та подібні хактивістські угруповання використовують DDoS-атаки переважно для привернення уваги та створення інформаційного ефекту, а не для завдання масштабної шкоди. Більшість атак триває менш ніж 12 годин, а серед основних векторів фіксувалися TCP SYN, TCP ACK та аномальні мережеві пакети. Для проведення операцій група ймовірно використовує DDoS-скрипти, стресери, залучені ботнети та підміну джерел трафіку. Відсутність будь-яких вимог щодо викупу свідчить про те, що Killnet не прагне отримати фінансову вигоду.

Орієнтовний цикл операції KillNet

1. Обрання цілі: Зазвичай триггером служить якась політична подія
2. Розвідка: passive/active recon
3. Підготовка до атаки:
    a. Публічне оголошення кампанії
    b. Мобілізація прихильників
    c. Підготовка інфраструктури для атаки
4. Проведення DDoS-операції
5. Інформаційна експлуатація результатів
    a. Поширення наративів, медійна компанія
    b. Залучення нових учасників за рахунок “успішності операції”

Для координації атак KillNet використовує власні Telegram-канали, через які публікує цілі та надає своїм прихильникам вказівки щодо часу й напрямків проведення DDoS-атак. Серед основних технік, які застосовує угруповання, фігурують ICMP Flood, IP Fragmentation, TCP SYN Flood, TCP RST Flood, TCP SYN/ACK Flood, NTP Flood, DNS Amplification та LDAP Connection-less (CLDAP) Amplification.

Згодом, Killnet,також розширили свій арсенал, додавши до нього шкідливе програмне забезпечення типу ransomware-wiper. У 2022му вони використали конструктор Chaos 4.0, який має особливість: замість шифрування великих файлів користувачів він перезаписує їх випадковими даними, роблячи відновлення неможливим. Саме тому цей шкідливий код класифікується як вайпер (wiper) — програма, призначена для безповоротного знищення даних.

Якщо такі загрози, як Killnet, не будуть своєчасно виявлені та зупинені, єдиним способом відновлення інформації залишаться наявні резервні копії. Водночас усі дані, які не були включені до резервного копіювання на момент атаки, можуть бути втрачені безповоротно. (4)

MITRE ATT&CK

- **T1498 – Network Denial of Service**

Confidence: High

Найбільш характерна техніка KillNet, використовувалися: TCP SYN Flood, TCP ACK Flood, ICMP Flood, DNS Amplification, CLDAP Amplification.

У своєму аналізі за березень 2023 року Microsoft Security зазначила, що основним інструментом KillNet залишаються DDoS-атаки. Такий тип атак є відносно простим, недорогим та анонімним способом порушення роботи вебсайтів і онлайн-сервісів

- **T1595 – Active Scanning**

Confidence: High

Перед проведенням DDoS-кампаній група повинна ідентифікувати: IP-адреси цілей, вебресурси, DNS-інфраструктуру і т.д.

- **T1583 – Acquire Infrastructure**

Confidence: High

Практично всі великі DDoS-кампанії KillNet вимагали використання сторонньої інфраструктури: VPS, ботнетів, орендованих серверів для проведення атак, особливо це було характерно для раннього етапу існування групи як DDoS-for-hire сервісу.

- **T1589 – Gather Victim Identity Information**

Confidence: Medium

У кейсі Lockheed Martin, KillNet заявляла про отримання персональних даних співробітників. Для такого таргетування зазвичай використовується: збір email, аналіз профілів співробітників, відкриті бази даних.

- **T1584 – Compromise Infrastructure**

Confidence: Medium

Частина ботнет-інфраструктури могла складатися з вже скомпрометованих систем. Використання скомпрометованої інфраструктури є типовим для DDoS-операцій такого масштабу.

- **T1499 – Endpoint Denial of Service**

Confidence: Medium

У низці випадків група намагалася перевантажити конкретні сервіси та вебзастосунки. Однак більшість підтверджених кейсів все ж належить до Network DoS.

- **T1485 – Data Destruction**

Confidence: Low-Medium

Після повідомлень про використання Chaos 4.0 та ransomware-wiper можна припустити використання технік знищення даних. Але ця техніка не є основною для KillNet.

Джерело: https://www.acronis.com/en/tru/posts/killnet-ransomware-a-wiper-from-the-chaos-family/?utm

Information Operations

KillNet використовує DDoS не стільки як інструмент руйнування інфраструктури, скільки як механізм підтримки інформаційно-психологічних операцій. У багатьох випадках фактичний вплив атак був обмеженим або короткочасним, проте медійне висвітлення та активність у Telegram дозволяли угрупованню створювати враження значно масштабніших результатів. Це свідчить про те, що інформаційний ефект є одним із головних результатів діяльності KillNet поряд із технічним впливом на цільові системи.

Подібно до російських спецслужб, KillNet активно застосовує інструменти інформаційного впливу, включаючи пропаганду, дезінформацію та поширення неправдивих відомостей. Так, в одному з інтерв'ю RT, лідер групи KillMilk заявив про нібито наявні докази того, що США створили вірус COVID-19.

Джерело: https://russian.rt.com/world/article/1059107-killnet-hakery-ssha-razoblachenie

У своїх Telegram-каналах KillNet та KillMilk активно використовують сучасні візуальні формати подачі інформації, зокрема меми, GIF-зображення, емодзі та короткі відеоролики для поширення погроз, пропаганди та повідомлень про проведені атаки. Подібні дії свідчать про те, що угруповання уважно відстежує публікації дослідників кіберзагроз та матеріали відкритих джерел, присвячені його діяльності.

Підсумок

Основними характеристиками та тактиками KillNet є:

- вибір цілей серед країн НАТО та держав, політичні інтереси яких суперечать інтересам Росії;
- переважне використання DDoS-атак як основного інструменту впливу;
- орієнтація на урядові вебресурси та сайти державних установ;
- попереднє анонсування атак і цілей через Telegram-канали;
- співпраця з іншими проросійськими хактивістськими та кіберкримінальними угрупованнями.
- Інформаційно-психологічні операції

Значення та оцінка загрози

Хоча більшість атак KillNet не мала довгострокових наслідків, діяльність угруповання демонструє тенденцію до зростання ролі неофіційних проросійських хактивістських спільнот поряд із державними кібер угрупованнями, такими як Fancy Bear та Sandworm. Такі групи стають дедалі організованішими та здатними здійснювати атаки проти будь-яких цілей, які вони вважають ворожими до Росії. Подібна тенденція спостерігається з обох сторін російсько-українського конфлікту та свідчить про вихід кібер протистояння на глобальний рівень. Участь у ньому можуть брати добровольці з будь-якої країни світу, що мають доступ до мережі Інтернет. Відсутність географічних обмежень та складність ідентифікації учасників таких груп значно ускладнюють роботу фахівців із кібербезпеки та державних структур/

Попри те, що керівництво KillNet має досвід роботи з DDoS-сервісами та ботнетами, більшість операцій групи здійснювалася із застосуванням загальнодоступних DDoS-скриптів та IP-стресерів(Це інструмент, що імітує інтенсивний інтернет-трафік). Експерти з кібербезпеки застерігають від недооцінки політично мотивованих кіберзлочинців, оскільки вони не зацікавлені у прибутку від своїх операцій і можуть застосовувати дедалі більш руйнівне шкідливе програмне забезпечення в майбутньому.

Основною силою угрупування є не складні кібероперації, а здатність швидко мобілізувати велику кількість учасників для проведення масових DDoS-кампаній та створення значного інформаційно-психологічного ефекту. Важливим елементом діяльності KillNet є активне інформаційне супроводження власних операцій, що дозволяє посилювати суспільний резонанс навколо атак незалежно від їхнього фактичного впливу, наприклад, як у випадку атаки на американські аеропорти [https://www.npr.org/2022/10/10/1127902795/airport-killnet-cyberattack-hacker-russia], що подавалось KillNet ледь не як смерть Америки, але атака не задала ніякої шкоди і тривала менш ніж 20 хвилин. У низці випадків публічна активність угруповання сприяла формуванню перебільшенного сприйняття його можливостей, через що окремі інциденти могли помилково пов'язуватися з KillNet або отримувати значно ширше висвітлення, ніж їхній реальний технічний ефект.

Попри значну медійну увагу до діяльності KillNet, більшість операцій угруповання не призводила до тривалого порушення роботи критичної інфраструктури або масштабних технічних наслідків. На мою думку, основною силою KillNet є не складність або руйнівність кібератак, а здатність використовувати кібероперації як інструмент інформаційно-психологічного впливу.

Таким чином, DDoS-атаки виступають переважно засобом привернення уваги, мобілізації прихильників та підтримки проросійських наративів у інформаційному просторі. Найбільшу загрозу становлять не самі технічні наслідки атак, а формування інформаційного резонансу, поширення пропагандистських повідомлень та створення перебільшеного уявлення про можливості угруповання серед цільових аудиторій.

Рекомендації щодо протидії DDoS-атакам

Повністю усунути ризик DDoS-атак неможливо, однак організації можуть значно підвищити свою стійкість до таких інцидентів. Національний центр кібербезпеки Великої Британії (NCSC) рекомендує зосередитися на п’яти ключових напрямках:

1) Розуміння критичних сервісів, використання захисту на боці провайдера.

2) Масштабування ресурсів.

3) Підготовка плану реагування

4) Регулярне тестування.

5) Моніторинг інфраструктури.

Для підвищення рівня захисту організаціям рекомендується:

- впроваджувати рішення класу Web Application Firewall (WAF) для фільтрації шкідливого трафіку та захисту веб-застосунків від атак на прикладному рівні;
- використовувати спеціалізовані сервіси DDoS Mitigation та забезпечувати взаємодію з інтернет-провайдерами й хмарними постачальниками, які можуть здійснювати фільтрацію трафіку на рівні мережевої інфраструктури;
- застосовувати архітектуру Multi-CDN, яка дозволяє розподіляти навантаження між декількома мережами доставки контенту та зменшує ризик відмови окремого провайдера;
- забезпечувати масштабованість критичних сервісів за рахунок використання хмарних технологій, балансування навантаження та механізмів автоматичного горизонтального масштабування;
- впроваджувати системи моніторингу мережевого трафіку, логування та виявлення аномалій для оперативного виявлення ознак атак;
- використовувати механізми обмеження швидкості запитів (Rate Limiting), географічної фільтрації трафіку та сегментації мережі;
- розробити та підтримувати актуальний план реагування на DDoS-інциденти, який передбачає розподіл ролей і відповідальності, канали комунікації, процедури дії на випадок атаки;
- регулярно проводити навчання, кібернавчання (tabletop exercises) та тестування ефективності захисних механізмів для перевірки готовності персоналу та технічних засобів до реальних атак.

Мінімізація обсягів публічно доступних даних дозволяє знизити ризики їх використання хактивістськими групами, кіберзлочинцями або іншими суб’єктами загроз для підготовки інформаційно-психологічних операцій, кампаній з дискредитації чи цільових кібератак.

Джерела

1. https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf
2. https://www.ncsc.gov.uk/guidance/preparing-denial-service-dos-attacks
3. https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/ddos.html
4. https://westoahu.hawaii.edu/cyber/uncategorized/killnet-russian-hacktivists-ddos-us-airports-government-websites/
5. https://www.hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf
6. https://flashpoint.io/blog/killnet-killmilk-private-military-hacking-company/
7. https://www.lawfaremedia.org/article/what-impact-if-any-does-killnet-have