

OSINT-звіт

Anonymous Sudan

● Походження

Угрупування виникло у середині січня 2023 року у формі Telegram-каналу, що презентував себе як проісламських хактивістів. Назва запозичена від хакерської операції "Anonymous Sudan" 2019 року; оригінальний рух Anonymous публічно відмежувався від нового угруповання одразу після його появи.[6]

● Атрибуція

Оцінки Truesec, Trustwave, Mandiant та Microsoft вказують на можливу координацію або взаємозв'язки угруповання з проросійським хактивістським середовищем, зокрема з Killnet. Microsoft відстежує актора Anonymous Sudan під ідентифікатором Storm-1359 та зазначає ймовірні зв'язки з Killnet і можливу підтримку з боку РФ. Водночас наявних відкритих даних недостатньо для однозначного підтвердження прямого організаційного підпорядкування або контролю з боку Killnet чи російських державних структур.[3]

● Судовий статус

16 жовтня 2024 року Мін'юст США розкрив обвинувальний висновок федерального журі присяжних щодо двох громадян Судану (братів Омер) як реальних операторів угруповання. Кваліфікація в документах — кіберзлочинна організація, відповідальна за десятки тисяч DDoS-атак проти критичної інфраструктури, корпоративних мереж та державних установ у США та світі. [9]



2. Ідеологія, мотивація та вибір цілей

2.1. Заявлена ідеологія угруповання

Ґрунтується на захисті релігійних інтересів ісламу, при цьому вибір цілей обґрунтовується наявністю в країни-жертви дій, що кваліфікуються угрупованням як "антимусульманські" (публічне спалення примірників Корану, підтримка Держави Ізраїль, участь у військових операціях проти угруповання ІДІЛ). Зазначене формулювання є достатньо широким для ретроспективного обґрунтування вибору практично будь-якої цілі.

2.2. Геополітичний аспект і антизахідна риторика

Наявні поведінкові дані підтверджують заявлену ідеологічну мотивацію лише частково, угрупованням систематично ігноруються задокументовані випадки утисків мусульманського населення в країнах, що не належать до західного блоку, ця обставина, не характерна для автентичного релігійно мотивованого руху. Натомість можна побачити стійку кореляцію між переліком фактичних цілей угруповання та переліком держав, що надають підтримку Україні в контексті російсько-української війни, а саме: Швеція, Нідерланди, Австралія, Німеччина, а на подальшому етапі — банківська система США та країн Європейського Союзу.

1. Шведський напрям особливо добре демонструє перетин релігійного та геополітичного мотивів. Формальним приводом для атак були акції зі спаленням Корану, однак кампанія відбувалася одночасно з процесом вступу Швеції до НАТО. Це саме по собі не доводить, що НАТО було справжньою або єдиною мотивацією групи, однак демонструє, що релігійний привід накладався на актуальний геополітичний конфлікт.
2. Anonymous Sudan, не здійснив жодного нападу на саму Україну, це може свідчити про свідоме небажання створити вигляд проросійськості і мати ширше поле для маневрів, не роблячи при цьому відкрито проросійського позиціонування центральною частиною власної публічної ідентичності.
3. Окремого розгляду потребує Ізраїль. На відміну від атак на Швецію чи Нідерланди, тут релігійно-політичне обґрунтування було значно безпосереднішим: Anonymous Sudan посилалася на палестинське питання, «окупацію Палестини» та пізніше брала участь в атаках, приурочених до Quds Day. У травні 2023 року, під час загострення в секторі Гази, Anonymous Sudan заявила, що вивела з ладу низку цивільних застосунків-оповіщувачів про ракетну небезпеку (Red Alert, Cumta, Halamish, Evigilo), і приписала собі зниження ефективності перехоплення Iron Dome того дня. Відкриті дані цього періоду не дозволяють однозначно встановити іранське керування Anonymous Sudan, однак вони демонструють, що група могла діяти в інформаційному та операційному середовищі, де російські, іранські та антиізраїльські інтереси частково перетиналися.

При цьому важливо не перебільшувати роль Ірану. Сам факт збігу антиізраїльської кампанії Anonymous Sudan із Quds Day або контакту з іранським хактивістським середовищем не є доказом координації з іранською державою. Навпаки, наявні дані дозволяють говорити передусім про збіг наративів, цілей та окремих операційних активностей, тоді як питання прямої координації залишається невстановленим.

В даному випадку релігійна риторика добре пояснює частину конкретних кампаній, але не дає достатнього пояснення всієї сукупності цілей, тож вона могла виконувати не лише функцію ідеологічного обґрунтування, а й надавати групі додаткову правдоподібність та простір для визначення власної політичної приналежності. Водночас афіліація з KillNet та відповідність значної частини цілей російським геополітичним інтересам роблять проросійський контекст суттєвим фактором оцінки діяльності Anonymous Sudan, хоча самі по собі не доводять її прямого контролю з боку Росії.

2.3. Фінансовий шар мотивації

На самому початку виникнення групи, ознак комерційної мотивації було небагато, лише кілька рекламних постів. Але вже за рік картина стала зовсім іншою: платні DDoS-атаки на замовлення, вимагання викупу в жертв (від кількох тисяч доларів до вимоги 3 мільйонів у Scandinavian Airlines), пропозиція відключення інтернет-провайдера в обраній країні за 500 доларів на годину. Тобто якщо в лютому 2023-го мотивація виглядала переважно ідеологічною, то після березня 2024-го, вона перенаправлена на пошук фінансових стимулів. [4]

2.4. Що не вписується в ідеологічну мотивацію угруповання

1. Непослідовна вибірковість цілей, яка корелює з геополітикою Кремля і водночас з геополітичними суперниками Ірана(який є союзником РФ), а не зі станом мусульманських спільнот у світі;
2. Поява прайс-листа на послуги, який не має жодного стосунку до релігійного наративу;
3. Готовність атакувати об'єкти, що напряду шкодять цивільному населенню (лікарня, служба екстреного оповіщення в Ізраїлі) — поведінка, яка погано узгоджується з образом борців за справедливість, але добре узгоджується з логікою найманця.[14]
4. В якості цілі виступили як Reddit так і PayPal, які не мають жодного стосунку, до антимусульманської діяльності.



3. Хронологія діяльності

Дата	Подія
18 січня 2023	Створення Telegram-каналу "Anonymous Sudan"; [6]
23 січня 2023	Початок DDoS-атак на шведські та нідерландські цілі під приводом протесту проти спалення Корану. [2]
19 лютого 2023	Публічне афілювання з Killnet — репост скріншотів у каналі Killnet. [7]
Березень 2023	Атаки на Австралію, Німеччину, Нідерланди; Trustwave починає моніторинг. [3]
14 червня 2023	Спільна з Killnet і REvil заява про "Darknet parliament" і кампанію проти банківської системи США та ЄС [4]
Червень 2023	Масштабна DDoS-кампанія Storm-1359 проти сервісів Microsoft; Microsoft офіційно пов'язала активність із Storm-1359. Anonymous Sudan вимагала \$1 млн за припинення атак. [5]
Липень 2023	Атака на PayPal. [8]
Жовтень 2023	Після 7 жовтня — удар по ізраїльській системі оповіщення "червона тривога" та по The Jerusalem Post у рамках кампанії #OpIsrael. [13]
Листопад-грудень 2023	Атаки на OpenAI/ChatGPT. [8]
Березень 2024	ФБР за судовим ордером вилучає й виводить з ладу ключові компоненти інструмента DCAT (він же Godzilla / Skynet / InfraShutdown); фактичне припинення активності групи, хоча про це не повідомляли публічно ще півроку. [10]
16 жовтня 2024	Мін'юст США розкриває обвинувальний висновок проти Ахмеда та Алаа Омерів. [9]

4. Організаційна структура та зовнішні зв'язки

4.1. Загальна структура

Ядро операції — це двоє братів із чітким розподілом ролей, плюс щонайменше троє неназваних співучасників, які фігурують анонімно. Інфраструктурний слід підтверджує тезу про серйозне фінансування. Ще в лютому 2023-го Trueesec виявив кластер щонайменше із 61 платного сервера, орендованого в IBM/Softlayer у Німеччині, з трафіком, що додатково маршрутизувався через відкриті проксі для маскуваня джерела. CyberCX пізніше оцінив географічний розкид опорної інфраструктури групи як 1720 автономних систем у 132 країнах — масштаб, який жодна маленька команда не може собі дозволити без стороннього фінансування. Інфраструктура такого рівня потребує великих фінансів, хоч і питання "чиї це гроші" залишається відкритим навіть після висунення звинувачень конкретним фізичним особам. [1]

4.2. Лідери угруповання

Ахмед Салах Юсіф Омер (Ahmed Salah Yousif Omer) Громадянство — Судан, на момент висунення звинувачень 22 роки. Псевдоніми: WilfordCEO, Zac, Soldi01. За версією прокурорів, саме він виконував "публічну" функцію: запускав атаки, вів комунікацію в Telegram, домовлявся з клієнтами про ціну й оплату DDoS-послуг. Саме йому висунуто додаткові три пункти про пошкодження захищених комп'ютерів. Максимальне покарання за сукупністю звинувачень — довічне ув'язнення, це пов'язують з атакою на ізраїльську систему екстреного оповіщення 7 жовтня 2023 року, кваліфікуючі її як спробу, що могла призвести до загибелі людей. [12]

Алаа Салах Юсуф Омер (Alaa Salah Yusuuf Omer) Громадянство — Судан, 27 років. Технічний розробник: писав програмний код, зокрема архітектуру WebSocket API (WSAPI), яку Ахмед використовував для координації серверів атаки. У коментарях до вихідного коду він, за даними слідства, залишив власне ім'я та обліковий запис @alaaelrefaie — недбалість, яка, вочевидь, суттєво полегшила слідству атрибуцію. Максимальне покарання для нього — до п'яти років, що суттєво менше, ніж для брата, і відображає різницю в ролях: розробник інструмента проти оператора, що безпосередньо монетизував і застосовував цей інструмент проти живих цілей. [11]

Статус підозрюваних після операції березня 2024 року залишався окремим питанням від вилучення інфраструктури. У березні 2024 року американські правоохоронці за судовими ордерами вилучили та вивели з ладу ключові компоненти DCAT, однак про висунення обвинувачень Ахмеду та Алаа Омеру публічно було оголошено лише 16 жовтня 2024 року. DOJ не повідомляв у пресрелізі про затримання братів у березні 2024 року. [10]

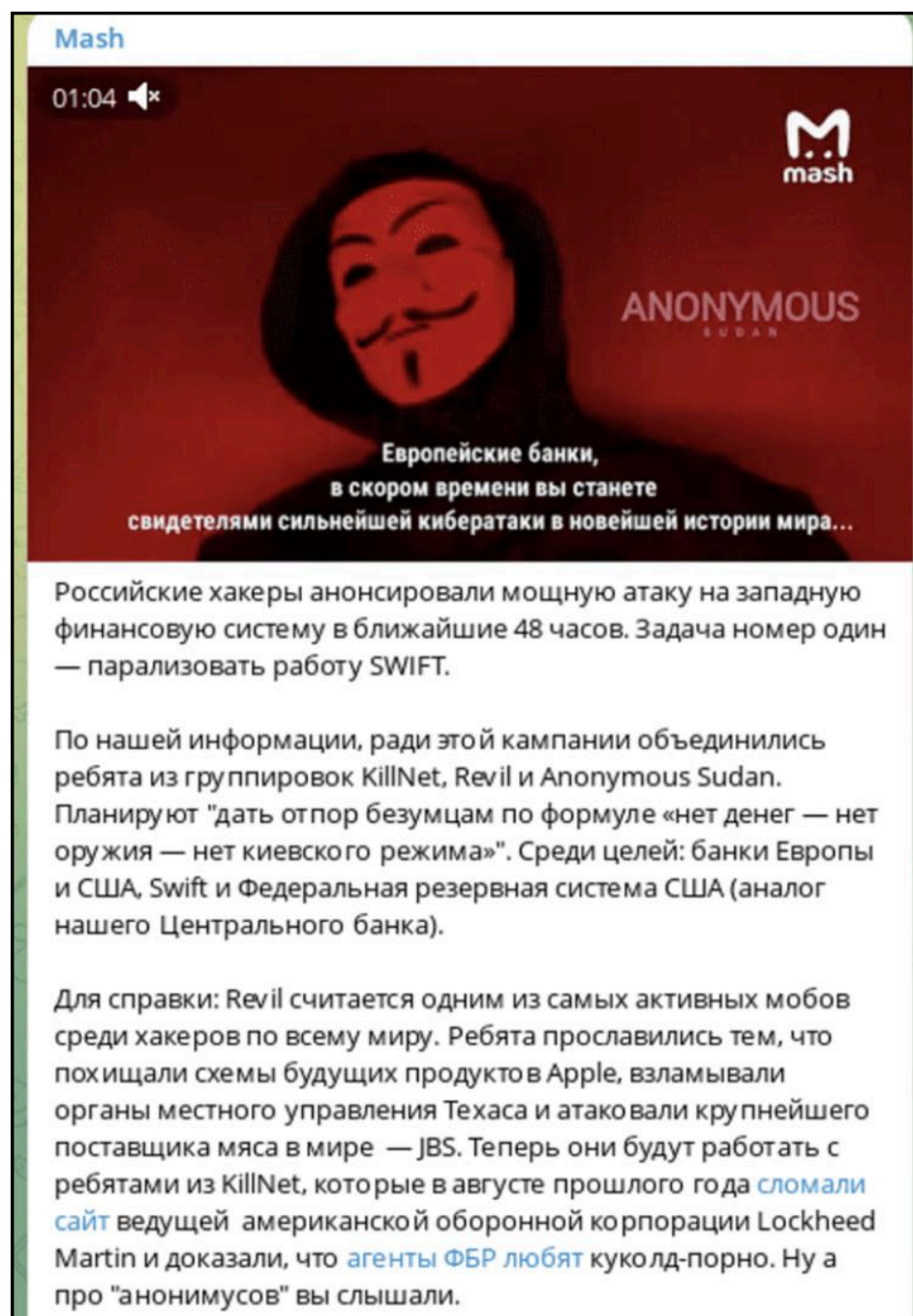
4.3 Зв'язок з killnet та REvil

Найбільш документованим зовнішнім зв'язком Anonymous Sudan є її взаємодія з KillNet. Вона проявилася практично від початку діяльності угруповання. Mandiant включив Anonymous Sudan до переліку KillNet-associated channels і станом на липень 2023 року оцінював її як активного афіліата KillNet [17]. За перше півріччя 2023 року Anonymous Sudan, за підрахунками Mandiant, відповідала за 63% усіх ідентифікованих DDoS-атак, заявлених KillNet та пов'язаними з ним групами.



Зв'язок із REvil має інший характер і значно краще підтверджується для конкретного періоду, ніж як постійна організаційна взаємодія. 14 червня 2023 року KillNet, Anonymous Sudan та угруповання, яке представляло себе як відроджений REvil, оголосили про спільну кампанію проти західної фінансової системи, заявленими цілями були європейські та американські банки та мережа SWIFT. Учасники пов'язували кампанію з припиненням західної військової підтримки України.

Повідомлення про об'єднання було поширене через Telegram-канали KillNet та Anonymous Sudan, а також російське медіа Mash.



Компанія проти SWIFT є найкращим прикладом того, що Anonymous Sudan могла діяти в рамках ширшої коаліції проросійських хактивістських акторів. При цьому сама афіліація з KillNet не є достатнім доказом прямого контролю або фінансування з боку російських державних структур. Зв'язок Anonymous Sudan з KillNet доцільніше розглядати як сильний індикатор її включеності до проросійського хактивістського середовища і операційну взаємодію, а не як доказ державного і операційного контролю над угрупованням.

5. Тактики, техніки та методи атак

5.1. Інфраструктурна модель

Однією з характерних особливостей Anonymous Sudan було використання орендованої серверної та хмарної інфраструктури у поєднанні з відкритими проксі. У лютому 2023 року Truesec та партнери виявили кластер із щонайменше 61 платного сервера IBM/SoftLayer у Німеччині, який використовувався в інфраструктурі атак. Microsoft пізніше описувала Storm-1359 як актора, що використовував VPS, орендовану хмарну інфраструктуру, відкриті проксі та DDoS-інструменти. [1]

За матеріалами американського слідства, інструмент Skynet, який використовувала Anonymous Sudan, фактично являв собою Distributed Cloud Attack Tool (DCAT), що складався з сервера командування та управління, набору хмарних серверів і масиву відкритих проксі, через які передавався DDoS-трафік до цілі. Така архітектура дозволяла розподіляти джерела трафіку та ускладнювала блокування атаки виключно за окремими IP-адресами. [11]

Використання платної і масштабованої інфраструктури свідчить про наявність у групи постійного доступу до фінансових ресурсів, необхідних для підтримання операцій, але встановити джерело фінансування не вдалось.

5.2. Орієнтовний операційний цикл

1. Ціллю обирається здебільшого країна чи організація, яку можна прив'язати або до "антимусульманського" наративу, або до підтримки України чи Ізраїлю.
2. Публічна заява-погроза в Telegram-каналі, часто із супровідною політичною риторикою.
3. Запуск L7-атаки (рівень застосунку) через власний інструмент DCAT — фірмову розробку групи, що продавалась і третім особам як DDoS-сервіс. [10]
4. Публікація доказів, наприклад, скриншоти сервісів на кшталт check-host.net, які самі по собі не є надійним підтвердженням реального збою, але добре працюють як медійний контент.
5. За наявності комерційного інтересу, вимога викупу за припинення атаки чи нерозповсюдження викрадених даних (від 3500 доларів до 3 мільйонів у випадку Scandinavian Airlines; окремо — пропозиція пакету відключення інтернет-провайдера в обраній країні за 500 доларів на годину). [14]
6. Перехід до наступної цілі, часто без паузи. Саме ця здатність вести кілька паралельних кампаній і різко перемикатися між цілями і створювала Microsoft та іншим жертвам враження набагато масштабнішого супротивника, ніж команда з двох-п'яти людей.

5.3. Технічний репертуар (за даними Microsoft)

Microsoft, що відстежувала групу під ідентифікатором Storm-1359, задокументувала три основні різновиди L7 DDoS, які застосовувались проти Outlook.com, OneDrive та порталу Azure [5] в червні 2023 року:

- HTTP(S) flood - мільйони розподілених по всьому світу запитів і SSL/TLS-рукописань, розрахованих на вичерпання обчислювальних ресурсів (CPU, пам'ять) на боці застосунку, а не мережевого каналу.

- Cache bypass - цілеспрямовано згенеровані URL-адреси, що змушують інфраструктуру обходити кэш CDN і направляти кожен запит напряму на оригінальний сервер, тим самим перевантажуючи саме ту ланку, яку CDN мав би захищати.
- Slowloris - атака "повільного виснаження": клієнт відкриває з'єднання, запитує ресурс і або взагалі не підтверджує завантаження, або підтверджує його вкрай повільно, змушуючи сервер тримати з'єднання відкритим і витратити на це пам'ять, поки пул доступних з'єднань не вичерпається.

5.4 Аналіз за MITRE ATT&CK

Техніка	Назва	Підтехніка / коментар
T1498	Network Denial of Service	T1498.001 (Direct Network Flood), T1498.002 (Reflection Amplification) — насичення каналу об'ємним трафіком
T1499	Endpoint Denial of Service	T1499.002 (Service Exhaustion Flood) — вичерпання ресурсів застосунку без обов'язкового насичення каналу; сюди ж відносяться Slowloris та Cache bypass
T1583.003	Acquire Infrastructure: Virtual Private Server	Оренда VPS та хмарних потужностей для проведення атак
T1090	Proxy	Використання відкритих проксі для маскуванню джерела трафіку
T1657	Financial Theft	DDoS-вимагання та продаж атак як послуги (застосовно радше до бізнес-моделі, ніж до окремої техніки)

5.5. Монетизація як частина тактики

З часом бізнес-модель угруповання набула такого ж тактичного значення, як і власне технічні прийоми атак. Серед публічно задокументованих фінансових вимог фігурують вимога \$1 млн за припинення атак на Microsoft, а також інші суми, пов'язані з комерційним використанням DDoS-інфраструктури. Наявність прайс-листа та продаж DDoS-послуг є аргументом на користь існування комерційної моделі, але не є доказом відсутності державного фінансування. Теоретично комерційна діяльність, самофінансування та зовнішня підтримка можуть існувати паралельно.

У березні 2024 року ФБР та прокуратура округу реалізували ордер на вилучення ключових елементів цієї інфраструктури — серверів управління й запуску атак, серверів-ретрансляторів команд та облікових записів із вихідним кодом DDoS-інструментів. Замість протидії трафіку на боці жертв, яку угруповання навчилося обходити, правоохоронні органи усунули саме той інфраструктурний шар, відновлення якого вимагає значних часових і фінансових ресурсів. [10]

6. Технічна спроможність: заявлений образ та підтверджені можливості

6.1. Заявлений образ

Заявлений образ Anonymous Sudan як технологічно просунутої групи, здатної на рівних конкурувати з державними кібер підрозділами, не повністю відповідає тому, що можна реконструювати з відкритих джерел. Водночас група продемонструвала високу практичну ефективність: за приблизно рік її діяльності атакам піддавалися сервіси Microsoft Azure, Outlook, ChatGPT, X та PayPal. CrowdStrike окремо відзначав масштаб отриманого результату у співвідношенні до кількості учасників групи, яку за найбільш обґрунтованими оцінками можна визначити у межах двох-п'яти осіб. [8]

Водночас є підстави говорити про наявність у групи власної технічної компетенції, а не лише здатності використовувати готові сервіси. Зокрема, Anonymous Sudan розробила власний DDoS-інструмент DCAT, також відомий як Godzilla, Skynet або InfraShutdown. За даними обвинувального висновку, код цього інструмента безпосередньо розробляв Алаа Салах. Це свідчить про наявність принаймні окремих учасників із достатніми навичками для створення спеціалізованого програмного забезпечення.

6.2. Підтверджені можливості

Однак технічна складність самих атак не дає підстав оцінювати групу як висококваліфікованого кібероператора. Trustwave ще у 2023 році оцінював рівень її технічної майстерності як низький або середній. Основні тактики Anonymous Sudan значною мірою збігалися з підходами Killnet і передбачали використання масованих L7-атак, зокрема HTTP-флуду, обходу кешування та Slowloris. Такі атаки не потребують експлуатації zero-day вразливостей, складного проникнення в інфраструктуру жертви чи тривалого перебування всередині її мережі.

Ключовою перевагою Anonymous Sudan була не унікальність використовуваних методів, а можливість забезпечити їх масштабування. За наявними оцінками, група використовувала понад 61 сервер у комерційних дата-центрах і мережу проксі, розподілену щонайменше у 132 країнах. Така інфраструктура суттєво збільшує потужність навіть відносно простих L7-атак. Відповідно, здатність завдати перебоїв роботі Microsoft чи інших великих технологічних компаній сама по собі не свідчить про наявність у нападників технологій рівня державних кібер підрозділів. [15]

Таким чином, Anonymous Sudan доцільніше розглядати як невелику, але добре організовану та ресурсно забезпечену групу, здатну ефективно масштабувати відносно нескладні DDoS-операції. Її основною перевагою були доступ до значної інфраструктури, фінансування та здатність концентрувати ресурси на окремих цілях. Це важливо і для оцінки вразливостей групи: її спроможність значною мірою залежить від доступу до серверів, проксі та інших інфраструктурних ресурсів. Саме фінансові та інфраструктурні зв'язки, а не пошук складніших технічних вразливостей, тому становлять один із найбільш перспективних напрямів для протидії такому оператору.

7. Обмеження та вразливі місця

- Залежність від невеликої кількості людей. Уся операція, трималася буквально на двох братах плюс кількох неназваних співучасниках. Арешт двох ключових фігур у березні 2024-го фактично зупинив активність групи — це нетипово стійка структура для угруповання, яке нібито мало державну підтримку; державні кібер підрозділи зазвичай витримують затримання окремих операторів без повної зупинки діяльності.
- Централізована й дорога інфраструктура. Ставка на орендовані комерційні сервери замість розподіленого ботнета — це палиця на два кінці: вона дає стабільність і потужність, але створює єдину точку відмови. Коли ФБР вилучило ключові сервери й облікові записи з вихідним кодом у березні 2024-го, у групи, судячи з усього, не знайшлося швидкого способу відновити операції. [10]
- Внутрішня суперечність наративу. Погано прихована мотивація з вибіркоким ігноруванням реальних випадків утисків мусульман поза західним контекстом і практично стовідсотковий збіг цілей із геополітичною картою. Репутаційно, заявлена ідеологія групи є вразливою для будь-якого уважного аналітичного розслідування.

Висновок

Якщо простежити траєкторію від січня 2023-го до березня 2024-го, вимальовується доволі послідовна дуга: релігійно-хактивістський дебют, прив'язка до проросійського інформаційного кластера, нарощування власної технічної та інфраструктурної бази, комерціалізація, удар по інфраструктурі та ключових операторах, затишшя, яке за часом ідеально збігається з моментом арешту братів, хоча про сам арешт публічно не повідомляли ще півроку.

Це не траєкторія типової державної кібер підрозділу (який після провалу одного проекту зазвичай перезапускається під новою вивіскою чи просто продовжує роботу з новими виконавцями), і не траєкторія суто ідеологічного руху (який рідко настільки послідовно рухається в бік прайс-листа й вимагання). Вони спробували знайти нішу, в якій можна резонувати з певною аудиторією, відкрити доступ до партнерств, відпрацювати технологію на гучних цілях заради розголосу, а потім монетизувати напрацьовану впізнаваність і інфраструктуру напямую.

Логіка бізнес-моделі підказує: у бік дедалі відвертішого DDoS-за-наймом сервісу з дедалі тоншим ідеологічним прикриттям, за аналогією з тим, як і сам Killnet із часом усе відвертіше поведився як група кіберманманців, а не ідейних "патріотів".

8. Оцінка значення та рівня загрози

За рік активності Anonymous Sudan продемонструвала, що невелика за чисельністю група може створювати значний ефект без використання технологій рівня державних кібер підрозділів. Її спроможність ґрунтувалася передусім на поєднанні доступу до платної серверної та проксі-інфраструктури, можливості масштабувати DDoS-атаки та активного використання публічності для посилення ефекту операцій. Серед підтверджених цілей були великі технологічні компанії, державні установи США, фінансові та медичні організації, а також об'єкти транспортної інфраструктури. Американське слідство оцінило сукупну шкоду від атак щонайменше у понад 10 млн доларів. Ця оцінка відображає документовані економічні збитки й не охоплює потенційні непрямі витрати, зокрема репутаційні наслідки або витрати на додаткові заходи захисту. [16]

Окреме значення має геополітичний контекст діяльності групи. На початковому етапі Anonymous Sudan послідовно використовувала релігійну та антизахідну риторику для обґрунтування вибору цілей. Водночас, подальша географія та характер атак демонстрували помітний збіг із ширшим антизахідним і проросійським хактивістським середовищем, а група публічно взаємодіяла з Killnet. Це не є достатньою підставою для висновку про прямий контроль з боку російських державних структур, однак дозволяє розглядати Anonymous Sudan як актора, діяльність якого перетинається з цілями російських угруповань. [4]

Висновок

Таким чином, Anonymous Sudan доцільніше характеризувати не як високотехнологічного кібер оператора, здатного конкурувати з державними структурами на рівні технічної складності, а як невелику та організовану групу, яка ефективно масштабувала відносно доступні DDoS-технології. Її сила полягала у поєднанні інфраструктури, фінансових ресурсів, організаційної координації та медійного ефекту. Саме це поєднання дозволило перетворити технічно відносно простий інструмент на операційно значущий засіб тиску.

Водночас комерціалізація DDoS-інфраструктури та вимагання коштів показують, що діяльність Anonymous Sudan не можна пояснювати виключно політичною чи релігійною мотивацією. У її операціях одночасно простежуються хактивістський наратив, геополітичний контекст і фінансовий інтерес. Саме поєднання цих компонентів, а не якась одна ідеологічна мотивація, найкраще пояснює модель діяльності групи.

9. Рекомендації щодо протидії

- L7-захист на рівні застосунку. Увімкнення й тонке налаштування сервісів на кшталт Azure WAF або аналогів, з окремими правилами під сигнатури HTTP-флуду; налаштування захисту від ботів і обмеження швидкості запитів (rate limiting) на рівні окремих ендпоінтів, а не лише всього домену.
- Географічна й інфраструктурна фільтрація. Оскільки атакуюча інфраструктура групи історично концентрувалася на кількох комерційних хостинг-провайдерах і відкритих проксі, варто відстежувати й за потреби тимчасово обмежувати трафік з відомих діапазонів, які раніше фігурували в звітах Truesec, CyberCX і Microsoft, без повного покладання на геоблокування за країною.
- Моніторинг і рання ідентифікація сплесків. Автоматичні алерти на аномальні сплески трафіку до того, як вони переростають у повноцінний збій сервісу.
- Резервування каналів і географічно розподілена архітектура для критичних сервісів, особливо в секторах, які вже потрапляли в поле зору угруповання: охорона здоров'я, державні реєстри, фінансові сервіси.
- Протокол реагування на вимагання. Не вести переговори і не платити викуп (це підтверджує робочість бізнес-моделі та фінансує подальші атаки), але ретельно документувати всі вимоги й комунікацію для подальшої передачі правоохоронцям — саме такі деталі лягли в основу обвинувального висновку 2024 року.

Список джерел

1. <https://www.truesec.com/hub/report/anonymous-sudan-threat-intelligence-report>
2. <https://www.truesec.com/hub/blog/hacktivists-target-denmark-in-simultaneous-attacks>
3. <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/>
4. <https://www.avertium.com/resources/threat-reports/an-update-on-pro-russia-threat-actor-killnet>
5. <https://www.microsoft.com/en-us/msrc/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks>
6. <https://thecyberwire.com/stories/19e7d683bdd34891b42158c8c6d3a52e/anonymous-sudans-questionable-provenance>
7. <https://cyberscoop.com/anonymous-sudan-killnet-russia-onlyfans/>
8. <https://www.crowdstrike.com/en-us/blog/anonymous-sudan-hacktivist-group-ddos-indictment/>
9. <https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals>
10. <https://krebsonsecurity.com/2024/10/sudanese-brothers-arrested-in-anonsudan-takedown/>
11. <https://flashpoint.io/blog/usa-vs-ahmed-salah-yousif-omer-alaa-salah-yusuuf-omer/>
12. <https://sudantribune.com/article292154/>
13. <https://www.jpost.com/international/article-825144>
14. <https://www.cbsnews.com/news/2-sudanese-nationals-charged-cyber-attack-for-hire-gang/>
15. <https://www.securityweek.com/anonymous-sudan-ddos-service-disrupted-members-charged-by-us/>
16. <https://therecord.media/anonymous-sudan-brothers-charged-ddos-attacks-hospital-critical-infrastructure>
17. <https://cloud.google.com/blog/topics/threat-intelligence/killnet-new-capabilities-older-tactics>