Аннотация – В этом документе представлен анализ группы Anonymous Sudan и различным аспектам деятельности группы, включая их происхождение, мотивацию, методы и последствия их действий.

Выводы, полученные в результате этого анализа, полезны экспертам по кибербезопасности, ИТ-специалистам и правоохранительным органам. Понимание методов работы Anonymous Sudan дает этим заинтересованным сторонам знания, позволяющие предвидеть потенциальные атаки, укреплять свою защиту и разрабатывать эффективные контрмеры против аналогичных хакерских угроз.

I. Особенности группы и мотивация

Anonymous Sudan – хактивистская группа, получившая известность благодаря серии распределённых атак типа "отказ в обслуживании" (DDoS) на различные глобальные цели. Группа представляет собой уникальное сочетание политических и религиозных мотиваций, используя цифровые инструменты для продвижения своих целей и создания сбоев. Они нацелены на организации, связанные с инфраструктурой и ключевыми услугами, в том числе в государственном и частном секторах.

Группа работает с января 2023 года, с тех пор постоянно попадая в заголовки газет по всему миру, отдавая предпочтение таким странам как Швеции, Нидерландам и Дании. Они также нацелились на такие страны, как Израиль, ОАЭ, Франция и Австралия. Что касается недавних действий – атака на телекоммуникационного провайдера Sudachad и ChatGPT из-за поддержки сотрудником OpenAI Израиля

Однако до сих пор ведутся серьёзные споры об истинном происхождении и принадлежности к Anonymous Sudan, а использование русского языка в сообщениях, что с точки зрения всех западных стран однозначно говорит об истинном происхождение (или скорее умственном развитии).

Группа набирает членов через онлайн-платформы, используя влияние других групп, предлагая финансовые стимулы и внедряя процесс предварительного отбора для обеспечения определённого уровня квалификации среди новобранцев в отличие от более широкого коллектива Anonymous, который известен тем, что приветствует любого независимо от уровня квалификации. Эти методы помогают группе поддерживать операционную безопасность и эффективность. Группа часто набирает новых участников через онлайн-платформы, хакерские форумы и каналы социальных сетей, Telegram. Эти платформы позволяют им охватить широкую аудиторию, интересующихся кибербезопасностью, хакерством и активизмом.

Anonymous Sudan утверждает, что её мотивами являются как политические, так и религиозные убеждения. Например, они ссылались на геополитические события, которые они воспринимают как антимусульманские, в качестве катализатора своих действий. Атаки на шведские и датские организации и объекты критической инфраструктуры были в ответ на сожжение копии Корана в Швеции.

II. Тактика

Группа в основном использует DDoS-атаки, используя комбинацию веб-DDoS-атак и чередующихся потоков UDP / SYN для нарушения работы сервисов. Они также компрометируют учётные записи электронной почты. Группа часто доводит дело до конца, атакуя цели, которым они публично угрожают, и пагубное воздействие этих атак часто демонстрируется с использованием инструментов достижимости. Они также часто ретроспективно берут на себя ответственность за несвязанные перебои в обслуживании.

Группа использует стандартные услуги DDoS-атак по найму и аренду ботнетов, отходя от традиционного менталитета и возможностей и ведя себя скорее как APT-группа. Они используют инфраструктуру общедоступных облачных серверов для генерации трафика и проведения атак. Атаки группы происходят с десятков тысяч уникальных IP-адресов источников, при этом трафик UDP достигает 100 Гбит /с.

Перед началом атаки группа часто заранее угрожает целям. Обычно это делается с помощью публичных постов в социальных сетях или других онлайн-платформах, где они объявляют о своих намерениях и причинах своих действий. Такой подход не только служит предупреждением для намеченной цели, но и помогает привлечь внимание к делу и действиям группы.

Группа использует разные подходы к DDoS-атакам:

- **Атаки с высокой пропускной способностью**: отправляются большие сетевые пакеты / большие объёмы сетевого трафика для увеличения числа TCP-атак; максимальная наблюдаемая пропускная способность атаки составила 284 Гбит / с и 57 Mpps

- **Флуд-атаки**: комбинация различных UDP, DNS, SSDP SYN-атак для «подавления» цели.
- **Веб-DDoS-атаки**: нарушают работу веб-сервисов, перегружая цель потоком интернет-трафика.
- **Инфраструктура серверов публичного облака**: облачные сервисы для формирования трафика и потоков атак, что обеспечивает анонимность и затрудняет точное определение источника атак.

III. Целевой профиль

Операционные схемы группы и секторы, на которые они нацелены, предполагают стратегический подход к их хактивизму, направленный на то, чтобы вызвать сбои и привлечь внимание к их причинам. Вот несколько ключевых моментов, характеризующих жертв.

Период активности – группа была наиболее активна в феврале и апреле, и за эти месяцы произошло значительное количество атак.

Целевые страны и секторы

- Наиболее упоминаемые страны: Швеция, Израиль, США, Нидерланды, Дания, Австралия, Франция, Германия, ОАЭ, Иран
- Израиль был главной мишенью, более 70 нападений, на долю которых приходится более 20% от общего числа жертв, особенно во время кампании " OpIsrael"
- Скандинавские компании, включая Scandinavian Airlines (SAS), подверглись атаки после антиисламской акции протеста сожжения Корана
- К числу важнейших целевых секторов относятся финансы, авиация, здравоохранение и государственные организации

Публичность и вовлечение сообщества

Группа жаждет публичности и общественного признания, активно взаимодействуя со своей аудиторией и привлекая подписчиков к целевому отбору

A. Пострадавшие компании

В число крупнейших пострадавших компаний входят:

- Технологический гигант Microsoft
- Авиакомпания Air France
- Система онлайн-платежей PayPal
- Корпорация финансовых услуг American Express:
- Компания Cloudflare, занимающаяся веб-инфраструктурой и безопасностью веб-сайтов, подверглась DDoS-атаке, в результате которой её веб-сайт был отключён на несколько минут
- Государственная дубайская авиакомпания Flydubai:
- Информационное агентство Associated Press (AP)

B. Отрасли

- **Транспорт**: системы бронирования, базы данных клиентов и другие сетевые системы.
- **Госсектор**: общедоступные веб-сайты, системы электронной почты и другая сетевая инфраструктура.
- **Образование**: информационные системы для учащихся, платформы онлайн-обучения и системы электронной почты.
- **Здравоохранение**: системы электронной медицинской документации, системы записи на приём и другие сетевые медицинские устройства.
- **Финансы**: системы онлайн-банкинга, базы данных клиентов и системы электронной почты.
- **Производство**: системы промышленного контроля, системы управления цепочками поставок и другие сетевые системы.
- **Технология**: общедоступные веб-сайты, базы данных клиентов и облачные сервисы.

C. Последствия

- **Нарушение работы сервисов**: Основным методом атаки группы является DDoS, который может нарушить работу сервисов в различных секторах, включая финансы, авиацию, здравоохранение и государственные структуры. Это может привести к значительным перебоям в обслуживании, затрагивающим как предприятия, так и потребителей
- **Экономический эффект**: Затраты на смягчение последствий DDoS-атак могут быть значительными. Сюда входят затраты на дополнительную полосу пропускания, аппаратное и программное обеспечение для предотвращения атак, а также потенциальная потеря доходов из-за перебоев в обслуживании
- **Общественное восприятие и доверие**: огласка, вызванная этими атаками, может повлиять на общественное восприятие и доверие к объектам, которым они подвергаются, и на способность страны защищаться от кибер-угроз
- **Распределение ресурсов**: реагирование на эти атаки и смягчение их последствий требует значительных ресурсов, что может отвлечь ресурсы от других критически важных областей
- **Потенциал эскалации**: риск того, что со временем группа может ужесточить свою тактику, потенциально перейдя от DDoS-атак к более разрушительным формам кибератак
- **Политическое воздействие**: Нападения группы часто носят политический характер, что может усугубить существующую напряжённость и конфликты

D. Последствия [Транспортная отрасль]

- **Перебои в обслуживании**: Атаки могут привести к нарушению работы критически важных служб, таких как выполнение рейсов, продажа билетов и обслуживание клиентов, что доставит неудобства пассажирам и может вызвать проблемы с безопасностью.
- **Экономические потери**: Авиакомпании и другие транспортные организации могут понести

экономические потери из-за простоев в обслуживании, затрат на смягчение последствий атак и потенциальной компенсации пострадавшим клиентам.

- **Репутационный ущерб**: Повторяющиеся атаки могут нанести ущерб репутации компаний-мишеней, что приведёт к потере доверия клиентов и потенциально повлияет на будущий бизнес.
- **Оперативная нагрузка**: Реагирование на DDoS-атаки и восстановление после них может привести к перегрузке операционных возможностей целевых объектов, требуя значительных ресурсов и потенциально отвлекая внимание от других важных задач

E. Последствия [Государственная промышленность]

- **Нарушение работы государственных служб**: правительственные веб-сайты и онлайн-сервисы могут быть переведены в автономный режим, что повлияет на доступ граждан к важной информации и услугам
- **Экономические издержки**: Финансовые последствия включают затраты на устранение последствий атак и потенциальную потерю производительности из-за простоя службы
- **Подрыв общественного доверия**: повторяющиеся атаки могут подорвать доверие общественности к способности правительства обеспечить безопасность своей цифровой инфраструктуры
- **Нагрузка на ресурсы**: Государственным учреждениям, возможно, потребуется выделить значительные ресурсы для реагирования на эти атаки и восстановления после них, которые в противном случае могли бы быть использованы для оказания государственных услуг.
- **Последствия для безопасности**: если правительственные сети будут восприниматься как уязвимые, это может подтолкнуть других злоумышленников к дальнейшим атакам

F. Последствия [Индустрияобразования]

- **Нарушение работы образовательных служб**: DDoS-атаки могут нарушить доступность образовательных онлайн-ресурсов, включая веб-сайты, системы управления обучением и виртуальные классы. Это может затруднить доступ учащихся к образованию и повлиять на их успеваемость.
- **Экономические издержки**: Финансовые последствия включают затраты на устранение последствий атак и потенциальную потерю производительности из-за простоя службы.
- **Подрыв общественного доверия**: повторяющиеся атаки могут подорвать доверие персонала, семей и студентов к способности учреждения обеспечить безопасность своей цифровой инфраструктуры.
- **Нагрузка на ресурсы**: образовательным учреждениям, возможно, потребуется выделить значительные ресурсы для реагирования на эти атаки и восстановления после них.
- **Последствия для безопасности**: если образовательные сети будут восприниматься как уязвимые, это может подтолкнуть других злоумышленников к дальнейшим атакам.

G. Последствия [Индустрияздравоохранения]

- **Нарушение работы критически важных служб**: DDoS-атаки могут нарушить доступность основных медицинских услуг, таких как электронные медицинские карты, телемедицина и онлайн-порталы для пациентов. Это может затруднить оказание медицинской помощи пациентам и повлиять на важнейшие медицинские операции
- **Нарушение безопасности пациентов**: если системы здравоохранения нарушены, безопасность пациентов может быть поставлена под угрозу, поскольку доступ к медицинской информации и своевременная помощь пациентам имеют решающее значение
- **Экономические издержки**: Учреждения здравоохранения могут столкнуться со значительными расходами, связанными со смягчением последствий атак, восстановлением услуг и потенциальной юридической ответственностью, если данные пациента будут скомпрометированы
- **Потеря конфиденциальности**: Кибератаки могут привести к раскрытию конфиденциальной информации о пациентах, что приведёт к нарушению конфиденциальности и потенциальной краже личных данных или мошенничеству
- **Ущерб репутации**: Повторяющиеся атаки могут нанести ущерб репутации медицинских работников, что приведёт к потере доверия среди пациентов и общественности
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекая внимание от ухода за пациентами и других важных услуг

H. Последствия [Финансовая отрасль]

- **Нарушение работы финансовых служб**: Атаки могут нарушить доступность онлайн-банкинга, обработки платежей и других финансовых услуг, затрагивая как предприятия, так и потребителей
- **Экономические издержки**: Финансовые учреждения могут столкнуться со значительными расходами, связанными со смягчением последствий атак, восстановлением услуг и

потенциальной юридической ответственностью, если данные клиентов будут скомпрометированы
- **Потеря доверия клиентов**: повторяющиеся атаки могут нанести ущерб репутации финансовых учреждений, что приведёт к потере доверия среди клиентов и потенциально повлияет на будущий бизнес
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекая внимание от других важных служб
- **Последствия для безопасности**: DDoS-атаки могут служить прикрытием для более разрушительной кибер-деятельности, такой как проникновение в системы и утечка данных, создавая дополнительную нагрузку на и без того ограниченные ресурсы

I. *Последствия [Обрабатывающая промышленность]*

- **Нарушение работы**: DDoS-атаки могут нарушить доступность основных производственных служб, таких как системы производственного контроля, управление цепочками поставок и порталы обслуживания клиентов
- **Экономические издержки**: Производственные предприятия могут столкнуться со значительными расходами, связанными с устранением последствий атак, восстановлением служб и потенциальной потерей производительности из-за простоя служб
- **Потеря интеллектуальной собственности**: Многие атаки в производственном секторе включают кражу интеллектуальной собственности, которая может привести к потере доли рынка или прекращению производственной деятельности
- **Ущерб репутации**: Повторяющиеся атаки могут нанести ущерб репутации компаний-производителей, что приведёт к потере доверия среди клиентов и потенциально повлияет на будущий бизнес
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекающих внимание от производства и других важных услуг

J. *Последствия [Технологическая отрасль]*

- **Нарушение работы сервисов**: DDoS-атаки могут привести к отключению веб-сайтов и онлайн-сервисов, что повлияет на доступность цифровых продуктов и услуг
- **Экономические издержки**: Компании могут столкнуться со значительными расходами, связанными с устранением последствий атак, восстановлением служб и потенциальной потерей доходов из-за простоя служб
- **Ущерб репутации**: Повторяющиеся атаки могут нанести ущерб репутации технологических компаний, что приведёт к потере доверия среди клиентов и потенциально повлияет на будущий бизнес
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекая внимание от инноваций и других важных услуг
- **Последствия для безопасности**: DDoS-атаки могут служить прикрытием для более разрушительной кибер-деятельности, такой как проникновение в системы и вывоз данных