I. Введение

KillNet – кибер-группа, которая стала лидером среди более чем сотни подобных групп, возникших в результате прокси-кибервойн. Основные стратегии KillNet вращаются вокруг проведения низкоуровневых распределённых атак типа "Отказ в обслуживании" (DDoS) против критической инфраструктуры, государственных служб, веб-сайтов аэропортов и медиапредприятий в странах НАТО.

KillNet также известен своими активными и конфронтационными усилиями по дезинформации, нацеленными на 90 000 подписчиков Telegram. Эти кампании включают в себя буллинг над жертвами их DDoS-атак и распространение угроз. Например, атака KillNet'а на веб-сайте Европарламента привело к его временной недоступности. В ответ на расследование, начатое против KillNet в связи с нападением на Европейский парламент, группа атаковала бельгийский центр кибербезопасности.

Группа Anonymous Sudan, очевидно, расширила возможности KillNet, и стала самым продуктивным филиалом коллектива в 2023 году, проведя большинство заявленных DDoS-атак. KillNet также заявила, что насчитывает 280 членов в США, приписывая атаку на Boeing своим американским "коллегам".

Виктимология KillNet обширна и включает в себя различные сектора и страны:

- **География (атак)**: Большинство жертв KillNet находятся в Европе; зарегистрировано более 180 атак, из них не менее 10 – в Северной Америке атак
- **Целевые отрасли**: Общие цели включают финансовую отрасль, транспорт, правительственные учреждения и бизнес-услуги
- **Сектор здравоохранения**: таргетирование отрасли здравоохранения США также вызывает опасения из-за потенциального воздействия на важнейшие службы здравоохранения
- **Государственные службы**: сообщалось об атаках на правительственные веб-сайты в нескольких странах, включая Румынию, Молдову, Латвию и Соединённые Штаты
- **Транспорт**: Аэропорты и другие транспортные системы США подверглись DDoS-атакам
- **Предприятия средств массовой информации**: также пострадали медиакомпании в странах НАТО

Со временем KillNet разработала полуофициальную организационную структуру со значительным присутствием в Telegram и начала расширять свою деятельность. Группа начала создавать глобальную команду операторов из даркнета, предлагая такие услуги, как дезинформация, воздействие на сетевую инфраструктуру, репутационные атаки, эксфильтрация данных и утечки данных, наряду с DDoS атаками. Они также разработали свои собственные инструменты и ботнеты после первоначального использования инструментов с открытым исходным кодом.

II. Тактика

Основные стратегии KillNet основаны на DDoS-атаках и bruteforce-атаках.

A. DDoS-атаки

KillNet в основном использует низкоуровневые DDoS-атаки. Группа обычно не использует сложных инструментов или стратегий, и, хотя их DDoS-атаки могут вызвать перебои в обслуживании, они обычно не приводят к серьёзному ущербу. KillNet проводит DDoS-атаки на уровень 4 модели OSI (SYN flood-атаки) и уровень 7 (массовые запросы POST/GET). Целью этих атак является истощение ресурсов путём заполнения целевой службы вредоносными запросами на подключение.

B. bruteforce-атаки

KillNet также использует bruteforce-атаки против различных сервисов. В этих атаках используются предопределённые списки слов для поиска незащищённых сервисов, которые пытаются использовать учётные данные по умолчанию или слабые учётные данные. Группа в первую очередь нацелена на такие сервисы, как FTP (порт 21), HTTP (порт 80), HTTPS (порт 443) и SSH (порт 22), а также на серверы Minecraft и TeamSpeak.

C. Цели DDoS-атак

DDoS-атаки в первую очередь были нацелены на критически важную инфраструктуру, правительственные службы и медиа-компании в странах НАТО, включая США, Канаду, Австралию, Италию. Не исключением стали и международные институты, партнёры НАТО, и страны, включая Германию, Данию, Швецию, Францию, Польшу, Словакию, Украину, Израиль, Объединённые Арабские

Эмираты (ОАЭ) и другие страны-союзники и партнёры НАТО, такие как Япония.

Группа также нацелена на организации в секторах здравоохранения, финансовой индустрии, транспортной и секторах бизнес-услуг. Отдельные цели KillNet включают военные объекты, морские терминалы и объекты материально-технического обеспечения, другие виды транспорта и системы онлайн-торговли.

Важно отметить, что, хотя DDoS-атаки KillNet могут вызывать перебои в обслуживании на несколько часов или даже дней, они обычно не наносят серьёзного ущерба. Однако они могут нарушать работу основных служб и представлять серьёзную угрозу для организаций, особенно в таких критически важных секторах, как здравоохранение.

D. Методы атак

Основным вектором атаки KillNet является DDoS, который включает в себя «заполнение» целевой службы вредоносными запросами на подключение, что приводит к истощению ресурсов. Известно также, что группа занималась извлечением данных из целевых сетей, включая почтовые ящики высокопоставленных чиновников и банковские данные.

Что касается инструментов, KillNet использовала множество методов, включая сценарии DDoS и вербовку ботнетов и использование поддельных источников атак для маскирования, а в октябре 2023 года KillNet начала продавать новый инструмент для DDoS-атак с арендой (на день, неделю, месяц). Всё это ожидаемо должно увеличить количество новых атак.

Группа использует несколько известных DDoS-инструментов, включая "Aura-DDoS", "Blood", "DDoS Ripper", "Golden Eye", "Hasoki" и "MHDDoS". Они также используют инструмент под названием "CC-Attack", который автоматизирует использование открытых прокси-серверов и включает методы рандомизации, позволяющие избежать обнаружения на основе сигнатур. Кроме того, было замечено, что KillNet использует slow-POST DDoS атаки и ICMP-флуд, атаки с IP-фрагментацией, TCP SYN flood, TCP RST flood, TCP SYN / ACK, NTP flood, DNS amplification и CLAP-атаки (LDAP connectionless).

E. Подбор персонала

Деятельность KillNet не ограничивалась кибератаками. Группа занималась вербовкой, сбором средств и продвижением своих идей по различным каналам, включая социальные сети. для расширения своей базы поддержки, ориентируясь на людей с различными наборами навыков, включая программистов, сетевых инженеров, тестировщиков на проникновение, системных администраторов и социальных инженеров. Несмотря на заявления лидера группы KillMilk об уходе из группы в середине 2022 года, он продолжает оставаться центральным координатором коллектива KillNet.

В 2023 году группа объявила о запуске своей Dark School, школы по борьбе с киберпреступностью, целью которой является обучение следующей когорты и пополнение рядов коллектива. KillNet набирает новых участников, активно подыскивая подходящих кандидатов среди сторонников своего дела, используя различные каналы социальных сетей, такие как Telegram и VK. У них есть подробная форма, которую потенциальные новобранцы должны заполнить, прежде чем их будут рассматривать для вступления. KillNet работает с военной структурой, с чёткой иерархией сверху вниз и множеством небольших отрядов, которые они называют своим "Легионом" которые действуют в соответствии с инструкциями, раздаваемыми в их Telegram-каналах.

III. Цели, воздействие и последствия атак

Последствия атак KillNet могут варьироваться от временных перебоев в обслуживании до потенциальных финансовых потерь и ущерба репутации. Правительственные меры реагирования включали классификацию KillNet как террористической организации и рассылку предупреждений через агентства кибербезопасности.

A. Индустрия здравоохранения

KillNet нацелен на сектор здравоохранения США (HPH) с декабря 2022 года. Их фирменные DDoS-атаки на критически важные секторы инфраструктуры обычно приводят к перебоям в обслуживании, длящимся несколько часов или даже дней. Эти атаки имеют серьёзные последствия, поскольку они могут прервать уход за пациентами, привести к потере данных о них и нарушить связь между поставщиками медицинских услуг. В январе 2023 года KillNet и ее филиалы провели многочисленные скоординированные DDoS-атаки на организации здравоохранения в США, что привело к перебоям в обслуживании и значительным нарушениям рутинных и важнейших повседневных операций, длящимся несколько часов или даже дней. В некоторых случаях группа также крала данные из ряда больниц. Эти атаки в первую очередь были нацелены на системы здравоохранения как многопрофильные больницы, также и одиночные в том числе с травматологическими центрами первого уровня.

Роль правоохранительных органов в противодействии атакам KillNet включает расследование инцидентов, координацию с международными правоохранительными группами и принятие мер по пресечению деятельности группы. Например, ФБР в координации с международными правоохранительными органами и Европолом ранее проникало в инфраструктуру других групп, представляющих киберугрозу.

Агентство по кибербезопасности и инфраструктурной безопасности (CISA) также играет важную роль в оказании помощи организациям в реагировании на такие атаки. CISA предоставляет ресурсы и рекомендации, помогающие организациям защищаться от киберугроз, и работает с пострадавшими организациями над смягчением последствий атак.

B. Энергетическая и финансовая промышленность

В энергетическом секторе атаки могут нарушить работу промышленных систем управления, поддерживающих энергетическую инфраструктуру США. Хотя влияние на

способность энергетического сектора предоставлять локализованные услуги пока было минимальным, угроза сохраняется. В случае успеха эти атаки потенциально могут нарушить энергоснабжение, что приведёт к перебоям в подаче электроэнергии и повлияет на критически важную инфраструктуру.

В финансовом секторе DDoS-атаки становятся все более серьёзной проблемой. Эти атаки могут вызывать периодические простои, вынуждая сотрудников службы безопасности отражать атаки, потенциально нарушая финансовые транзакции. KillNet даже пригрозил неминуемыми атаками на банковскую систему SWIFT и другие финансовые учреждения. Хотя фактическое воздействие этих угроз является неопределённым, в случае успеха они потенциально могут нарушить глобальные финансовые транзакции.

Важно отметить, что, хотя KillNet использует DDoS в качестве своего основного инструмента, этот метод обычно используется скорее для привлечения внимания, чем для нанесения серьёзного ущерба. Тем не менее, группа наращивает свои возможности и демонстрирует готовность атаковать критически важные объекты инфраструктуры. Таким образом, хотя фактический ущерб, причинённый атаками KillNet, до сих пор был минимальным, существует потенциал для более значительных сбоев.

C. Авиационная промышленность

Эти атаки в первую очередь были нацелены на общедоступные веб-сайты аэропортов, в результате чего они замедлили работу или стали полностью недоступны. Группа атаковала более 30 европейских аэропортов и несколько крупных аэропортов США, включая международный аэропорт Атланты Хартсфилд-Джексон, международный аэропорт Лос-Анджелеса, международный аэропорт Чикаго О'Хара, международный аэропорт Орландо, международный аэропорт Денвера, международный аэропорт Феникс Скай Харбор и другие.

DDoS-атаки привели к сбоям в работе веб-сайтов аэропортов, что повлияло на взаимодействие клиентов с авиакомпаниями. Однако теракты не повлияли на важнейшие операции аэропорта и не сорвали полёты. Европейское агентство по управлению воздушным движением Eurocontrol, подтвердило, что DDoS-атака KillNet затронула его веб-сайт, но не нарушила полеты и не создала какой-либо угрозы воздушному движению.

Эксперты предупреждают о возможности более серьёзных атак в будущем. Группировка продемонстрировала готовность атаковать критически важные объекты инфраструктуры и призвала другие группировки начать аналогичные атаки против гражданской инфраструктуры США, включая морские терминалы, объекты логистики, центры мониторинга погоды и системы здравоохранения. Таким образом, хотя фактический ущерб, нанесённый авиационной отрасли атаками KillNet, пока был минимальным, существует потенциал для более значительных сбоев.

Авиакомпании, пострадавшие от атак KillNet, не раскрываются. Однако атаки были нацелены на веб-сайты нескольких крупных аэропортов США, что может косвенно повлиять на авиакомпании, работающие в этих аэропортах, нарушив взаимодействие клиентов с ними.

Проводимые группой распределённые атаки типа "Отказ в обслуживании" (DDoS) были нацелены на веб-сайты нескольких крупных аэропортов США, в результате чего они замедлили работу или стали полностью недоступны. Однако эти атаки не повлияли на важнейшие операции аэропорта и не нарушили полёты.

Воздействие на авиакомпании, работающие в этих аэропортах, в первую очередь будет проявляться в виде нарушения взаимодействия с клиентами. Например, пассажиры могли испытывать трудности с доступом к информации о рейсе, бронированием или сменой рейсов, а также с онлайн-регистрацией, пока веб-сайты аэропортов не работали. Однако фактический масштаб этого сбоя не обнародован публично.

D. Другие отрасли

Помимо секторов здравоохранения и энергетики, KillNet нацелился на множество других секторов и отраслей. К ним относятся:

- Правительственные службы: в прошлом году KillNet атаковал правительственные веб-сайты в нескольких странах, включая по меньшей мере три штата в США
- Транспорт: веб-сайты аэропортов США стали жертвами DDoS-атак KillNet
- СМИ и новостные агентства: деятельность KillNet также затронула медиакомпании
- Рынки темной сети: KillNet участвовал в атаках на рынки темной сети
- Финансовый сектор: Группа угрожает финансовому сектору, включая банковскую систему SWIFT и другие финансовые учреждения