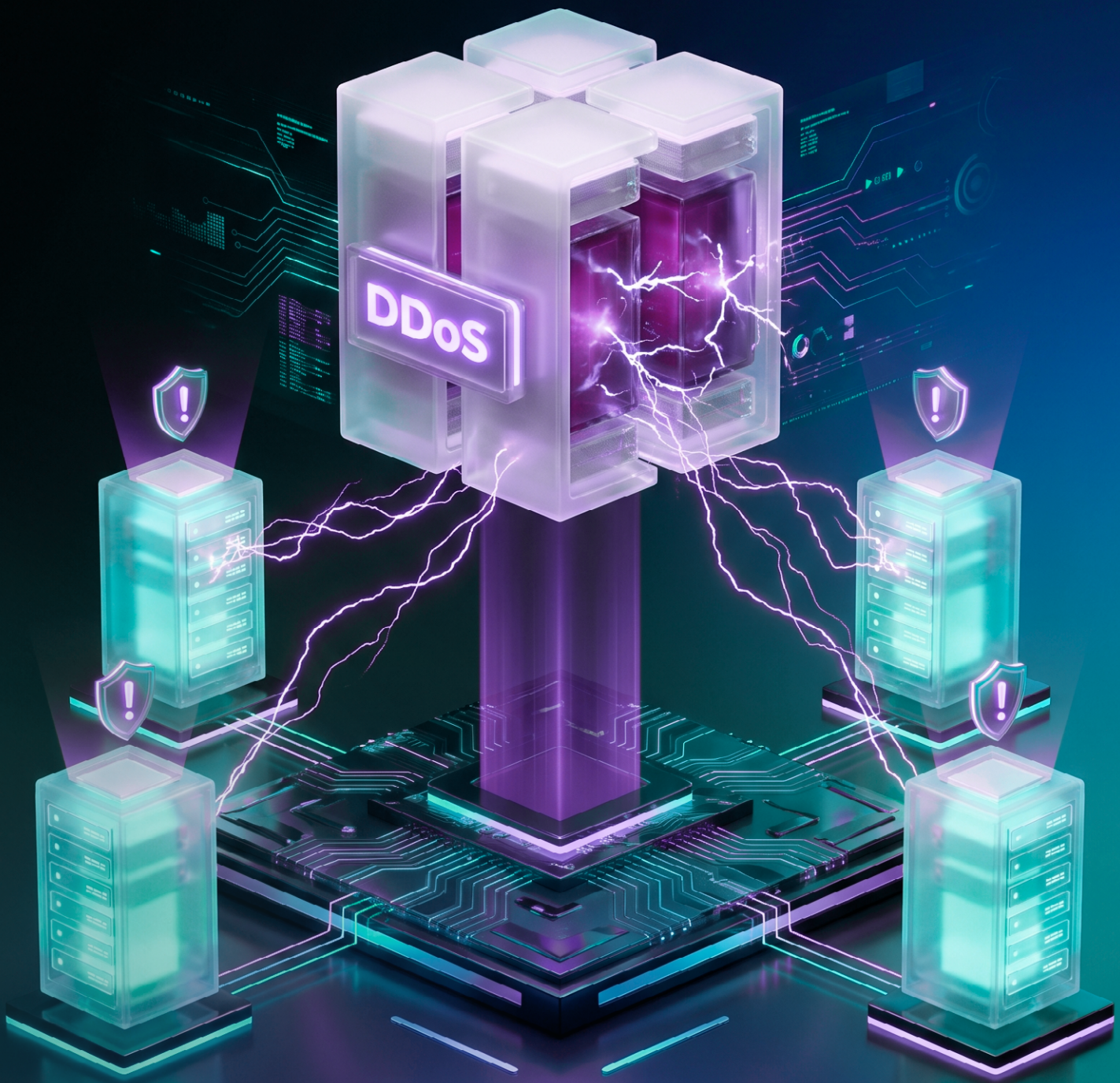
kaspersky



DDoS-экономика:
сколько стоит «положить» сайт

Введение

Рост количества DDoS-атак[1] стал серьезной проблемой для ИБ-индустрии. Но сами атаки — лишь часть большой мозаики. Их организацией занимаются дельцы на теневых рынках, где подобная услуга зачастую стоит дешевле, чем подписка на стриминговый сервис.

Изучая этот рынок, мы проанализировали более 256 000 сообщений в даркнете и дипвебе и выявили 148 активных поставщиков DDoS-услуг, работающих как минимум с 2024 года. Однако подлинная картина начала вырисовываться лишь тогда, когда мы проследили их историю вплоть до 2015 года. Проработав базу накопившихся за эти годы рекламных объявлений и стоящих за ними реальных предложений, проанализировав сценарии атак и обнаружив, что в них часто замешаны одни и те же действующие лица, мы поняли, что имеем дело не просто с набором услуг по проведению атак, а с целой отраслью подпольной киберпреступной экономики — устойчивой, адаптивной и куда более организованной, чем могло бы показаться на первый взгляд. На следующих страницах мы подробно рассмотрим этот рынок: торговцев, киберорудия, которое они продают, цены на него и цели, против которых оно применяется; мы также выясним, как DDoS-экономика эволюционирует, чтобы выживать.

Структура исследования включает три раздела:

В разделе Орудия хаоса рассматриваются сами атаки — их разновидности, цели, а также способы подготовки к их проведению. Раздел Цена удара посвящен коммерческой стороне вопроса — ценообразованию и стратегиям продаж разных типов услуг и их эволюции в конкурентной среде. В разделе Стратегии выживания мы поговорим о самих злоумышленниках — сколько длится их активность, как они конкурируют за внимание «клиентов», как используют DDoS-ресурсы для предоставления смежных услуг и адаптируют свои предложения к актуальным потребностям Теневого рынка.

Этот материал подготовлен для специалистов по техническим и стратегическим аспектам ИБ — от аналитиков киберугроз до менеджеров по информационной безопасности.

[1] https://www.kaspersky.ru/about/press-releases/chislo-ddos-atak-na-rossijskie-kompanii-v-nachale-2026-goda-vyroslo-na-27

Орудия хаоса

Инструменты для перегрузки систем

Исходя из того, как злоумышленники описывают предлагаемые услуги, мы различаем две масштабные категории атак: L3/L4 и L7. Ещё можно выделить атаки на игровые серверы и onion-атаки. Но это, скорее, отдельные сценарии внутри больших категорий. 91 из 148 злоумышленников в нашей выборке давали в своих объявлениях достаточно информации для определения категории атаки. В 20 из них тип атаки не был указан прямо, поэтому вывод был сделан исходя из контекста, например перечисленных в публикации средств защиты от DDoS-атак.

L3/L4

Атаки на уровнях L3/L4 забивают трафиком сетевой канал жертвы.

Чаще всего злоумышленники упоминают атаки на уровнях L3 и L4 вместе, поэтому мы рассматриваем их как одну категорию. Лишь 9% злоумышленников предлагали отдельные атаки на уровне L3, например ICMP, GRE или ESP-флуд. L4-атаки встречались гораздо чаще: 74% злоумышленников предлагали ACK/SYN-флуд на уровне TCP, UDP-флуд, DNS-амплификацию и другие атаки на транспортном уровне.

10 Гбит/с–8,2 Тбит/с

- направлены на перегрузку каналов связи
- относительно просты в исполнении
- просты в обнаружении
- осуществляются посредством резкого увеличения объёма трафика

Игры*

особый сценарий L3/L4-атак

> 1 Тбит/с

* специально конструируемые UDP-пакеты

Важным частным случаем являются атаки на игровые серверы. Технически, это атаки уровня L4[2], но злоумышленники часто рассматривают их как отдельную категорию атак. Отчасти это обусловлено спецификой работы игровых серверов, которые во многом отличаются от традиционных веб-инфраструктур. Они используют больше памяти, вызывают скачки загрузки процессора и активно используют дисковую подсистему. Чаще всего для такой атаки нужны пакеты данных, специально созданные для конкретных игр (обычно это пакеты протокола UDP). Именно поэтому атаки на игровые серверы не считают обычной разновидностью флуда, а выделяют в отдельное предложение. В нашей выборке 23% злоумышленников позиционировали услуги по проведению таких атак как конкурентное преимущество.

[2] DDoS-атаки на игровые серверы могут осуществляться на уровнях L4 и L7, однако проанализированные рекламные объявления прямо предлагали только атаки уровня L4.

L7

Атаки на уровне L7 работают по-другому. Они не забивают сетевой канал и не парализуют обработку соединений, а создают нагрузку непосредственно на приложения.

В нашей выборке L7-атаки рекламировались чаще других: такую услугу предлагали 92% злоумышленников. В частности, это связано с тем, что для их проведения существует множество готовых инструментов с открытым исходным кодом, которые достаточно немного доработать перед продажей, что снижает барьер входа. Еще одна причина – сравнительно простая инициализация цели. Для запуска атаки не требуется практически ничего, кроме адреса целевого сайта.

Атаки на ресурсы .onion — особый сценарий L7-атак. В этом случае преступники манипулируют не только и не столько объемом трафика, сколько механизмами обработки соединений в сети Tor. Такую услугу предлагали только 3% злоумышленников.

100 000–8 500 000 запросов в секунду

- направлены на исчерпание ресурсов приложений
- маскируются под легитимную активность
- сложны в обнаружении
- требуют изучения цели

.onion*

особый сценарий L7-атак

*эксплуатирует механизмы сети Tor

Охотники и жертвы

Преступники могут выбирать одни и те же методы атаки для достижения абсолютно разных целей. Выбор зависит от того, кто инициатор, что им движет и какие препятствия стоят у него на пути. Несмотря на различия в подходах, конечная цель остается неизменной — преднамеренное нарушение работоспособности систем. Ниже приведены основные профили атакующих, которые мы выявили при анализе нашей выборки.

Экономические антагонисты

Причинение финансового ущерба в результате снижения доступности сервисов и нанесения вреда репутации.

Причинение финансового ущерба за счет сокращения времени бесперебойной работы, ухудшения позиций в поисковой выдаче и истощения бюджета на рекламу через «мусорный» трафик.

Вымогатели

Принуждение жертвы к уплате выкупа за восстановление работоспособности систем или прекращение атаки.

Получение финансовой прибыли путем вымогательства денег под угрозой проведения или продолжения атаки.

Хактивисты

Привлечение внимания к событию или «наказание» организации исходя из идеологических соображений.

Продвижение политических или социальных взглядов путем нарушения работы организации и привлечения внимания публики.

Оппортунисты

Отвлечение внимания специалистов с целью провести другую вредоносную кампанию или получение преимущества в игре.

Ситуационная или личная выгода.

Цель Мотивация Жертвы

Приобретение инструментов

По способу организации мы выделили три подхода к организации атак: DDoS-атака через посредника, DDoS как услуга и атака из своей инфраструктуры. В первых двух случаях к проведению атаки привлекаются сторонние поставщики ресурсов, а атаки третьего типа злоумышленники проводят самостоятельно с использованием инфраструктуры, которую сами же выстраивают и поддерживают.

Поставщик ресурсов — злоумышленник, у которого есть инфраструктура, необходимая для проведения атаки.

DDoS-атака через посредника

атака проводится другим злоумышленником по договоренности

DDoS как услуга

доступ к необходимым для атаки ресурсам открывается по подписке

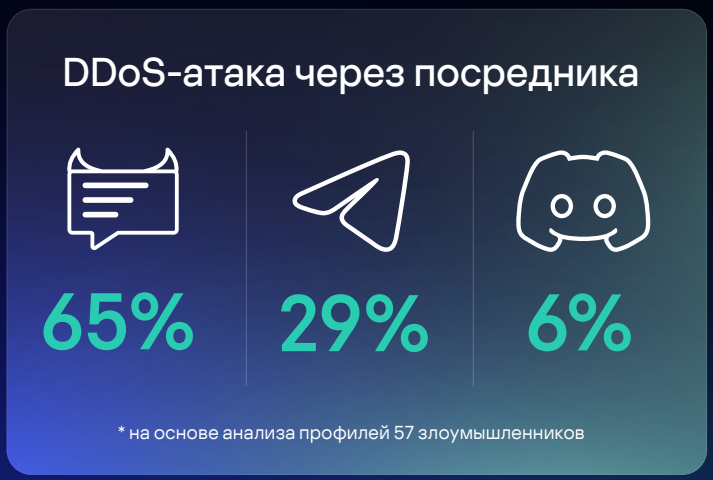
Атака из своей инфраструктуры

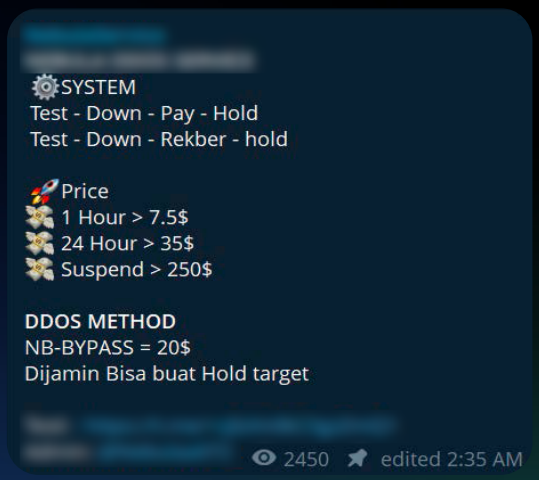
все ресурсы под контролем инициатора атаки

DDoS-атака через посредника

Самая простая из выявленных моделей: инициатор атаки обращается к посреднику с запросом на проведение атаки. В этом случае посредник является поставщиком ресурсов и сам же проводит атаку. Стороны могут найти друг друга в даркнете, но дальнейшее общение перенесут в другую платформу, в основном в Telegram или Discord. В такой модели поставщик берет на себя все технические задачи: выбирает методы атаки, профилирования трафика и обхода защитных мер.

Инициатор атаки — злоумышленник, который планирует атаковать систему, сервис или онлайн-ресурс.





Пример рекламного объявления с предложением услуг по проведению DDoS-атак

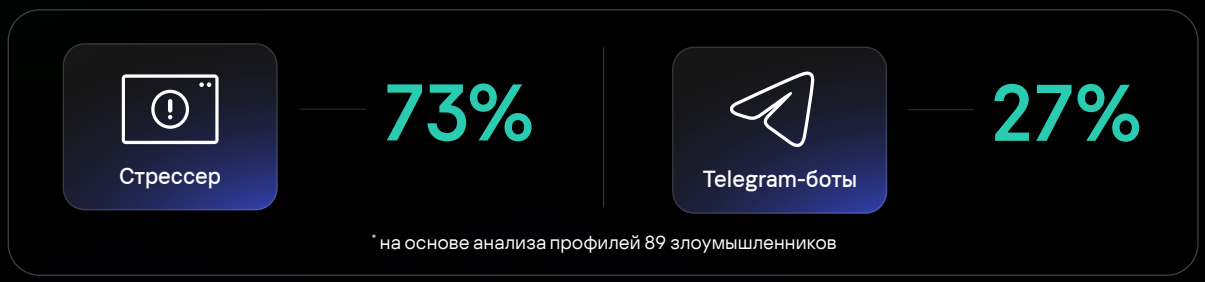
Наш анализ показал, что из 57 злоумышленников, предлагавших DDoS-услуги, 65% использовали подпольные форумы в качестве основной рекламной платформы. Остальные отдавали предпочтение мессенджерам, в основном Telegram и Discord.

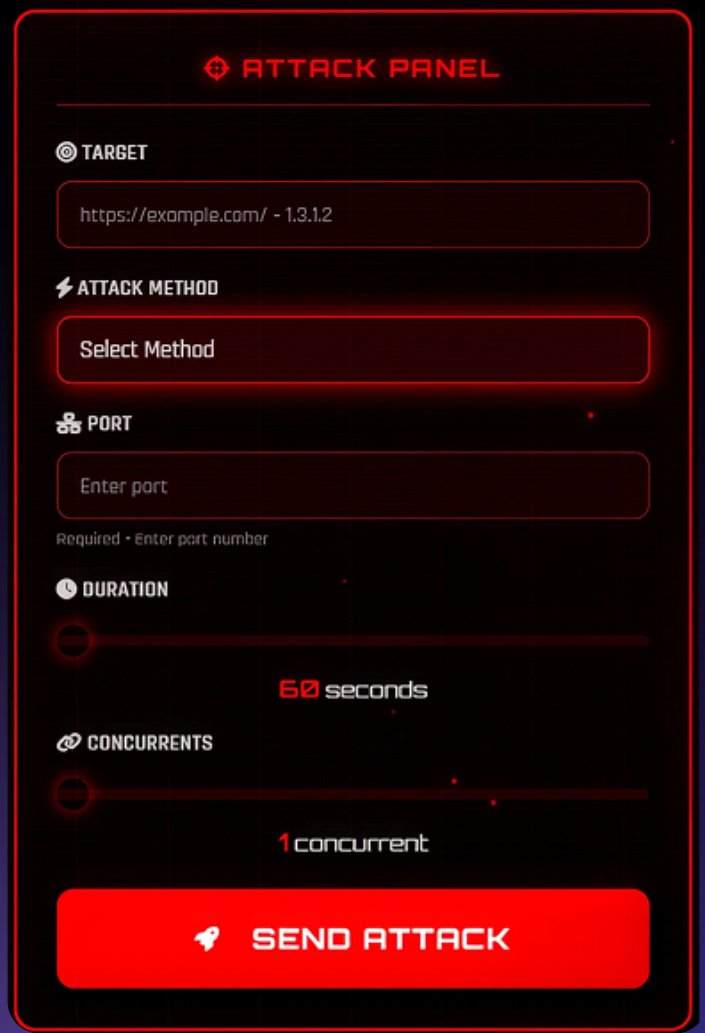
DDoS как услуга

Во втором подходе к организации атаки прямое взаимодействие с поставщиком ресурсов не требуется. Вместо переговоров инициатор просто покупает доступ к стрессеру или Telegram-боту и запускает атаку самостоятельно. План подписки можно выбрать: он зависит от метода и продолжительности атаки, а также от количества одновременных атак. Некоторые сервисы еще больше упрощают этот процесс. Например, они позволяют запустить простейшую тестовую атаку бесплатно — для этого нужно отправить в чат всего одну команду.

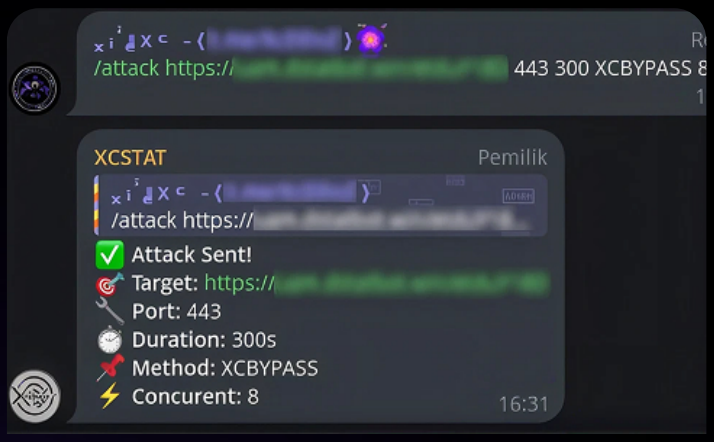
Стрессер — управляемый поставщиком ресурсов интерфейс, который используется для проведения атак по модели DDoSaaS.

Изначально этот подход подразумевал взаимодействие с веб-интерфейсами стрессеров. Но, по нашим наблюдениям, в 2022 году резко увеличилось (по сравнению с предшествующими годами) число рекламных объявлений, предлагающих стрессер с основным или единственным интерфейсом в Telegram-боте. Таким образом, этот рынок постепенно мигрирует с классических сайтов на более удобные, быстрые и регулярно обновляющиеся платформы.





Пример веб-интерфейса стрессера



Пример запуска атаки через Telegram-бот

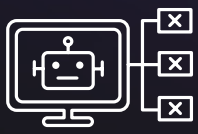
Атака из своей инфраструктуры

Инициаторы атак не всегда привлекают к ним третьих лиц. Они могут использовать и свою инфраструктуру. На практике это обычно означает, что они либо запускают скрипты, реализующие один или несколько методов DDoS-атаки, либо строят и обслуживают собственный ботнет.

Эти подходы отличаются как техническими, так и операционными особенностями.

На базе скриптов

Скрипты лучше подходят для частных единичных атак или непродолжительных кампаний. Их легко найти в общем доступе бесплатно, что существенно снижает порог входа для технически подкованных злоумышленников.



На базе ботнета

Ботнет — более сложный подход.
Он требует времени и ресурсов не только для создания, но и для поддержания работоспособности. Поэтому ботнеты обычно ассоциируются с более технически продвинутыми злоумышленниками.
Ботнеты распространяются реже и стоят дороже — зачастую актуальные сборки можно только купить.

К апрелю 2026 года нам удалось обнаружить более 1000 репозиториев на GitHub, через которые распространялись скрипты для стрессеров, и еще 500 репозиториев, которые, по заявлениям их создателей, содержали исходный код ботнета.

Цена удара

Модель оплаты зависит от подхода к организации атаки. Если инициатор привлекает посредника, цена каждой запрошенной атаки обговаривается отдельно. В модели DDoSaaS цены фиксированы и определяются тарифным планом.

DDoS-атака через посредника

Когда атаку проводит посредник, стороны согласовывают стоимость услуги в каждом отдельном случае. Получив запрос от инициатора атаки, поставщик анализирует цель и назначает цену.

По результатам нашего исследования, среди 36 поставщиков, предлагавших эту модель, стоимость одной атаки варьировалась от 30 до 2000 долл. США, в зависимости от ее продолжительности, цели и заявленной мощности.

$30–$2 000

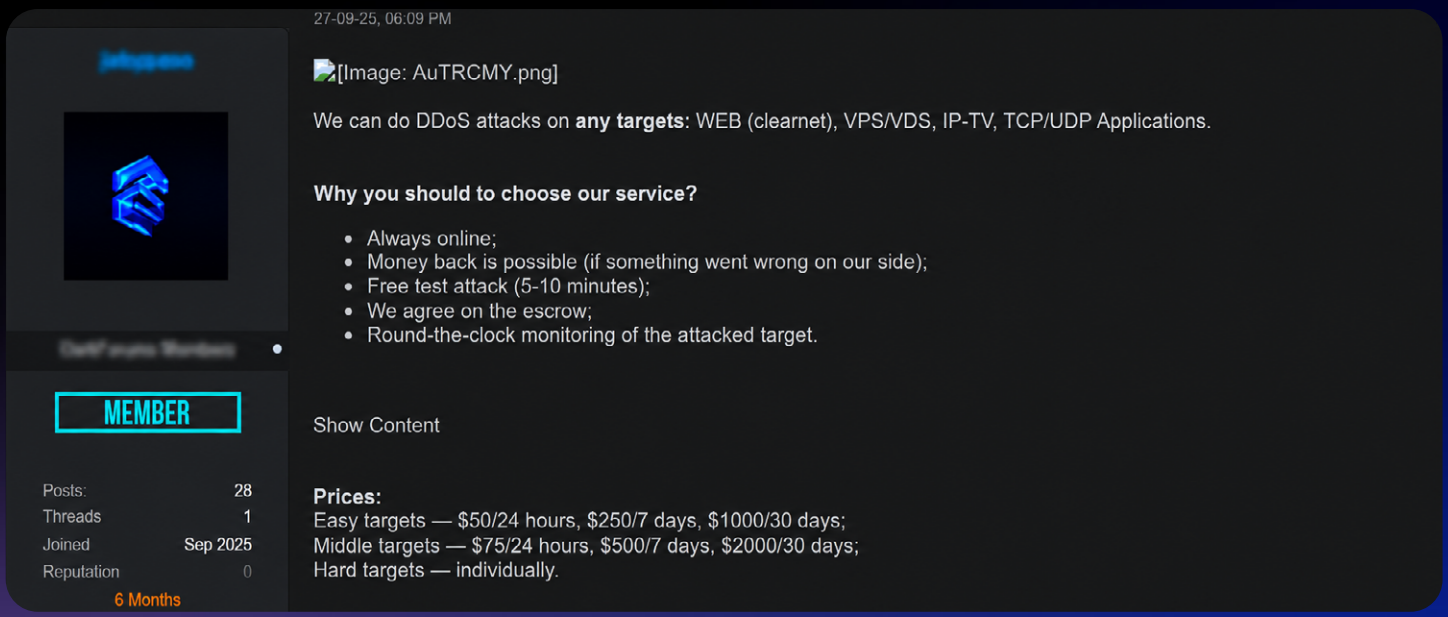
стоимость одной атаки

*ценовой диапазон для атак продолжительностью от 1 до 30 дней

$10	$100	$500	$1 250
тестовая атака	1 день	7 дней	30 дней

*средняя стоимость одной атаки, по результатам анализа предложений от 36 поставщиков

Типичное предложение включает кратковременную тестовую атаку, которая позволяет инициатору проверить функциональность сервиса, прежде чем оплачивать более масштабную кампанию. Стоимость тестовой атаки может достигать 10 долларов, а некоторые злоумышленники предлагают такую проверку бесплатно.



27-09-25, 06:09 PM

[Image: AuTRCMY.png]

We can do DDoS attacks on **any targets:** WEB (clearnet), VPS/VDS, IP-TV, TCP/UDP Applications.

Why you should to choose our service?

- Always online;
- Money back is possible (if something went wrong on our side);
- Free test attack (5-10 minutes);
- We agree on the escrow;
- Round-the-clock monitoring of the attacked target.

Show Content

Prices:
Easy targets — $50/24 hours, $250/7 days, $1000/30 days;
Middle targets — $75/24 hours, $500/7 days, $2000/30 days;
Hard targets — individually.

MEMBER

Posts: 28
Threads 1
Joined Sep 2025
Reputation 0
6 Months

Пример рекламного объявления с предложением услуг по проведению DDoS-атак через посредника

DDoS как услуга

В отличие от модели атаки через посредника, подписка предлагает более гибкие возможности. В этом случае инициатор платит за доступ к инструментам для атаки, а не за проведение одной атаки. Приобретая такой доступ, инициатор получает возможность запускать атаки продолжительностью от 1 минуты до 48 часов в течение всего периода подписки.

$1–$30 000

стоимость подписки в зависимости от предоставляемых возможностей

* для 30-дневных подписок

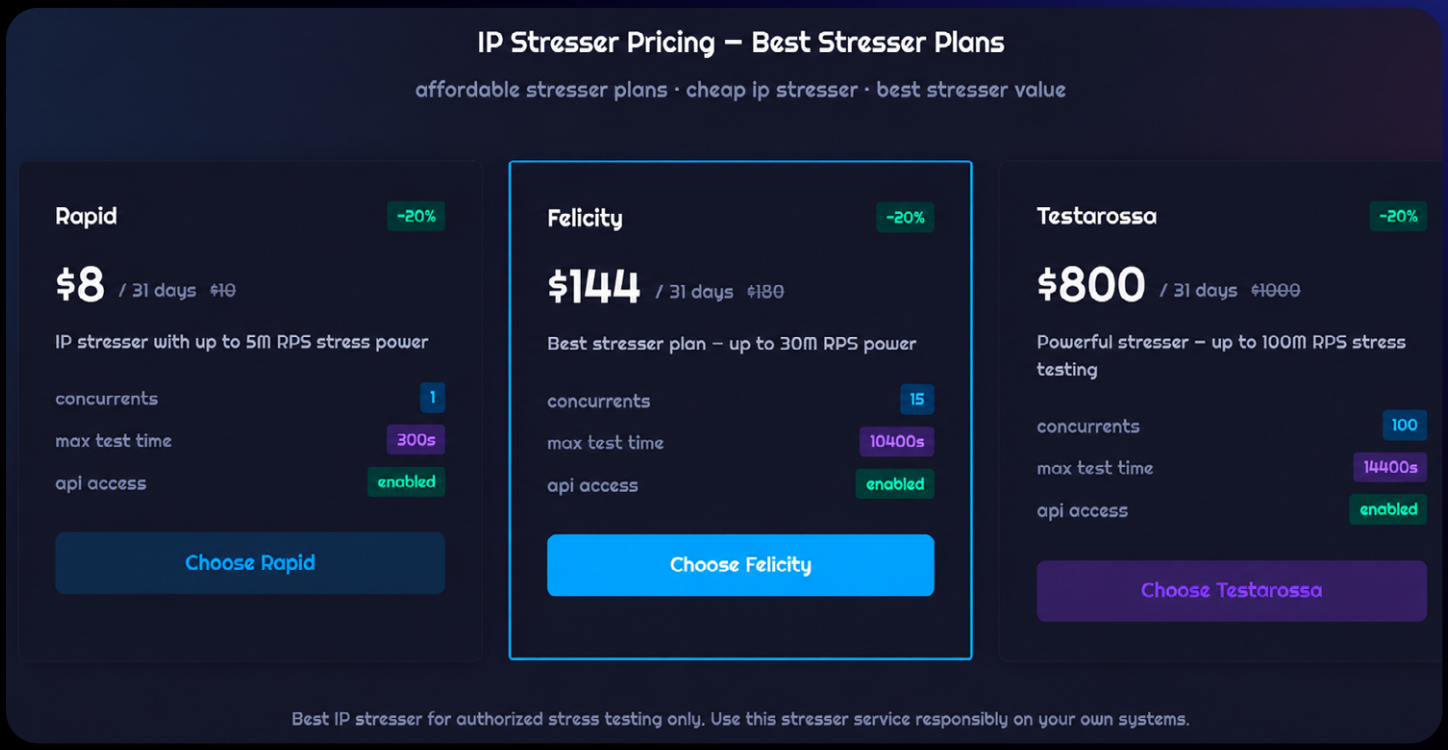
64 злоумышленника из нашей выборки предлагали подписку с указанием цены. Стоимость подписки на 30 дней варьировалась от 1 до 30 000 долл. США. Некоторые предлагали подписку на 7 дней, но такие объявления встречались значительно реже.

Подписки обычно действуют в течение 30 дней и различаются доступными методами и максимальной продолжительностью атаки, количеством одновременных атак и возможностью доступа к API. Более высокие тарифы предоставляют расширенный набор указанных возможностей, но сама модель не меняется.

$20	$191	$2 160
60–600 сек.	300–3600 сек.	> 3600 сек.

* средняя стоимость месячной подписки по результатам анализа предложений от 64 злоумышленников

Во многих объявлениях повторялась необычная деталь: продолжительность атаки указывалась в секундах, а не минутах или часах, что выглядело довольно неинтуитивно. По нашим наблюдениям, эта практика сложилась давно, во времена использования DoS-скриптов, разработанных для Unix/POSIX-систем, где стандартной единицей времени были секунды, и их счетчик являлся просто целым числом, с которым было удобно работать.



Пример расценок для подписки на доступ к стрессеру

Сервисная модель	Что оплачивается	Участие покупателя	Продолжитель-ность одной атаки	Относительная стоимость
DDoS-атака через посредника	Одна атака на одну цель по запросу	Практически не требуется — поставщик сам проводит атаку	1, 7, 30 дней или определяется индивидуально	Выгодно для долгосрочных атак и атак на сложные цели
DDoS как услуга	30-дневный доступ к инструментам для атаки, набор которых ограничен условиями подписки	Покупатель выбирает метод и мощность атаки, в некоторых случаях он должен сам запускать атаку повторно	От 1 минуты до 24 часов, в зависимости от плана	Выгодно для краткосрочных атак и атак на простые цели

Мощность атак

Заявления о мощности атак фигурировали только в объявлениях, рекламирующих DDoS как услугу. Посредники практически никогда не указывают такую информацию, а мощности тех, кто использует собственную инфраструктуру, зависят только от бюджета. Поэтому представленные ниже данные получены исключительно по результатам анализа услуг, предоставляемых через стрессеры по подписке.

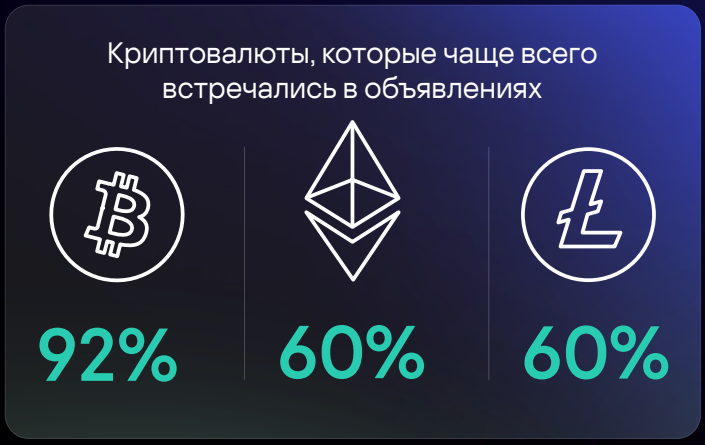
В этом сегменте рынка мощность атаки определяется цифрами: поставщики предлагают разрушительный потенциал в диапазоне от 15 Гбит/с до 7 Тбит/с стоимостью от 30 до 4500 долл. США.

В 36% объявлений, содержащих данные об интенсивности атак, предлагаемая разрушительная мощь была указана в Тбит/с. Однако относиться к этим цифрам следует с осторожностью — проверить заявленную мощность практически невозможно. Коммерческие DDoS-сервисы в основном ориентированы на L3/L4-атаки средней мощности, поскольку такой формат обеспечивает быстрый заработок. Крупномасштабные атаки мощностью в несколько Тбит/с обычно проводятся группировками, действующими при поддержке государства, с целью дестабилизации. Модели с оплатой по факту использования для таких атак, как правило, не применяются.

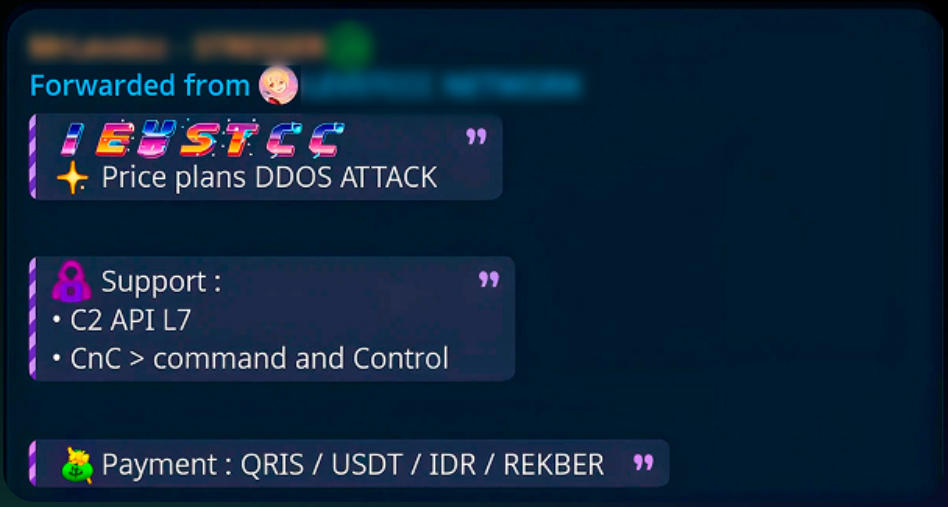
Кому доллар, кому талер

Информация о расчетных методах публиковалась в основном в объявлениях типа «DDoS как услуга», чтобы минимизировать взаимодействие между инициатором и владельцем стрессера. В объявлениях посредников такие данные практически никогда не встречались, а уточнялись при личном взаимодействии.

В рамках исследования мы обнаружили 25 способов и валют для оплаты. Как правило, расчеты проводятся в криптовалюте. Из тех, кто принимал оплату в криптовалюте, Bitcoin принимали 92% поставщиков, а 60% вели расчеты в Ethereum и Litecoin. Оплата иными способами встречалась гораздо реже — всего 7%, — поскольку они не обеспечивают достаточный уровень приватности.



Однако стоит отметить, что непопулярные методы оплаты служат полезным индикатором для атрибуции злоумышленников.



Примеры сообщений с указанием метода оплаты

Атака из своей инфраструктуры

Расходы злоумышленников, которые используют собственную инфраструктуру для проведения атак, носят совершенно иной характер. Никаких платных доступов, подписок и удобных сценариев покупки. Атака происходит в результате слаженной работы множества ресурсов — скриптов, серверов и зараженных устройств, если используется ботнет. Проанализировав сценарии атак, мы выделили две крупные модели собственной инфраструктуры: простую на базе скриптов и более масштабную на базе ботнета.

На базе скриптов

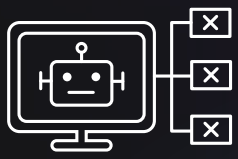
Скрипт

$0-$100

Аренда VPS-сервера

$10-$30/месяц

На базе ботнета



Исходный код

$2 000+

Аренда C2-сервера

$10-$30/месяц

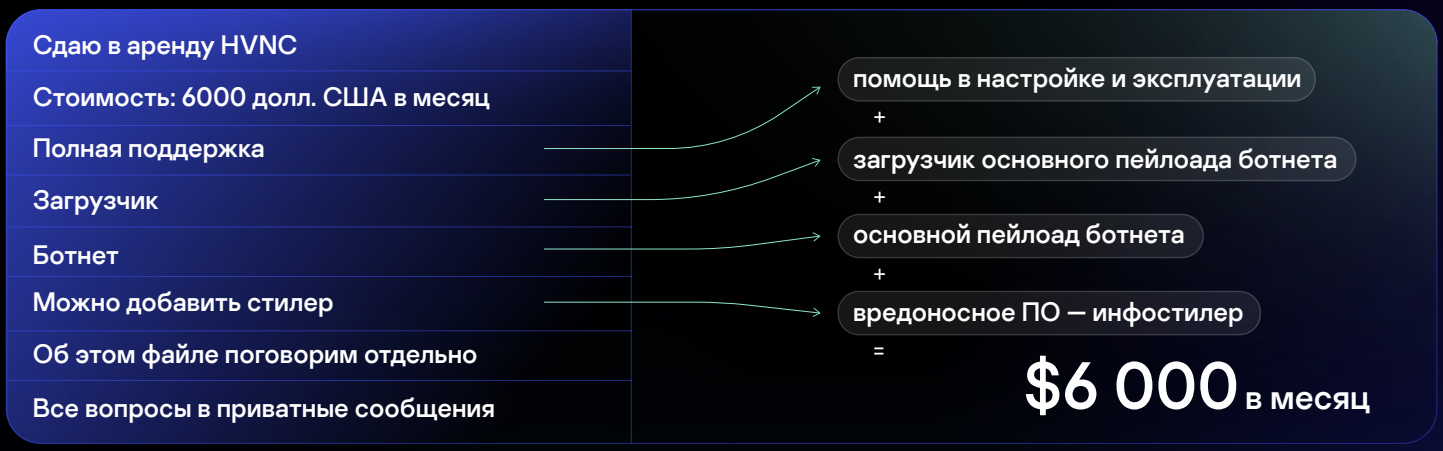
Установки

$0,1+/установка

В первом случае злоумышленник развертывает на одном или нескольких арендованных серверах бесплатные или недорогие скрипты для атаки. Большая часть расходов связана с арендой инфраструктуры и зависит от количества используемых серверов, их спецификаций, а также того, как хостинг-провайдер реагирует на жалобы на злоупотребление ресурсами.

Развертывание ботнета требует совершенно другого уровня вложений. Конечно, в сети можно найти какой-нибудь древний исходный код для его создания, но, как правило, более мощные ботнеты предоставляются платно. Стоимость кода для них начинается от 2000 долл. США.

При использовании ботнета злоумышленникам приходится также платить за аренду командных серверов, установленные экземпляры ботов, трафик, регулярные меры маскировки для обхода антивирусов и обслуживание. В отличие от скрипта, который достаточно лишь запустить, ботнет требует постоянного поддержания работоспособности.



Объявление об аренде ботнета на теневом форуме

Из этого примера видно, как формируется стоимость аренды ботнета. В рассмотренном случае пакет услуг по аренде ботнета стоит 6000 долл. США в месяц и включает не только доступ к самому ботнету, но и загрузчик, поддержку со стороны оператора и дополнительные возможности (инфостилер). То есть инициатор приобретает не только исходный код для создания ботнета, а комплексный сервис.

Ценовая конкуренция

При анализе динамики цен на DDoS-услуги мы выявили две тенденции. Во-первых, большая часть рынка сравнительно стабильна: примерно на 64% сервисов из нашей выборки цена не менялась в течение длительного времени, иногда больше десяти лет. Во-вторых, стоимость оставшихся 36% сервисов менялась непредсказуемо. В частности, мы нашли одного поставщика, услуги которого за 20 дней подешевели на 50%.

Это говорит о том, что рынок стабилен в одних секторах, но крайне неоднороден в других.

Если сузить анализ с рынка в целом до отдельных его участников, то картина становится менее стабильной. Выше мы рассмотрели динамику цен на услуги одного поставщика, который предлагает подписку на день, неделю и месяц. Цены на графике падают и взлетают совершенно непредсказуемо, без каких-либо закономерностей. Самый интересный случай — 22 октября 2024 года, когда злоумышленник предлагал одни и те же услуги на разных форумах по совершенно разным ценам. Это яркий пример того, как преступники адаптируют цены к целевой аудитории.

Стратегии выживания

Пришел, продал, исчез

Среди 148 злоумышленников, активных в 2024 году и ранее, среднее «время жизни» (период между публикацией первого и последнего объявлений о проведении DDoS-атак) составляет 2,5 года, при том старожилы рынка недавно отпраздновали свой первый юбилей — 10 лет.

До 2022 года новичков на рынок приходило относительно мало. Их количество выросло значительно только в 2023 году, и эта тенденция сохраняется по сей день. Только в первом квартале 2026 года мы обнаружили 16 новых злоумышленников. Если тренд не изменится, то количество новичков на этом рынке в 2026 году превысит показатель 2025 года по меньшей мере на 25%.

На это есть несколько причин. За последние годы DDoS-атаки стали заметно более распространенным явлением. С ростом геополитической напряженности хактивисты все чаще проводят свои собственные DDoS-кампании. Вместе с тем в интернете появилось множество стрессеров с открытым исходным кодом, что существенно снизило порог входа и сделало организацию атак доступнее.

Борьба за внимание

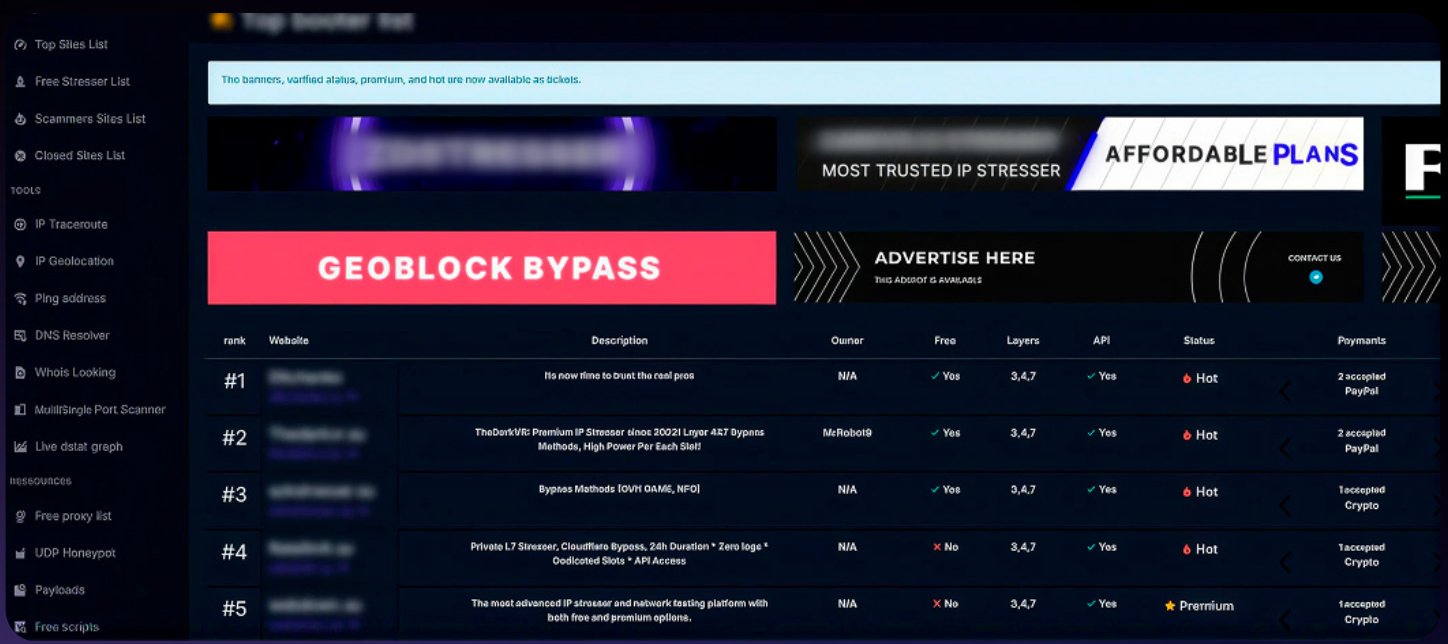
Чтобы преуспевать на этом рынке, важен не только разрушительный потенциал, но и заметность. Какие бы методы атаки ни предлагал поставщик ресурсов, вряд ли он обзаведется клиентами, если его невозможно найти или никто его не знает. Чтобы оставаться на виду, злоумышленники продвигают свои услуги в разных сегментах интернета — от клирнета в виде DDoS-агрегаторов до частных теневых форумов.

Эти платформы используются по-разному. Одни предназначены для сравнения сервисов, другие — для массовой рассылки рекламных объявлений, третьи полагаются на получение клиентов при помощи репутации. Все вместе они образуют рекламную экосистему, внутри которой злоумышленники конкурируют за внимание клиентов.

Помимо популярных каналов, мы обнаружили новый, уникальный рекламный механизм — рейтинговые платформы. Они отличаются от традиционных рекламных каналов и по форме, и по функциям, поэтому мы поговорим о них отдельно — в разделе Теневые рейтинги.

DDoS-агрегаторы

Это сайты, которые объединяют множество предложений о проведении DDoS-атак в одном интерфейсе. Они ранжируют поставщиков по «уровню доверия», оценкам пользователей и заявленным уровням атаки. По сути, это каталоги подпольных услуг с возможностью поиска.

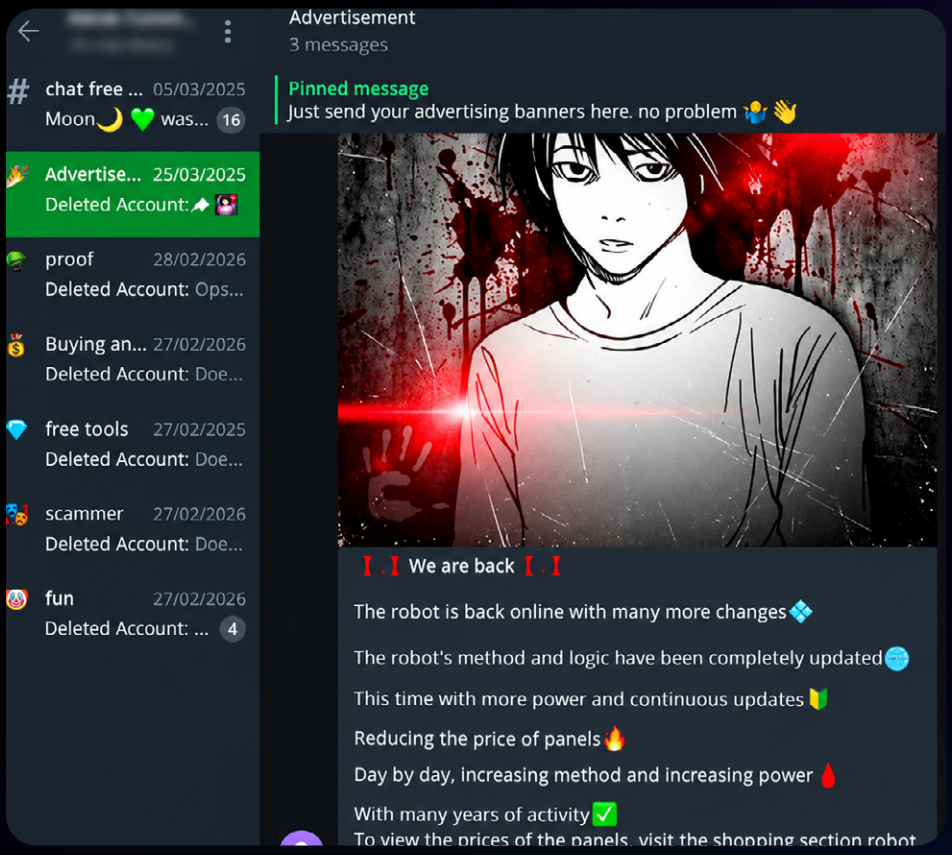


Пример DDoS-агрегатора

Спам-реклама в мессенджерах

Мессенджеры — еще один популярный канал продвижения сервисов. Для рекламы своих услуг злоумышленники наводняют один или несколько каналов сообщениями, пытаясь привлечь внимание за счет их количества, а не опираясь на собственную репутацию.

Иногда администраторы каналов создают отдельные ветки для рекламы, чтобы такие спам-сообщения не мешали общению в чате.



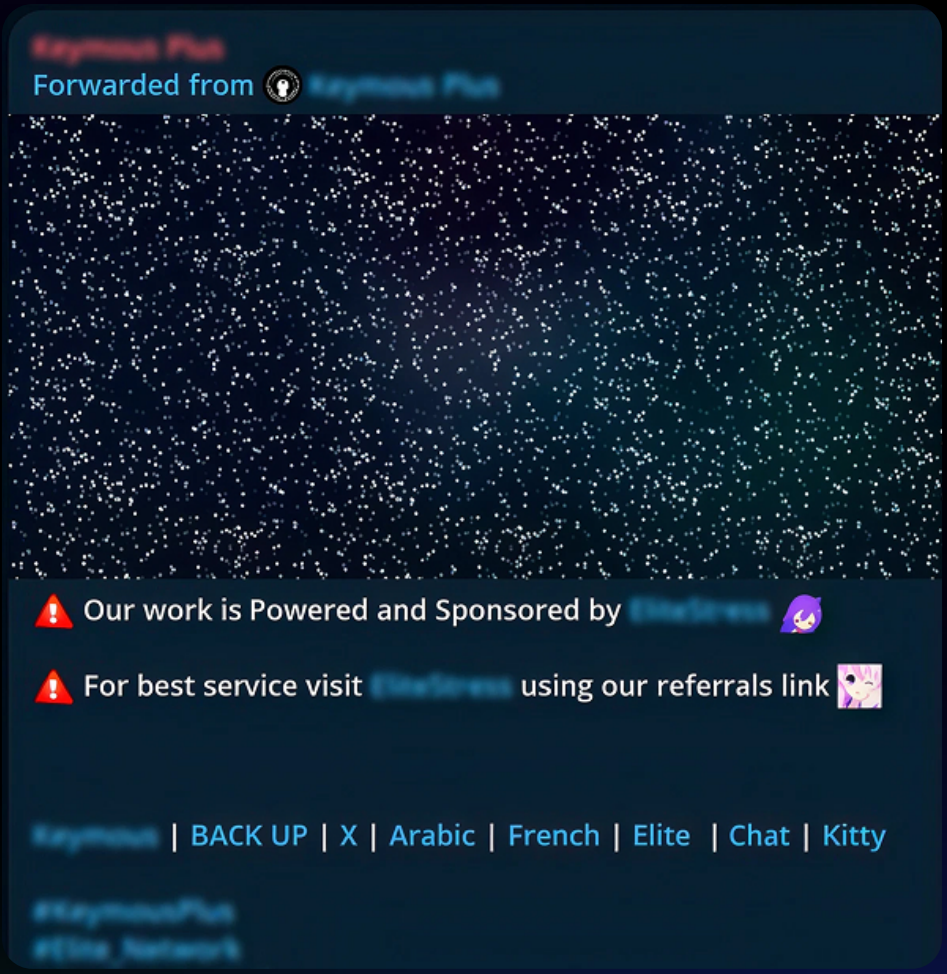
Пример отдельной рекламной ветки

Пример спам-рекламы в мессенджере

Сотрудничество с хактивистами

Хактивисты работают не только с идеологически мотивированными участниками. Иногда они объединяются с поставщиками ресурсов для DDoS-атак, создавая альянсы, которые позволяют нарастить разрушительный потенциал кампаний. Более продвинутые группировки и вовсе могут располагать ресурсами для создания собственной инфраструктуры. По меньшей мере четыре активные группы хактивистов предлагали DDoS-инструментарий собственной разработки.

Поставщикам такие альянсы тоже выгодны. Каналы хактивистов становятся для них своего рода витриной: здесь анонсируются предстоящие атаки и публикуются их результаты, фактически демонстрируя эффективность предлагаемых услуг. Участие же поставщика в активных кампаниях делает его заметным и узнаваемым. В ходе исследования мы выявили девятерых поставщиков, связанных с хактивистами.

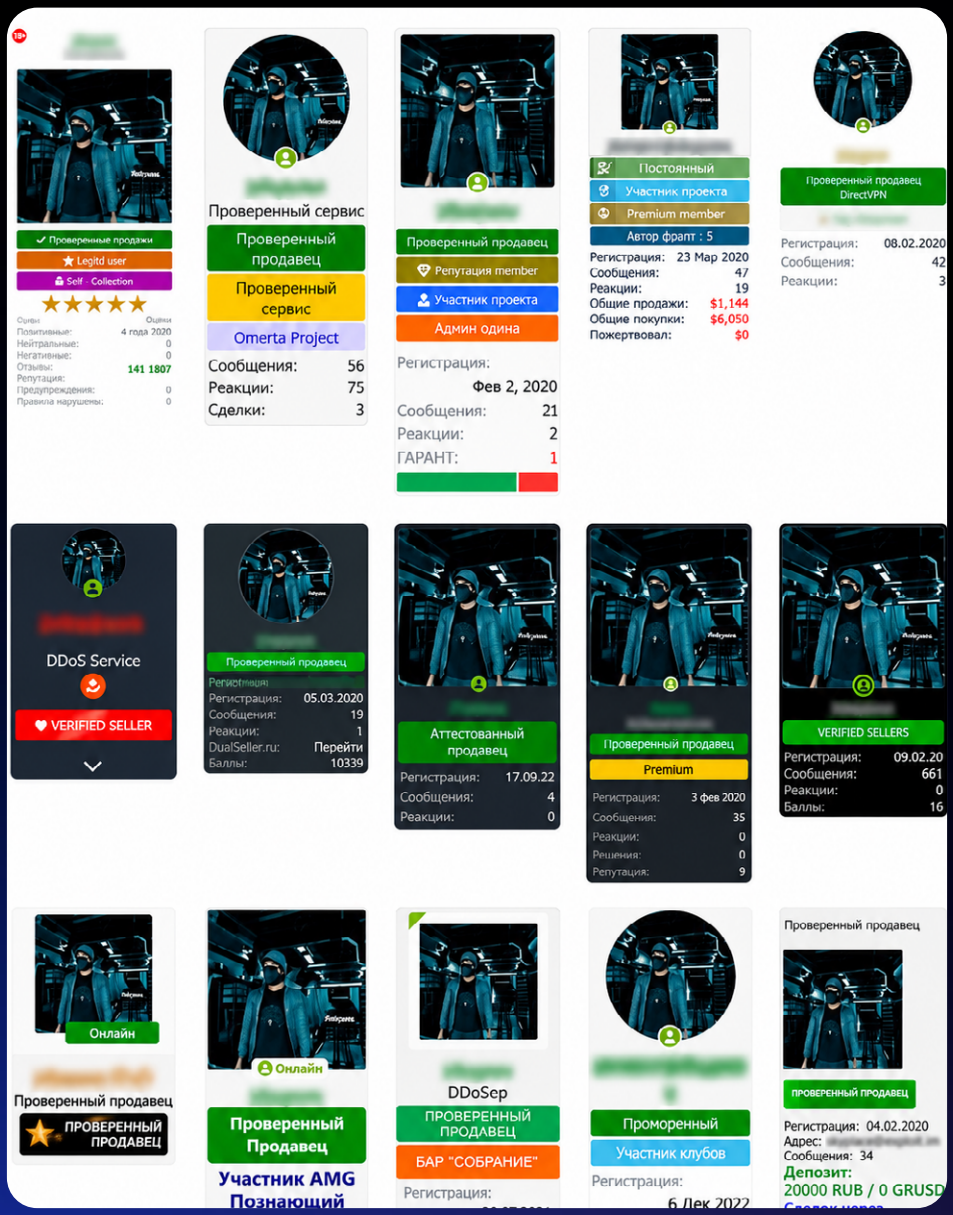


Пример объявления, в котором указана связь оператора стрессера с хактивистами

Теневые форумы

Теневые форумы остаются самыми популярными площадками для продвижения DDoS-услуг. Некоторые специализированные форумы позиционируют себя как платформы для обсуждения технологий защиты от DDoS-атак, однако анализ показывает, что на деле злоумышленники используют их для продвижения собственных услуг. На более универсальных теневых форумах, где обсуждаются разные темы, нередко есть отдельные ветки для рекламы DDoS-услуг.

Действующие на форумах системы репутации тоже способствуют продвижению услуг. Многие преступники рекламируют свои сервисы сразу на нескольких форумах, публикуя ссылки на другие платформы, чтобы повысить свой рейтинг или пройти антискам-проверку.



Профили одного и того же поставщика на разных форумах

Ссылки на профили поставщика на разных форумах

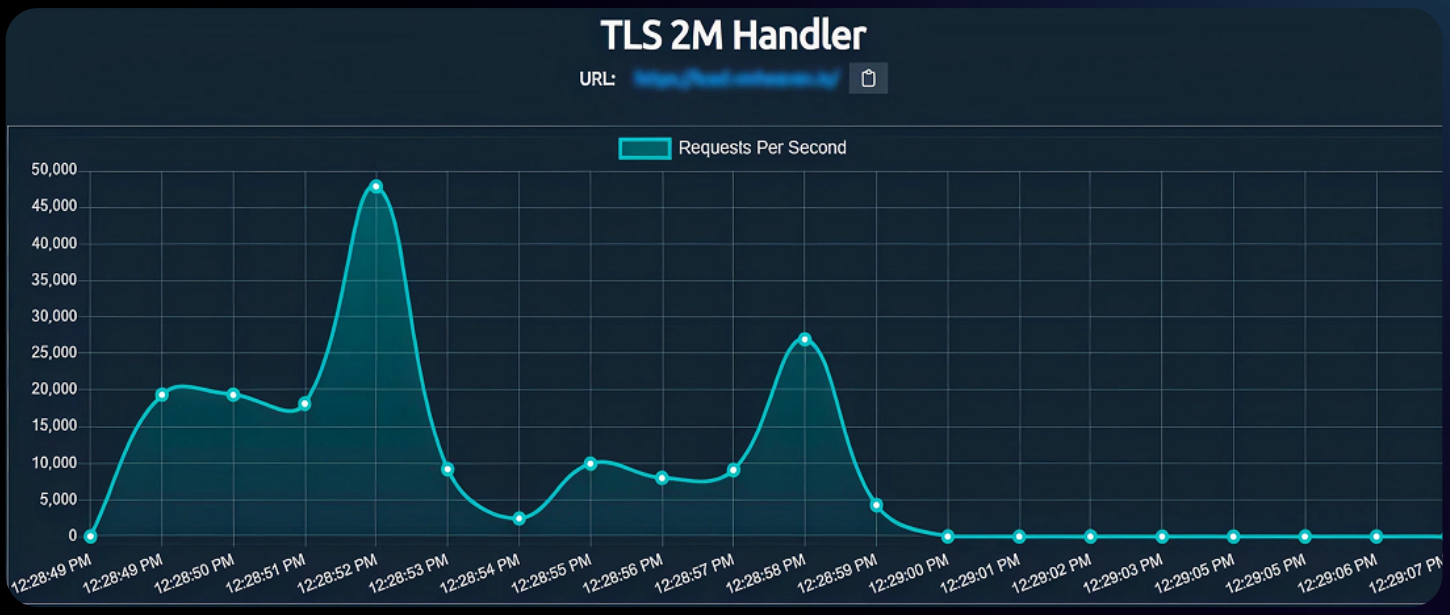
Теневые рейтинги

Некоторые преступники и вовсе не рассматривают традиционные каналы как инструмент продвижения. Они используют специализированные сайты или Telegram-боты, чтобы представить свои возможности по организации атак как нечто измеримое и осязаемое. Такие системы часто именуют DSTAT — по названию утилиты для мониторинга производительности системы. Они размещаются на серверах и поддерживаются поставщиками DDoS-услуг или создаются специально для формирования рейтингов активности. Сайт или Telegram-бот в этом случае выступает интерфейсом, через который можно отслеживать показатели атаки и сравнивать результаты пользователей.

Участник выбирает сервер и метод атаки, получает адрес целевого ресурса и запускает атаку. На протяжении периода наблюдения система фиксирует параметры трафика, такие как количество запросов в секунду и скорость передачи данных. Результат попадает в публичную рейтинговую таблицу под ником участника.

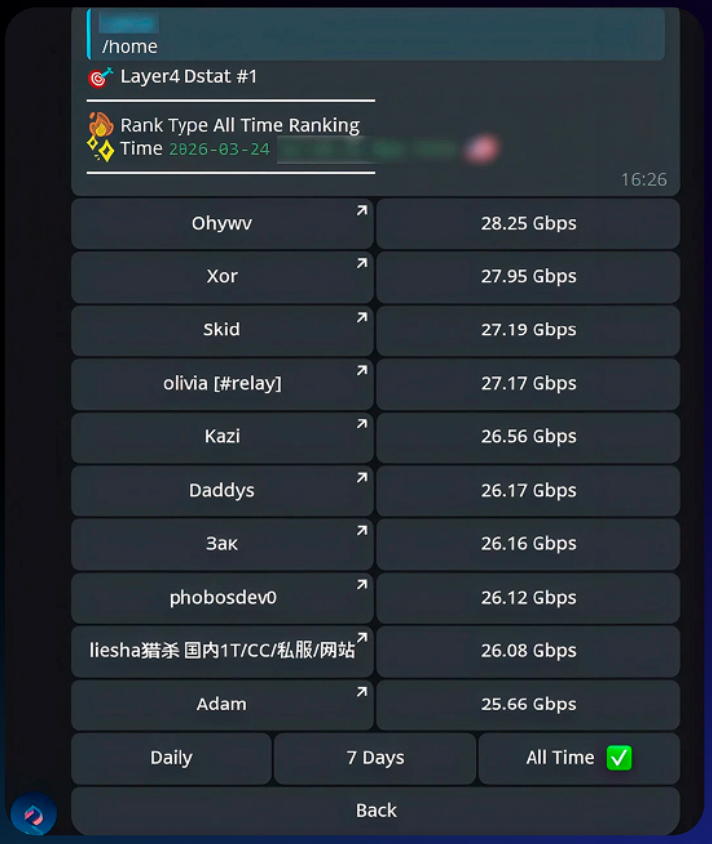
	Веб-сайт	Telegram-бот
Стандартное название	dstat.*	*Count*
Мониторинг атаки в реальном времени	Да	Нет
Выбор уровня атаки	Да	Да
Выбор метода	Да	Да
Возможность анонимного использования	Да	Нет (по умолчанию)
Удобство доступа	Низкое	Высокое

Дело здесь не только в измеримых показателях. Такие рейтинговые платформы позволяют поставщикам закрепить за собой публичный статус, оценивать предложения конкурентов, бороться за внимание потенциальных клиентов и продвигать свои услуги в едином цифровом пространстве. В некоторых чатах этот подход доведен до крайности: там проводят длительные конкурсы с призами для тех, кто удержался на вершине рейтинга шесть месяцев подряд.



Пример графика атаки на рейтинговой платформе

Пример отчета о проведенной атаке в Telegram-боте



Пример рейтинговой таблицы в Telegram-боте

За пределами DDoS

Как правило, DDoS-функциональность живет не изолированно. Инфраструктура для генерации трафика и знания, необходимые для обхода защиты, могут использоваться и для другой вредоносной активности. По данным нашего исследования, 43% поставщиков, чьи объявления мы нашли на теневых форумах, предлагали также смежные услуги.

Мы разделили их на две большие категории. Первая связана с повторным использованием имеющихся активов в других целях, то есть адаптацией инфраструктуры, вредоносных программ и инструментов для решения смежных задач. Вторая предполагает использование накопленных знаний и опыта для организации защиты, консультирования и обучения.

Активы

Массовые атаки

- подмена номера вызывающего абонента
- почтовый спам
- блокировка учетных записей и массовые жалобы
- внесение сайта в список запрещенных
- запросы на блокировку доменов

33%

Инструментарий

- ботнеты инфостилеров
- аренда VPS-серверов
- продажа скриптов или ботнетов
- продажа эксплойтов для DDoS-атак

38%

Передача опыта

- Сервисы защиты от DDoS-атак
- Обучающие курсы по DDoS-атакам

19%

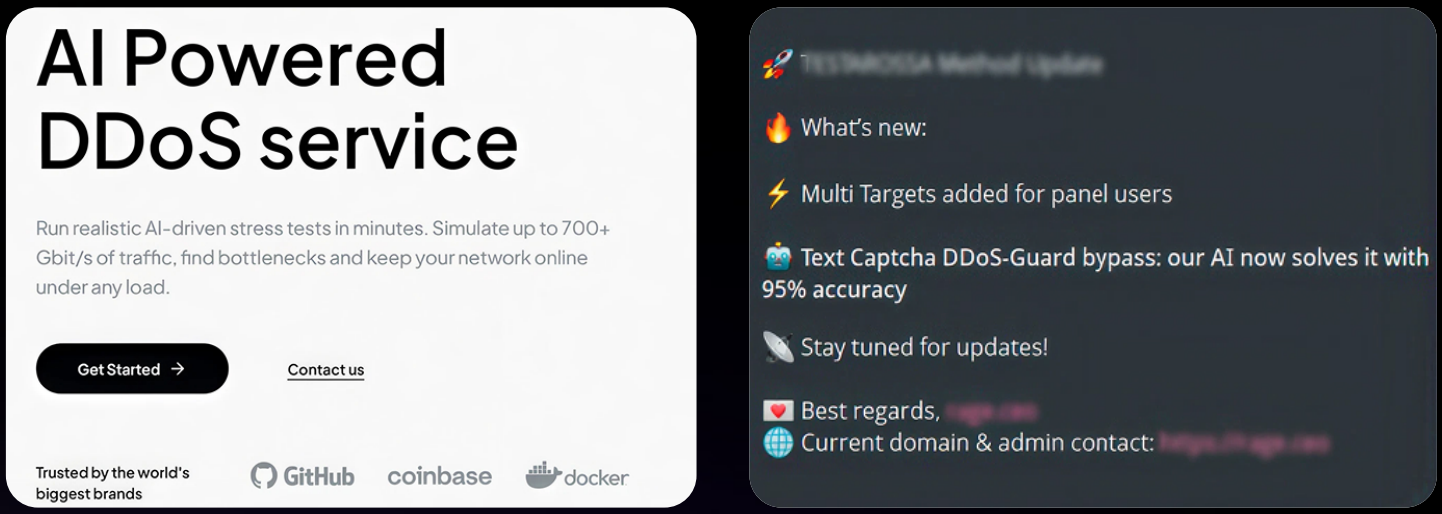
Некоторые из этих предложений, например, продажа скриптов, аренда VPS-сервера или сервисы защиты от DDoS-атак, близко связаны с услугами по организации DDoS-атак. Другие смежные услуги предоставляются на базе той же инфраструктуры или алгоритмов — от спам-кампаний до массовых жалоб и запросов на блокировку доменов.

Растущая мощь

Чтобы оставаться на плаву, поставщикам ресурсов приходится регулярно совершенствовать подходы к проведению атак. В рамках исследования мы выяснили, что они отдают предпочтение проприетарным DDoS-решениям и редко используют общедоступные инструменты. Несмотря на доступность скриптов с открытым исходным кодом, злоумышленники используют кастомизированные решения, которые позволяют проводить более разрушительные кампании и эффективнее обходить защиту от DDoS-атак.

В таких решениях применяются специализированные приемы увеличения трафика, продвинутые методы обработки запросов и адаптивные техники обхода защиты, затрудняющие обнаружение атак в потоке легитимного трафика. Некоторые участники рынка сообщали, что используют известные уязвимости к DoS-атакам и средства имитации нормального поведения браузера, чтобы оставаться незамеченными.

Конкурентное давление прослеживается в рекламных объявлениях — 33% злоумышленников прямо заявляли о наличии инструментов для обхода DDoS-защиты. Среди таких объявлений были обнаружены упоминания 32 ИБ вендоров, предоставляющих услуги защиты от DDoS-атак. На удивление, гораздо реже злоумышленники пытались привлечь внимание клиентов ИИ-технологиями для обхода CAPTCHA.



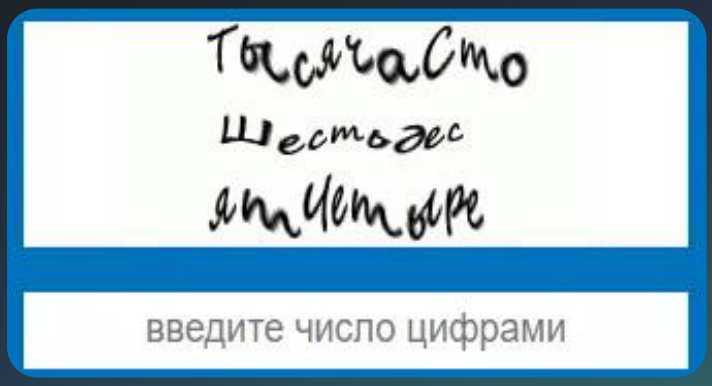
Примеры объявлений с указанием использования ИИ

Ограничения

Большинство поставщиков не указывали никаких ограничений по выбору цели. Однако небольшая часть из них все же установила четкие границы, указав возможные цели. В основном такие ограничения были вызваны техническими особенностями той или иной атаки, но в некоторых случаях они отражали индивидуальные предпочтения.

Мы разделили эти ограничения на несколько групп:

- Домены верхнего уровня: целевые ресурсы на доменах *.org, *.gov, *.edu и *.med
- Технически нецелесообразные задачи: атаки на домены *.r2.web и статические сайты, требующие несоизмеримо большого объема трафика
- Отдельные механизмы защиты от DDoS-атак: ресурсы с капчей на кириллице, которую ИИ-сервисы практически никогда не распознают правильно
- Отдельные категории сервисов: особенно игровые серверы и .onion-ресурсы
- Функциональность сервиса: например, крупные учреждения и банки



Примеры капчи на кириллице

Такие ограничения говорят о том, что, даже если задача участников рынка — дестабилизация, они не готовы атаковать все цели без разбора. Некоторые злоумышленники действуют прагматично и отказываются атаковать цель, если это слишком сложно или невыгодно.

При этом возможность выбора целей обычно не зависит от географического положения. Большинство поставщиков заявляют, что могут атаковать системы в любой точке мира.

Например, в приведенном объявлении из нашей выборки злоумышленник прямо пишет о глобальном охвате. Многочисленные прокси позволяют обходить механизмы геоблокирования, применяемые поставщиками DDoS-защиты.

Краткий обзор

Из отдельной вредоносной техники DDoS-атаки превратились в целую отрасль киберпреступной экономики.

Один из главных факторов роста этого рынка — достаточно низкий порог входа как для начинающих, так и для опытных злоумышленников. Сегодня DDoS-услуги распространяются через посредников, платформы-стрессеры и Telegram-ботов, которые набирают популярность с 2022 года.

Telegram-боты для DDoS-атак

- 27% атак по модели DDoS-as-a-Service используют исключительно Telegram-боты
- вместо сайтов все чаще используется интерфейс Telegram

DDoS-атаки проводят злоумышленники, имеющие самые разные цели: от хактивистов и операторов шифровальщиков до одиночек, ищущих легких денег.

С DDoS-атакой может столкнуться компания любого размера и из любой отрасли

Стоимость проведения атаки

$1–$30 000

С 2023 года наблюдается рост числа новых операторов, что свидетельствует о расширении рынка. Среди возможных причин такого роста — геополитическая напряженность, которая стимулирует хактивистов проводить больше атак, а также популярность стрессеров с открытым исходным кодом, снижающая порог входа в эту сферу.

Инфраструктура DDoS-атак расширяется за счет смежных видов киберпреступной деятельности: 43% операторов рекламируют сопутствующие услуги, например продажу DDoS-эксплойтов, скриптов и ботнетов, массовую отправку жалоб и спама, сервисы защиты от DDoS-атак и прочее. Рост конкуренции заставляет их постоянно искать новые технические возможности, в частности для обхода защиты, проведения специализированных кампаний и повышения мощности атак.

23% поставщиков рекламируют атаки на игровые сервера

36% поставщиков заявляют об атаках мощностью в несколько Тбит/с

33% поставщиков заявляют о возможности обхода защиты от DDoS

Злоумышленники все чаще используют ИИ-технологии для обхода капчи, а также эмуляцию браузеров.

Сейчас рынок DDoS-атак представляет собой устойчивую киберпреступную экосистему, с различными моделями подписки, развитыми средствами автоматизации и глобальной доступностью, действующую при поддержке непрерывно эволюционирующих технологий.

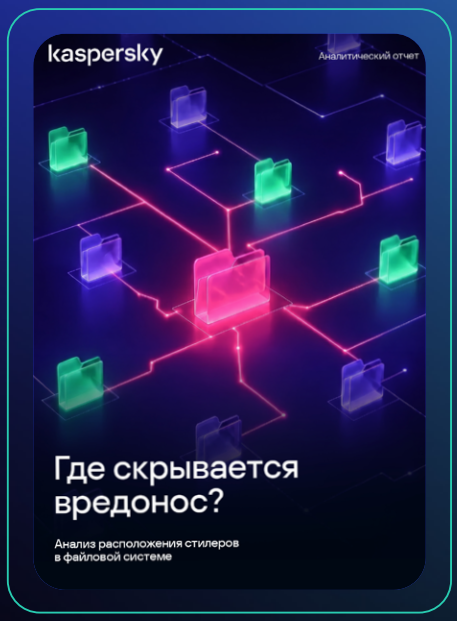
Рекомендации

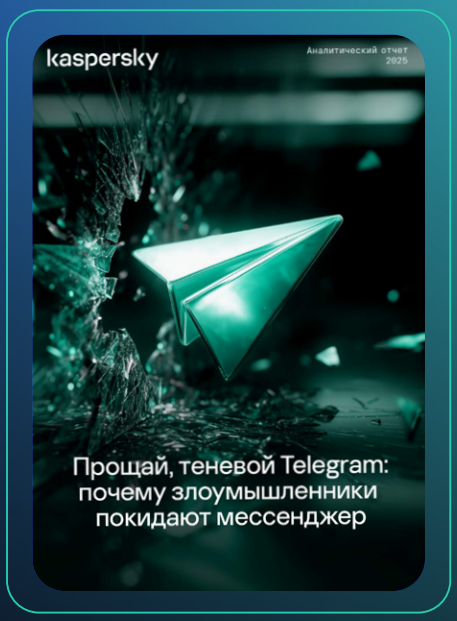
Сложность внедрения

Проводите контролируемые симуляции DDoS-атак	Регулярно проводите стресс-тесты или используйте методы хаос-инженерии для проверки уровня защиты – сейчас, когда DDoS-сервисы широко доступны и стоят недорого, шансы столкнуться с атакой всегда высоки
Разверните многоуровневую защиту от DDoS-атак	Современные атаки не только забивают каналы связи на уровнях L3/L4, но и перегружают вычислительные ресурсы узлов инфраструктуры — процессоры и память — изощрёнными L7-запросами.
Отслеживайте аналитику по ботнетам и добавляйте новые IoC в системы обнаружения	Используйте доступные данные об инфраструктурах, индикаторах и злоумышленниках, чтобы быстрее обнаруживать и блокировать вредоносную активность
Автоматизируйте процессы обнаружения и реагирования	Автоматизированные решения позволяют быстрее нейтрализовать стремительные DDoS-атаки, генерирующие огромные объемы телеметрии
Разверните CDN и обратный прокси	Для противодействия DDoS-атакам важно распределить сетевой трафик, скрыть исходные серверы и устранить единые точки отказа
Изолируйте критически важные сервисы и включите динамическое масштабирование	Изолируйте критически важные процессы от остальной инфраструктуры и оперативно масштабируйте их при необходимости

Крупные компании

Небольшие
и средние компании





С остальными отчетами можно ознакомиться на сайте

Подробнее

kaspersky

www.kaspersky.com