Кибербезопасность крупного бизнеса

KASPERSKY lab

Kaspersky DDoS Protection

Защита вашей компании от финансового и репутационного ущерба

www.kaspersky.ru

#ИстиннаяБезопасность

Kaspersky DDoS Protection

DDoS-атака (распределенная атака, приводящая к отказу в обслуживании) – один из самых распространенных приемов киберпреступников. Цель атаки: нарушить доступ обычных пользователей к информационным системам (например, веб-сайтам и базам данных). Мотивы DDoS-атак бывают разными – от киберхулиганства до нечестной конкуренции и даже вымогательства. В качестве цели злоумышленники могут выбрать любой доступный из интернета ресурс, будь то сервер, сетевое устройство или неиспользуемый адрес в подсети жертвы.

Сценарии DDoS-атаки

Наиболее распространены два сценария DDoS-атаки: запросы от большого количества ботов напрямую к атакуемому ресурсу и запросы, усиленные через публично доступные серверы с уязвимым программным обеспечением.

В первом сценарии киберпреступники превращают множество компьютеров (серверов, устройств IoT и т. д.) в удаленно контролируемые «зомби» (боты), которые по команде одновременно отправляют на ресурс жертвы огромное количество разнообразных запросов — проводят «распределенную атаку».

Во втором сценарии, то есть при атаке с усилением, для организации атаки злоумышленники используют серверы, арендованные в центре обработки данных, а для усиления, как правило, используют публичные серверы с уязвимым программным обеспечением. Сейчас распространены два варианта усиления – через серверы доменных имен (DNS) или синхронизации времени (NTP).
В некоторых случаях вместо уязвимых серверов киберпреступники задействуют сайты на платформе WordPress CMS (чаще всего блоги) с включенной функцией Pingback. Атака усиливается путем спуфинга (подмены) обратных IP-адресов и отправки на сервер или веб-сайт короткого запроса, который требует значительно более объемного ответа. Полученный ответ направляется на подмененный IP-адрес, принадлежащий жертве.

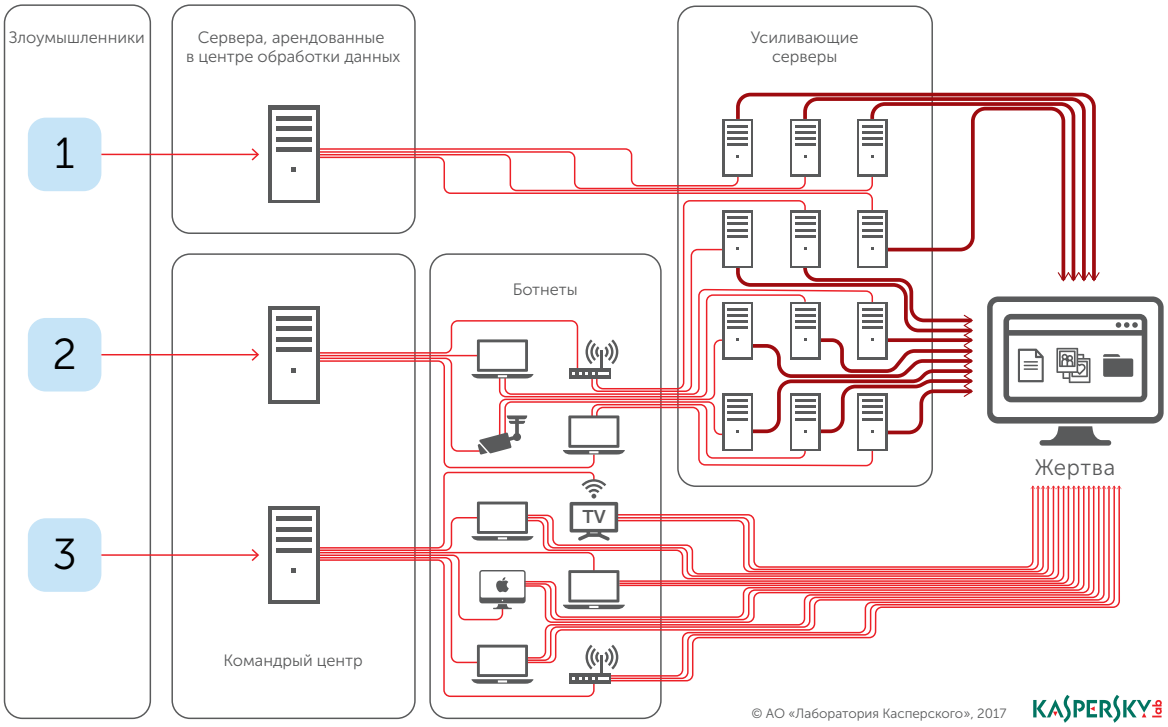

Рисунок 1. Схема самых популярных сценариев DDoS-атак

«Прайс-лист» услуг по проведению DDoS-атак:

- За сайт, сервер на Shared-хостинге — от $50
- За сайт, сервер на VPS-сервере — от $75
- За сайт, сервер на VDS-сервере — от $100
- За сайт, сервер, пользующийся услугами анти-DDoS — от $400
- Блокировка домена (сайта) на уровне регистратора — от $1000
- Флуд телефона (сотовый, стандартный) — от $75

(информация скопирована с одного из подпольных ресурсов)

Вероятные потери

Опасность усугубляется из-за широкой распространенности вредоносных программ, уязвимых устройств IoT и серверов, пригодных для создания ботнетов и организации атак с усилением. Их так много, что DDoS-атаку может запустить практически каждый. Киберпреступники рекламируют свои услуги, обещая всем желающим сделать выбранный сайт недоступным всего за 50 долл. США в сутки.

Низкая стоимость и сравнительная простота организации атак повышают и спрос, и предложение: сегодня заказать атаку — легко и незатратно, а обрушивать сайты – выгодно. Оплата обычно производится в криптовалюте, поэтому незаконную сделку почти невозможно отследить по финансовым потокам.

При таких расценках и простоте организации жертвой DDoS-атаки может стать практически любая организация, не только крупная и известная. Конечно, вывести из строя веб-ресурсы огромной корпорации гораздо сложнее, но в случае успеха ущерб от простоя будет значительно больше. Помимо прямых убытков из-за упущенной выгоды (например, интернет-продаж), жертвы DDoS-атак могут потерять деньги на штрафах за невыполнение обязательств и понести значительные расходы на дополнительные меры безопасности. Нередко при этом страдает и репутация компании, что приводит к потере существующих и потенциальных клиентов.

Объем ущерба зависит от размера компании, отраслевого сегмента, который она обслуживает, и типа выведенного из строя интернет-сервиса. По подсчетам «Лаборатории Касперского» и аналитической компании B2B International, в среднем убыток от DDoS-атаки составляет около 106 000 долл. США для небольших компаний и более 1,6 млн для крупных корпораций. В отдельных случаях DDoS-атаки обходились компаниям в 160 млн долл. США.

Методы противодействия DDoS-атакам

Учитывая высокую вероятность финансовых и репутационных потерь, бизнесу требуются надежные средства безопасности. Существует три основных метода защиты от DDoS-атак:

- установить специализированные решения в IT-инфраструктуре компании
- обратиться за помощью к интернет-провайдеру
- купить сервис по защите от DDoS-атак

В основе всех этих методов лежит один и тот же принцип – фильтрация «мусорного» (то есть созданного киберпреступниками) трафика. Однако, несмотря на принципиальную схожесть, эти подходы имеют разную эффективность.

Установка фильтрующего оборудования или сетевого экрана на стороне клиента считается наименее эффективной. Во-первых, для регулярного обслуживания оборудования и коррекции его работы требуется специально обученный персонал, а следовательно, нужны дополнительные вложения и ресурсы. Во-вторых, этот способ защищает от атак только сами сервисы, но не может помешать блокировке интернет-канала. Работающий сайт бесполезен, если к нему нельзя получить доступ из интернета, а перегрузить интернет-канал жертвы с помощью DDoS-атак с усилением или просто большого количества IoT-ботов совсем несложно. В-третьих, встроенное оборудование неэффективно против «умных» DDoS-атак, которые трудно отфильтровать стандартными методами.

Фильтрация трафика интернет-провайдером более надежна благодаря широкому интернет-каналу, который гораздо сложнее вывести из строя. Однако интернет-провайдеры не специализируются на услугах безопасности, а потому фильтруют только самый очевидный мусорный трафик, пропуская более сложные атаки – например, те, которые используют шифрование (HTTPS) или имитируют поведение пользователей. У провайдеров просто нет должных знаний и опыта для тщательного анализа подобной атаки и быстрой реакции на нее. Наконец, такой тип защиты укрепляет зависимость клиента от конкретного провайдера и может вызвать трудности, если потребуется использовать резервный канал связи или сменить провайдера.

Таким образом, самый надежный способ полностью нейтрализовать DDoS-атаки любого типа — обратиться к специалистам по защите от DDoS-атак, которые располагают собственными центрами очистки и пользуются различными методами фильтрации трафика.

Kaspersky DDoS Protection

Благодаря сочетанию собственных уникальных разработок, передовой аналитики и обширной экспертизы решение Kaspersky DDoS Protection способно защитить ваш бизнес от всех видов DDoS-атак.

Передовые технологии и богатый опыт

Первый и важнейший компонент решения Kaspersky DDoS Protection – **эксперты**. Уже 20 лет «Лаборатория Касперского» успешно противостоит широкому спектру онлайн-угроз. За это время наши аналитики приобрели уникальный опыт и знания, в том числе о механизмах проведения DDoS-атак. Эксперты «Лаборатории Касперского» постоянно следят за ландшафтом угроз, изучают новые методы кибератак и совершенствуют средства защиты от них. Благодаря этому решение способно обнаруживать DDoS-атаки сразу же после их запуска, до перегрузки целевого веб-ресурса. Kaspersky DDoS Protection поддерживает изменение правил фильтрации непосредственно во время атаки, что позволяет эффективно противостоять даже самому изощренному воздействию.

Второй компонент – **сенсор**, который устанавливается либо в облаке Kaspersky DDoS Protection, либо в инфраструктуре клиента. Сенсор анализирует трафик, поступающий на ресурс клиента: типы используемых протоколов, количество переданных байтов и пакетов данных, поведение посетителей на сайте клиента и другие метаданные (то есть сведения об отправленных данных). На основе этой информации для каждого клиента создается статистический профиль, который отражает типичную картину обмена информацией с учетом изменений в зависимости от времени суток и дня недели. Заметные отклонения трафика от статистического профиля могут быть признаком атаки.

И наконец, последний уровень защиты – **система аналитики DDoS**. Она создана для перехвата и анализа команд, посылаемых ботам командными серверами, и помогает экспертам «Лаборатории Касперского» собрать важную информацию о DDoS-атаках, которая может пригодиться в дальнейшем.

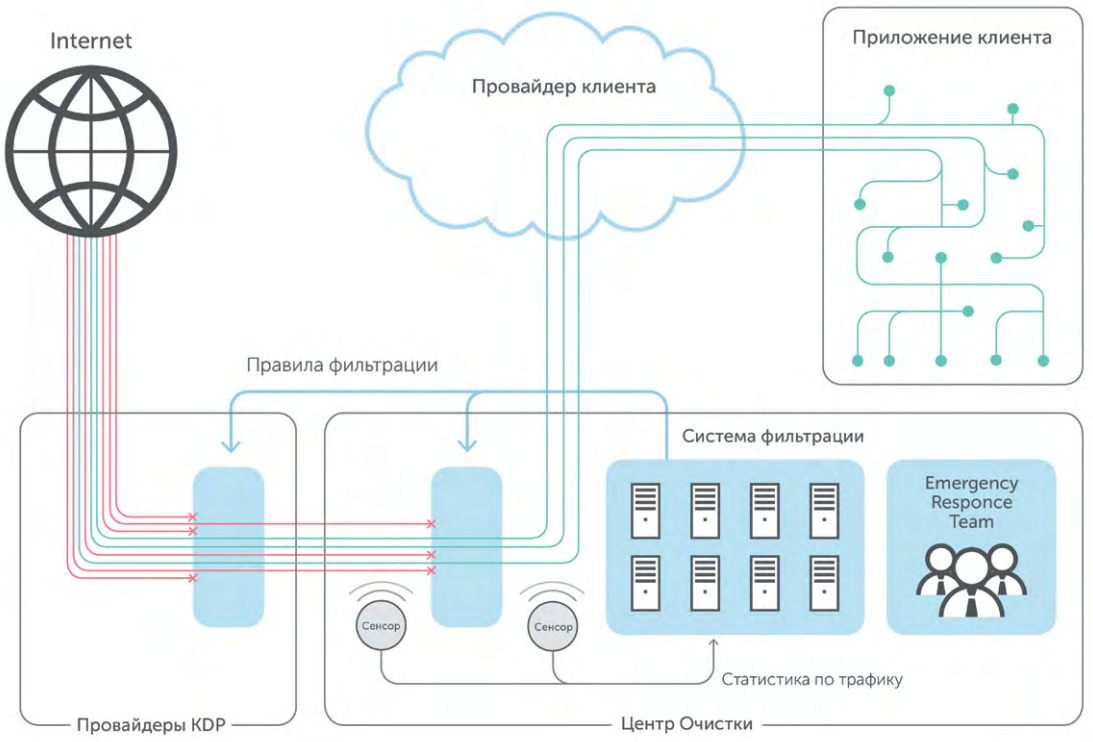

Рисунок 2. Схема работы Kaspersky DDoS Protection

Принцип работы

Перенаправление и доставка трафика

В зависимости от тарифа решение реализует две модели фильтрации трафика: перенаправление по запросу, когда трафик поступает в центры очистки только в случае атаки, и постоянное перенаправление – в этом случае трафик проходит через центры очистки постоянно.

Само перенаправление можно включить одним из двух способов: либо анонсировав подсеть клиента по протоколу динамической маршрутизации BGP, либо изменив DNS-запись на адрес центра очистки. Для первого варианта клиенту необходимы автономная система (AS) и независимое от провайдера адресное пространство – например, блок IP-адресов, предоставленный региональным интернет-регистратором.

Существует несколько вариантов доставки очищенного от трафика до площадки клиента. Самый простой и быстрый – с помощью обратного proxy или методами маршрутизации (по виртуальному туннелю GRE или выделенной линии между центром очистки и IT-инфраструктурой клиента).

Методы перенаправления трафика в центр очистки и доставки очищенного трафика клиенту, а также место установки сенсора зависят от выбранного клиентом типа защиты Kaspersky DDoS Protection.

Тип защиты	Перенаправление трафика	Доставка трафика	Место установки сенсора
Kaspersky DDoS Protection Control	OnDemand; BGP-маршрутизация	Маршрутизация	На площадке заказчика
Kaspersky DDoS Protection Connect	AlwaysOn; изменение DNS-записи	Проксирование, маршрутизация	В облаке
Kaspersky DDoS Protection Connect+	AlwaysOn; BGP-маршрутизация	Маршрутизация	В облаке

Рисунок 3. Тарифы Kaspersky DDoS Protection

Kaspersky DDoS Protection Control

При выборе этого варианта трафик защищаемого ресурса перенаправляется в центры очистки только в случае атаки, для чего сенсор необходимо установить в IT-инфраструктуре клиента. Сенсор анализирует трафик, не передавая его в центры очистки.

В случае отклонения профиля трафика от нормального значения, информация передается дежурному эксперту «Лаборатории Касперского». Если факт атаки подтверждается, клиент незамедлительно получает уведомление об этом, после чего производится перенаправление трафика на центры очистки. После отражения атаки трафик снова идет по обычному маршруту.

Перенаправление трафика начинается с анонсирования подсети клиента по протоколу динамической маршрутизации BGP. Очищенный трафик возвращается к защищаемым ресурсам по виртуальному туннелю или по выделенной линии между центром очистки и площадкой клиента.

Такой метод удобен крупным компаниям, которые не хотят, чтобы их трафик постоянно проходил через центры очистки, однако требует дополнительных затрат: во-первых, на установку в корпоративной сети серверов с работающими сенсорами; во-вторых, на круглосуточное обслуживание этих серверов квалифицированными сотрудниками, способными переключить трафик на центры очистки «Лаборатории Касперского» в случае атаки.

Kaspersky DDoS Protection Connect

В этом варианте сенсор является частью инфраструктуры «Лаборатории Касперского» и трафик клиента проходит через центры очистки постоянно. Поскольку все компоненты защиты размещены в облаке Kaspersky DDoS Protection, сервис полностью управляется «Лабораторией Касперского» и предусматривает круглосуточный мониторинг защищаемых ресурсов специалистами экспертной группы KDP. При этом ни сенсор, ни эксперты «Лаборатории Касперского» не могут просматривать, редактировать или копировать содержимое трафика.

В случае атаки клиент заменяет IP-адрес в A-записи DNS на IP-адрес, назначенный центром очистки, после чего весь трафик, поступающий на адрес клиента, начинает постоянно проходить через центр очистки. Однако, чтобы избежать организации атаки на оригинальный IP-адрес защищаемого ресурса, необходимо, чтобы провайдер заблокировал весь поступающий на него трафик. Очищенный трафик может поступать клиенту по протоколу Generic Routing Encapsulation (GRE) или через обратный прокси-сервер.

Использование данного метода защиты удобно компаниям с небольшим количеством онлайн ресурсов, у которых нет собственной автономной системы (AS) и которым важна простота организации и эксплуатации услуги по защите от DDoS-атак.

Kaspersky DDoS Protection Connect+

При использовании Kaspersky DDoS Protection Connect+ сенсор также является частью инфраструктуры «Лаборатории Касперского», а трафик защищаемого ресурса постоянно проходит через центры очистки. Разница в том, что переключение трафика начинается с анонсирования подсети клиента по протоколу динамической маршрутизации BGP.

Вариант Connect+ предназначен для крупных компаний, которые не могут позволить себе ни минуты простоя. DDoS-защита необходима им постоянно, однако большое количество корпоративных IP-адресов не позволяет воспользоваться DNS-заменой.

Преимущества подхода «Лаборатории Касперского»

- 20 лет опыта анализа киберугроз и борьбы с ними по всему миру.
- Гибкие возможности организации защиты: Kaspersky DDoS Protection Control, Connect и Connect+ подходят разным типам компаний с разными политиками безопасности и сетевой инфраструктурой.
- Правила фильтрации разрабатываются индивидуально для каждого клиента в зависимости от специфики его сервисов.
- Команда экспертов KDP наблюдает за всеми процессами и при необходимости корректирует правила фильтрации, а также круглосуточно оказывает услуги поддержки.
- В случае атаки защитные меры можно применить практически мгновенно – даже если ваша компания прежде не являлась клиентом «Лаборатории Касперского».
- Уникальные патентованные разработки позволяют отражать даже самые сложные атаки.
- Партнерство с интернет-провайдерами помогает фильтровать трафик при любом типе DDoS-атаки, включая объемные атаки, сложные атаки, атаки IoT-ботнетов и т. п.
- «Лаборатория Касперского» имеет богатый опыт применения Kaspersky DDoS Protection в России, где решение успешно защищает таких клиентов, как Министерство финансов Российской Федерации, Росалкогольрегулирование, Министерство связи республики Татарстан, ВТБ24, Russia Today и многие другие организации – в частности, государственные учреждения, финансовые организации, средства массовой информации, онлайн-магазины.

Процедура очистки

Как только эксперты «Лаборатории Касперского» определяют тип атаки, применяются правила фильтрации, специфичные для конкретного сценария и защищаемого ресурса. Часть правил, касающихся фильтрации самых «грубых» атак, передается в инфраструктуру провайдера KDP и применяется на принадлежащих провайдеру маршрутизаторах. Оставшийся трафик поступает на серверы центра очистки, где фильтруется по ряду признаков, таких как черный список IP-адресов, географические данные, информация из заголовков HTTP, корректность протоколов и обмена SYN-пакетами и т. д.

При этом сенсор продолжает анализировать поступающий к клиенту трафик. Если в нем еще остаются признаки DDoS-атаки, сенсор уведомляет центр очистки и трафик подвергается более глубокой поведенческой и сигнатурной фильтрации. Благодаря этим методам вредоносный трафик можно очищать на основании сигнатур, то есть полностью блокировать определенный тип трафика или все IP-адреса, отвечающие заданным критериям. Таким образом отражаются даже самые изощренные атаки, включая HTTP/HTTPS, при которых имитируются обычные действия пользователей – только «пользователи» ведут себя хаотично и работают неестественно быстро, а запросы обычно поступают одновременно с большого количества ботов. Если злоумышленники используют шифрование (HTTPS), выявить атаку и отразить атаку можно как с передачей ключа в центр очистки, так и без.

Если атака организованна с использованием нескольких методов или злоумышленники меняют способы в течении атаки, экспертная группа KDP может «на лету» изменять правила фильтрации или алгоритм обработки трафика, добиваясь полноценного отражения атаки. Клиент также имеет возможность следить за работой решения и состоянием трафика через клиентский портал.

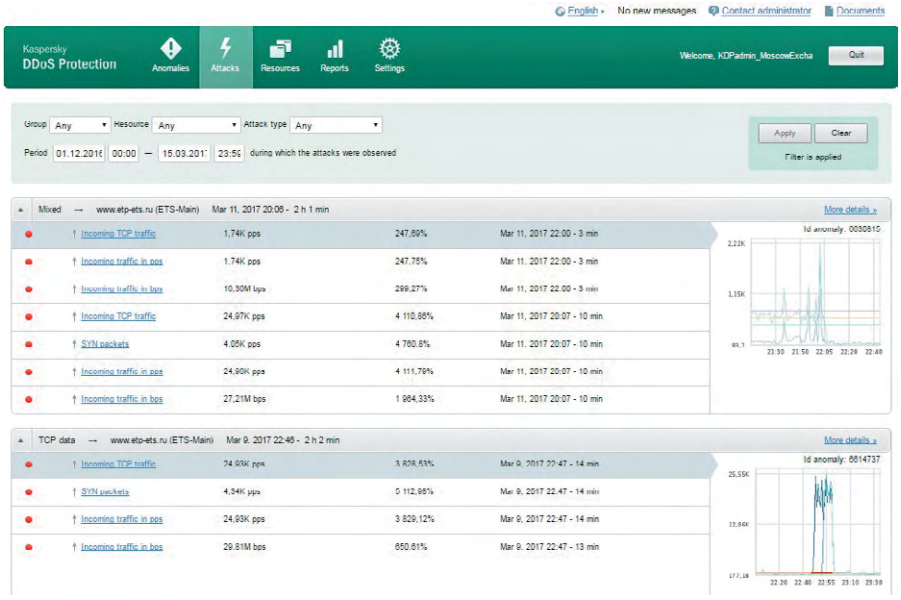

Рисунок 4. Клиентский портал

После окончания атаки клиент получает подробный отчет об инциденте, включая детальное описание хода географического распределения источников атаки, а также графики с динамикой измеряемых параметров.

www.kaspersky.ru

#ИстиннаяБезопасность