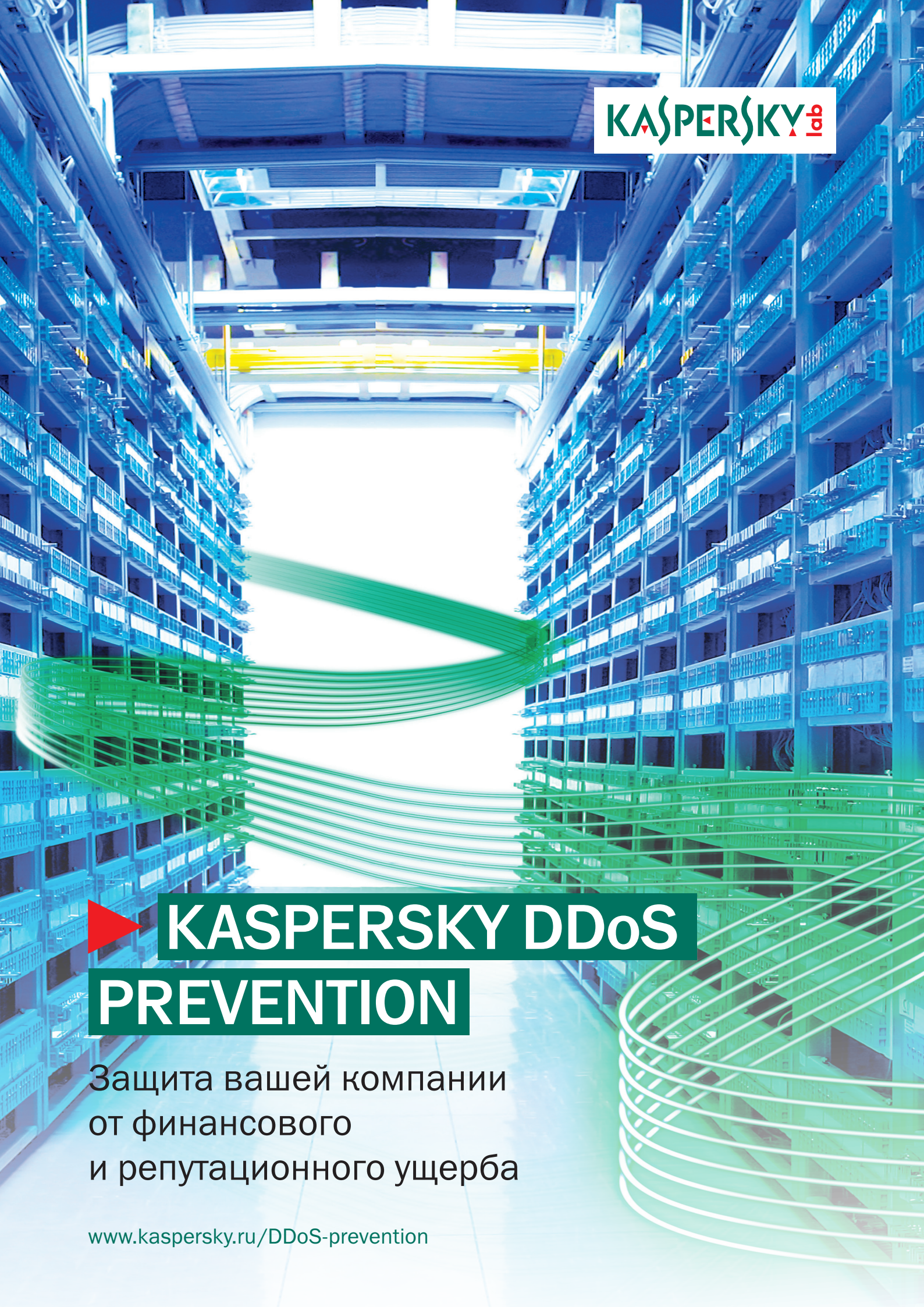

KASPERSKY lab

KASPERSKY DDoS PREVENTION

Защита вашей компании
от финансового
и репутационного ущерба

www.kaspersky.ru/DDoS-prevention

DDoS-атака (Distributed-Denial-of-Service) — один из самых распространенных приемов киберпреступников. Ее цель — довести информационную систему предприятия-жертвы (например, веб-сайт или базу данных) до такого состояния, при котором легитимные пользователи не могут получить к ней доступ. Мотивы злоумышленников могут быть разными — хулиганство, терроризм, нелегальная конкурентная борьба или даже вымогательство.

Современная DDoS-индустрия — это многоуровневая структура. В нее входят: заказчики атак; создатели ботнетов, сдающие их в аренду; посредники, занимающиеся организацией атаки и общением с заказчиками, а также лица, ответственные за монетизацию услуг. В качестве мишени может быть выбран любой доступный из Интернета узел — сервер, обслуживающий какой-либо сервис, сетевое устройство или неиспользуемый адрес в подсети жертвы.

Наиболее распространенных сценариев DDoS-атак два: запросы от большого количества ботов напрямую к атакуемому ресурсу (сценарий 1 на рис.1) или запросы от ботов, усиленные с использованием публично доступных серверов с уязвимым программным обеспечением (сценарий 2А на рис.1). В первом случае злоумышленники превращают множество компьютеров в удаленно контролируемые «зомби» (боты), которые затем одновременно по команде хозяина ботнета отправляют на интернет-ресурс жертвы какие-либо запросы (осуществляют «распределенную атаку»). Иногда вместо ботнета используется завербованная хакерами группа пользователей, снабженная специальными программами для осуществления DDoS-атаки.

При втором сценарии, то есть при усиленной атаке, вместо ботов также могут быть использованы арендованные в дата-центре серверы (сценарий 2Б на рис.1), а для усиления, как правило, применяются публичные серверы с уязвимым ПО. В данный момент распространены два варианта усиления — через серверы системы доменных имен (DNS) или серверы синхронизации времени (NTP). Усиление атаки производится за счет подмены обратных IP-адресов и отправки на сервер короткого запроса, который требует гораздо более объемного ответа. Полученный ответ отсылается на подменный IP-адрес, принадлежащий жертве.

Сценарии DDoS-атак

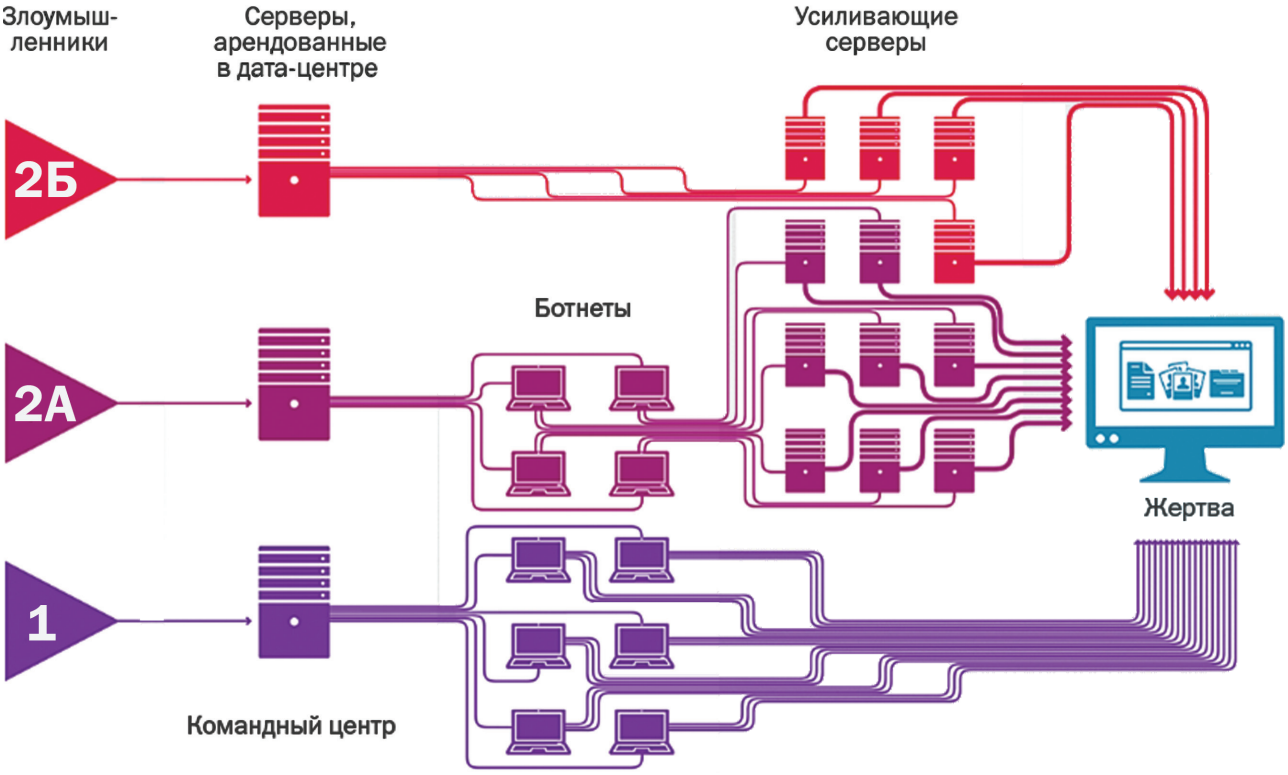

Рисунок 1. Схема наиболее распространенных сценариев проведения DDoS-атак

Ситуация усугубляется тем, что в связи с широким распространением вредоносного ПО и ростом количества активных ботнетов, создаваемых разнообразными хакерскими группами, заказать такую атаку сегодня может практически каждый. Киберпреступники рекламируют свои услуги, обещая всем желающим сделать выбранный сайт недоступным всего за $50 в сутки. Причем оплата, как правило, производится при помощи криптовалюты, так что вычислить злоумышленников по финансовым потокам практически невозможно.

При таких расценках и доступности услуги жертвой DDoS-атаки может стать сайт не только крупной и известной организации, но и практически любой ресурс. Конечно, интернет-ресурсам крупных компаний навредить гораздо сложнее, но и ущерб от простоя в этом случае будет заметно больше. Ведь помимо прямых убытков от упущенных бизнес-возможностей (например, электронных продаж) компании могут потерять деньги на штрафах за невыполнение обязательств, а также потратить значительные средства на принятие экстренных мер по защите от атаки. Не говоря уже о подрыве репутации и, как следствие, потере существующих и потенциальных клиентов.

Объем потерь зависит от размера бизнеса, индустрии и типа атакованного интернет-ресурса. По подсчетам аналитической компании IDC, в среднем часовая недоступность интернет-сервиса обходится компаниям в сумму от 10 до 50 тыс. долларов.

Методы противодействия DDoS-атакам

На рынке немало компаний, предлагающих услуги по защите от DDoS-атак. Одни из них предлагают установку программно-аппаратных комплексов в ИТ-инфраструктуре клиента, другие используют возможности провайдера интернет-услуг, а третьи перенаправляют трафик клиента через специальные центры очистки. Однако основной принцип у всех один — фильтрация «мусорного», то есть сгенерированного злоумышленниками, трафика.

Наименее эффективным методом считается установка фильтрующего оборудования на стороне клиента. Во-первых, это требует наличия в защищаемой компании специально обученного персонала, который будет обслуживать и корректировать работу оборудования, что влечет за собой дополнительные расходы. Во-вторых, такой метод эффективен только против атак непосредственно на ресурс, и никак не сможет помешать атакам, «забивающим» интернет-канал клиента. Работающий ресурс бесполезен, если к нему нет доступа из Сети, а перегрузить интернет-канал жертвы с помощью технологии усиления DDoS-атаки достаточно просто.

Фильтрация трафика провайдером более надежна благодаря наличию широкого интернет-канала, который гораздо сложнее вывести из строя. В то же время, поскольку провайдеры не специализируются на услугах по защите, они фильтруют только самый очевидный мусорный трафик, упуская из внимания более изощренные атаки. Для тщательного анализа атаки и оперативного принятия контрмер необходимы соответствующие знания и опыт. Кроме того, такой тип защиты привязывает клиента к конкретному провайдеру, создавая сложности в случае необходимости использования резервного канала связи или при смене провайдера.

Таким образом, наиболее эффективным решением для нейтрализации DDoS-атак следует считать специализированные центры очистки, комбинирующие различные методы фильтрации трафика.

Kaspersky DDoS Prevention

Kaspersky DDoS Prevention — это решение для защиты от любых типов DDoS-атак, представляющее собой распределенную инфраструктуру центров очистки данных. Решение сочетает в себе различные методы: это и фильтрация трафика на стороне провайдера, и установка в инфраструктуре заказчика удаленно контролируемого аппаратно-программного комплекса для анализа трафика, и использование специализированных центров очистки с гибко настраиваемыми «фильтрами». Работа решения постоянно контролируется экспертами «Лаборатории Касперского», что позволяет в кратчайшие сроки определить начало атаки и в случае необходимости внести коррективы в работу фильтров.

Схема работы Kaspersky DDoS Prevention

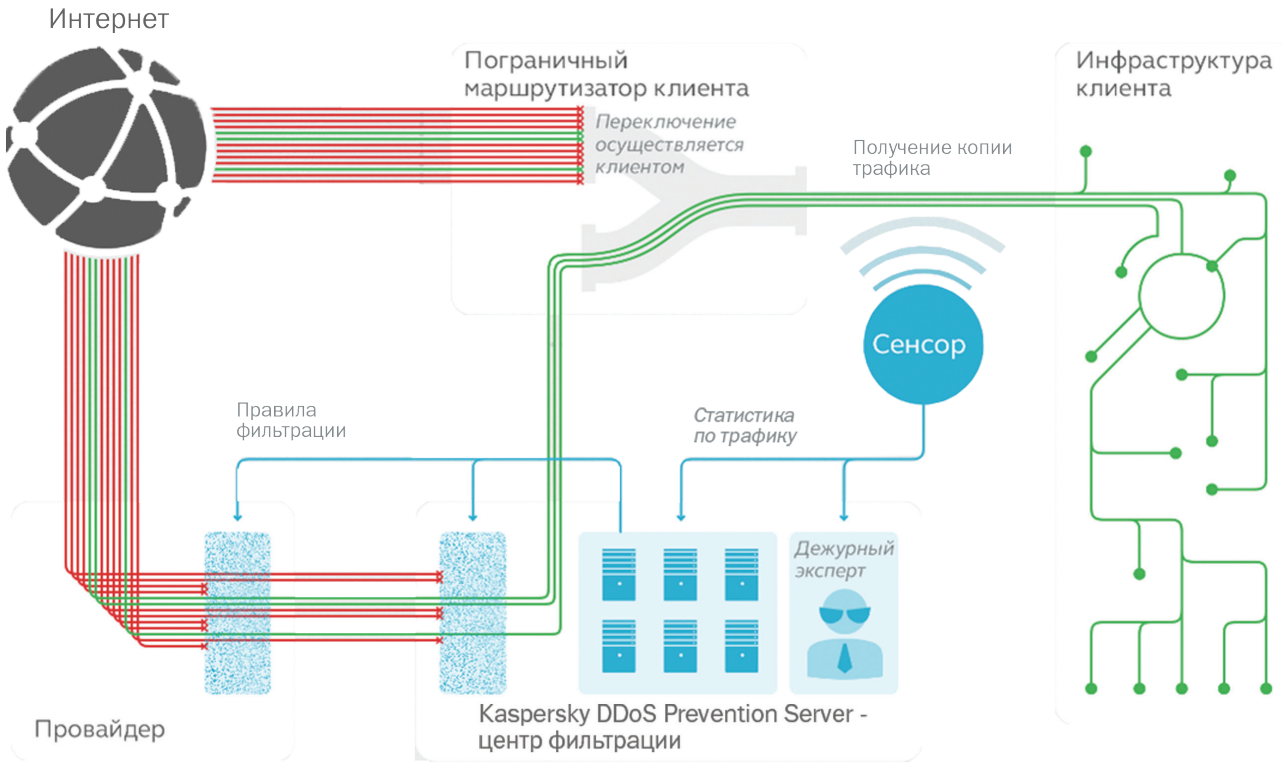

Рисунок 2. Схема работы Kaspersky DDoS Prevention

Наш арсенал

«Лаборатория Касперского» уже не первое десятилетие эффективно борется с различными онлайн-угрозами. За это время аналитики компании приобрели уникальные знания, в том числе о механизмах, используемых киберпреступниками для проведения DDoS-атак. Эксперты «Лаборатории Касперского» постоянно следят за ситуацией в интернете, изучают новые методы кибератак и совершенствуют средства защиты от них. Благодаря этому, в частности, существует возможность обнаружить атаку на самых ранних стадиях, когда в бот-сети только начинают поступать команды на проведение атаки.

Важный элемент решения Kaspersky DDoS Prevention — сенсор, устанавливаемый в непосредственной близости от информационной инфраструктуры клиента. Сенсор представляет собой программное обеспечение, работающее на сервере стандартной архитектуры x86 под управлением операционной системы Ubuntu. Он анализирует типы применяемых протоколов, количество переданных байтов и пакетов, поведение пользователей на сайте и другие метаданные (сведения о передаваемых данных), не перенаправляя трафик и не изменяя его, а также не изучая его содержимое. Статистика затем передается в облачную инфраструктуру Kaspersky DDoS Prevention, где на основе собранных метаданных создаются статистические «профили» для каждого из клиентов. Эти профили отражают типичную для клиента картину обмена информацией, с учетом изменений в зависимости от времени суток и дня недели. В дальнейшем, при анализе трафика, отличие имеющейся картины от статистического профиля служит индикатором возможной атаки.

Ключевой элемент Kaspersky DDoS Prevention — центры очистки, подключенные к крупнейшим интернет-магистралям — в Москве, Франкфурте, Амстердаме и т.д. В каждом регионе «Лаборатория Касперского» одновременно использует несколько центров, чтобы иметь возможность разделить или перенаправить трафик, нуждающийся в очистке. Центры очистки объединены в облачную информационную инфраструктуру, но при этом проходящий через них трафик остается в пределах соответствующего региона (например, трафик клиентов в Российской Федерации не покидает Россию, а трафик европейских клиентов — территорию Европы).

Другим ключевым механизмом борьбы с DDoS-трафиком является его фильтрация на стороне провайдера. При этом провайдер не просто предоставляет канал доступа в интернет, но и состоит с «Лабораторией Касперского» в технологическом партнерстве, благодаря чему Kaspersky DDoS Prevention осуществляет фильтрацию очевидного мусорного трафика, который генерируется в ходе большинства DDoS-атак, как можно ближе к его источникам. Это препятствует слиянию DDoS-потоков в единую мощную атаку и снижает нагрузку на центры очистки, в которых фильтруется более сложный мусорный трафик.

Инструменты перенаправления трафика

Для эффективной работы защитного решения необходимо в первую очередь организовать канал связи между центрами очистки и информационной инфраструктурой клиента. В решении Kaspersky DDoS Prevention эти каналы функционируют по протоколу Generic Routing Encapsulation и служат для создания виртуального туннеля между центром очистки и сетевым оборудованием клиента, по которому осуществляется доставка последнему очищенного трафика.

Само переключение может быть произведено двумя методами — путем анонсирования подсети заказчика по протоколу динамической маршрутизации BGP или путем изменения DNS-записи на адрес центра очистки. Первый метод предпочтительнее, поскольку позволяет перенаправить трафик гораздо быстрее, а также дает возможность обеспечить защиту от атак, направленных напрямую на IP-адрес. Однако для применения BGP-маршрутизации необходимо, чтобы у клиента было независимое от провайдера адресное пространство — блок IP-адресов, предоставленных региональным интернет-регистратором.

По схеме переключения разница между BGP-маршрутизацией и изменением DNS-записи невелика. В первом случае BGP-маршрутизаторы клиента и центра очистки постоянно поддерживают связь через виртуальный туннель, а в случае атаки анонсируется новый маршрут к клиенту — через центр очистки. При использовании второго метода клиенту назначается IP-адрес из пула адресов центра очистки. 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, предварительно проходит через центр. Однако для того, чтобы избежать продолжения атаки на старый IP-адрес, необходимо чтобы провайдер заблокировал весь поступающий на него трафик, за исключением потока от центра очистки.

Как работает решение

В обычном режиме (в отсутствие атак) весь трафик из интернета поступает непосредственно к клиенту. В некоторых случаях аналитики «Лаборатории Касперского» фиксируют появление в интернете команд на проведение атаки до ее начала и немедленно информируют клиента — тогда защиту можно включить превентивно. В противном случае защитные мероприятия начинаются при поступлении сигнала с сенсора. Сигнал об отклонении поступающего к клиенту трафика от статистического профиля поступает дежурному DDoS-эксперту «Лаборатории Касперского». Если факт атаки подтверждается, клиент извещается о ее начале и должен отдать приказ о переключении своего трафика на центры очистки (в некоторых случаях, по договоренности с клиентом, переключение происходит автоматически).

Как только технологии «Лаборатории Касперского» определяют тип атаки, применяются специфические для этого типа и для конкретного ресурса правила очистки. Часть правил, касающихся фильтрации самых грубых атак, передается в инфраструктуру провайдера и применяется на принадлежащих провайдеру маршрутизаторах. Оставшийся трафик поступает на серверы центра очистки, где производится фильтрация по ряду признаков — например, по черным спискам IP-адресов, по географическому признаку, по статистическим критериям, по информации из HTTP-заголовков; производится проверка корректности обмена SYN-пакетами и корректности протокола и т.д.

При этом сенсор продолжает анализировать поступающий к клиенту трафик. Если он все еще содержит признаки DDoS-атаки, сенсор сообщает об этом в центр очистки, и трафик подвергается более глубокой поведенческой и сигнатурной фильтрации. Эти методы позволяют фильтровать мусорный трафик на основании сигнатур, то есть полностью блокировать определенный тип трафика или IP-адреса, отвечающие определенным критериям. Таким образом нейтрализуются даже самые изощренные атаки, в частности http-flood — атака, при которой имитируются обычные действия пользователя на сайте, но совершаются они хаотично, неестественно быстро и одновременно с большого количества зомби-машин (ботов).

Эксперты «Лаборатории Касперского» следят за ситуацией через специальный интерфейс. Если атака оказывается нетипичной или сложной, эксперт может вмешаться, чтобы изменить правила фильтрации. Клиент также имеет возможность следить за работой решения и состоянием трафика через специальный портал.

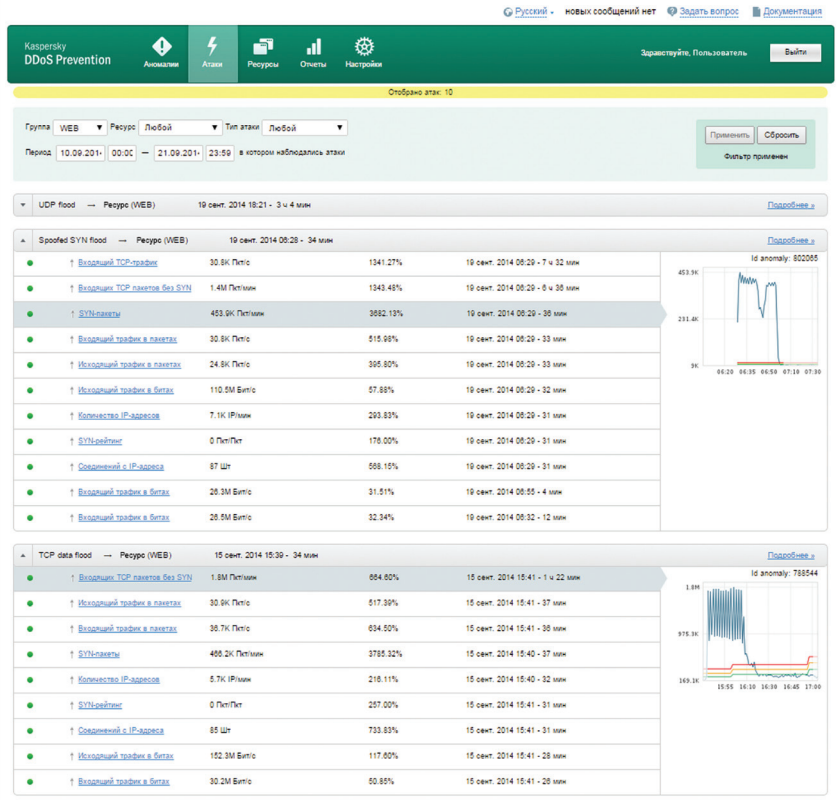

Рисунок 3. Клиентский портал

После завершения атаки трафик вновь перенаправляется на серверы клиента, Kaspersky DDoS Prevention переключается в режим ожидания, а клиенту предоставляется подробный отчет об имевшем место инциденте с детальным описанием хода атаки, графиками, отражающими динамику трафика, и географическим распределением источников атаки.

Преимущества подхода «Лаборатории Касперского»

- Благодаря переключению трафика только на время атаки, а также фильтрации на стороне провайдера, стоимость услуги для клиента значительно снижается.
- Правила фильтрации разрабатываются индивидуально для каждого клиента, в зависимости от специфики его сервисов.
- Эксперты «Лаборатории Касперского контролируют процесс и при необходимости оперативно корректируют правила фильтрации.
- Тесное сотрудничество специалистов, обслуживающих Kaspersky DDoS Prevention, и разработчиков «Лаборатории Касперского» позволяет в кратчайшие сроки вносить изменения в алгоритмы работы решения.
- Для обеспечения высочайшего уровня надежности сервиса на территории Европы «Лаборатория Касперского» работает только с европейскими поставщиками оборудования и услуг.
- «Лаборатория Касперского» имеет богатый опыт применения Kaspersky DDoS Prevention в России, где решение успешно защищает таких клиентов, как Министерство финансов Российской Федерации, Росалкогольрегулирование, Министерство связи республики Татарстан, ВТБ24, Russia Today и др.

О «Лаборатории Касперского»

«Лаборатория Касперского» — крупнейшая в мире частная компания, специализирующаяся в области разработки программных решений для обеспечения IT-безопасности. Компания входит в четверку ведущих мировых производителей защитных систем класса Endpoint Security*. Вот уже более семнадцати лет «Лаборатория Касперского» создает эффективные защитные решения для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. Ключевым фактором успеха компании на рынке является инновационный подход к обеспечению информационной безопасности. Технологии и решения «Лаборатории Касперского» защищают более 400 миллионов пользователей почти в 200 странах и территориях мира. Более подробная информация доступна на сайте www.kaspersky.ru.

* Компания заняла четвертое место в рейтинге аналитического агентства IDC «Выручка вендоров от продажи решений класса Endpoint Security» (Worldwide Endpoint Security Revenue by Vendor) за 2013 год. Рейтинг был включен в отчет IDC «Прогноз развития мирового рынка решений класса Endpoint Security на 2014-2018 гг. и доли вендоров в 2013 г.» (Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares), опубликованный в августе 2014 года (IDC #250210). В основу рейтинга легли данные о выручке от продаж решений класса Endpoint Security в 2013 году.

ЗАО «Лаборатория Касперского», Москва, Россия
www.kaspersky.ru

Всё об интернет-безопасности:
www.securelist.ru

Купить в вашем городе:
www.kaspersky.ru/find_partner_office

KASPERSKY lab