Kaspersky DDoS Prevention

Сервис **Kaspersky DDoS Prevention** предназначен для обеспечения надежной эшелонированной защиты сетевых ресурсов от распространенных атак типа «отказ в обслуживании», применяемых современными киберпреступниками

DDoS-атаки: реальная опасность

Среди компьютерных злоумышленников растет популярность DDoS-атак (Distributed Denial of Service – распределенный отказ в обслуживании). Цель атаки состоит в том, чтобы заблокировать легальным пользователям доступ к какому-либо интернет-ресурсу или крайне затруднить его. Для этого используется два типа воздействия: атака на канал связи, который «забивается» огромной массой бесполезных данных, и атака на исчерпание вычислительных мощностей обслуживающих ресурс серверов, которые обрабатывают множество ложных запросов.

Кто под прицелом?

Сегодня мишенью DDoS-атак все чаще становятся государственные и корпоративные ресурсы. По отношению к государственным информационным системам DDoS-атака используется в случае:

- кибертерроризма
- попытки вмешательства во внутренние дела
- выражения недовольства
- нанесения экономического, имиджевого и другого ущерба

По отношению к корпоративным информационным системам это может быть:

- вымогательство
- конкурентная борьба
- месть
- прикрытие иных атак

DDoS-атака изнутри

Сетевое нападение типа DDoS осуществляется с помощью ботнета (зомби-сети) – большого количества зараженных специальной вредоносной программой компьютеров, с которых по команде из центра управления (от злоумышленника) на атакуемый компьютер отправляется множество запросов, блокирующих доступ к нему легальных пользователей. Мощности существующих ботнетов огромны: в иных сетях под управлением злоумышленников может находиться более 1 миллиона компьютеров и серверов, распределенных по всему миру.

В преступной схеме задействовано довольно много участников: те, кто пишет ПО для создания ботнета, те, кто его заказывает, администрирует и сдает в аренду зомби-сеть, заказчик атаки. Общение этих людей между собой ведется через большое число посредников, так что выявить этих злоумышленников нелегко. Усилия специалистов по безопасности и правоохранительных органов позволяют выявлять и ликвидировать некоторые ботсети, но на смену им постоянно приходят новые.

Почему неэффективна существующая защита?

Существует несколько способов защиты от DDoS-атак, которые не достаточно надежны даже при небольшом, но хорошо спланированном и организованном нападении:

- файерволы, системы IDS\IPS: находятся непосредственно перед защищаемым ресурсом и бессильны против атаки на переполнение канала связи
- маршрутизация в «черные дыры»: применятся провайдерами и заключается в перенаправлении атакующего трафика. В процессе перенаправляются и легальные запросы, то есть злоумышленники достигают своей цели – ресурс становится недоступным для пользователей
- правильная настройка системы: помогает только от небольших и плохо подготовленных атак
- многократное резервирование ресурсов: крайне дорогой, вследствие чего недоступный большинству организаций способ

KASPERSKY lab

Kaspersky DDoS Prevention – надежная защита от атак

Сервис KDP представляет собой уникальную для российского рынка мощную систему распределенной фильтрации трафика, состоящую из высокопроизводительных серверов, расположенных в разных странах и подключенных к интернету по высокоскоростным каналам связи. Такое решение позволяет выдержать DDoS-атаку практически любой мощности.

Система KDP является программно-аппаратным комплексом, состоящим из нескольких компонентов: сенсоров, коллекторов и центров очистки трафика, которые могут быть установлены в любом месте Сети. Сенсор предназначен для сбора информации о запросах, адресуемых защищаемому ресурсу, и последующей передачи ее коллектору. Коллектор является самым многофункциональным элементом KDP, который отвечает за анализ получаемой с сенсоров статистики и построение профиля легального пользовательского трафика. Благодаря уникальным технологиям «Лаборатории Касперского», коллектор умеет выявлять аномалии, выходящие за рамки пользовательского профиля, и принимать решения о фильтрации опасного трафика путем перенаправления всех запросов, адресованных защищаемому ресурсу, на центр очистки. Центр очистки фильтрует опасный трафик DDoS-атаки, оставляя только легальные обращения.

Преимущества Kaspersky DDoS Prevention

- Построение статистического профиля по трафику конкретного ресурса, что обеспечивает индивидуальную защиту.
- Услугой Kaspersky DDoS Prevention можно воспользоваться как заранее, для предотвращения атаки, так и после того как она уже началась.
- Территориально распределенные компоненты KDP подключены к Сети по мощным каналам связи, что исключает их одновременный выход из строя вследствие нападения. Сервис KDP не зависит от какого-либо конкретного провайдера, что также повышает его надежность и отказоустойчивость.
- Огромный опыт «Лаборатории Касперского» в борьбе с ботнетами. В структуру ЛК входит специальное подразделение, которое занимается исключительно изучением зомби-сетей и борьбой с ними, поэтому мы обладаем самой свежей информацией о тех методах, которые используют злоумышленники, и можем эффективно противостоять им.
- DDoS-атака – это только следствие, верный признак того, что у вашей организации есть недоброжелатели. Для обеспечения безопасности нужно бороться с причиной нападения. Аналитики «Лаборатории Касперского» помогут подготовить пакет документов, необходимый для обращения в правоохранительные органы.

Наш опыт

«Лаборатория Касперского» имеет большой опыт успешного взаимодействия с крупными корпоративными и государственными заказчиками в области проектирования, построения и настройки эффективных систем информационной безопасности. Нашимиклиентами являются МВД и ФСО РФ, Сбербанк России, Центральный банк РФ, ФНС России, Министерство финансов РФ, Билайн, ГидроОГК, другие крупнейшие компании и органы государственной власти.