DDoS-атака: защищаться эффективно

Николай Хлапонин

Коммерческий директор компании "Свит ИТ"

Виктор Калинин

Эксперт по информационной безопасности

Мы живем в век информационных технологий. Современный бизнес все больше напоминает ИТ-компанию со своими информационными активами. Зависимость бизнеса от информационных технологий очевидна. Низкая эффективность работы сети и простой веб-сайта может быть серьезной угрозой для бизнеса, как в плане недополучения прибыли, так и в отношении потери репутации. DDoS-атаки продолжают оставаться одним из наиболее серьезных инструментов злоумышленников, которые способны остановить работу бизнеса на длительный период. Поэтому задачи защиты от DDoS-атак чрезвычайно актуальны сегодня, в особенности для таких структур, как банки, Интернет магазины, а также государственные учреждения, предоставляющие гражданам услуги через Интернет.

DDoS (distributed denial-of-service) - распределённая, то есть выполняемая одновременно с большого числа компьютеров, атака на систему с целью довести её до отказа в обслуживании. Самые популярные DDoS-атаки - это, атаки, организованные с помощью ботнетов. Это доступный способ сделать атаку распределенной.

Мы выделяем атаки базового типа:

- до четырех тысяч ботов;
- проведение на уровне приложения;
- один - два вектора.

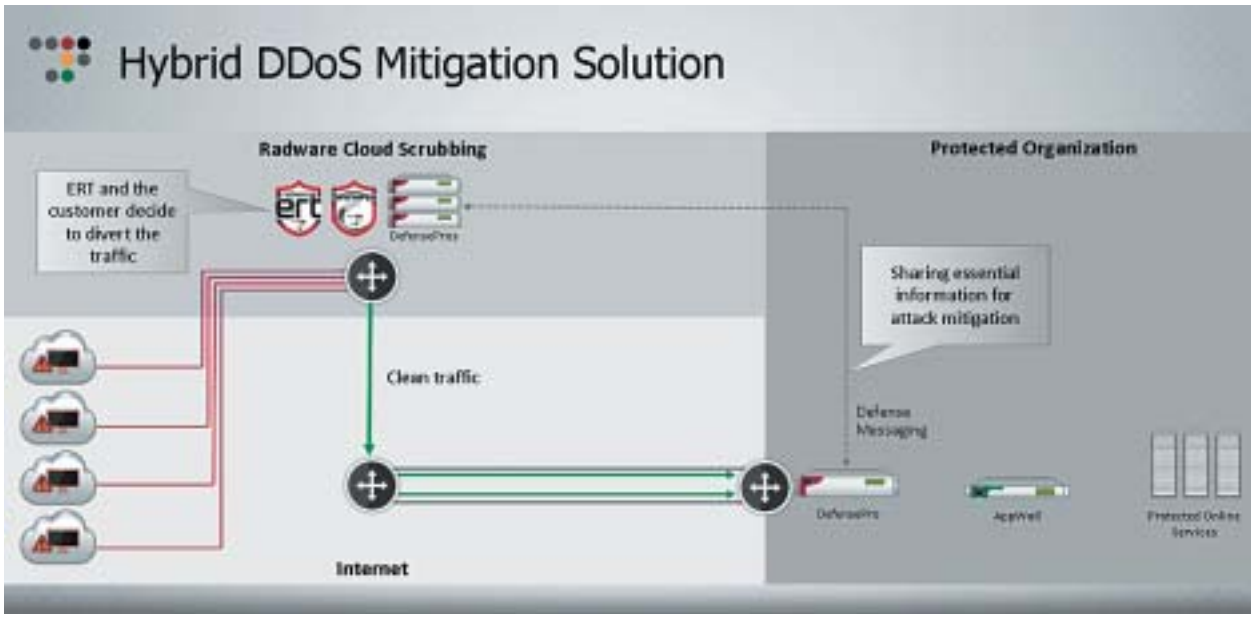
Стоимость атаки базового типа может составлять до $100 в сутки.

Но есть и атаки другого рода, когда заметно, что работает команда, и работает она в режиме 24/7 - на результат. Если у нее не получается добиться результата, она постоянно переключает режимы атаки, меняет векторы атаки, пытается найти уязвимое место и прорваться. Конечно, это стоит уже далеко не $100 в сутки.

Принята следующая классификация атак:

- атаки на приложения;
- атаки на канальную полосу (скорость измеряется в гигабитах/с);

Рис. 1. Комплекс для защиты от DDoS-атак



- атаки на сетевую инфраструктуру (скорость измеряется в пакетах в секунду).

Для полноценной защиты от DDoS-атак необходимо использовать как услуги провайдера, так и оборудование на стороне клиента. Таким образом, обеспечиваются два рубежа защиты: очистка трафика на стороне провайдера от объемных атак на канальную полосу и более точная (тонкая) очистка на стороне клиента для защиты от атак на приложения, атак медленного чтения и атак внутри SSL (Secure Sockets Layer). Такого подхода придерживаемся мы, предоставляя заказчикам комплекс, состоящий из оборудования двух вендоров: Radware и Genie (рис. 1).

Исходя из опыта нашей компании, приведём несколько аргументов в пользу применения решений Radware, в частности устройств DefensePro (рис. 2 и 3) на стороне заказчика.

1. Вариант защиты с помощью услуг провайдера предназначен, в основном, для работы с сетевыми флудами. Борьба с атаками, например, на HTTP, проводится либо простым перезапросом (который обходят большинство ботов) или путём rate limit (ограничения количества поступающих запросов), что приводит к высокому уровню false positive. У DefensePro, кроме 302 redirect, внедрен Javascript-перезапрос, что позволяет точнее бороться с аппликационными и DNS-атаками.

2. Перезапрос и rate limit применяются по отношению ко всем клиентам, в то время как DefensePro применяет перезапрос только к сессиям, имеющим странное с точки зрения NBA поведение.

3. С устройством DefensePro поставляется услуга Emergency Response Team (включена в сто-

Рис. 2. DefensePro

DefensePro - это специализированная платформа с двумя процессорами Dual-Core Opteron, с от 6 до 10 Гбайт оперативной памяти, со встроенными высокопроизводительными сетевыми процессорами компании EZChip Technologies, со специализированными ASIC и FPGA для аппаратного ускорения обработки сетевого трафика. DefensePro со встроенным IPS содержит также высокопроизводительный контекстный процессор NETL7 ком пании NetLogic Microsystems для аппаратного ускорения сигнатурного анализа сетевых пакетов.

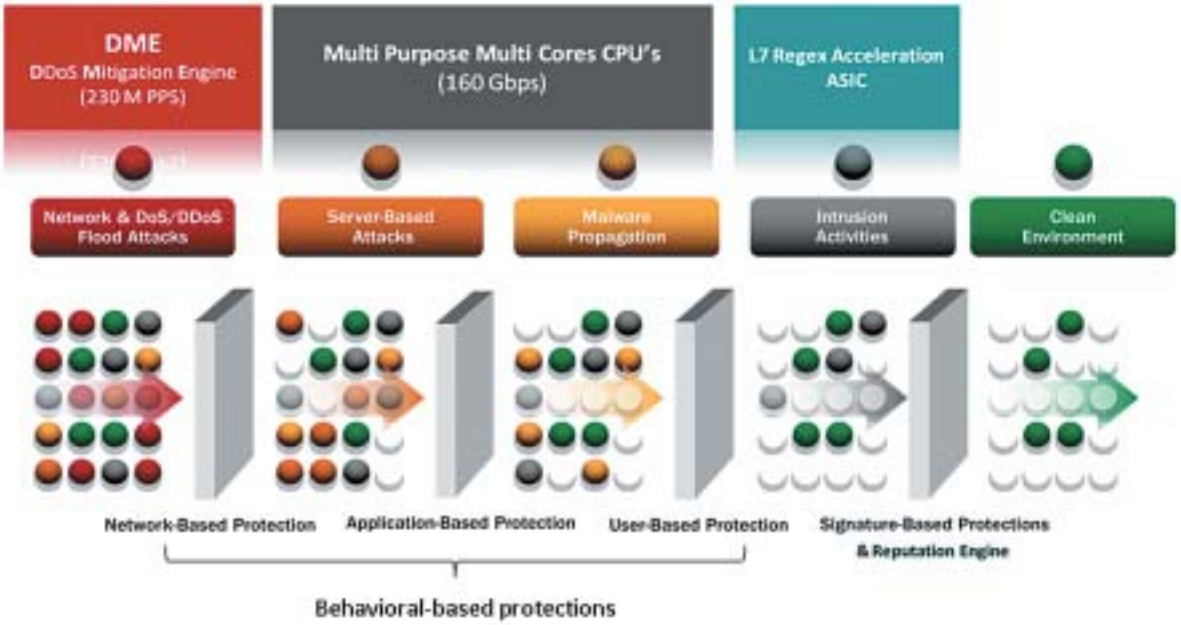
Рис. 3. Обработка сетевого трафика в DefensePro

Обработка сетевого трафика осуществляется поэтапно с использованием различных механизмов защиты. При этом суммарное время задержки сетевого пакета для всех линеек DefensePro не превышает 60 микросекунд.

В DefensePro реализованы следующие механизмы защиты:

- Behavioral DDoS Protection;
- TCP SYN Flood Protection;
- Signature Protection (IPS);
- Connection Limit;
- Stateful Inspection;
- BandWidth Management;
- HTTP Mitigator;
- Behavioral Server-Cracking Protection;
- Anti-Scanning Protection;
- Stateful Firewall (ACL).

Одно из достоинств DefensePro - это возможность увеличения производительности по мере необходимости.



имость поддержки), позволяющая в режиме 24x365 получать квалифицированную помощь специализированного подразделения, обеспечивающего дополнительный уровень защиты для клиентов по всему миру на случай непредвиденных обстоятельств (рис. 4). Вариант защиты с помощью услуг провайдера в таких случаях фактически предлагает обратиться к сообществу клиентов за советом. При этом они не несут ответственности за эти рекомендации.

4. Поскольку существует и DDoS в SSL-трафике, есть необходимость его чистить: раскрыть, почистить (опять зашифровать при необходимости, даже на ключе 1K) и отдать на обработку серверу и пропускать только легитимный SSL-трафик. Такая возможность также обеспечивается с помощью решений Radware AMS (рис. 4). В частности, задачу по SSL offloading выполняет балансировщик Alteon.

5. Поскольку провайдер достаточно грубо защищает и предназначен, в основном, для противодействия атакам на канальную полосу, атаки медленного чтения могут быть серьезной угрозой даже для тех клиентов, которые защищаются на уровне провайдера. Одна из типовых - Slow Loris. Она направлена на 7-й уровень модели OSI - уровень приложения. Проще всего объяснить ее работу на примере протокола HTTP и запроса POST. Атакующий отправляет HTTP POST-запрос, указывая в нем большой размер пакета (<content length>), после чего медленно передает данные по 1 байту. По стандарту, HTTP-сервер должен дождаться полной передачи данных (получив содержимое размером <content length> байт) и может закрывать соединение только по таймауту. Таким образом, в случае подобной DDoS-атаки медленными соединениями атакуемый сервер открывает огромное количество соединений, катастрофически расходуя свои ресурсы

Применение локального оборудования минимизирует уровень таких угроз. У DefensePro

Рис. 4. Radware AMS

поведенческий анализ доходит до 7-го уровня (анализируя поведение хост-приложения) - анализируется 20 параметров, в сигнатуре используется до 7. Соответственно DefensePro создает многократно более точную поведенческую модель атаки и на порядки меньшую вероятность нанесения ущерба легитимным сессиям.

Radware AMS - портфель решений для борьбы с современными многоцелевыми атаками, направленными на сетевое оборудование, серверы и приложения. Данный комплекс состоит из:

- **DefensePro**: борьба с DDoS (поведенческий и сигнатурные алгоритмы очистки) с автоматическим распознаванием и блокированием атаки;
- **Alteon:** аппаратное ускорение SSL (SSL offloading), оптимизация (кеширование, компрессия, мультиплексирование) и балансировка трафика для повышения отказоустойчивости сервисов и скорости их доставки потребителю;
- **AppWall:** фаервол уровня приложений (WAF - Web Application Firewall) для гранулярной очистки Web-трафика от атак на прикладной уровень (SQL-injection, Cross Site Scripting, Slow Rate Attack и пр.).

В заключение хотелось бы подчеркнуть, что только комплексный подход даёт хороший результат при защите от DDoS-атак. Оборудование для защиты должно быть и у провайдера, и у клиента. При этом лучше, если с обеих сторон используется оборудование одного типа.

НОВОСТИ

В УКРАИНЕ БУДЕТ СОЗДАНА НОВАЯ КИБЕРПОЛИЦИЯ

В рамках реформирования и развития подразделений МВД Украины, в нашей стране будет создана киберполиция, которая будет бороться с киберпреступностью, сообщил министр внутренних дел Украины Арсен Аваков. Высококвалифицированные специалисты в экспертных, оперативных и следственных подразделениях полиции, будут задействованы в борьбе с киберпреступностью и применять на высоком профессиональном уровне новейшие технологии в оперативно-служебной деятельности, написал он на своей странице Facebook.

Семь основных задач киберполиции:

1. Реализация государственной политики в сфере противодействия киберпреступности.

2. Противодействие киберпреступности: в сфере использования платежных систем, в сфере электронной коммерции и хозяйственной деятельности, в сфере интеллектуальной собственности, в сфере информационной безопасности.

3. Заблаговременное информирование населения о появлении новых киберпреступлений.

4. Внедрение программных средств для систематизации и анализа информации о киберинцидентах, киберугрозах и киберпреступлениях.

5. Реагирование на запросы зарубежных партнеров, которые будут поступать по каналам Национальной круглосуточной сети контактных пунктов.

6. Участие в повышении квалификации работников полиции по применению компьютерных технологий в противодействии преступности.

7. Участие в международных операциях и сотрудничество в режиме реального времени. Обеспечение деятельности сети контактных пунктов между 90 странами мира.

Министр внутренних дел Украины заявил, что старт набора в киберполицию и подробные условия конкурса будут объявлены с 15 октября. С 26 октября начнется атестационный конкурс для всех будущих киберполицейских. До 5 ноября штат киберполиции будет сформирован и начнется заключительный переходный этап выстраивания нового функционала киберполиции и переподготовки персонала на марше.