

ПОДЕЛИТЕСЬ ОТЧЕТОМ



Содержание

01

Основные положения

- » Важнейшие выводы

02

Введение

- » Задачи отчета
- » Отраслевое исследование
- » Примеры из практики ERT

03

Тенденции

- » Организации используют устаревшие методы защиты
- » Год DNS-атак
- » Проблема HTTPS
- » Сеть CDN – не препятствие для хакеров
- » 2012 в сравнении с 2011 – Краткий обзор тенденций

04

Тенденции развития инструментов атаки

- » DDoS "Сделай сам"
- » Сервисы, доступные армии ботнетов

05

Тенденции развития методов борьбы с атаками

- » Борьба с атаками, которые ведутся в обход CDN сети

06

Заключение

- » Рекомендации специалистам по безопасности



Основные положения

Атаки DoS и DDoS часто встречаются в мире интернет-безопасности. Во-первых, они не направлены на уязвимости, которые могут быть исправлены; во-вторых, каждый отдельный пакет является вполне легитимным — лишь их совокупность приводит к разрушительным последствиям, и, в-третьих, такие атаки носят продолжительный характер — они длятся несколько часов или дней, вместо нескольких секунд или минут.

В течение многих лет атакам DoS и DDoS не уделяли должного внимания, поскольку они считались нишевыми. Ситуация резко изменилась в 2011 году, когда группа Anonymous выбрала DoS/DDoS-атаки в качестве основного метода нападения. Воодушевленная мощностью и разрушительными последствиями такой атаки, группа Anonymous превратила ее в основной метод борьбы, привлекая к нему внимание не только сообщества специалистов по безопасности, но и широкой публики. Несмотря на то, что активность группы снизилась в 2012 году, она заложила основу для дальнейшего развития данного типа атак. Многие группы хакеров начали использовать DoS/DDoS — активисты, финансово мотивированные преступные организации и даже правительственные структуры заинтересовались открывающимися возможностями. К сожалению, похоже, что и в 2013 году DoS/DDoS-атаки будут представлять значительную и постоянную угрозу.

Этот отчет посвящен обмену результатами исследований и знаниями относительно обеих сторон DoS/DDoS-войны — атакующих и защищающихся. Будем надеяться, что данное исследование позволит узнать больше о противниках, а также, что более важно, позволит организациям более эффективно выявлять, противостоять и одерживать победу в длительной и постоянной DoS/DDoS-войне. Кроме того, представленные здесь идеи имеют более широкое применение и могут использоваться в других областях обеспечения безопасности, которые также являются полем битвы для длительных кампаний атак. Полученные сегодня знания о DoS/DDoS-атаках могут найти применение и в других областях — ведь принципы борьбы не меняются.

Что изменилось в сфере безопасности в 2012 году?

В 2012 году мы могли наблюдать за появлением новой тенденции в кибербезопасности – устойчивым развитием сложных и продолжительных кампаний DoS- и DDoS-атак. Такие кампании включают множество векторов атак, которые занимают больше времени и являются более сложными. Сегодня можно часто наблюдать атаки с четырьмя, пятью или даже десятью векторами, которые длятся три дня, неделю или даже месяц. Тенденция к возникновению продолжительных угроз создает большие проблемы для организаций, которые не подготовлены должным образом.

Организации используют устаревшие методы защиты.

Здесь мы подразумеваем, что они вступают в бой за безопасность без понимания истинной природы атаки, что не позволяет им принять адекватные меры по подготовке. Они вкладывают средства в подготовку на этапе, предшествующем атаке, и замечательно анализируют ситуацию после атаки. Однако, организации имеют критический недостаток – у них нет возможностей или ресурсов для защиты в активной фазе атаки, они не могут противостоять длительной кампании, в которой используются изощренные методы атак. Злоумышленники, с другой стороны, знают об этом пробеле и используют его в своих интересах. Результатом являются перебои в доступности услуг, даже среди наиболее уважаемых онлайн-бизнесов.

Как остановить изощренные кампании атак

Чтобы остановить такие кампании, организациям требуется изменить стратегию защиты, перейдя с двухэтапной защиты на трехэтапную. Двухэтапный подход подразумевает предварительный этап подготовки к атаке – выбор решений по обеспечению безопасности, развертывание систем безопасности и другие меры, и этап после атаки – проведение экспертизы, подведение итогов и совершенствование используемых средств защиты в ожидании следующей атаки. Этих действий было достаточно, пока атаки носили непродолжительный характер.

Теперь, когда кампании длятся днями или неделями, организациям требуется добавить третий этап – защитную стратегию, используемую ВО ВРЕМЯ атаки. Наиболее важным компонентом такой стратегии является команда экспертов, которые могут не только динамически реагировать на действия злоумышленников во время нападения, но также применять контрмеры для остановки атаки, и затем анализировать полученную информацию для совершенствования методов борьбы с будущими атаками. Для организаций неразумно содержать требуемое количество людских ресурсов и квалифицированных специалистов на постоянной основе, учитывая, что в год они подвергаются всего нескольким атакам. Организации, таким образом, должны найти дополнительные внешние ресурсы – экспертов по безопасности, отраслевые альянсы или государственные службы. Только с помощью таких услуг по требованию и усилению своей команды специалистов услугами сторонних экспертов можно одержать победу в борьбе за безопасность.

Чему мы можем научиться в борьбе с атаками?

Усовершенствованные и продолжительные DoS- и DDoS-атаки безусловно опасны и сложны, однако они предоставляют некоторые весьма ценные возможности для развития. Эксперты по безопасности могут собрать актуальные сведения об атакующих – кем они являются, и какие инструменты используют. В конечном итоге, это позволяет организациям отразить атаку, применить контрмеры и победить атакующих на их поле.



Введение

Ежегодный глобальный отчет по вопросам безопасности сетей и приложений от Radware позволяет ознакомиться с тенденциями сетевой безопасности с особым фокусом на DoS/DDoS-атаках. Он предназначен всему сообществу специалистов по безопасности и разработан таким образом, чтобы предоставить всеобъемлющую и объективную информацию о событиях в мире сетевой безопасности и DoS/DDoS атаках, которые были зафиксированы в 2012 году, с анализом типов атак, тенденций и технологий противодействия. В целом, в отчете содержится информация от 274 организаций, полученная двумя способами:

Отраслевое исследование

Первым источником для данного годового отчета является отраслевое исследование, проведенное компанией Radware. Исследование охватывало широкий круг организаций по всему миру – как клиентов компании Radware, так и организации, не имеющие отношения к нашей компании. Был разработан опрос для сбора объективной информации, независимо от производителей, о проблемах, с которыми столкнулись администраторы сетей при борьбе с DoS/DDoS-атаками в 2012 году. Опрос состоял из 29 вопросов, которые затрагивали следующие темы:

- **Вводная информация** – об организации и респонденте, заполняющем опрос
- **Общие вопросы безопасности** – сведения о безопасности, не связанные с DoS/DDoS-атаками
- **DoS/DDoS** – вопросы, касающиеся данного типа атак, их последствий и методов борьбы с ними



Анализ примеров из практики Radware ERT

Вторым источником информации послужил анализ 95 ключевых примеров атак – представляющих различные типы организаций по всему миру – в борьбе с которыми участвовали эксперты команды экстренного реагирования (Emergency Response Team, ERT) Radware. Это позволило дополнить отчет опытом людей, которые непосредственно участвовали в процессе борьбы с атаками, и получить исчерпывающую информацию о тенденциях атак, а также технические данные.

Специалисты команды Radware ERT обеспечивают экстренную поддержку в реальном времени, предлагая проактивные, практические решения по борьбе с активными угрозами. Команда ERT содействует заказчикам, находящимся под DoS / DDoS атакой в реальном времени, получая непосредственный доступ к сетевому оборудованию заказчика, изучая файлы трафика, анализируя ситуацию и предлагая различные варианты противодействия.

В то время, как главной целью ERT является противодействие атакам и помощь в восстановлении сервисов заказчиков, специалисты команды получают уникальный опыт наблюдения за каждой атакой. Благодаря своему непосредственному участию в процессе борьбы команда просматривает в реальном времени информацию о внутренних параметрах атаки и имеет возможность измерить уровень ее воздействия на систему. Как правило, команда ERT вызывается только в случае возникновения атак от среднего до наивысшего уровня тяжести. Это позволяет осуществить глубокое исследование Dos/DDoS-атак, которое не может быть выполнено на уровне опроса.



Организации используют устаревшие методы борьбы с атаками

Первые сетевые атаки появились почти одновременно с возникновением сети Интернет. Сегодня почти невозможно найти ИТ-организацию, которая не была бы осведомлена о существующих видах угроз безопасности. Сложно найти группу специалистов по ИТ-безопасности, которая бы не предпринимала меры предосторожности, не приобретала бы оборудование и не создавала бы различные линии защиты.

И все же, несмотря на осведомленность о существующей опасности, подготовку и превентивные меры – мы должны заметить, что слишком большое количество организаций не могут адекватно защитить себя от атак. Новостные заголовки за несколько последних лет показывают, что атакам подвергались и некоторые известные компании. Эти компании, несомненно имеющие высокий ИТ-бюджет и богатые ресурсы, пали жертвами интенсивных атак, которые вывели из строя их сетевую инфраструктуру.

Мы исследовали это явление – почему, несмотря на все усилия, организации не способны защитить себя от атак? Что требуется делать иначе?

По нашей оценке, организации используют устаревшие и неэффективные методы защиты. Они вступают в борьбу за безопасность без адекватного оборудования и подготовки. Они используют устаревшие стратегии без понимания размаха и мощи действий своих противников, а также без возможности динамически менять тактику обороны в случае длительной атаки со сменой векторов. Тем не менее, если бы перед нами стояла задача выделить единственную, наиболее значимую причину их неудачи, мы бы обозначили тот факт, что организации до сих пор не вполне понимают, в каком типе битвы им приходится участвовать, и не оценивают ее размах, сопутствующие обстоятельства и обстановку.

Крупные организации, испытывавшие перебои в оказании своих сервисов за последние 18 месяцев



Двухэтапные методы защиты больше не являются достаточными

Традиционно организации в сфере безопасности фокусировали свое внимание и усилия на двух этапах борьбы с нападениями:

- **Подготовительный этап**, на котором группы обеспечения безопасности приобретают средства противодействия атакам, развертывают системы безопасности, проводят испытания на проникновение и другие защитные действия.
- **Восстановительный этап**, на котором группы обеспечения безопасности используют системы регистрации и анализа, нанимают экспертов, чтобы проанализировать журналы регистрации событий и провести подробную экспертизу, делают выводы и выполняют необходимые усовершенствования системы безопасности.

Отраслевое исследование

Сколько средств было инвестировано в следующие аспекты обеспечения безопасности вашей компании в прошлом году?

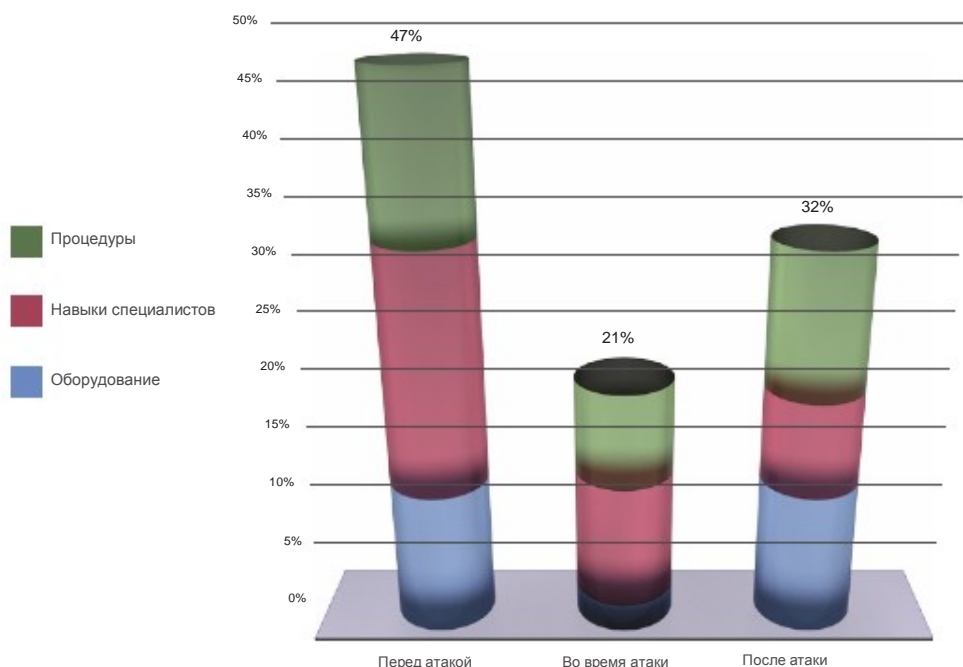


Рисунок 1: Только 21% усилий компании расходуется в ходе нападения, в то время как 79% расходуется на подготовительном и восстановительном этапах.

Такое поведение также отражено в результатах опроса по затраченным средствам на обеспечение безопасности, показывая, что компании затратили 79% своих усилий на подготовительном и восстановительном этапах, и только 21% - непосредственно в ходе нападения, на управление системами защиты в реальном времени, и на создание команды специалистов по безопасности для реагирования на атаку и контрмер.

Такая модель поведения подразумевает, что атаки являются непродолжительными, и что предварительных мер будет достаточно для того, чтобы им эффективно противостоять. И действительно, так происходило на протяжении многих лет, но не в теперешней ситуации. Все больше и больше атак могут длиться в течение нескольких дней или даже недель. Эту битву уже нельзя выиграть, не будучи готовыми бросить средства и ресурсы на борьбу во время нападения. Это утверждение верно для всех областей обеспечения безопасности, несмотря на то, что данный отчет уделяет больше внимания защите от DDoS/DDoS атак.

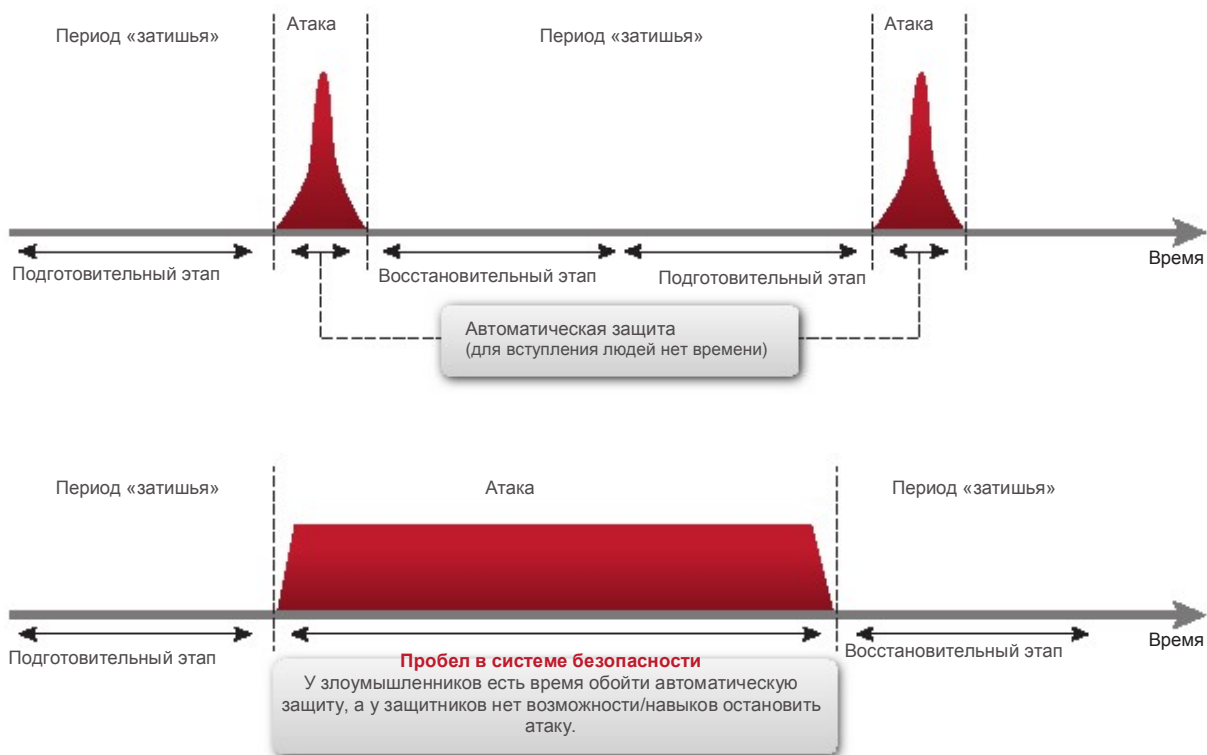


Рисунок 2: Все больше атак занимают продолжительное время и могут длиться днями или неделями.

Другим аспектом атак, помимо их продолжительности, является использование нескольких векторов атак и возможность динамически переключаться между ними. Например, рассмотрим атаку, начатую с UDP-флуда. Атака была обнаружена и заблокирована; однако после этого атакующие поменяли вектор и переключились на HTTP-флуд, к отражению которого защищающаяся сторона была не готова и не смогла справиться своевременно. На практике нападающие используют более двух векторов атак, превращая противодействие атаке в гораздо более сложную задачу.

Новый мир с иным масштабом и размахом атак

Команда Radware ERT ежегодно наблюдает за сотнями DoS/DDoS-атак. Мы проанализировали эти атаки и задали вопрос: "каково главное изменение в профиле атак в 2012 году"? Однозначный ответ – сложность атак значительно возросла. Атаки стали гораздо более мощными, сложными и постоянными. Другими словами, нападающие борются лучше, сильнее и быстрее.

Более серьезные нападения с возросшим показателем APT

Для оценки наблюдений мы разработали рейтинг Advanced Persistent Threat (APT, постоянные угрозы повышенной сложности). Термин APT повсеместно используется в контексте интернет шпионажа и кибервойн. Мы определили систему показателей, которая позволяет методично классифицировать атаки согласно степени серьезности. Каждой атаке присваивается APT балл от 1 до 10 (10 для наиболее мощных атак) на основе трех факторов:

- **Продолжительность атаки** – чем длительнее атака по времени, тем выше показатель APT.
- **Число векторов атаки** – чем большее число векторов атак регистрируется, тем выше показатель APT. К векторам атак относятся различные методы, например HTTP, DNS флуд, флуд из "мусорных" пакетов SSL и другие виды атак.

- **Сложность атаки** – чем более сложные векторы атак, тем выше рейтинг АРТ. Например, атака SYN-флуд имеет сравнительно низкий рейтинг; «медленная» атака получает более высокий рейтинг; а экзотические атаки, которые очень редко встречаются, получают наивысший балл.

На рисунке 3 показано увеличение степени серьезности DoS/DDoS-атак, которое было рассчитано на основе анализа примеров из практики Radware ERT. Для того, чтобы при анализе не учитывались сравнительно простые атаки, и можно было сфокусироваться на более изощренных, мы не принимали во внимание простые атаки, имеющие рейтинг АРТ 3 балла и ниже.

Примеры из практики ERT – Рейтинг АРТ

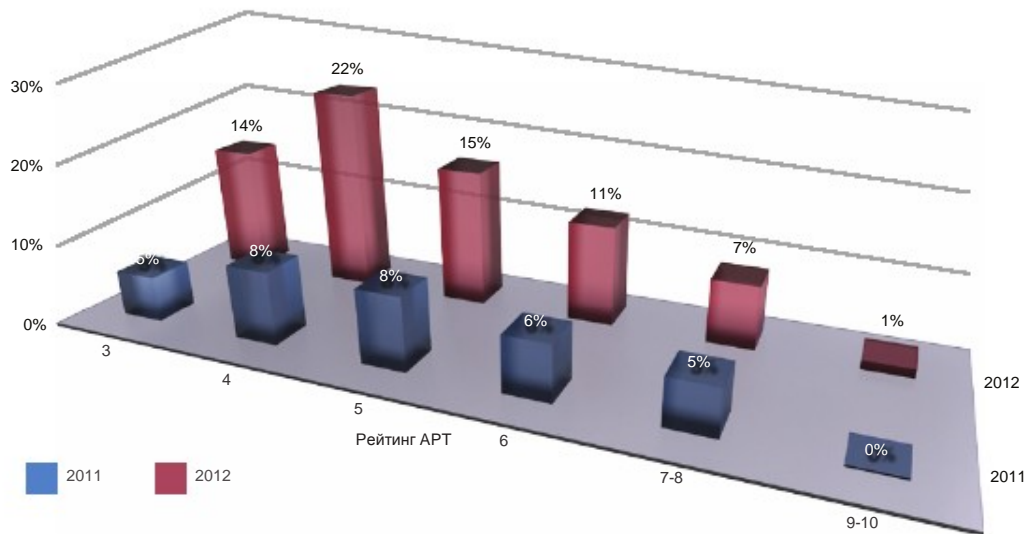


Рисунок 3: Растет количество серьезных атак – количество DoS/DDoS-атак, имеющих высокий рейтинг АРТ, возросло в 2012 году

Примеры из практики ERT – Изменение длительности атак

Важно отметить, что и в 2011 году были зафиксированы мощные атаки, особенно если вспомнить атаки группы AnonymouS. Следовательно, профиль АРТ за 2011 год очень схож с профилем за 2012 год, однако возросло количество атак с высоким рейтингом АРТ. В 2012 году мы также наблюдали рост отдельных параметров, влияющих на АРТ рейтинг (продолжительность атаки, количество векторов, сложность атаки).

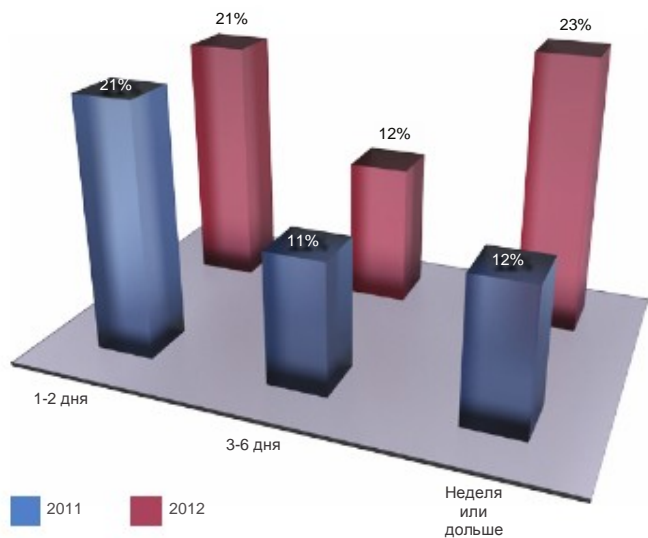


Рисунок 4: Рост продолжительности атак – количество DoS/DDoS-атак длительностью более недели удвоилось в 2012 году.

Экспертная оценка

Злоумышленники планируют и запускают атаки регулярно, по сути превращая организацию DoS/DDoS-атак в свою «профессию». В этом контексте, злоумышленники разработали цепь доставки DDoS-атак, которая включает наборы инструментов для DDoS-атак, механизмы распространения и услуги по организации DoS-атак на заказ. С помощью легко доступной информации и инструментов для DDoS-атак начинающие хакеры могут воспользоваться опытом, собранным их более опытными коллегами, для того, чтобы организовать сложную атаку. Более подробное описание этой тенденции содержится в главе DDoS «Сделай сам».

С другой стороны, защищающиеся организации значительно отстают в скорости совершенствования методов защиты, поскольку они, как правило, подвергаются DDoS-атакам лишь несколько раз в год. Хотя после отражения нескольких атак они могут сделать некоторые выводы, их опыт слишком ограничен для того, чтобы выстроить необходимую базу знаний.



Рисунок 6: защищающиеся организации отстают в квалификации, поскольку ежегодно они подвергаются лишь нескольким DoS/DDoS-атакам.

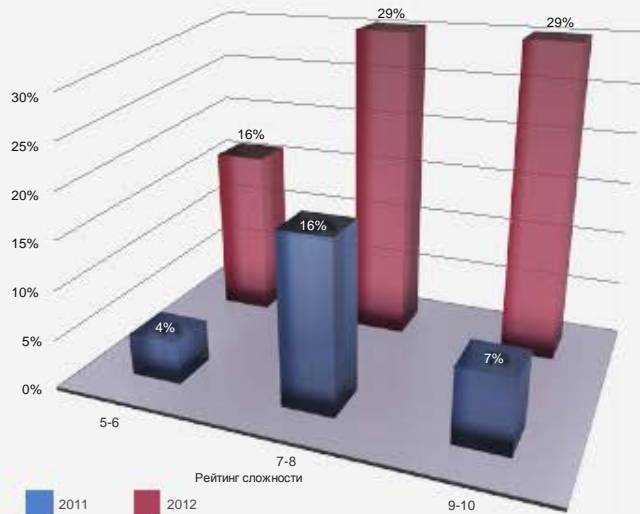


Рисунок 5: Атаки стали более сложными: в 2012 году DoS/DDoS-атаки стали более изощренными, включая больше векторов атак. Обратите внимание на количество атак с уровнем сложности в 7-10 баллов.

Отраслевое исследование

Какова вероятность того, что ваша организация подвергнется нападению в кибервойне?



Рисунок 7: Более половины опрошенных организаций считают, что они, с большой долей вероятности, могут подвергнуться нападению в кибервойне

Отраслевое исследование

Каковы ваши шансы выжить в кибервойне?



Рисунок 8: 81 % организаций считают, что они не способны защитить себя в кибервойне.

Кибервойна уже началась

Термин «кибервойна» имеет несколько значений, но обычно он относится к атакам, которые организуются по политическим мотивам. В кибервойне присутствует постоянная угроза атаки, сами атаки являются более изощренными, их весьма сложно отразить. Ранее считалось, что в кибервойне под прицел попадали только государственные организации, такие, как электростанции, предприятия атомной энергетики и другие подобные объекты. Это уже не так. В 2012 году ERT отразила многочисленные мощные атаки, которые были нацелены на финансовые институты, интернет-магазины, сотовые сети и другие коммерческие объекты. Несмотря на то, что трудно с уверенностью утверждать, что все атаки являлись частью кибервойны (спонсированной правительством), они обладали всеми атрибутами кибервойны с точки зрения мощности, сложности и постоянства.

Организации также осознают угрозу кибервойны. Как можно увидеть в результатах опроса, 55% опрошенных организаций верят, что они могут быть объектами атаки в кибервойне. Как ни парадоксально, большинство из опрошенных компаний (81%) считают, что они не готовы отразить такую атаку. Это подтверждает тот факт, что организации используют устаревшие, неэффективные способы борьбы.

Вывод

Организации не в состоянии защитить себя, главным образом, по причине того, что они все еще пользуются методами защиты от устаревших типов атак. Сегодняшние нападения видоизменились – они тщательно спланированы, они мощные и длятся на протяжении недель, переключаясь с одного вектора атаки на другой. Решения по обеспечению безопасности организаций разработаны таким образом, чтобы поглотить первый удар, но когда нападение затягивается, они обладают весьма ограниченными ресурсами и знаниями для того, чтобы бороться дальше. К тому времени, когда им удается заблокировать первые два вектора атак, злоумышленники уже переключаются на третий, наиболее мощный вектор. Требуется новый подход к обеспечению безопасности.

Решение

Как организации могут активизировать методы обороны и гарантировать, что используются решения, равные средствам нападения по мощности и оригинальности? Разрыв в силах нападающих и защищающихся не так легко закрыть. Даже крупным организациям трудно содержать команду специалистов по безопасности, готовую противостоять атакам в любое время дня и ночи. Более того, такая команда не способна поддерживать должный уровень опытности и квалификации, поскольку организации сталкиваются только с несколькими нападениями в год.

Обращаясь к аналогии из мира здравоохранения – местная клиника не может успешно решить глобальные проблемы здравоохранения. Требуется доступность, оперативность и должный уровень опыта, которыми обладают высококвалифицированные, узконаправленные специалисты.

Решение заключается в поиске таких специалистов за пределами компании – обращении к командам экспертов по безопасности. Такой командный пункт по безопасности должен включать:

- Группу хорошо обученных экспертов по безопасности, обладающих необходимыми знаниями и навыками для того, чтобы динамически реагировать на смену действий злоумышленников и отражать продолжительные атаки, которые длятся несколько дней.
- Самые современные методы и инструменты, которые облегчают анализ трафика и быстро формируют новые средства защиты в режиме реального времени, во время самого нападения.
- Накопленный опыт, полученный путем еженедельного или даже ежедневного противостояния серьезным кибератакам.
- Готовность реагировать на нападение в любое время дня и ночи.
- Способность применять техники контратаки для нейтрализации нападения.

Мы также считаем, что поскольку угрозы безопасности носят глобальный характер и выходят за пределы интересов отдельных компаний, правительства и государства станут более активно участвовать в процессе сбора знаний и обмена опытом эффективной защиты.

Постановка уровня ожиданий

Ниже можно найти пример ответной реакции на атаку. В таблице приводится сравнение типичного понимания атаки и действий, которые предпринимаются в условиях ограниченности ресурсов, по сравнению с другой реакцией, основанной на более обширной базе знаний и более глубоком анализе.

| Вопрос тех./ген. директора | Какие ответы бывают сегодня | Какие ответы должны быть |
|--|--|--|
| <p>Как мы боремся с атакой?</p> | <p>Система отражения DoS/DDoS-атак блокирует некоторое количество трафика, сокращая пропускную способность на 60%, однако 40% трафика все еще поступает в сеть и оказывает негативное воздействие на межсетевой экран. Мы работаем над расширением таблицы сеансов межсетевого экрана; но для выполнения этого потребуется его перезагрузка.</p> | <ul style="list-style-type: none"> Атака SYN-флуд была успешно заблокирована с помощью системы для борьбы с DoS-атаками. Атака HTTP-флуд была более изощренной, она не была остановлена технологией «запрос-ответ». Вместо этого была активирована технология поведенческого анализа, и это оказалось эффективным. Используемая атака типа R.U.D.Y. представляет собой новую версию и не была эффективно остановлена существующими средствами защиты. Мы создали для ее блокировки специальную сигнатуру. |
| <p>Кто ответственен за это?</p> | <p>Это нельзя выяснить. Однако было замечено, что трафик поступает из различных точек мира. Мы не хотим использовать геозащиту, чтобы не потерять наших европейских клиентов.</p> | <p>IP-адреса злоумышленников принадлежат к известной ботсети, которая контролируется восточноевропейской киберорганизацией. Эта организация предлагает «DDoS на заказ»; стоимость атаки, вероятно, составляет \$1 000. Мотивом для заказчиков атаки обычно служит коммерческая конкуренция.</p> |
| <p>Можем ли мы их остановить?</p> | <p>Нет, что мы можем сделать?</p> | <p>Да, мы используем техники контратаки, чтобы остановить нападение. Мы смогли замедлить один из инструментов с помощью отправки TCP RST пакетов, а также полностью парализовали другой инструмент с помощью пакета с нулевым значением поля «размер окна».</p> |
| <p>Существуют ли другие риски?</p> | <p>По нашим сведениям, нет.</p> | <p>Мы знаем, что в данной группе есть хакеры, которые могут попытаться проникнуть во внутреннюю сеть нашей организации, поэтому мы отслеживаем не только журналы регистрации DDoS-атак, но и все другие события безопасности. Очень важно, чтобы межсетевой экран, IPS и WAF были доступны и оставались запущенными все время.</p> |
| <p>Атака была полностью остановлена?</p> | <p>Да, активность нападающих снизилась по сравнению с тем, что мы наблюдали утром. Мы заблокировали 70% действий нападающих. Сайт по-прежнему работает медленно, но, по крайней мере, он работает.</p> | <p>Да. Сайт работает очень хорошо с обычным временем задержки. Несанкционированного доступа к системе зарегистрировано не было.</p> |

Год DNS-атак

2012 год был годом DNS-атак. Хотя DNS-атаки уже давно известны, за прошедший год они возникали гораздо чаще обычного, и, что более важно, – они стали более изощренными и влекут за собой более серьезные последствия.

Почему популярность DNS-атак возросла? Ответ можно найти, изучив недавнюю историю DoS/DDoS-атак. Хотя DoS/DDoS-атаки появились одновременно с появлением сети Интернет, они заняли лидирующую позицию среди атак со второй половины 2010, в частности с тех пор, как группа Anonymous выбрала их в качестве основного метода нападения. Вначале организации были абсолютно не готовы к защите, и любые атаки злоумышленников достигали цели.

Положение изменилось к концу 2011 года, когда организации стали внедрять системы отражения для противодействия DoS/DDoS атакам, что побудило злоумышленников искать пути обхода защитных систем, используя более изощренные векторы атак. При таком положении вещей DNS-сервер стал подходящей целью.

Изучив информацию об атаках за 2012 год, можно отметить рост числа DNS-атак на 170% по сравнению с 2011 годом. Почти половина состоит из изощренных атак с использованием отражения запросов или рекурсивных запросов, для осуществления которых, даже не требуется наличия DNS-сервера у организации, являющейся целью атаки.

DNS-атаки показывают динамику развития сферы DoS/DDoS в целом. Несмотря на часто встречающееся наивное восприятие DoS/DDoS как атак, для эффективности которых требуется грубая отправка большого количества трафика, DNS-атаки доказывают обратное. Сложные DNS-атаки могут носить асимметричный характер, и могут быть мощными и разрушительными при относительно низкой скорости и интенсивности атаки. Растущая сложность относится не только к DNS-атакам, но является общей чертой развития сферы DoS/DDoS-атак.

Ссылки по теме

- [Cyber War Rooms: Why IT Needs New Expertise To Combat Today's Cyberattacks](#) - Avi Chesla
- [Counterattack – Radware Global Network and Application Security Report 2011](#) (см. Главу 10)

Крупномасштабные DNS-атаки 2012 года

В 2012 году были проведены крупномасштабные DNS-атаки на следующие авторитетные организации:

AT&T

В августе 2012 года AT&T подверглась DDoS-атаке, которая вывела из строя DNS-серверы компании в двух территориальных точках. В ходе атаки, которая продлилась по меньшей мере 8 часов, сайт компании AT&T был недоступен для пользователей. Однако наиболее критическое значение имел тот факт, что коммерческие сайты в сети AT&T также были не доступны.



Рисунок 10: Сообщения в твиттере компании GoDaddy.

“Из-за DDoS-атаки, посредством которой была предпринята попытка вывести из строя наши DNS-сервера в двух территориальных точках, некоторые клиенты компании AT&T испытывали периодические сбои в обслуживании. Усилия по восстановлению обслуживания принимаются в полном объеме, мы приносим извинения за любые неудобства, которое могли испытать наши клиенты. Наши самые квалифицированные технические специалисты вовлечены в борьбу по ликвидации данной проблемы”.

- Сообщение представителя компании AT&T во время атаки

Рисунок 9: Источник - Martyn Williams, IDG News Service.

GoDaddy

10 ноября компания GoDaddy, крупнейший хостинг-провайдер и регистратор доменных имен, пострадала от атаки типа DNS-флуд, которая нанесла ущерб миллионам доменов в сети интернет. Был недоступен не только домен www.godaddy.com, но и все домены, зарегистрированные через компанию GoDaddy, которые использовали ее имя сервера, DNS записи были также недоступны.

Атака группы Anonymous на корневые серверы

31 марта хактивисты группы Anonymous угрожали вывести из строя всю сеть Интернет путем атаки на 13 корневых DNS-серверов. Группа планировала использовать технику «усиленного отражения» DNS-запросов, ими была выпущена утилита Ramp, которая была разработана для подключения ресурсов множества интернет-провайдеров и других корпоративных DNS-сервисов для выведения из строя корневых серверов. В конечном итоге, нападение так и не состоялось, но изощренный план (см. ниже раздел «Атака путем отраженных DNS-запросов») обладал разрушительный потенциалом.

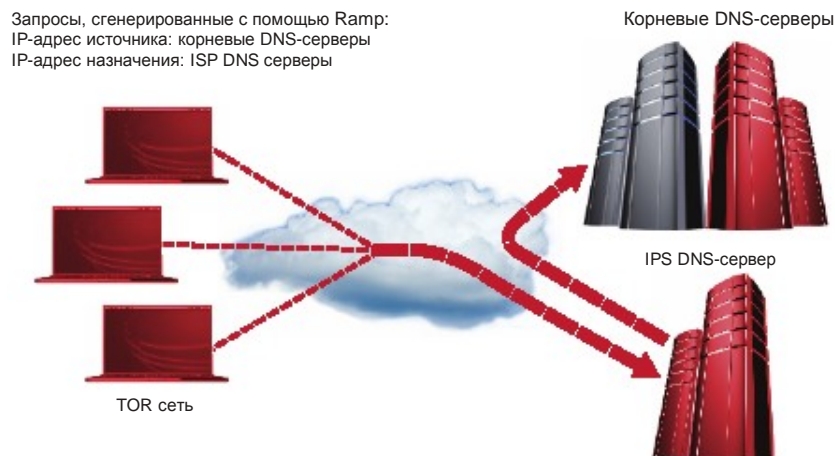


Рисунок 11: атака посредством отражения DNS-запросов.

Четыре типа атак на DNS-серверы

DNS DoS-атаки можно классифицировать, взяв за основу четыре метода, которые отличаются используемым подходом, процессом и получаемым усилением атаки.

Простой DNS-флуд

Используя простой DNS-флуд, злоумышленник отправляет множественные DNS-запросы на DNS-сервер, переполняя сервер запросами и потребляя его ресурсы. Такой метод атаки является привлекательным, поскольку он относительно прост в исполнении и позволяет скрыть личность злоумышленников.

Как это работает? Злоумышленник генерирует DNS-пакеты, которые отправляются посредством **UDP-протокола** на DNS-сервер. Стандартный ПК может сгенерировать 1000 DNS-запросов в секунду, тогда как обычный DNS-сервер может обработать только 10000 DNS-запросов в секунду. Другими словами, для того, чтобы вывести из строя DNS-сервер, потребуется всего 10 компьютеров. Поскольку DNS-сервера главным образом используют UDP-протокол, злоумышленникам не требуется устанавливать соединения, и они могут изменить IP-адрес источника и замаскироваться.

Это свойство также на руку злоумышленникам – атаку, исходящую от множества измененных IP-адресов источника, тяжелее отразить, чем ту, которая исходит от ограниченного списка IP-адресов.



Рисунок 12: Используя простой DNS-флуд, атакующий отправляет большое количество DNS-запросов на целевой DNS-сервер, переполняя его запросами и выводя его из строя.

Атака посредством отраженных DNS-запросов

Благодаря асимметричному характеру, атака с помощью отраженных DNS-запросов позволяет создать эффект переполнения, имея в распоряжении ограниченные ресурсы.

Как это работает? Злоумышленник отправляет DNS-запрос на один или несколько сторонних DNS-серверов, которые не являются реальными объектами нападения. Злоумышленники изменяют IP-адрес источника DNS-запроса на IP-адрес целевого сервера (объекта нападения), тогда ответ сторонних серверов будет отправлен на сервер, который является целью нападения.



Рисунок 13: В процессе атаки путем отражения DNS-запросов злоумышленник посылает DNS-запросы сторонним серверам, заменяя IP-адрес источника запроса на IP-адрес целевого сервера (объекта нападения). Ответ, отправляемый сторонними серверами, достигает целевого DNS-сервера, увеличившись в 3-10 раз.

В процессе атаки используется эффект усиления, при котором ответ на DNS-запрос в 3-10 раз больше, чем сам DNS-запрос. Другими словами, на атакуемый сервер поступает гораздо больше трафика по сравнению с небольшим количеством запросов, сгенерированных злоумышленником. Атака посредством отраженных запросов демонстрирует, что организации не требуется владеть DNS-сервером, чтобы стать объектом DNS-атаки, поскольку целью атаки является вывод из строя канала интернет-соединения или межсетевого экрана.

Атаки, выполняемые посредством отраженных DNS-запросов, могут включать несколько уровней усиления:

- **Естественный** – DNS-пакеты, отправляемые в ответ на запрос, в несколько раз крупнее пакетов, которые отправляются при запросе. Таким образом, даже самая базовая атака может получить 3-4 кратное усиление.
- **Выборочный** – ответы на DNS-запросы имеют различный размер: в ответ на некоторые DNS-запросы отправляется короткий ответ, в ответ на другие ответ гораздо больше. Более находчивый злоумышленник может сначала определить, какие доменные имена в ответе сервера имеют больший размер. Отправляя запросы только для таких доменных имен, злоумышленник может достигать 10-кратного усиления.
- **Настроенный вручную** – на высоком уровне злоумышленники могут разработать определенные домены, для отправки имен которых требуется пакеты огромных размеров. Отправляя запросы только на такие специально созданные доменные имена, злоумышленник может достигать 100-кратного усиления.

Степень анонимности при такой атаке возрастает с увеличением ее размаха. Помимо изменения SRC IP (как при простом DNS-флуде), атака сама по себе производится не напрямую – запросы на атакуемый сервер отправляются сторонним сервером.

Атака с помощью рекурсивных DNS-запросов

Атака посредством рекурсивных запросов является наиболее сложным и асимметричным методом атаки на DNS-сервер, для ее организации требуются минимальные вычислительные ресурсы, а результат приводит к интенсивному потреблению ресурсов DNS-сервера, который подвергается нападению.

Как это работает? При такой атаке используются особенности работы рекурсивных DNS-запросов. В рекурсивных DNS-запросах, когда DNS-клиент делает запрос с именем, которое отсутствует в кэш-памяти DNS-сервера, сервер отправляет повторяющиеся запросы другим DNS-серверам до тех пор, пока нужный ответ не будет отправлен клиенту. Воспользовавшись особенностями данного процесса, злоумышленник отправляет рекурсивные запросы с использованием фальшивых имен, которые, как он знает, не существуют в кэш-памяти сервера (смотрите пример скриншота экрана). Чтобы разрешить такие запросы, DNS-сервер должен обработать каждую запись, временно сохраняя ее, и отправить запрос другому DNS-серверу, затем дождаться ответа. Другими словами, потребляется все большее количество вычислительных ресурсов (процессора, памяти и пропускной способности), до тех пор, пока ресурсы не заканчиваются.

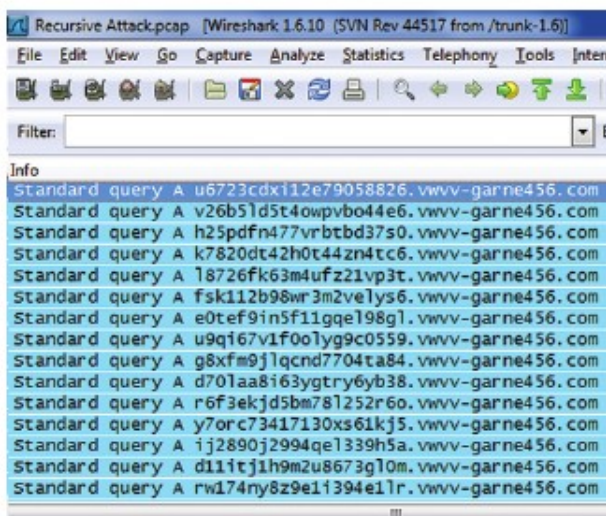


Рисунок 14: атака через рекурсивные DNS-запросы осуществляется путем отправки имен, которых не существует в кэш-памяти DNS-сервера. Это вынуждает сервер повторно отправлять запросы другим DNS-серверам, в то время как свободные вычислительные ресурсы стремительно сокращаются.

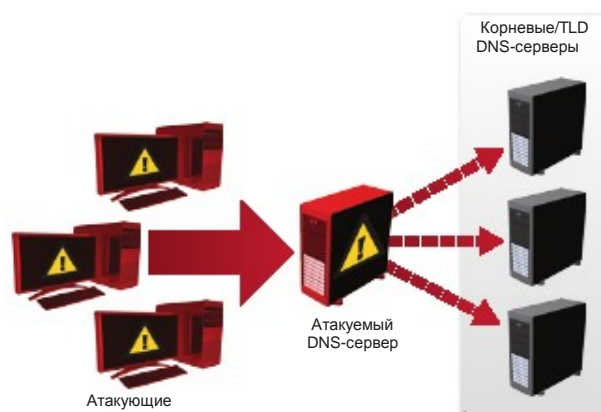


Рисунок 15: Рекурсивный DNS-флуд, злоумышленник отправляет DNS-запросы с фальшивыми именами, которых нет в кэш-памяти DNS-серверов. Вследствие этого серверу требуется выделять дополнительные вычислительные ресурсы, многократно отправляя запросы другим DNS-серверам до тех пор, пока ресурсы не заканчиваются.

Асимметричный характер рекурсивной атаки и низкая скорость затрудняют борьбу с такими атаками. Рекурсивная атака может быть пропущена как системами защиты, так и людьми, которые больше сосредоточены на выявлении атак с большим объемом.

Атака типа Garbage DNS

Как подразумевает ее название, такая атака переполняет DNS-сервер «мусорным» трафиком, отправляя пакеты данных большого размера (1500 байт или больше) на его UDP-порт 53. Концепция такой атаки состоит в том, чтобы переполнить сетевой канал пакетами данных большого размера. Злоумышленники могут генерировать потоки «мусорных» пакетов и с помощью других протоколов (UDP-порт 80 также часто используется); но при использовании других протоколов объект может остановить атаку, заблокировав порт на уровне ISP без каких-либо последствий. Протоколом, для которого такая защита недоступна, является протокол DNS, поскольку большинство организаций никогда не закрывает этот порт.



Рисунок 16: Во время «мусорного» DNS-флуда злоумышленник переполняет DNS-сервер пакетами данных большого размера, которые отправляются на UDP-порт 53. При организации такой атаки злоумышленники пользуются тем, что организации всегда держат DNS порт открытым и не станут блокировать его трафик на уровне маршрутизатора.

Выводы

Атаки на DNS приобрели высокую популярность, поскольку они предоставляют злоумышленникам множество преимуществ:

- **Ведется атака на критически важную инфраструктуру** – DNS-сервер является важным элементом инфраструктуры. Это означает, что если нарушается работа DNS-сервиса организации, отключается весь ее интернет-трафик. На более высоком уровне, если вывести из строя корневые DNS-серверы – весь интернет перестанет функционировать (что попыталась осуществить группа Anonymous в «Операции Blackout»).
- **Асимметричный характер атаки** – асимметричное усиление позволяет атакам на DNS вызвать отказ в обслуживании, пользуясь ограниченными ресурсами и небольшим трафиком.
- **Сохранение анонимности** – не использующий информацию о состоянии протокол DNS позволяет злоумышленникам изменить их IP-адрес источника и легко замаскироваться. Используя метод отражения, злоумышленник даже не посылает трафик непосредственно на объект атаки. В современных условиях, после большого количества арестов хакеров и членов группы Anonymous, сохранение анонимности является важным преимуществом.

Проблема HTTPS

Есть два допущения в отношении борьбы с DoS/DDoS-атаками. Во-первых, требуется остановить атаку как можно раньше, прежде чем она проникнет глубоко в сеть. Во-вторых, что является более очевидным, требуется проверять весь трафик. Этого нелегко добиться при атаках, основанных на использовании протокола HTTPS. Команда ERT столкнулась с возросшим количеством просьб о помощи в борьбе с HTTPS-атаками. Удивительно, что такие атаки раньше не так часто использовались, однако теперь ожидается резкий рост их популярности.

Понимание уязвимостей SSL и HTTPS

Почему HTTPS-атака представляет такую угрозу? Несмотря на то, что в ней используется протокол, аналогичный протоколу HTTP, она представляет угрозу совершенно иного уровня. Причина в следующем: как правило, HTTP-атаки можно обнаружить и ликвидировать с помощью системы защиты от DDoS-атак, которая расположена на клиентском оборудовании (CPE), в облаке или, в идеальном случае, и там, и там. Такие решения могут справиться с HTTP-атаками уровня приложений или атаками на переполнение сети

Ссылки по теме

- Operation Blackout – Get Yourself Prepared - Ronen Kenig
- DNS Amplification Attack (YouTube)

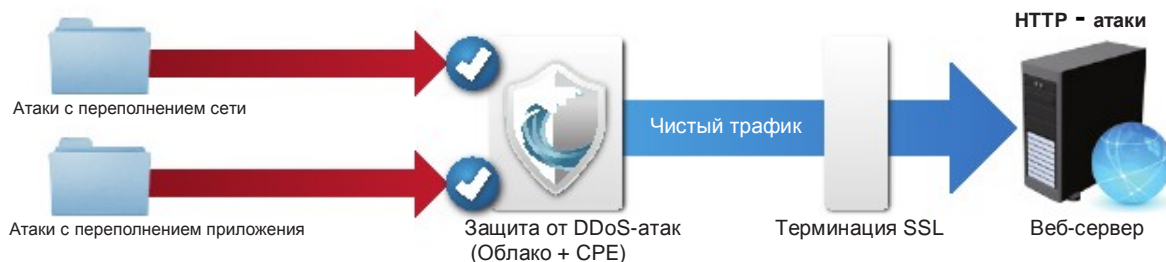


Рисунок 17: HTTP-атаки, отраженные системами защиты от DDoS-атак.

Однако когда те же самые атаки выполняются посредством протокола HTTPS, дела обстоят по-другому. Сетевые флуды могут быть остановлены; данные пока не шифруются, и SYN-флуд, к примеру, по HTTPS выглядит точно также, как и по HTTP. Однако атаки на приложения достаточно сложно обнаружить.



Рисунок 18: Атаки по протоколу HTTPS не фиксируются системами защиты, расположенными в облаке или на оборудовании клиента. Трафик по HTTPS на уровне приложения шифруется, и поэтому он не может быть проверен защитными механизмами. Кроме того, HTTPS уязвим для атак с уникальным SSL.

Как показано на рисунке, зашифрованный HTTPS-трафик обычно дешифруется только на веб-сервере, балансировщике нагрузки или выделенном устройстве для SSL-терминации. Данные объекты обычно лежат дальше в сети после того уровня, где трафик проверяется системами защиты от DoS-атак (в облаке или CPE):

- Поскольку организации неохотно соглашаются на передачу своих ключей SSL и сертификата в MSSP облака, ведь такое действие несет определенные риски, система защиты от DoS-атак, расположенная в облаке, не может проанализировать зашифрованный трафик, и, следовательно, не может обнаружить атаку.
- CPE-устройство также видит данные в зашифрованном виде, и тоже не может их проанализировать. Следовательно, заметить атаку получается слишком поздно, после того, как она уже достигла своей цели.

SSL-атаки

Помимо HTTPS-атак, существуют атаки, присущие именно уровню SSL, которые нацелены непосредственно на механизм обмена данными по SSL. SSL-атаки, которые выполняются с помощью инструмента THC-SSL-DOS, подробно обсуждались в отчете за 2011 год, однако мы вкратце изложим этот вопрос.

Обычно SSL-подтверждение выполняется только единожды с целью установки безопасного соединения. Для атаки используется опция протокола на «повторное согласование» для установки нового секретного ключа. Отправляя многократные запросы на повторное SSL-согласование, злоумышленник значительно повышает нагрузку на процессор целевого сервера до того момента, когда тот уже не может дальше работать.

Ссылки по теме

- THC-SSL-DOS Attack Tool - YouTube
- THC-SSL-DOS - Radware 2011 Global Application and Network Security Report (см. Главу 8)

В тех случаях, когда сервером не поддерживается опция «повторного согласования», злоумышленник может открывать новые SSL-соединения, что приведет к такому же эффекту. SSL-атака носит асимметричный характер - ресурсы, необходимые серверу для обработки подтверждения, в 15 раз больше тех, которые требуются от устройства, запросившего подтверждение (атакующего).

Выводы и рекомендации

Протокол HTTPS поддерживается практически всеми веб-сайтами и является важным компонентом финансовых сайтов, где с его помощью защищаются денежные операции. С учетом сложности выявления HTTPS-атак, мы ожидаем увидеть резкий рост популярности таких атак и рекомендуем организациям, особенно тем, кто работает в финансовом секторе, приобрести решение по борьбе с данной проблемой.

Сеть CDN - не препятствие для хакеров

Благодаря способности значительно повышать производительность сети, в течение последних лет сети доставки контента (Content Delivery Network, CDN) быстро набирают популярность, контролируя все большее количество трафика в интернете. Сети CDN работают путем сохранения статического контента в кэш-памяти своих собственных серверов и размещения его ближе к пользователям по всему миру, что позволяет ускорить доступ. Вероятно вследствие того, что большинство данных хранятся на серверах сети CDN, пользователи начали верить, что сети CDN, помимо всего прочего, обеспечивают защиту от DoS/DDoS-атак. Согласно опросу, проведенному Radware, 70% пользователей сетей CDN верят, что CDN также предоставляет решение защиты от DoS/DDoS-атак.

Считаете ли вы, что сеть CDN является решением защиты от DoS/DDoS-атак?

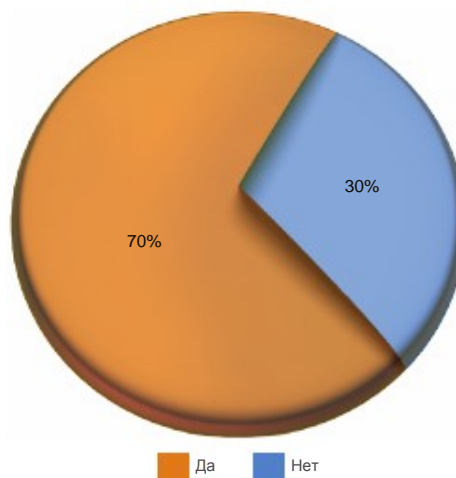


Рисунок 19: 70% компаний, использующих сети CDN, верят, что CDN сеть защищает от DoS/DDoS-атак.

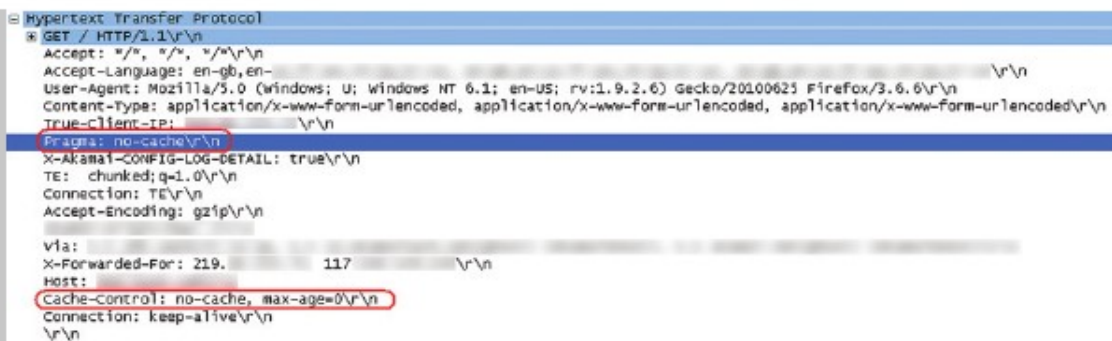
Действительно, сеть CDN может поглотить крупномасштабные атаки, превращая перегрузку центра обработки данных сетей CDN в сложную задачу. Сеть полностью контролирует сохраняемые данные и доступ к ним пользователей. Данные также защищены с помощью тестов для распознавания людей и машин (*Captcha*) или других методов аутентификации пользователей.

К сожалению, такие меры создают ложное чувство безопасности. Сети CDN не призваны и не оборудованы для полной защиты от DoS/DDoS-атак, и способны защитить только те данные, которые хранятся в пределах таких сетей; а данные в ЦОД клиентов остаются незащищенными. В сложных DDoS-атаках используются несколько векторов атак для того, чтобы направить атаку непосредственно на уязвимости ЦОД клиента в обход сети CDN. Вот несколько примеров того, как это может произойти.

Пробелы в безопасности сетей CDN, которые могут быть использованы для организации DoS-атак

Динамические данные – в сетях CDN хранятся только статические данные. Все динамические данные, такие как рыночные котировки, текущие погодные условия, заголовки последних новостей и другие, хранятся в ЦОД клиента. На практике запросы на динамический контент идут в обход сети CDN и направляются непосредственно в ЦОД клиента. На этом строятся DoS-атаки, обходя сети CDN и системы защиты. Злоумышленник также может получить доступ к динамическому контенту, изменяя параметры рекурсивных запросов и заставляя сеть CDN «приподнять занавес» и направить запрос непосредственно в ЦОД.

Директивы системы кэширования данных – директивы системы кэширования представляют собой особые параметры HTTP-заголовка, которые дают указания сети CDN передать запрос серверу баз данных или отправить ответ, используя кэш-память. Команда Radware ERT была свидетелем множества ситуаций, когда злоумышленники использовали директивы системы кэширования, такие как «*cache-control: no-cache*» или подобные им указания «*Pragma: no cache*». С помощью этих директив злоумышленники обходят защитный уровень сети CDN даже для статических данных.



```
Hypertext Transfer Protocol
GET / HTTP/1.1
Accept: */*, */*, */*
Accept-Language: en-gb,en-...
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6
Content-Type: application/x-www-form-urlencoded, application/x-www-form-urlencoded, application/x-www-form-urlencoded
true-client-ip:
Pragma: no-cache
X-Akamai-CONFIG-LOG-DETAIL: true
TE: chunked;q=1.0
Connection: TE
Accept-Encoding: gzip
Via:
X-Forwarded-For: 219.117.
Host:
Cache-Control: no-cache, max-age=0
Connection: keep-alive
```

Рисунок 20: Злоумышленники используют директивы системы кэширования, такие как “*Pragma: no cache*” и “*cache-control: no-cache*” для того, чтобы обойти сеть CDN.

Особо распределенные атаки – распределенные в значительной степени атаки не достигают большого объема на любом из узлов сети CDN, и их мощность возрастает только по достижении атакуемого ЦОДа, в обход сети CDN вызывая отказ в обслуживании. Крупномасштабная сеть CDN не способна в реальном времени синхронизировать данные и статистику во всех ее точках, что мешает эффективно отследить распределенную атаку крупного или небольшого объема.

Примеры таких уязвимостей отчетливо показывают, что хотя сеть CDN дает надежную защиту от многих векторов атак, она, тем не менее, не может обеспечить полную защиту от DoS/DDoS-атак. Принцип 80/20 не может применяться в контексте обеспечения безопасности, поскольку хакеры всегда пользуются открытыми «дырами» или слабыми точками системы, эффективно используя те вектора атак, которые не покрываются системой защиты.

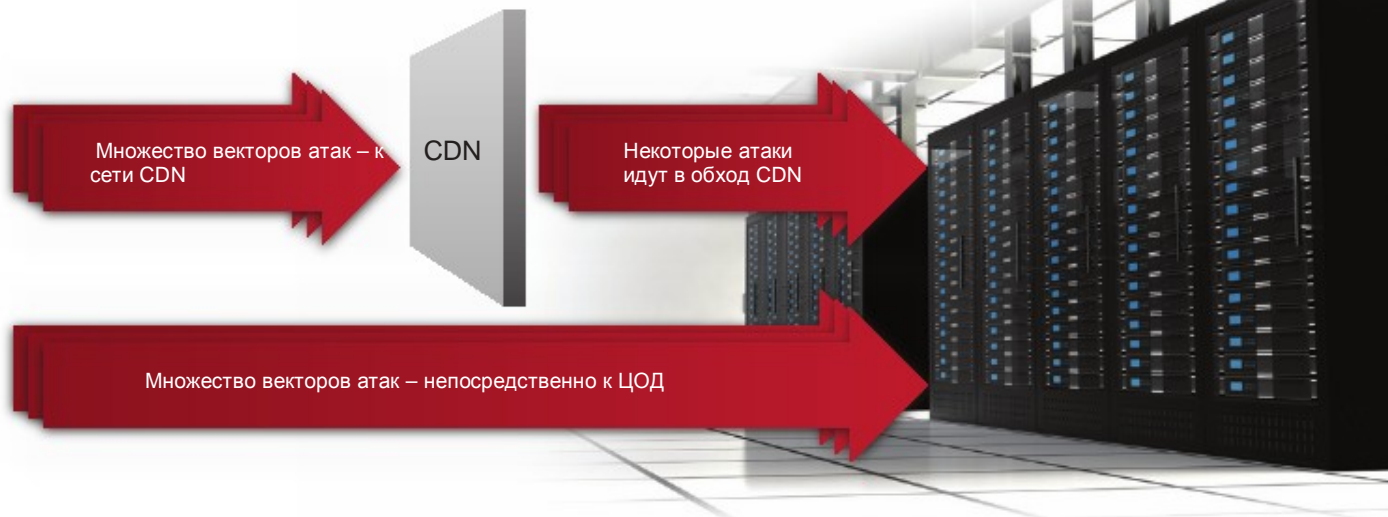


Рисунок 21: Несмотря на возможность CDN сетей блокировать некоторые векторы атак, существует множество способов обойти ее защиту и нацелить атаку типа "отказ в обслуживании" непосредственно на ЦОД.

Анализ примера DDoS-атак на сети CDN

Проанализируем атаку на крупную корпорацию, которую назовем BCDN. BCDN размещала некоторую часть своего контента на серверах крупного CDN-провайдера, однако динамические данные хранились в ЦОД компании. В процессе DDoS-атаки, нацеленной на BCDN, хакеры использовали три различных вектора атак.

По первому вектору искаженные TCP пакеты отправлялись на публичный IP-адрес BCDN, в то время как по второму вектору «мусорные» UDP пакеты отправлялись на порт 53 (DNS-порт). Компания BCDN использовала надлежащую систему защиты, благодаря которой первые два вектора атак были успешно остановлены.

Хакеры были осведомлены, что BCDN хранит данные в сети CDN, и использовали третий вектор атак. Данный вектор – простая атака типа HTTP-флуд – могла бы быть легко заблокирована, если бы система защиты не была бы расположена за сетью CDN. Как бы то ни было, здесь была использована техника обхода CDN – отправление запросов на доступ к динамическим данным ЦОД. Такая тактика привела к тому, что CDN пропустила хакеров к ЦОД.

Поскольку данный вектор проходил через сеть CDN, IP-адрес источника всех запросов представлял собой IP-адрес CDN и был признан легальным. Серверы сети CDN, а также любой легальный пользователь за пределами CDN, легко проходили проверку запрос-ответ, отправляемую системой отражения атак. В контексте обеспечения безопасности, после прохождения всех проверок IP-адрес помечается как «безопасный» (временно добавленный в белый список) и ему разрешается доступ к серверам. Как только CDN IP был помечен, как безопасный, все запросы, как легитимные, так и отправленные злоумышленниками, достигли ЦОД, вызвав отказ в обслуживании.

Была предпринята попытка ограничить трафик, установив пороговую величину. Однако избирательно заблокировать определенных клиентов было невозможно, и ограничение было установлено для всех CDN соединений. Поскольку большая часть соединений относилась к атаке, легитимные пользователи, расположенные за CDN сетью, не могли получить доступ к серверам компании BCDN. Данный метод отражения атаки оказался неэффективным и не помог остановить DoS-атаку, поскольку как легитимный трафик, так и трафик злоумышленников исходили от одного и того же IP-адреса.

Единственным местом, где содержался фактический IP-адрес пользователя, являлся заголовок XFF (X-Forwarded-For) HTTP-пакета. Чтобы заблокировать атаку, на основе XFF данных был произведен офлайн анализ IP-адресов атакующих. Как только IP-адреса были идентифицированы, их заблокировали путем проверки XFF на IP-адреса злоумышленников. Данный пример наглядно демонстрирует тот факт, что отражение атаки, которая проходит в обход CDN, является сложной задачей, для решения которой требуется вмешиваться вручную, что занимает много времени.

2012 год в сравнении с 2011-м – краткий обзор тенденций

Каждый год мы оглядываемся назад и сравниваем статистику сетевых атак за прошедший год с предыдущим годом. Мы обращаем внимание на набор ключевых параметров, таких, как распространенность атак, проблемные места инфраструктуры, инвестиции в решения против DoS-атак, мотивы и вероятность подвергнуться DoS-атаке. В данном разделе мы представляем результаты наших исследований с анализом полученных данных.

Распространенность атак – без существенных изменений

При анализе распространенности определенных типов атак не замечено никаких серьезных изменений в контексте используемых протоколов. Также соотношение атак на приложения к атакам на сеть сохранилось в районе 50:50, каким оно было и в 2011 году.

Разнообразие типов атак возникает вследствие использования злоумышленниками множества векторов атак. Эффективная атака обычно состоит из двух атак на сеть и двух атак на приложение. Таким образом, возросшая популярность определенного типа атаки не оказывает заметного влияния на общую распространенность тех или иных видов атак, поскольку он представляет собой только один из векторов кампании в целом. Это отражено в статистике, которая показывает большое разнообразие типов атак.

Отраслевое исследование – Статистика распространенности отдельных типов атак

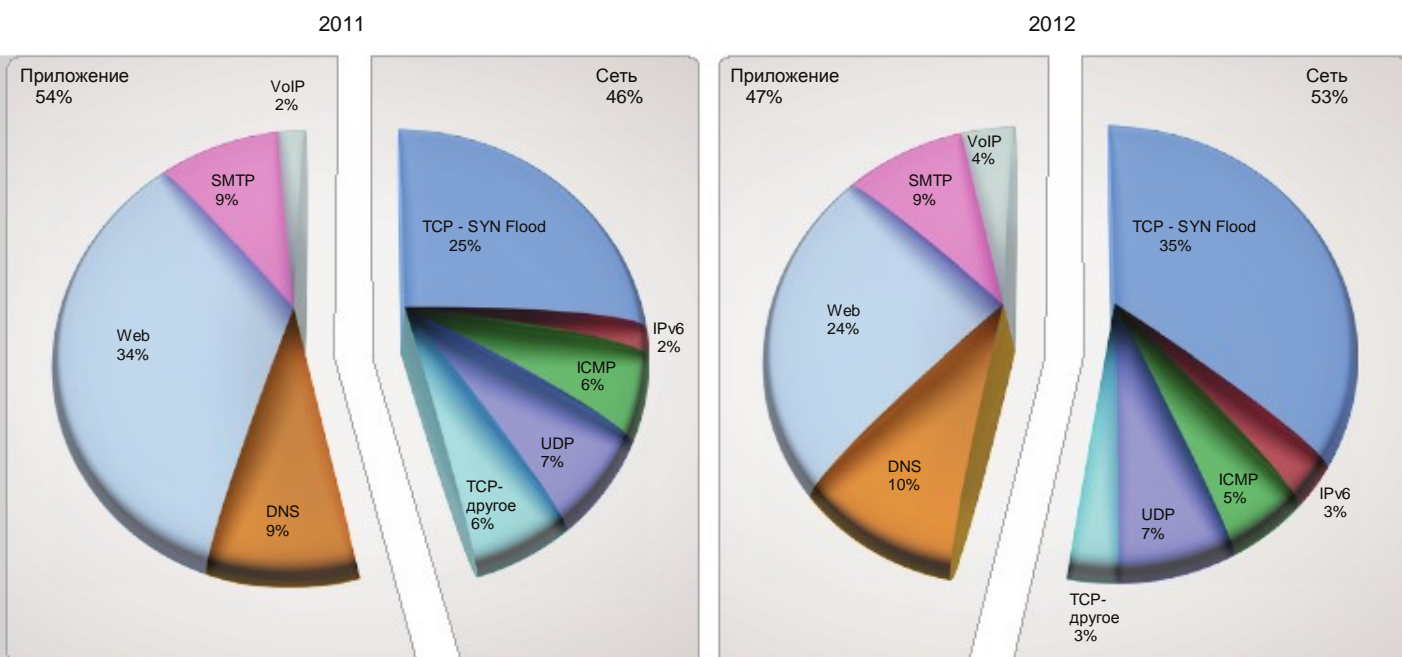
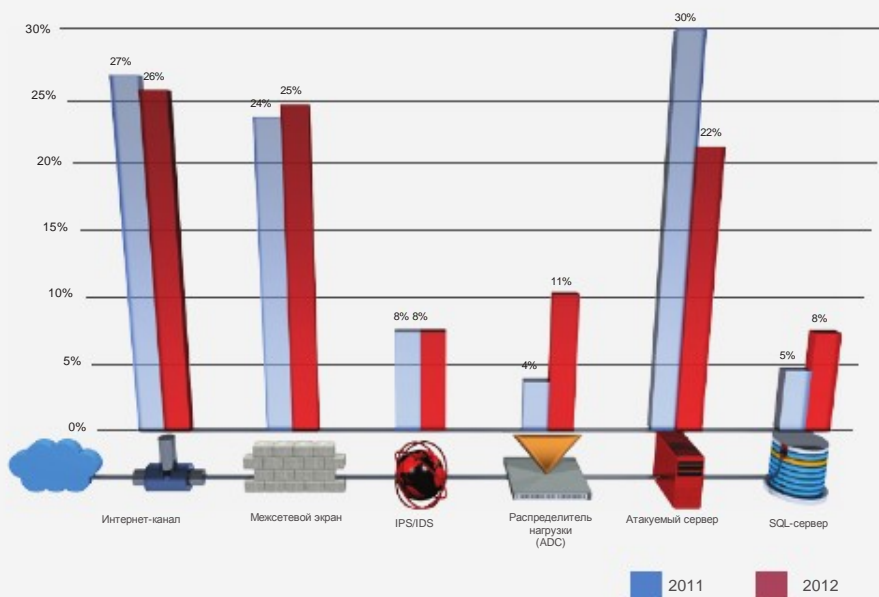


Рисунок 22: Сохранялось большое разнообразие атак различных типов. Это демонстрирует тот факт, что злоумышленники применяют многовекторные атаки.

Отраслевое исследование Какие службы или сетевые элементы являются (или являлись) уязвимыми для DoS-атак?

Рисунок 23: Три элемента, которые всегда уязвимы для DoS/DDoS-атак, - это атакуемый сервер, межсетевой экран и интернет-канал.



Уязвимыми элементами являются сервер, межсетевой экран и канал интернет

По аналогии с прошлым годом, тремя наиболее уязвимыми элементами, которые часто использовались для DoS/DDoS-атак, являются сервер, межсетевой экран и интернет-канал.

- **Серверы** являются уязвимыми по той простой причине, что злоумышленники часто организуют свои атаки таким образом, чтобы они потребляли больше ресурсов, чем те, которыми обладает сервер.
- **Интернет-канал** становится уязвимым для атак, которые нацелены на истощение пропускной способности, и называются «объемный флуд». К таким атакам относятся UDP-флуд или TCP-флуд, потребляющие много пропускной способности канала.
- Несмотря на то, что **межсетевой экран** является инструментом обеспечения безопасности и не должен служить уязвимым местом для DoS/DDoS-атаки, во время проведения таких атак, как SYN-флуд, UDP-флуд и переполнение соединения, злоумышленники могут генерировать многие состояния, что истощают ресурсы межсетевого экрана до тех пор, пока он сам не становится слабым местом инфраструктуры.

Организации увеличивают инвестиции в системы отражения DoS/DDoS-атак

Поскольку DoS/DDoS-атаки являлись наиболее часто используемым типом атак в 2011 году, у организаций было время отреагировать на такое положение вещей. К 2012 году компании стали более ясно осознавать необходимость приобретения решений, специально разработанных для борьбы с DoS/DDoS-атаками, вместо того, чтобы использовать ограниченные возможности решений более широкого круга действия. В частности:

- Использование «общих» решений по борьбе с DoS/DDoS-атаками, таких, как межсетевой экран и IPS, сократилось на 13% в 2012 году. Причиной также послужил тот факт, что известные производители межсетевых экранов больше не позиционируют свой продукт в качестве решения для борьбы с DoS-атаками.
- Организации стали больше надеяться на помощь специальных решений по борьбе с DoS-атаками, обращаясь к компаниям, предоставляющим свои услуги в области обеспечения безопасности (Managed Security Service Provider, MSSP).
- Как уже обсуждалось во вводной главе, организации используют устаревшие методы борьбы. Компании по-прежнему редко обращаются к услугам экспертов по борьбе с DoS/DDoS-атаками, но мы надеемся, что число таких компаний возрастет.

Отраслевое исследование Какие решения для борьбы с DoS-атаками использует ваша организация?

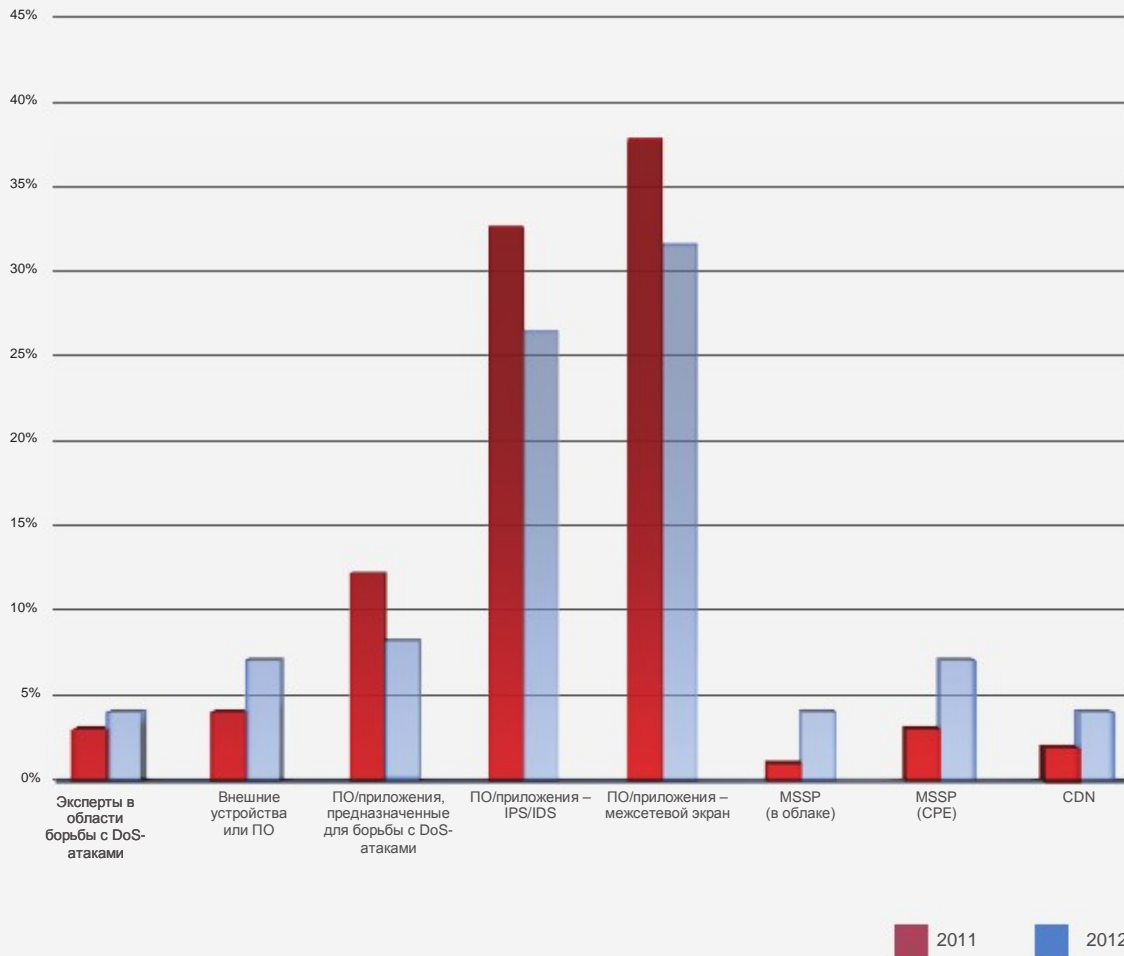
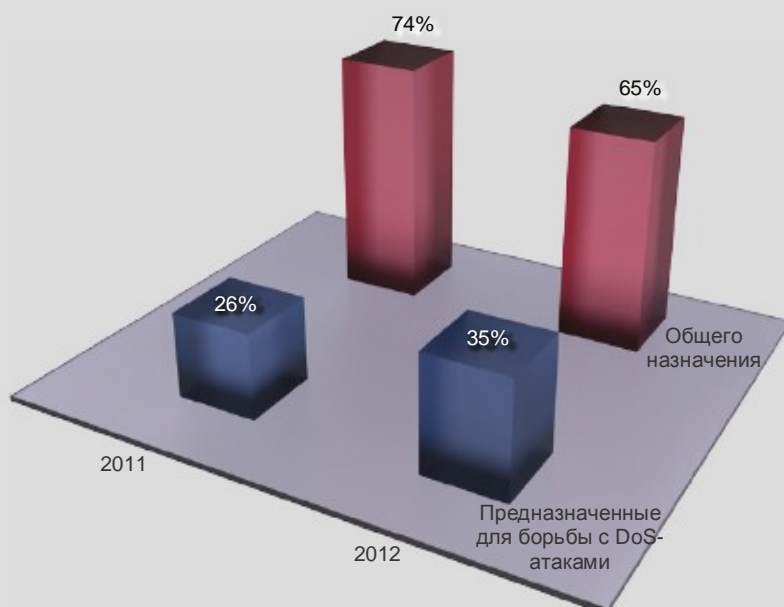


Рисунок 24: Какие решения по борьбе с DoS-атаками использует ваша компания?



Отраслевое исследование Специализированные решения в сравнении с решениями общего назначения

Рисунок 25: В 2012 году организации чаще использовали решения, специально разработанные для борьбы с DoS-атаками, а не общие решения по обеспечению безопасности.

Мотивы организации DoS-атак не изменились

В отличие от 2011 года, когда наблюдалось резкое увеличение случаев «хактивизма» и политически-ориентированных атак, в 2012 году не наблюдалось каких-либо изменений.

Мотивы большинства атак по-прежнему не ясны. В тех случаях, когда мотивы известны, политические причины/хактивизм лежат в основе 50% всех нападений. У нас есть основания полагать, что в 2012 году политические причины набрали большую популярность, по сравнению с атаками групп хактивистов. Появилось большее количество атак, организованных по политическим мотивам при поддержке правительства.

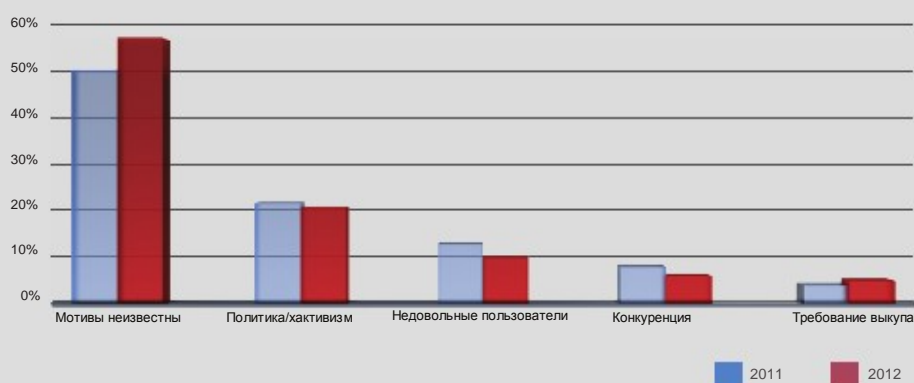


Рисунок 26: Мотивы DoS-атак не изменились в 2012 году по сравнению с прошлым годом.

Отраслевое исследование Какие из следующих причин послужили мотивами организации DoS/DDoS-атак на вашу компанию?

Рисунок 27: Мотивы организации большинства DoS-атак по-прежнему не ясны. Среди атак, мотивация которых была известна, более половины являлись атаками хактивистов по политическим причинам.



Линия огня приближается к финансовым организациям

В 2012 году правительственные сайты по-прежнему находились под прицелом DoS/DDoS-атак, также, как и годом ранее. Изменения 2012 года состояли в том, что финансовый сектор также приблизился к тому, чтобы стать главной мишенью для злоумышленников.

Одной из крупномасштабных атак является так называемая Operation Ababil, которая проходила в сентябре 2012. Тогда атаке подверглось большое количество банков и финансовых организаций США. Как утверждается, атака была связана с выпуском трейлера фильма «Невинность мусульман», который был загружен на YouTube. Фильм содержал сцены, которые, по некоторым оценкам, являлись оскорбительными, и вызвал волну демонстраций, протестов и насильственных атак на посольства США в мусульманских странах. 18 сентября 2012 года группа, называющая себя «Кибер воины Изз ад-Дин Аль Кассам», объявила о готовящейся кампании кибератак на то, что они называли «американские и сионистские» цели.

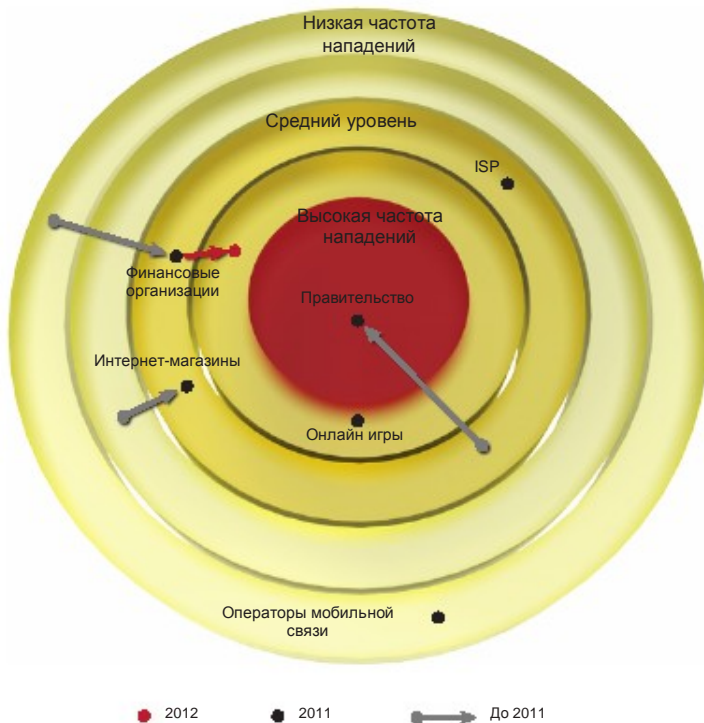


Рисунок 28



Тенденции развития инструментов атаки

DDoS – «Сделай сам»

Инструменты для организации DDoS-атак превратилась в предмет торговли. Конечно, их еще нельзя найти в свободной продаже в интернет-магазинах, но на нелегальных сайтах можно найти огромное количество различных вариантов – пакеты инструментов DDoS, прайс-листы и даже услуги организации DDoS-атак. Доступность таких DDoS пакетов снизила требования к организации сетевых атак и атак на приложения. Любой желающий, от частных лиц до криминальных киберорганизаций, может легко настроить ботнет для запуска атаки.

Пакеты инструментов для DDoS-атак

Пакеты инструментов, для использования которых не требуется писать код или быть опытным хакером, позволяют новичкам легко настроить ботнет. Пакет инструментов для DDoS-атак представляют собой пакет ПО, состоящего из двух компонентов - конструктора ботов и сервера управления.

- **Bot Builder** - инструмент для пошагового создания ботов с графическим интерфейсом, который позволяет атакующему создать исполняемый файл (бот), распространяемый на компьютеры, которые будут являться частью ботнета. Созданный бот содержит адрес сервера управления, с которым он может обмениваться данными.
- **Центр управления (Command and Control, C&C)** - представляет собой страницу администратора, которая используется злоумышленником для отслеживания состояния ботов и отправления команд.

Текущие цены на российском черном рынке:

Пакет для взлома корпоративного почтового ящика: \$500
 Винлокер (блокирующая вирусная программа) для требования выкупа: \$10-\$20
 Пакет эксплоитов (неинтеллектуальный): \$25
 Интеллектуальный пакет эксплоитов: \$10-\$ 3000
 Базовый криптор (для вставки кода в файл): \$10-\$ 30
 Бот SOCKS (для обхода межсетевых экранов): \$100
 Заказ DDoS-атаки: \$30-\$70/день, \$1200/месяц ←
 Ботнет: \$200 за 2000 ботов
 Ботнет для DDoS-атаки: \$700 ←
 ZeuS исходный код: \$200-250
 Руткит для Windows (для установки вредоносных драйверов): \$292
 Инструменты взлома Facebook или Twitter аккаунтов: \$130
 Инструменты взлома Gmail аккаунта: \$162
 Инструменты для рассылка спама по электронной почте: \$10 за миллион электронных писем
 Инструменты для мошенничества по электронной почте (с помощью клиентской базы данных) \$50-\$500 за один миллион писем

Рисунок 29: DDoS продукты и сервисы, предлагаемые на российском черном рынке.

Сразу после установки C&C и подготовки исполняемого бота, злоумышленник должен передать бот как можно большему количеству других компьютеров, которые станут частью ботнета, используя общедоступные методы, такие как социальная инженерия и атаки для попутной загрузки, когда веб-браузер, будь это Internet Explorer или Chrome, используется для того, чтобы обманным образом побудить пользователя загрузить и запустить вредоносное ПО. Как только армия ботов достигает нужных размеров, можно запускать атаку.

Как любые профессиональные разработчики ПО, разработчики инструментов для DDoS-атак совершенствуют свои продукты и выпускают новые версии, которые затем публикуются и продаются. В мире нелегального ПО большинство таких пакетов представляют собой версии других ботов, исполняемые файлы и/или исходный код которых был изменен и переименован. Группа инструментов, произведенных от общего источника, обычно называется «семейством».

DDoS-атаки на заказ

Распространенность DDoS-программ способствовала также появлению услуг заказных DDoS-атак. Преступные киберорганизации пользуются простотой применения пакетов для DDoS, чтобы на различных нелегальных форумах предлагать услуги выполнения таких атак.

Типичный «бизнес-сценарий» заказа DDoS-атаки может включать такие предложения, как «вывести из строя веб-сайт конкурентов» или, наоборот, применить вымогательство типа «заплатите нам за то, чтобы мы не выводили из строя ваш сайт».

TOP- DDOS Service (Support)
Order a ddos attack! Removable poster competition!

MENU

- Home
- Reviews
- Rates
- Methods of payment
- Contacts

Top-ddos

It seems that all is well and business have long gained its momentum, but has recently appeared a number of competitors with whom you just can not cope? Our company offers a **ddos attack order** , by which time your competitors go out of control due to *off and hang on their sites* .

Ddos-attack - this is one of the varieties of attacks on computers. Their goal is to prevent getting users to a particular site, resulting in attendance will be limited resources and competition with those of firms weakened. It should be noted that not all providers are able to protect against **attacks Doss** , and it follows that all the cards in your hand and you can earn more money while your competitors are trying to find a way out. **Order ddos attack** on our site is easy and very easily, and besides, our prices will pleasantly surprise you. Our *ddos service* will help you. Web sites of your competitors will be based on how much you need.

Type of attack

- ✓ HTTP (GET, POST)
- ✓ DOWNLOAD
- ✓ ICMP
- ✓ UDP
- ✓ SYN

Рисунок 30: Страница, предлагающая выполнение различных типов DDoS-атак «по требованию». Текст обещает, что потребитель будет приятно удивлен уровнем цен и простотой услуги

Вывод

Доступность инструментов для подготовки и выполнения DDoS-атак превратила такие атаки в предмет торговли, доступный для каждого. Можно с уверенностью предположить, что рынок таких инструментов будет развиваться, предлагая все новые возможности. Это вынуждает обороняющуюся сторону, организации-объекты нападений, изменять стратегии защиты.

Учитывая снижение требований к ресурсам и опытности хакера, организациям не следует удивляться тому, что число таких атак из года в год будет расти. Не меньше беспокойства вызывает тот факт, что цель доставки DDoS-атак растет и развивается. Для организаций, которые являются мишенью таких атак, это означает только одно: более изощренные и сложные атаки.

Пакет Dirt Jumper

Dirt Jumper представляет собой широко известное «семейство» DDoS-программ, которое породило другие известные варианты ботов, например, Pandora, Di-BotNet и DIY. Dirt Jumper продается примерно за \$800 и относится к разряду решений DIY («Сделай сам»). Он также используется для выполнения DDoS-атаки на заказ и может быть взят в аренду на нелегальном рынке за 30-70\$ в день. В последней 5-й версии пакета Dirt Jumper было заявлено о наличии многих возможностей (как было опубликовано на нелегальных форумах), таких как поддержка HTTP 2.0, антиотладка и антивиртуализация. Пока не подтвердилось наличие ни одной из этих возможностей.

Конструктор ботов

Конструктор ботов пакета Dirt Jumper создает build.exe файл, который затем используется для заражения других компьютеров. Продвинутые пользователи могут даже использовать пакеры для того, чтобы избежать обнаружения антивирусной программой.

Command & Control

Компонента Command and Control (C&C) позволяет злоумышленнику следить за новыми и активными ботами, а также отправлять ботам подробную информацию о цели и используемом векторе атаки. Боты отправляют HTTP POST запросы с фиксированными интервалами для того, чтобы обмениваться данными с C&C-сервером.

Режимы атаки

Dirt Jumper предлагает несколько режимов атак. Все атаки используют динамические заголовки referer, в сочетании со случайными агентами пользователя. Это создает уровень случайности, усложняющий обнаружение источника атаки для IPS и анти-DDoS решений, которые работают со статическими сигнатурами.



Рисунок 31



Рисунок 32

Для атаки **POST-флуд** используется запрос POST, в котором в теле запроса содержится целевая URL с рассчитанным числом в заголовке content-length.

Для атаки **HTTP-флуд** используются запросы GET без особых параметров, направляемые циклически по списку URL.

Атака **SYN-флуд** проводится так же, как HTTP флуд, при этом используется большее количество соединений для более агрессивной атаки.

При атаке **флуд из запросов на загрузку** используются простые HTTP GET запросы, хотя название подразумевает интенсивную загрузку с источника.

Флуд Анти-DDoS предположительно сбивает со следа стандартные решения по борьбе с DDoS-атаками. Однако этот метод не показал себя как простой и эффективный.

Серверы включаются в армию ботнетов

На заре возникновения атак DoS основным средством для запуска служила примитивная инфраструктура серверов. Однако на протяжении последнего десятилетия серверы исчезли со сцены, и на смену им пришли распределенные DoS-атаки на основе бот-сетей с сотнями и тысячами персональных компьютеров.

Недавно команда Radware ERT была свидетелем новых разительных перемен в сфере DDoS-атак – использованию серверов для организации ботнетов. В отличие от ранних атак, когда использовался всего один сервер, в новые DDoS-атаки включается множество серверов, расположенных в разных точках земного шара и объединенных в мощный ботнет. DDoS-атака с такой архитектурой на основе серверов по нескольким причинам может представлять большую угрозу, чем атаки обычных ботнетов:

- **Мощность атаки** – серверы обладают гораздо большей пропускной способностью загрузки, что позволяет, используя всего несколько машин, организовать атаку, равную атаке ботнета со многих клиентов. Примем, что средняя скорость подключения домашнего ПК составляет 600 Кбит/с, в то время как обычный сервер предлагает скорость от 1Мбит/с до 100Мбит/с – почти в 150 раз большая пропускная способность.
- **Надежность** – серверы работают более стабильно, нежели домашние ПК. Домашние ПК часто выключают или отключают от интернета, так что злоумышленники должны охватить гораздо большее количество компьютеров, чем фактически нужно для атаки. Серверы же всегда включены и доступны онлайн для атаки.
- **Управление атакой** – управление небольшим количеством доступных серверов позволяет избежать множества проблем, которые возникают при работе с тысячами ненадежных компьютеров ботнета.

Хотя инфраструктура ботнета из серверов является весьма эффективной, ее использование связано с некоторыми трудностями для злоумышленников:

1. Возможность отследить злоумышленников

Гораздо легче отследить и обнаружить группу или лицо, управляющее атакой с серверов, чем тех, кто прячется за домашними ПК, поскольку на серверах содержатся гораздо более эффективные и доступные журналы регистрации событий. Кроме того, системам противодействия атакам гораздо эффективнее удастся заблокировать DoS-атаку, исходящую от небольшого списка легко отслеживаемых атакующих по сравнению с распределенной ботнет атакой.

2. Мониторинг производительности

Поскольку производительность сервера находится под постоянным наблюдением, и их владельцы обычно платят за количество генерируемого трафика, гораздо легче обнаружить сервер, который начинает загружать огромное количество трафика в процессе атаки.

3. Защищенная среда

Обычно серверы расположены в контролируемой и защищенной ИТ-среде, так называемых серверных хозяйствах. В такой среде, вероятнее всего, существуют системы защиты приложений (антивирусные программы) и защиты сети (IPS или межсетевые экраны), которые повышают вероятность того, что атака будет обнаружена и заблокирована.

4. Высокие начальные требования

Создание армии серверов с ботами требует высоких специальных навыков. Например, ботнет с домашними ПК можно легко купить на черном рынке, или взломать и эксплуатировать в своих целях с помощью широко известных методов. Серверы, с другой стороны, потребуют более продвинутых, изощренных атак. Обычно атаки, исходящие из серверного ботнета, указывают на более сильного противника.

Некоторые вопросы, касающиеся ботнетов с использованием серверов, остаются открытыми. Например, оплачивают ли злоумышленники услуги онлайн-хостинга, чтобы беспрепятственно использовать сервера, или они атакуют сервера, взламывают и используют их в своих целях? Если взламывают, то какие векторы атак используются? Какие методы применяются для координации атак? И наконец, самый интересный вопрос – кто эти атакующие, которые пользуются новыми серверными ботнетами? Являются ли они хактивистами, совершающими нападения по политическим причинам? Или они принадлежат к преступным организациям, совершающим нападения по финансовым соображениям? Или это правительственные организации, начинающие кибервойну?

Пример из практики: 5 серверов = 100 бот-клиентов

В сентябре 2012 года некоторые из крупнейших финансовых институтов США подверглись массовым DDoS-атакам. Атака, известная как **Operation Ababil**, была направлена на такие организации, как NYSE, Bank of America, Chase Bank и другие. Веб-сайты были переполнены запросами, что привело к недоступности сервисов для потребителей, транзакции были нарушены на несколько часов.

Образцы данных, полученные при анализе данной атаки, указывают на то, что в атаке участвовали только несколько десятков ресурсов, разбросанных по нескольким странам, таким как Турция, США, Российская Федерация, Боливия, Китай.

Средняя пропускная способность сервера в данной атаке составила 10Мбит/с. Другими словами, пять атакующих серверов имели тот же эффект, как 100 клиентских машин в обычной ботнет атаке.

Изменения инфраструктуры DoS/DDoS-атак за последние годы

| | | | |
|--|---|---|---|
| <p>1998-2002</p> <p>Отдельные серверы Вредоносные программы, установленные на отдельных хостах и серверах (расположенных в большинстве своем в российских и восточноевропейских университетах), контролировались единым субъектом путем непосредственного обмена данными.</p> <p>Примеры: Trin00, TFN, Trinity</p> | <p>1998- по сегодня</p> <p>Сети ботнет Малозаметное вредоносное ПО устанавливалось, главным образом, на персональных компьютерах без согласия владельца; ПО контролировалось одним субъектом через не прямые каналы связи (IRC, HTTP)</p> <p>Примеры: Agobot, DirtJumper, Zemra</p> | <p>2010-по сегодня</p> <p>Добровольное вступление в ботнет Многие пользователи, являясь членами группы хактивистов, охотно позволяют пользоваться своими ПК. Используются доступные публично и установленные заранее методы и инструменты для атаки, по желанию создается канал связи для удаленного управления этими инструментами.</p> <p>Примеры: LOIC, HOIC</p> | <p>2012</p> <p>Бот-сети, состоящие из серверов Мощные, хорошо продуманные атаки, при которых используется расположенная в разных точках мира инфраструктура серверов. Несколько атакующих серверов генерируют тот же объем трафика, что и сотни клиентов.</p> |
|--|---|---|---|



Тенденции развития методов борьбы с атаками

Отражение атак, проходящих через сеть CDN

В главе [Сеть CDN – не препятствие для хакеров](#) подробно рассказывается о том, что CDN-сети не обеспечивают должного уровня защиты от DoS/DDoS-атак. Злоумышленники используют множество векторов атак для того, чтобы добраться до центров обработки данных (ЦОД) – атака при этом направляется в обход CDN-сети, она маскируется так, что ее становится сложно обнаружить и отразить.

Как решить данную проблему – пересылать контент посредством CDN, но в то же время обеспечить адекватные стратегии отражения DoS-атак? В этой главе предлагается решение в виде двухуровневого подхода. Сочетая защитные механизмы сети CDN и клиентского оборудования, данный подход использует сильные стороны обеих систем, чтобы обеспечить эффективное обнаружение и блокировку атак, которые маскируются под трафик сетей CDN.

Почему неэффективен «независимый» подход, при котором защита устанавливается только на СРЕ-оборудование

Одним из подходов к защите, который первоначально представляется вполне логичным, является установка защитного СРЕ-устройства в ЦОД, без учета роли CDN. Теоретически такое устройство должно преуспеть в выявлении и обработке любого трафика, независимо от его происхождения. Однако если DoS-атака маскируется под CDN-трафик, СРЕ-устройство не сможет защитить сеть.

При использовании CDN важно понимать, что такая сеть действует как прокси-сервер; любой трафик, прибывающий из сети CDN в центр обработки данных, будет содержать IP-адрес CDN в качестве адреса источника вместо того, чтобы содержать IP-адрес исходного пользователя. Следовательно, в случае DoS-атаки на ЦОД, вредоносный трафик будет сформирован таким образом, будто он исходит от CDN. Блокировка IP-адреса CDN приведет к блокировке всего трафика, направляющегося в ЦОД, что по сути приведет к отказу в обслуживании. В то же время IP-адреса CDN пропускают вредоносный трафик, что препятствует блокировке DoS-атаки.

Другой проблемой является обработка трафика после техники мультиплексирования, которая используется в сети CDN, при которой в одной сессии агрегируется множество запросов от пользователей. Этот подход позволяет экономить ресурсы, поскольку подтверждение TCP-соединения выполняется единожды. Тем не менее, даже если CPE-устройство фиксирует сомнительный запрос, оно не может заблокировать сессию целиком, поскольку в сессии содержится большое количество легитимных запросов. Частичная блокировка сессии сделает видимым CPE-устройство, в то время как его ресурсы будут истощаться, поскольку оно будет выступать в роли прокси-сервера, который должен изменить любые значения SEQ\ACK пакетов.

Выигрышный подход - сочетание защиты CPE-устройств и сети CDN

Двухуровневый подход сочетает средства защиты сети CDN и CPE-устройства, используя сильные стороны обоих элементов для максимального усиления защиты.

- **Обнаружение атаки** – располагаясь в ЦОД, CPE устройство способно тщательно анализировать все данные, независимо от используемого вектора атак, и вынести решение о типе атаки и требуемом способе ее отражения.
- **Отражение атаки** – CPE и CDN могут взаимодействовать и работать сообща в борьбе с атаками, когда CDN защищает кэшируемые данные, а CPE защищает все остальные данные. Такой подход позволяет использовать сильные стороны обоих компонентов, минимизируя их недостатки.
- **Защита от многовекторной атаки** – CPE-устройство способно отразить многовекторные атаки, которые включают непосредственное нападение на ЦОД, а также другие атаки, которые движутся в обход CDN.
- **Управление противодействием атакам** – средство отражения атак, размещенное в CPE, предоставляет единый пункт управления с полным контролем над всеми атаками и техниками борьбы с ними.

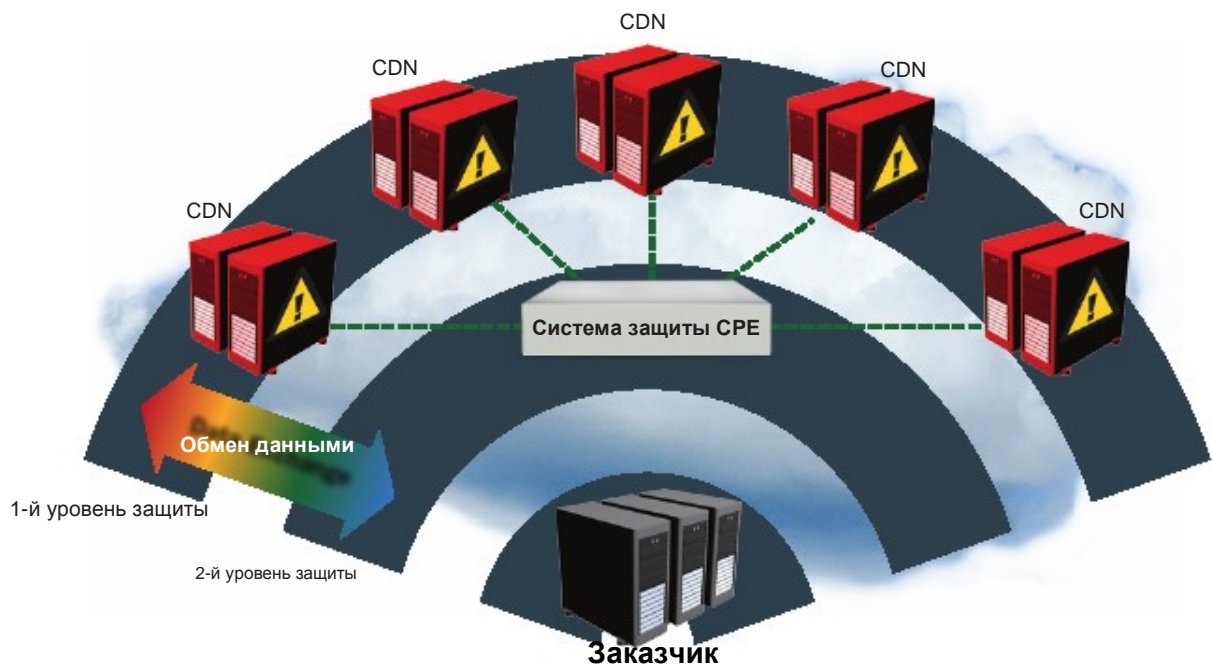
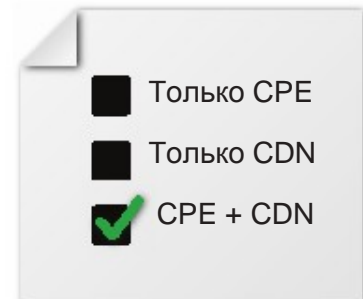


Рисунок 33: Два уровня защиты – CPE устройства и сеть CDN - для эффективной защиты заказчиков от DoS-атак, направляемых в обход CDN. Каждый уровень обеспечивает защиту от определенных типов атак, устройства обоих уровней взаимодействуют между собой.



Заключение

Рекомендации сообществу специалистов по сетевым технологиям и безопасности

В данном отчете подробно описываются выводы, полученные на основе двух исследований, проделанных командой Radware ERT. В заключение мы представляем свое мнение и соответствующие рекомендации.

Общие рекомендации

Создайте потенциал для борьбы с продолжительной и изощренной кибератакой

Результаты наших исследований наглядно демонстрируют тщательную подготовку злоумышленников к атаке, что позволяет им организовать и поддерживать эффективные весьма продолжительные атаки. Организациям требуется приложить не меньше усилий.

Проведенный нами анализ показывает, что разрыв между атакующими и защищаемыми лежит, прежде всего, в возможностях реагировать в реальном времени, но не в используемых технологиях или аналитических способностях. В частности, организации испытывают необходимость в экспертах, которые смогли бы динамично реагировать на смену векторов атак. (Более подробная информация по этому вопросу содержится в разделе [Организации используют устаревшие методы защиты](#)).

По этой причине организации должны проанализировать свои способности к удержанию обороны в течение длительного периода времени, к отражению изощренных атак, а также приблизительно оценить количество необходимых людских ресурсов. Например, если предположить, что в одну смену требуется наличие трех квалифицированных инженеров, а DoS-атака может длиться приблизительно три смены, организации потребуется минимум девять инженеров.

В большинстве случаев непрактично решать данную проблему посредством привлечения внутренних ресурсов, которые должны выполнять рутинные задачи, а также активно действовать во время атаки. Таким образом, организациям следует рассмотреть привлечение специалистов извне – из компаний, специализирующихся на предоставлении услуг по обеспечению безопасности, из отраслевых альянсов или государственных служб.

Отраслевое исследование

Как часто вы подвергались DDoS-атакам за последние 12 месяцев?

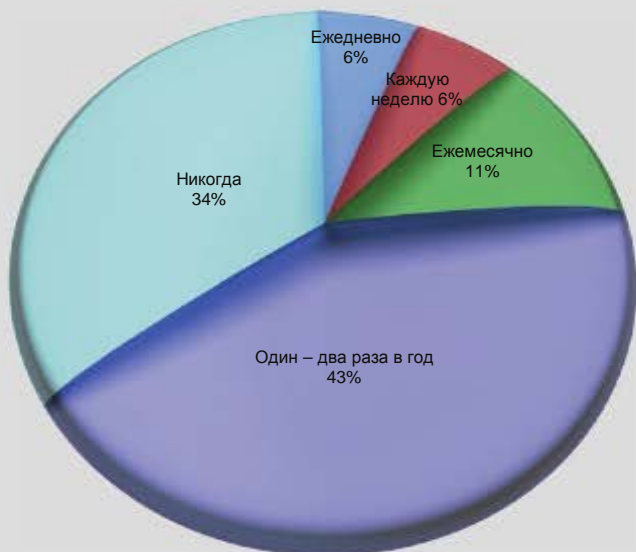


Рисунок 34: Частота DoS/DDoS-атак.

Убедитесь в наличии решений для следующих типов атак

- Объемные атаки (также в облаке)
- Атаки на приложение
- «Медленные» атаки
- DoS-атаки на уязвимости
- Команда реагирования
- HTTPS флуды (зашифрованный трафик)

Рекомендации по борьбе с DoS/DDoS-атаками

Ожидается, что DoS/DDoS-атаки сохранят свои позиции в качестве наиболее популярного типа атак в 2013 году

DoS/DDoS-атаки заняли лидирующие позиции в 2001 году, и эта тенденция продолжилась в 2012 году. Многие показатели указывают на это – начиная от сообщений средств массовой информации об организации крупномасштабных DoS-атак, до опроса Radware, который показывает, что 2/3 организаций подверглись атакам в прошедшем году, и заканчивая быстрым ростом числа атак, о котором сообщает наша команда ERT.

В 2013 году ожидается, что DoS/DDoS-атаки сохранят свои позиции в качестве основного типа атак. Характеристики DoS/DDoS-атак делают их чрезвычайно привлекательным. В отличие от некоторых уязвимостей в системе защиты, которые могут быть исправлены, простого решения по борьбе с DoS-атаками не существует. Кроме того, повсеместно распространяются инструменты для организации DoS-атак, требования к ресурсам и специалистам снижаются, буквально каждый желающий может совершить такую атаку.

Тщательно проверьте линии обороны против DoS/DDoS-атак

В 2012 году мы заметили тенденцию к инвестированию средств на поиск решений для защиты от DoS/DDoS-атак. Возможно, средства защиты улучшились, однако это побудило злоумышленников прийти к использованию более изощренных векторов атак и вкладывать средства в исследование уязвимостей систем защиты. Более подробная информация о данной тенденции содержится в разделе [2012 год в сравнении с 2011-м – Краткий обзор тенденций](#).

Организациям следует убедиться, что их линии защиты покрывают все части инфраструктуры и способны противостоять атакам с возросшим уровнем сложности. В рамках этого, следует полностью укомплектовать средства защиты, покрывая все возможные риски.

Многие организации реагируют на повышение популярности DoS/DDoS-атак, опираясь на существующие продукты по обеспечению безопасности: межсетевой экран, IPS или UTM и даже балансировщик нагрузки. Эти продукты способны заблокировать одну или несколько атак, но единственным реально действующим подходом является всеобъемлющая защита, покрывающая каждый из перечисленных компонентов:

- Решение, специально разработанное для защиты от DoS/DDoS-атак на клиентском оборудовании, используется для защиты от всех типов атак
- Решение, размещенное в облаке, защищающее канал от атак с большим объемом трафика
- Команда экспертов, доступная в любое время суток, способная реагировать на продолжительные и комплексные кибератаки.

Не рассматривайте дополнительные функции общей системы защиты в качестве полноценного решения для защиты от DoS/DDoS-атак

Как предлагается выше, наличие системы с некоторыми функциями по борьбе с DoS/DDoS-атаками нельзя сравнивать с полным, специально разработанным для защиты от таких атак решением. Далее представлен краткий пример, который поможет продемонстрировать верность данного утверждения.

Некая организация внезапно подверглась DoS/DDoS-атаке. Злоумышленники были настойчивы и постоянно меняли векторы атак для того, чтобы растянуть ее во времени. Положение было критическим, и организация обратилась к сторонним специалистам по безопасности, включая поставщиков межсетевого экрана и IPS. Представители организации обратились к ним с вопросом «кто из вас может остановить атаку?» Они не знали, что межсетевые экраны не рассчитаны на борьбу с DoS/DDoS-атаками, как не рассчитан на нее и IPS, поэтому возлагали на эти системы ложные ожидания. Это ложное чувство безопасности было основано на том факте, что используемые средства безопасности обладали некоторыми функциями по защите от DoS/DDoS-атак. Например, многие межсетевые экраны оснащены технологией защиты от атак типа SYN-флуд, однако те же самые межсетевые экраны не могут ничего противопоставить таким атакам, как HTTP-флуд. К Radware ERT часто обращаются с просьбой защитить продукт по обеспечению безопасности, который отказал первым, когда компания подверглась DoS/DDoS-атаке.

Тщательно спланируйте размещение DoS/DDoS решения в архитектуре сети

Для эффективной работы решение по борьбе с DoS/DDoS-атаками должно располагаться перед большинством других элементов сети. При типичной установке следует поместить его перед межсетевым экраном, чтобы оно могло защитить маршрутизатор, межсетевой экран, балансировщики нагрузки, интернет-сервисы и другие внутренние серверы. Кроме того, если решение развернуто внутри периметра, оно не может защитить интернет-канал от атаки с большим объемом трафика. Такую защиту можно получить, только используя решение, размещенное в облаке, которое гарантирует, что канал свободен от объемных атак.

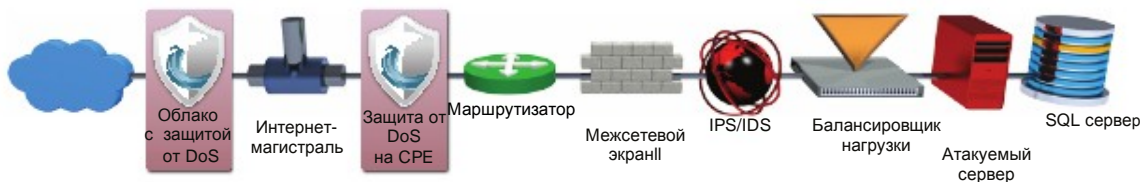


Рисунок 35

Используйте APT рейтинг

Как показано в данном отчете, в сфере кибербезопасности появилась новая тенденция – длительные кампании атак. В настоящее время на организации нацелены многовекторные атаки, в которых используются более сложные методы и более длительные удары. Поэтому мы ввели рейтинг угроз Radware APT, в котором учитывается протяженность во времени, количество используемых векторов атак и сложность каждого отдельного вектора.

Эта тенденция развивается, кампании становятся все более сложными и тщательно продуманными, злоумышленники фокусируются на том, чтобы добиться отказа в обслуживании и максимального воздействия на объекты нападения. Назначение рейтинга APT компании Radware – наглядно продемонстрировать повышение сложности атак и содействовать борьбе с ними. С помощью APT рейтинга организации лучше понимают новые векторы атак, какие компоненты затронуты атакой, могут анализировать ситуацию в реальном времени и, вовремя отказавшись от устаревших методов борьбы, сократить продолжительность нападений, прежде чем те нанесут какой-либо ущерб сети.

Об исследовании

Данные были получены из избирательного опроса 15766 практикующих IT специалистов и специалистов в области IT безопасности, которые были выбраны в случайном порядке и находятся в различных регионах Америки.

В этом году в опросе участвовали 179 различных компаний, большинство из которых не относятся к числу клиентов Radware. Как показано на рисунке 36, 95% участников опроса не используют системы защиты от DoS/DDoS-атак, разработанные компанией Radware. На рисунке 39 компании разбиты на категории, в зависимости от их годового дохода. Большинство компаний представляют собой компании крупного и среднего размера, некоторые небольшие организации также поучаствовали в опросе. На рисунке 37 показано, что большинство организаций ведут коммерческую деятельность по всему миру, не ограничиваясь конкретной страной или регионом.

Используется ли вашей организацией система Radware Attack Mitigation System (AMS)?

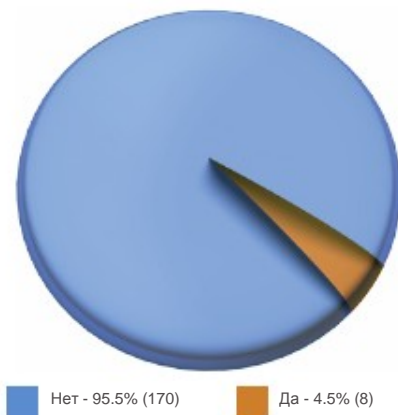


Рисунок 36: Большинство участников опроса не являются клиентами компании Radware.

Какова зона коммерческой деятельности вашей компании?

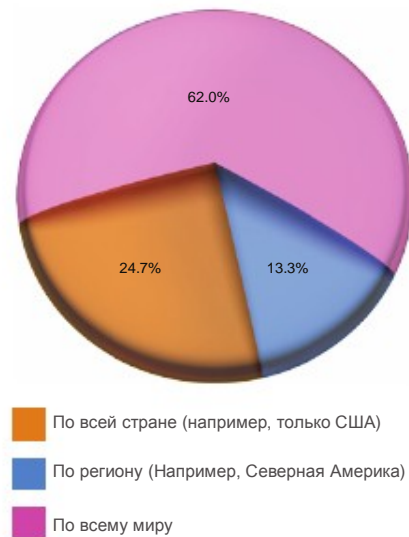


Рисунок 37: Географический охват деятельности компании.

Тип вашей организации?

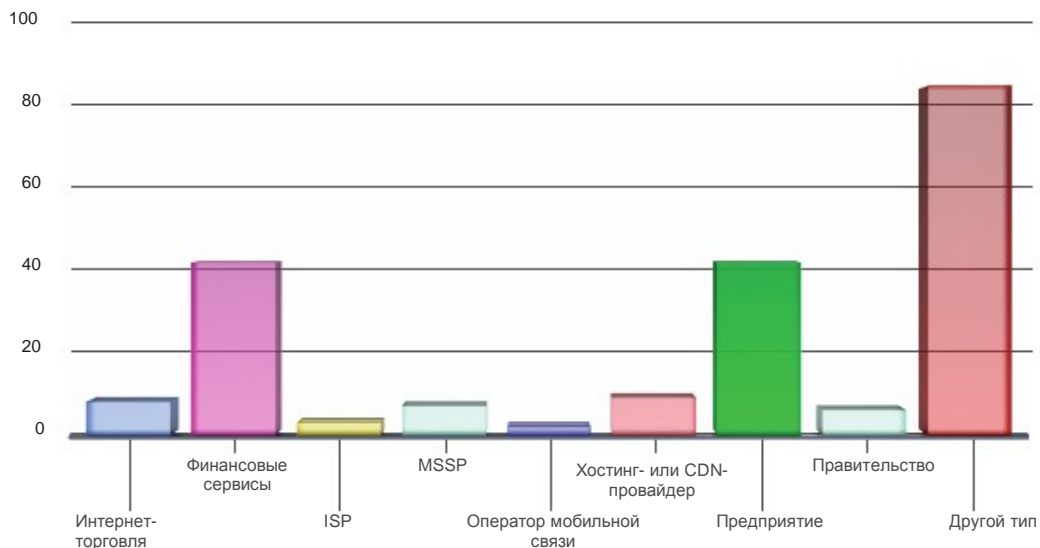


Рисунок 38: Распределение организаций по типу.

Годовой доход вашей компании?

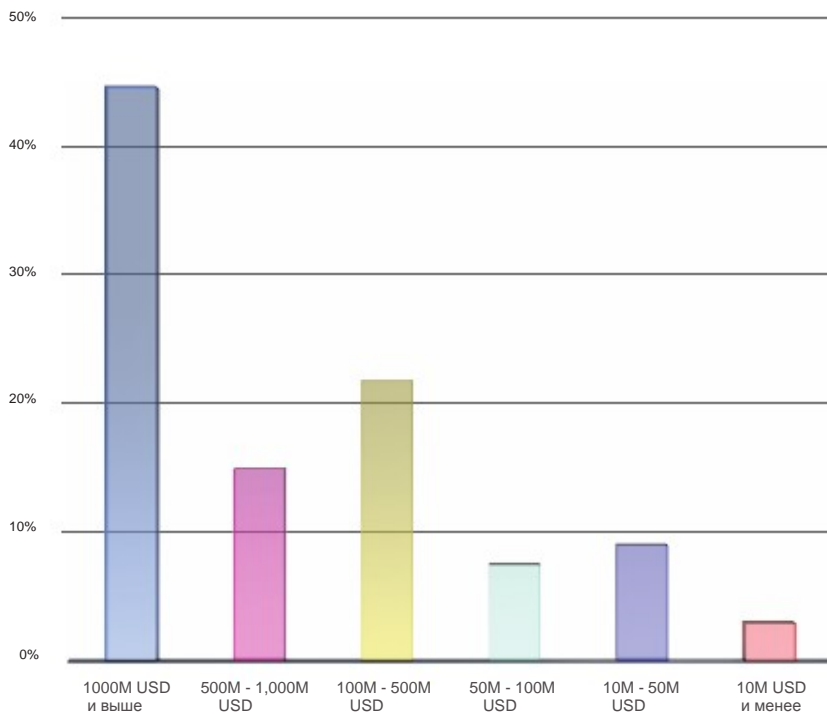


Рисунок 39: Годовой доход.

Текущее количество сотрудников вашей организации?



Рисунок 40: Количество сотрудников в организации.

Какова ваша роль в организации?

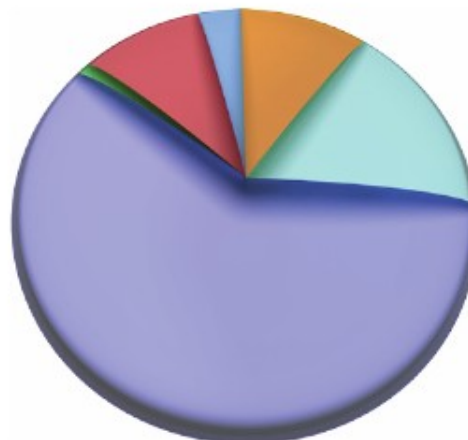


Рисунок 41: Роль участника опроса в компании.

Авторы документа

Авторы

Зив Гадот (Ziv Gadot)
*Руководитель группы
SOC/ERT,*
Radware

Эяль Беништи (Eyal Benishti)
*Исследователь информационной
безопасности,*
Radware

Лиор Розен (Lior Rozen),
Директор R&D DefensePro,
Radware

Янив Балмас (Yaniv Balmas)
*Исследователь информационной
безопасности,*
Radware

Матан Атад (Matan Atad)
*Исследователь информационной
безопасности,*
Radware

Экспертная комиссия

Ави Чесла (Avi Chesla)
Технический директор,
Radware

Карл Хербергер (Carl Herberger)
Вице-президент по безопасности,
Radware

Ронен Кениг (Ronen Kenig)
Директор по маркетингу продуктов,
Radware

Особая благодарность

Каролин Музыка (Carolyn Muzyka)
Старший менеджер по коммуникациям,
Radware

Об авторах

Radware (NASDAQ: RDWR) является мировым лидером в области доставки приложений и обеспечении безопасности приложений для виртуальных и облачных ЦОД. Отмеченный наградами портфель решений компании обеспечивает полную отказоустойчивость критически важных для коммерческой деятельности приложений, максимальную эффективность ИТ, а также гибкость бизнес решений.

Решения компании Radware помогают более чем 10000 предприятиям и поставщикам услуг быстро адаптироваться к проблемам рынка, поддерживать непрерывную коммерческую деятельность и достигать максимальной продуктивности одновременно со снижением расходов. Более подробную информацию можно получить на веб-сайтах www.radware-rus.ru и www.radware.com.

Команда быстрого реагирования Emergency Response Team (ERT) представляет собой аварийную службу, специалисты которой способны реагировать в реальном времени, предлагая проактивный практический опыт специалистов по безопасности и по оборудованию в борьбе с активными угрозами. Наши давние связи и репутация надежного советника и партнера по разработке совместных решений позволили нам выпустить данное руководство. Наша команда ERT имеет обширный опыт противостояния атакам "в естественных условиях" по мере их возникновения.

Radware ERT предлагает сотрудничество в реальном времени по борьбе с DoS/DDoS-атаками. Специалисты команды работают, получая доступ к сетевому оборудованию заказчиков и к файлам, анализируя ситуацию и обсуждая ее с заказчиком. Несмотря на то, что основным намерением службы является блокировка атаки и оказание помощи заказчику в восстановлении работы сервисов, команда также получает уникальный опыт борьбы с атаками. Благодаря практическому вовлечению в борьбу, они получают актуальную информацию о сущности атаки. Они способны оценить фактический урон от атаки. Другими словами, специалисты команды ERT получают доскональную информацию о том, что происходит на самом деле во время атаки на веб-сайт. Как правило, ERT вызывается только в том случае, когда заказчик подвергается атаке среднего или крупного масштаба.

За дополнительной информацией обращайтесь на наши веб-сайты: www.radware-ru.rus, www.radware.com и <http://www.ddoswarriors.com>, где также можно связаться с нашими экспертами.



© 2013 Radware, Ltd.
Все права защищены.
Radware и все другие
названия Radware
продуктов и сервисов
являются
зарегистрированными
торговыми марками
Radware в США и других
странах. Все прочие
торговые марки и названия
являются собственностью
соответствующих
владельцев.

Информация о компании

Radware (NASDAQ: RDWR) является мировым лидером в области доставки приложений и обеспечении безопасности приложений для виртуальных и облачных ЦОД. Отмеченный наградами портфель решений компании обеспечивает полную отказоустойчивость критически важных для коммерческой деятельности приложений, максимальную эффективность ИТ, а также гибкость бизнес решений. Решения компании Radware помогают более, чем 10000 предприятиям и поставщикам услуг быстро адаптироваться к проблемам рынка, поддерживать непрерывную коммерческую деятельность и достигать максимальной продуктивности одновременно со снижением расходов. Более подробную информацию можно получить на веб-сайтах www.radware.com и www.radware-ru.rus

Присоединяйтесь к нашему сообществу на [LinkedIn](#), [Radware](#)
[Blog](#), [Twitter](#), [YouTube](#) и приложении [Radware Connect](#) для iPhone®.