Эволюционируя, DDoS-атаки типа «отказ в обслуживании» заполняют Интернет

Общедоступность Интернета привела к стремительному развитию киберпреступности

Статья Гейл Бронсон (Gail Bronson), предпринимателя из Кремниевой долины, независимого писателя и блогера

DDoS-атаки стремительно увеличивают свои масштабы, частоту и техническую сложность. Неудивительно, что эта тенденция создала для производителей ПО особый (и быстро растущий) рынок продукции, предназначенной для обнаружения и защиты от таких атак. Отраслевые аналитики из компании IDC ожидают, что к концу 2015 года глобальный рынок решений для защиты от DDoS-атак составит 657,9 млн долларов США, а к 2018 году вырастет до 944,4 млн.

Производители соответствующего ПО активно борются за свою долю этого рынка. Те из них, кто не имел решений для защиты от DDoS-атак (или хотя бы отдельных инструментов для этой цели), начали в спешном порядке приобретать нужные технологии. В качестве примера приведу прошлогоднюю сделку, в результате которой компания F5 Networks приобрела компанию Defense.net.

Кроме того, многие производители, не связанные напрямую с упомянутым рынком, тоже стремятся проникнуть туда. Например, компания Akamai, крупнейшая сеть доставки контента, приобрела компанию Prolexic Technologies.

Любое предприятие, использующее в своей деятельности Интернет, — мишень для злоумышленников, и, скорее всего, оно уже неоднократно подверглось атакам. В прошлом году 38% из 300 корпораций, опрошенных компанией Arbor Networks, сообщили, что в 2014 году ежемесячно становились жертвой более чем 21 DDoS-атаки. Специалисты по информационной безопасности из компании Incapsula (разрабатывает продукты для защиты от DDoS-атак, принадлежит компании Imperva) предсказывают, что в будущем любая компания, имеющая отношение к Интернету, будет подвергаться DDoS-атакам несколько раз в году. «Не стоит рассматривать атаки как всего лишь возможное событие — лучше рассматривать их как событие неизбежное», — говорит Тим Мэттьюз (Tim Matthews), вице-президент компании Incapsula по маркетингу.

DDoS-атаки очень просты в осуществлении. Сначала злоумышленник незаметно заражает и берет под контроль любые устройства с операционной системой, подключенные к Интернету: ПК, планшеты, браузеры, мобильные телефоны, серверы и т.д. Захваченные устройства становятся частью удаленно управляемой сети ботов (сокр. от «робот») — ботнета. После этого владелец ботнета (т.н. «ботовод») заставляет зараженные устройства отправлять огромные объемы трафика (отсюда название: «лавинная атака») на адреса жертв, чтобы заполнить всю полосу пропускания до такой степени, пока не будет исчерпано место для полезной нагрузки.

«Доступность каналов с широкой полосой пропускания, открытый доступ к услугам киберпреступников и вредоносным инструментам через т.н. "темный Интернет" — все это привело к стремительной эволюции технологий DDoS-атак, используемых злоумышленниками всего мира для нападений на организации», — говорит Джерри Сталик (Jerry Stalick), вице-президент компании F5 Networks по глобальным услугам.

В последние годы DDoS-атаки стали существенно изощреннее и в то же время проще в реализации. Кроме того, теперь злоумышленники имеют возможность арендовать ботнеты через Интернет за небольшую сумму (всего несколько долларов за час или даже за несколько дней). Таким же образом можно воспользоваться услугами подрядчиков для управления атакой. У таких сделок

есть важное преимущество: заказчик атаки не имеет прямого отношения к реализации киберпреступления.

Специалисты по информационной безопасности рекомендуют организациям использовать гибридный подход к противодействию DDoS-атакам, т.е. подход, объединяющий возможности локальных и облачных решений для того, чтобы поддерживать и защищать как входящий, так и исходящий трафик. Локальные (расположенные на территории организации) решения распознают DDoS-атаки на уровне приложений. Как правило, такие атаки осуществляются с применением небольших объемов сравнительно медленного трафика. Атаки на уровне приложений генерируют постоянные обращения к ресурсам предприятия — например, к веб-сайтам, веб-приложениям, серверам и т.д. В результате приложения значительно замедляют или вовсе останавливают свою работу.

Как только локальные решения начинают под воздействием DDoS-атаки испытывать нехватку полосы пропускания, они могут переключить контроль на облачные службы, способные контролировать значительно большие объемы трафика. Локальные и облачные решения отслеживают резкий рост трафика и различные аномалии на пакетном уровне, что может сигнализировать о возможной DDoS-атаке. Как только подозрительные пакеты обнаруживаются, их тут же отделяют от основного потока трафика для того, чтобы изучить более подробно. Действительно же вредоносные пакеты просто сбрасываются до того, как они достигнут своего назначения.

Поставщики решений для ИБ докладывают, что многие DDoS-атаки демонстрируют постоянное изменение тактик, предусматривают изощренные лавинные атаки, короткие по длительности, зато очень частые. Специалисты по информационной безопасности полагают, что большинство таких атак — просто разведка боем. Тем самым злоумышленники пытаются обнаружить организации со слабой защитой, по-настоящему уязвимые для более агрессивных атак.

Кроме того, DDoS-атаки часто служат отвлекающим маневром. Киберпреступники начинают такую атаку на основные ресурсы организации, чтобы отвлечь внимание персонала, обеспечивающего безопасность. Параллельно осуществляется незаметное внедрение вредоносного кода через совсем другие, вспомогательные интернет-ресурсы организации. Работа вредоносного кода заключается в поиске и краже конфиденциальной информации, например, данных о заказчиках, коммерческих данных и интеллектуальной собственности. Позже злоумышленники могут попытаться

продать похищенную информацию на черном рынке или потребовать выкуп у законных владельцев.

«Киберпреступники применяют также упрощенные стратегии атак, чтобы тем самым повысить общую эффективность и отвлечь внимание ИТ-персонала от действительной цели нападения, которая заключается во внедрении вредоносного кода и похищении данных, — говорит Риши Агарвал (Rishi Agarwal), директор по маркетингу продукции в компании NSFocus. — Современные киберпреступники активно развиваются и постоянно совершенствуют методы своей деятельности».

Появление распределенной разновидности атак типа «отказ в обслуживании» привело к возникновению новых проблем, поскольку зараженные устройства, участвующие в нападении, расположены буквально по всему миру. Первые ботнеты формировались более десяти лет назад в среде компьютерных игроков, на базе ресурсов игровой индустрии и сайтов электронной торговли. Затем в течение нескольких последующих лет активность DDoS-атак была сравнительно невелика, но с 2012 года они начали проявлять себя все заметнее и с тех пор лишь укрепляют свои позиции. Игровая индустрия до сих пор остается привлекательным объектом для нападений. В то же время за последние несколько лет сфера применения DDoS-атак заметно расширилась и теперь включает в себя финансовый, правительственный, технологический секторы, а также сферу развлечений в целом.

Для организаций, полагающихся в своей деятельности на интернет-ресурсы и приложения (например, для предприятий сферы электронной торговли), последствия DDoS-атак могут быть разрушительными. Недоступные веб-сайты и серверы могут стать причиной того, что на репутацию компании будет брошена тень, а заказчики обратятся к ресурсам конкурентов.

При этом для успешной реализации DDoS-атаки не требуются ни особые знания, ни техническая оснащенность. Этот факт очень хорошо иллюстрируется ростом кибератак на образовательные учреждения. Зачастую учащиеся организовывают DDoS-атаки на свои учебные заведения просто самоутверждения ради. Например, не так давно 17-летний студент из штата Айдахо (США) заказал и оплатил злоумышленникам атаку на интернет-портал системы школьного округа West Ada School District. В результате учителя и студенты лишились возможности продолжать удаленную работу, а некоторым учащимся пришлось по нескольку раз пересдавать экзамены. «Для детей это

всего лишь игра, но для учреждений образования и коммерческих структур она может очень дорого стоить», — говорит Терренс Гаро (Terrance Gareau), главный научный сотрудник компании Nexusguard (работала с учебными заведениями, ставшими жертвами кибератак).

Шквал DDoS-атак побуждает производителей рассматривать возможности сотрудничества в сфере обмена информацией о значимых кибератаках и их организаторах. Вопрос в том, говорит вице-президент компании F5 Джерри Сталик, «насколько можно открыться, не рискуя потерять конкурентные преимущества?».

О компании Cisco

Cisco, мировой лидер в области информационных технологий, помогает компаниям использовать возможности будущего и собственным примером доказывает, что, подключая неподключенное, можно добиться поразительных результатов.

Чистый объем продаж компании в 2014 финансовом году составил 47,1 млрд долларов, а в первые 9 месяцев текущего финансового года — 36,3 млрд долларов. Информация о решениях, технологиях и текущей деятельности компании публикуется на сайтах www.cisco.ru и www.cisco.com.