This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

Рекомендация MAAWG

Управление портом 25 для стационарного или динамического IP-пространства Преимущества внедрения и риски бездействия

Введение

Спамеры и другие преступники все чаще используют вирусы и "шпионское программное обеспечение" в качестве способов получения контроля над большим количеством компьютеров. Постоянный рост числа компьютеров, всегда находящихся "во включенном" состоянии, например ЦАЛ, кабельные или корпоративные сети, создает все новые и новые мишени и увеличивает возможность нанесения серьезного ущерба. Посредством внесения незначительных технических изменений, наряду с обучением пользователей, включающим поощрение использования антивирусного и защитного программного обеспечения, любой поставщик электронной почты может обеспечить себе более эффективный контроль за потенциальным злоумышленным трафиком, исходящим из систем его пользователей. Управляя отправкой электронной почты, направляемой с личных компьютеров, поставщики услуг могут уменьшить затраты, связанные с управлением собственным предприятием, повысить степень удовлетворенности потребителей и снизить уровень злоупотреблений интернетом в связи с предоставлением своих услуг.

Угрозы и злоупотребления, связанные с передачей электронной почты

Непрерывный доступ к системам передачи (отправка электронной почты) с персональных компьютеров на серверы электронной почты, не управляемые или не контролируемые соответствующим поставщиком электронной почты, подвергает как поставщиков услуг, так и их клиентов серьезной опасности стать жертвой жуликов или вредоносного программного обеспечения. Персональные компьютеры, оказавшиеся под контролем несанкционированных или необнаруженных третьих лиц, обычно называемых "зомби" или "бот-сети," создают завесу анонимности для тех, кто использует их для того, чтобы напрямую соединиться с релейным сервером обмена почтой (MX) и незащищенным релейным SMTP-сервером и направить еще больше спама и вирусов. Через эти персональные компьютеры "зомби" проходит 80% от всех нежелательных сообщений без всякого ведома и разрешения владельцев этих компьютеров.

Риски бездействия

Негативные последствия для владельцев компьютеров-жертв сказываются незамедлительно и самым серьезным образом. Владельцы таких компьютеров зачастую на протяжении продолжительных периодов отмечают замедленный режим его работы, особенно при попытке использования интернета. Без их ведома спамер может насытить их восходящую ширину полосы и значительно ограничить нисходящую ширину полосы.

Поставщик услуг, с которым соединен такой компьютер, с трудом может заметить, что используется избыточная ширина полосы, однако обычно он также оказывается под негативным влиянием. Клиент-жертва может потребовать технической поддержки, которая может стоить поставщику услуг его месячного дохода и даже бульших затрат, или данный клиент может просто решить, что программное обеспечение поставщика, его услуги коммутируемого или широкополосного доступа не отвечают требованиям качества и поэтому может совсем отказаться от его услуг.

До тех пор пока пользователь будет оставаться подсоединенным, находясь в зараженном состоянии, поставщик услуг будет накапливать жалобы от тех, кто получает спамы, откачиваемые через зараженный компьютер его клиента. Даже при наличии небольшого количества ПК "зомби", недовольства по поводу клиентской поддержки, злоупотреблений и работы отделов управления сетью могут привести к увеличению

затрат до весьма ощутимых уровней. К тому же очень скоро поставщик услуг может обнаружить, что вся его сеть занесена в "черный список" или попала под запрет в отношении рассылки электронной почты по общедоступным адресам в связи с многочисленными случаями злоупотреблений, исходящими из его сети. Разумеется, что каждое направленное нежелательное сообщение означает также, что получено еще одно сообщение. Если позволить данному виду злоупотреблений продолжать беспрепятственно существовать, то это будет иметь глобальные пропорционально негативные последствия для *всех* пользователей интернета и поставщиков средств доступа, что выразится в снижении доверия потребителей, а следовательно и их готовности использовать интернет для связи, коммерческой деятельности и развлечений.

Примеры передового опыта в отношении передачи электронной почты

Саморегулирование отрасли является наиболее эффективной мерой по борьбе со злоупотреблениями в отношении передачи электронной почты, а масштабность проблемы спама требует осуществления немедленных действий. Правительственные учреждения во всем мире заявили об этом четко и во всеуслышание: в условиях отсутствия немедленных действий и результатов, перед отраслью встает возросшая необходимость внимательного изучения данного вопроса и его регулирования. В связи с этим MAAWG рекомендует следующий набор примеров передового опыта в отношении передачи электронной почты для использования поставщиками услуг интернета и электронной почты:

1 Обеспечить услуги представления электронной почты на порту 587, как описано в RFC 2476.

2 Требовать аутентификации представления электронной почты, как описано в RFC 2554.

3 Воздерживаться от вмешательства в подсоединение к порту 587.

4 Отконфигурировать клиентское программное обеспечение для электронной почты таким образом, чтобы использовать порт 587 и аутентификацию представления электронной почты.

5 Блокировать доступ к порту 25 со всех главных компьютеров вашей сети, за исключением тех, которым вы прямо разрешаете выполнять релейные функции протокола SMTP. Эти главные компьютеры обязательно будут включать ваши собственные серверы представления электронной почты, а также могут включать законные серверы представления электронной почты ваших ответственных клиентов.

6 Блокировать входящий трафик в вашу сеть с порта 25. Это предотвратит возможность потенциального злоупотребления со стороны спамеров, использующих ассиметричную маршрутизацию и спуфинг IP-адресов в вашей сети.

Эти примеры передового опыта приняты поставщиками услуг всех масштабов, в том числе многими наиболее известными в мире поставщиками услуг, а также многими членами MAAWG, без какого-либо заметного уменьшения клиентской базы.

Преимущества внедрения

Требование аутентификации и объединение трафика передачи электронной почты через SMTP реле обеспечивает поставщик услуг интернета со многими ценными преимуществами. Эти меры позволяют поставщику услуг интернета:

- определить сторону, ответственную за представленные сообщения;
- отфильтровать спам, вирусы и другое информационное наполнение, содержащее нежелательные сообщения;
- контролировать и ограничивать скорость передачи по каждому клиенту и/или по их совокупности;
- обеспечить реализацию политики приемлемого использования, а также условий обслуживания для представления электронной почты.

Кроме того, поставщики услуг интернета получают следующие конкурентные преимущества:

- улучшение доставки законных электронных сообщений, ввиду уменьшения риска быть занесенными в черный список принимающими поставщиками услуг интернета и электронной почты;
- сокращение затрат на службу помощи в связи со злоупотреблениями, затрат на клиентскую поддержку, а также на центры по эксплуатации сети;
- возможность предложить премиальный уровень обслуживания клиентам, имеющим обоснованную потребность эксплуатировать серверы электронной почты с прямым доступом к порту 25;
- сокращение затрат на инфраструктуру, ввиду уменьшения использования портов и ширины полосы;
- обеспечение пропорциональной доли получателя в глобальном сокращении объемов спама.

После того как эти меры будут внедрены, зараженные компьютеры больше не смогут быть средствами анонимной передачи информации. Компьютеры-жертвы могут быть достаточно быстро обнаружены и поставлены на карантин, до тех пор пока его владелец не выяснит суть проблемы и не устранит ее. При этом клиентов знакомят с угрозами системе безопасности и рекомендуют самим заботиться об обеспечении для себя лучшей защиты. Каждое из этих изменений повышает безопасность и конфиденциальность для *всех* конечных пользователей.

Обучение клиентов

MAAWG считает, что трудно переоценить важность поддержания связи с клиентами и обучения их по вопросам, касающимся этих угроз, мер, принимаемых для их устранения, а также роли, которую владельцы компьютеров должны играть при переходе на безопасные методы передачи электронной почты. Поставщики услуг интернета и электронной почты должны информировать своих клиентов о том, что они делают, почему они это делают и почему для подавляющего большинства из них это будет прозрачно. Всем компаниям-поставщикам электронной почты настоятельно рекомендуется как можно скорее внедрить эти технические правила, для того чтобы вновь установить контроль над портом 25 и обеспечить непрерывное обучение своих клиентов, поддерживая безопасность их обслуживания.

Литература по теме

SMTP Service Extension for Authentication, J. Meyers, March 1999: http://www.ietf.org/rfc/rfc2554.txt

Message Submission, R. Gellens and J. Klensin, December 1998: http://www.ietf.org/rfc/rfc2476.txt

Operation Spam Zombies, Federal Trade Commission, May 2005: http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

Anti Spam Technical Alliance Technology and Policy Proposal, Anti Spam Technical Alliance, June 11, 2004: http://www.postmaster.aol.com/asta/proposal_html.html

Stopping Spam – Creating a Stronger, Safer Internet, Industry Canada, April 2005: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html