МИНИСТЕРСТВО РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ И КОМУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИТСАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНСТКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ

Факультет: Компьютерный инжиниринг
Группа: 201-15 КИ рус (2в КИ)

Самостоятельная работа

По предмету:_____

На тему:_ Спам. История появения. Средство борьбы.

Сдал :

_____

Принял(а) :

_____

Введение

1. Спам. История появления. Средство борьбы.

ВВЕДЕНИЕ

В настоящее время, время высоких технологий, автоматизированного развития широкое распространение получила, так называемая электронная почта.

Сейчас многие фирмы регистрируют на каждого сотрудника почтовый ящик, на который работнику приходит различная информация от фирмы.

Помимо этого почти каждый человек на Земле имеет личный электронный ящик, и как правило, не один. Кроме писем от близких и коллег ящик засоряется спамом.

В силу чрезвычайно высокой прибыльности спамерского бизнеса технические средства борьбы со спамом не всегда достигают своей цели — спамеры без конца изобретают все новые и новые способы обхода фильтров. Поэтому для эффективного противодействия распространению незапрошенных электронных сообщений необходимо объединение различных усилий — технологических (производство программного обеспечения), политических (принятие законов) и общественных (разъяснение малому бизнесу, чем вреден спам).

Таким образом, спам как комплексная проблема требует комплексного решения, включающего следующие элементы:

просвещение (образовательная деятельность); организационная деятельность; технологические меры; законодательство.

Для эффективной борьбы со спамом требуется не только взаимодействие разных субъектов, но и активная позиция всех участников. Сложность проблемы обусловливает относительно длительные сроки ее решения; однако в целях повышения общественной значимости борьбы со спамом необходимо уже в кратчайшие сроки обеспечить достижение «промежуточных побед». В рамках решения проблемы следует также широко использовать международный опыт, накопленный в этой области

Актуальность данной темы обосновано тем, что сегодня каждый человек, имеющий электронный ящик и общающийся по электронной почте испытывает, мягко говоря определенные неудобства, когда на его адрес поступают «письма - спамы».

Таким образом, необходимо искать пути разрешения данной проблемы, которая на руку только «теневым менеджерам» сетевого маркетинга.

Цель данной работы - рассмотреть методы и возможности борьбы со спамом.

Задачи - оценить эффективность методов борьбы со спамом, выявить намечающиеся тенденции в методах борьбы со спамом.

1. СПАМ. ИСТОРИЯ ПОЯВЕНИЯ. СРЕДСТВО БОРЬБЫ.

1.1 БОРЬБА СО СПАМОМ: ИСТОРИЯ

Спам – это незаконно распространяемая путем массовых рассылок информация рекламного характера, получение которой не согласованно с пользователем. Про юридический аспект спама как явления можно прочитать на сайте apolog

История спама

Дата рождения спама – 1 мая 1978 года. Автором, инициатором или зачинщиком, первооткрывателем первой незаконной рассылки был отнюдь не какой-то самообучившийся в глухой американской деревне хакер, как можно было подумать, а самый что ни на есть рядовой, к сожалению так и не идентифицированный, сотрудник отдела маркетинга компании DEC, скрывший свою личность под псевдонимом Thuerk. Этот сотрудник в один прекрасный момент взял и разослал всем тогдашним пользователям Arpanet`а приглашение на презентацию DEC 2020 – так ничего не подозревавшие пользователи зачатков сети получили на свои головы первый спам6.

1.2 БОРЬБА СО СПАМОМ

Борьба со спамом: часть № 1 – профилактика

Если у спамера нет адреса Вашей электронной почты – то и спама Вы не получите.

Компания FrontBridge сформулировала 10 советов о том, как сделать, чтобы на электронный почтовый ящик стала часто приходить нежелательная корреспонденция. "Вредные советы" расположены в порядке убывания их вредоносного эффекта. Чем больший номер у совета, тем меньше шансов, что его использование приведет к началу спам-атаки.

Поместить адрес электронной почты на хорошо посещаемый сайт.

Написать письмо (или ответить на письмо) на сайт Usenet (на этом сайте можно скачать бесплатную музыку, фильмы и т.д.).

Поместить пост или ответить на пост на популярном интернет-форуме.

Зарегистрироваться или иным образом оставить свой адрес электронной почты на сайте фирмы, которая выходит из бизнеса и продает свою базу данных.

Зарегистрироваться или иным образом оставить свой адрес электронной почты на сайте, который продает свои базы данных.

Подписаться на порнорассылку.

Ответить на несанкционированный e-mail.

Дать простое имя своему адресу электронной почты. Например, director@compania

Зарегистрировать доменное имя.

Указать свой адрес электронной почты в интернет-чате.

Впрочем, профессиональные спаммеры обычно используют более продвинутые способы получения адресов. Существуют особые "словарные" программы, которые генерируют десятки тысяч всевозможных комбинаций букв и цифр, содержащихся в почтовых адресах (например, director@kompania, director1@kompania, director2@kompania и т.д.). Активно используются также программы-роботы, которые "скачивают" адреса электронной почты с серверов. Однако, вероятно, самый дешевый и быстрый способ - покупка готовых адресов. В США можно купить 100

млн электронных адресов за 100 долларов. В России пакет из 100 тысяч электронных адресов стоит от 50 до 100 долларов.

Никогда не отвечайте на письма спамеров - тем самым вы даете им знать, что ваш адрес существует и поступающая туда почта просматривается. Если в их письме сказано, что вы можете исключить себя из листа, послав по определенному адресу команду "remove" – в большинстве случаев это ложь. Последовав такому совету, вы только подтвердите возможность использования вашего адреса для дальнейших рассылок.

Борьба со спамом: часть № 2 – фильтры «черного списка»

Люди, которые недавно обзавелись новеньким адресом электронной почты, могут недоумевать: «А что здесь сложного? Удалил непрошеное письмо – и все!». Не все так просто: в настоящее время количество несанкционированных рекламных рассылок (спама) составляет примерно 30% от общего объема писем, пересылаемых по электронной почте. Более того, уже в течение нескольких ближайших месяцев этот показатель может достигнуть 50%. Если объем корреспонденции составляет несколько десятков и более писем в день, ручное удаление становится проблематичным, поскольку даже на просмотр темы письма приходится затратить некоторое время. Итак, Вы тратите время, внимание, а иногда и деньги.

Становится понятной необходимость автоматизации данного процесса. Одним из самых простых и интуитивных методов борьбы со спамом является настройка фильтра приема почты, который бы распознавал нежелательную корреспонденцию и не помещал ее в почтовый ящик пользователя. Таким фильтром, например, является «черный список» на большинстве почтовых серверов, который позволяет запоминать адреса, с которых приходит спам, и блокирует их. Подобный метод не очень эффективен, поскольку завести новый адрес для рассылки спама очень просто, поэтому в последнее время фильтр «черного списка» усовершенствовался: теперь можно вводить целые группы доменных имен (например, *@spam). В свою очередь, это заставляет почтовые сервисы серьезней отнестись к проблеме рассылки спама с их сервиса – в «черный список» попадают и почтовые ящики обычных пользователей, что приводит к потере писем, а следовательно, посетителей и дохода от показа рекламы. Более эффективным оказывается фильтр по теме письма. Достаточно проанализировать 20-30 писем, чтобы составить «словарь спамера», который успешно отфильтрует до 70% спама.

Для еще более качественной фильтрации целесообразно воспользоваться антиспамерскими программами , например, программой Kaspersky Anti-Spam и ее составляющей – бесплатным онлайновым интернет-сервисом СпамТест, который позволяет отсеять до 95% спама.

Фильтрация входящей почты производится с помощью четырехуровневого алгоритма, позволяющего анализировать корреспонденцию на пяти языках: русском, английском, испанском, французском и немецком. В первую очередь, письмо проверяется интеллектуальным модулем распознавания содержания письма SpamTest, которое, по заявлению разработчиков, способно отличить отличать различные типы спама от нормальных писем. Во-вторых, программой используется сигнатурный метод, когда каждое письмо сравнивается с существующими шаблонами в ежедневно обновляемой базе данных, содержащей образцы спама (это напоминает метод работы антивируса). Далее производится анализ по формальным признакам письма (способу рассылки, отправителю, адресу, пути следования и другим признакам). Наконец, Kaspersky Anti-Spam использует традиционный метод "чёрных списков" (blacklist), осуществляя фильтрацию писем по адресам, признанным источниками спама и занесенными в постоянно обновляемые общедоступные списки. В результате проверки каждое письмо получает специальную метку, соответствующую уровню его принадлежности к спаму. Обнаруженный спам, в соответствии с правилами обработки и настройками системы, может быть пропущен, удален, отложен, изменен или перенаправлен на другой адрес.

Борьба со спамом: часть № 3 – «белый список»

Задумывался ли кто над тем, почему пользователям ICQ практически не приходит спам? Все дело в том, что пользователи, которые для добавления своего номера в контакт-лист требуют авторизации, в будущем получают сообщения только от известных им пользователей. Подобный режим можно организовать и при работе с электронной почтой – так называемый «белый список».

Способ первый. Предположим, у нас есть ящик на бесплатном сервисе Mail. Заходим в наш ящик и первым делом создаем папку «Личное». Теперь нам прямая дорога в «Настройки». В «Настройках» выбираем режим «Фильтры», нажимаем «Добавить фильтр». Первый, очень важный, фильтр отсеет у нас те письма, в которых в качестве адресата не указан явным образом наш ящик user@mail, то есть, письмо явно адресовано «Всем», но только не нам. Настройка первого фильтра: если в полученном письме поле «Кому» НЕ СОДЕРЖИТ user@mail, то сделать следующее «Ответить нет такого адреса», а исходное сообщение «Не помещать в папку входящие». Второй фильтр: если в полученном письме поле «Кому» СОДЕРЖИТ user@mail и ТЕМУ «фильтр_от_спама», то переместить копию сообщения в папку «Личное», а исходное сообщение не помещать в папку «Входящие».Этим фильтром мы отсеиваем и укладываем письма, предназначенные только Вам, в папку «Личное». Третий фильтр: Если поле «Тема» не содержит «фильтр_от_спама» и поле «Кому» содержит user@mail, то ОТВЕТИТЬ АВТОМАТИЧЕСКИ «Письмо адресату user@mail было задержано фильтром почтового ящика.

Для того, чтобы адресат получил Ваше письмо, укажите в теме словосочетание «фильтр_от_спама» или нажмите эту ссылку: mailto:user@mail?subject=фильтр_от_спама для отправки нового письма. Приносим свои извинения за причиненные неудобства», а исходное сообщение НЕ ПОМЕЩАТЬ В ПАПКУ «ВХОДЯЩИЕ». Этим фильтром мы уведомляем наших отправителей о том, что они должны обязательно указывать в теме письма словосочетание «фильтр_от_спама». Последним фильтром мы должны указать, что все сообщения об адресатах, до которых не дошли письма, либо так же должны укладываться в специальную папку (вдруг вы и правда ошиблись при отправке), либо удалятся автоматически.

Представим себе, как будет эта система работать: Вам посылают письмо личного характера на ваш почтовый адрес. Отправитель получает автоматический ответ, что его письмо было задержано фильтром почтовой системы и отправителю необходимо указать в теме письма заветное словосочетание «фильтр_от_спама», тогда адресат получит это письмо. Недостаток подобного способа в том, что отправителю либо придется помнить, что необходимо указывать в теме письма ключевую фразу, либо отправить письмо повторно, воспользовавшись ссылкой в автоматическом ответе. Преимущества данного способа: во-первых, вы получаете только те письма, что предназначены именно для Вас, во-вторых, легко повторно остановить поток спамерских писем, просто сменив ключевую фразу.

Второй способ отличается тем, что вы вносите проверенные адреса в « белый список» адресов, таким образом, «освобождая» людей от необходимости использовать в теме письма словосочетание «фильтр_от_спама». Однако при этом существует жесткая привязка к адресу, и если ваш друг сменит адрес почты, Вам придется снова менять фильтры, то есть способ более трудоемкий. Замечу, что эти два метода можно комбинировать.

Эти идеи реализованы во многих антиспамерских программах, в частности, Win Anti SPAM

Борьба со спамом: часть № 4 – «серый список»

Простые методы, вроде составления "черных" и "белых" списков, являются негибкими. Черные списки легко обходятся сменой почтовых адресов и использованием альтернативных серверов, а белые списки не дают принимать почту с адресов, не разрешенных пользователем. Альтернативные методы, основанные на поиске ключевых словосочетаний или статистических методов, требуют длительной и кропотливой настройки.

Одним из перспективных методов является метод "серых списков", предложенный Эваном Гаррисом. Свое название метод получил из-за того, что он является промежуточным между методом черных и белых списков. Важным достоинством метода является то, что он почти не требует вмешательства пользователя и не отнимает больших ресурсов клиентской системы. Не менее важно и то, что система практически не имеет ложных срабатываний.

Идея метода похожа на ряд уже имеющихся систем, которые направляют запросы неизвестным отправителям, требуя подтвердить намерение отправить письмо. Однако важным преимуществом разработки Гарриса является то, что вмешательства человека, отправившего письмо, не требуется - всю работу берет на себя программа, пересылающая почту. В случае серых списков в расчет принимаются три параметра: IP-адрес узла, пересылающего сообщение, адрес отправителя и адрес получателя.

Если хотя бы один из этих параметров ранее не встречался почтовой программе, она заблокирует сообщение и попросит передающую сторону отправить письмо повторно. Все программы для пересылки почты, соответствующие общепринятым стандартам, в течение некоторого времени будут повторять передачу сообщения. Большинство же спамерских программ так не делают. Время блокировки сообщения по серому списку ограничено (по умолчанию оно составляет 1 час), и как только оно истекает, сообщение будет доставлено получателю. Практически все программы для передачи электронной почты повторяют отправку недоставленных сообщений в течение более длительных сроков, а значит, ложные срабатывания практически исключены.

Записи IP-адресов, адресов отправителя и получателя также хранятся в базе ограниченное время (по умолчанию четыре часа). Это может привести к некоторому снижению эффективности фильтров из-за задержки полезных писем, возникающей вследствие удаления их парметров из базы данных. Решить эту проблему Гаррис предлагает, введя дополнительный модуль фильтрации по белому списку, который составляется самим пользователем. Впрочем, и без этого эффективность работы фильтра по серому списку превышает 97%, а число ложных срабатываний стремится к нулю. Подробности о технологии фильтрации почты по серым спискам можно найти здесь.

Борьба со спамом: часть № 5 – ограничения возможностей почтового сервиса

Ну кому, как не почтовым сервисам, бороться за качество услуг электронной почты! От того, насколько пользователи почтового сервиса будут им довольны, напрямую зависит их количество, а следовательно, и доход владельца сайта. Если пользователи не имеют возможности эффективно защититься от рассылки вирусов и спама, а сам домен находится в «черном списке» как активный источник спама – прибыли не видать.

Что могут предложить сервисы? С одной стороны, для отправки письма система может потребовать Вашей авторизации, полного почтового адреса пользователя, а так же ограничить как число адресатов одного письма, так и количество отправляемых писем в течение определенного промежутка времени.

С другой стороны, это самые разнообразные фильтры, «черные» и «белые» списки, определитель «спам – не спам», папка « Рассылки » (Яndex). Внедряются новые идеи, такие как

инкрементальный (incremental) фильтр, Байесовские фильтры, «сертификаты» для отправки электронных писем, обновляемые библиотеки «спамерского» словаря и типовых шаблонов спамерских писем.

Борьба со спамом: часть № 6 – платный E-mail

Возможно, конец спаму положит введение принудительной оплаты за отправку сообщений по электронной почте. Сегодня идея введения платы за электронное письмо переживает "второе рождение", поскольку на нее обратили внимание "хозяева" двух крупнейших в мире почтовых серверов - Microsoft и Yahoo. Глава Microsoft не так давно заявил о скором решении проблемы спама, в том числе и при помощи оплаты e-mail. В Microsoft еще год назад начал разрабатываться антиспамовый проект, в честь первой почтовой марки названный Penny Black, предусматривающий оплату отправленных писем в любом виде: временем работы процессора и памяти, проведением тестов Тьюринга (которые доказывают, что почту отправляет человек, а не программа-робот) и, как во все времена, деньгами.

Компания Goodmail, с которой тесно сотрудничает Yahoo, предложила схему так называемых "электронных марок". Клиент покупает "пакет" марок, которые представляют цифровые коды, и активирует по одному коду перед посылкой электронного письма. Одно почтовое письмо будет обходиться отправителю в ничтожно малую сумму, при этом защита от спама системы массовой рассылки будет достаточно надежной.

Борьба со спамом: перспективы. Почему спам вообще существует? Да потому, что по сравнению с рекламой в прессе, на радио и телевидении рассылка писем по электронной почте сразу нескольким миллионам пользователей является быстрой, не требует особой квалификации и поэтому обладает низкой себестоимостью. Человек, распространяющий спам, в настоящее время получает значительную прибыль, кровно заинтересован в успехе своего бизнеса и вряд ли откажется от этих денег6.

2. ПРОБЛЕМА СПАМА С ДРУГОЙ СТОРОНЫ.

2.1 РОССИЙСКАЯ СТАТИСТИКА

Лаборатория «Спамтест», принадлежащая компании «Ашманов и партнеры», подвела итоги исследования активности спамеров в Рунете в первой половине этого года. В опубликованном отчете отмечается, что к концу первого полугодия уровень спама достиг значения 70-80% от общего объема почтового трафика Рунета. По данным лаборатории «Спамтест», в конце 2003 года доля спама составляла 65-70% от общего объема трафика.

Как было выявлено, спам подвержен сезонным колебаниям, коррелирующимся с движением почты и активностью рекламных кампаний.

Лаборатория «Спамтест» зафиксировала минимум спама 3 мая. В корпоративной почте некоторых небольших компаний доля спама в этот день снизилась до минимального показателя — 5%, а сразу после майских праздников спамеры возобновили свою деятельность, и нарастание объема рассылок идет так же активно, как до этого шел их спад.

Лаборатория «Спамтест» понимает под спамом незапрошенные коммерческие рекламные рассылки, отвечающие требованиям массовости и анонимности. Но рядовые пользователи склонны расширять границы этого понятия, приравнивая к спаму все виды неинформативных и нежелательных сообщений — автоответы почтовых роботов, письма с вирусами и т.п., тем более что для проведения некоторых видов подобных рассылок (например, для рассылки вирусов) все чаще используется специализированное спамерское программное обеспечение.

Тенденция объединения спамерских и хакерских технологий наметилась еще в 2003 году, когда спамерское ПО впервые было применено для массированной вирусной атаки. Эта тенденция наблюдается и в нынешнем году: в первом полугодии было зафиксировано несколько вирусных атак, во время которых вирусы рассылались по электронной почте

Эпидемии вирусов приводят к росту спамерского трафика. Они провоцируют появление большого количества не только содержащих вирусы писем, но и других видов нежелательной почты, например безобидных писем, от которых вирус был «отрезан» каким-либо антивирусом, или многочисленных автоматических отказов в доставке, информирующих пользователя о наличии вируса в корреспонденции с его машины.

Тематика коммерческих рассылок меняется в зависимости от многих факторов, например от сезона: летом спамеры предлагают кондиционеры и отдых в Турции.

Основные темы спама представлены в таблице.

По данным лаборатории «Спамтест», в первом полугодии 2004 года в спамерских потоках Рунета были отмечены несколько новых разновидностей спама. Многие из них одновременно являются неприкрытым мошенничеством (в англоязычной части Сети такие письма называются scam) — это новые разновидности «нигерийских» писем, попытки украсть логины/пароли от известных банковских систем или от почтовых ящиков и т.п.

«Нигерийские» письма — это сообщения, написанные от имени граждан стран с нестабильной экономикой. Автор такого письма обычно утверждает, что он располагает миллионами долларов, которые хранятся в обход закона, и по этой причине не может разместить деньги в банке. Ему срочно требуется счет, куда можно перечислить «грязные» деньги. В качестве вознаграждения за помощь он предлагает от 10 до 30% от заявленной в письме суммы. После того как доверчивый пользователь предоставляет автору письма доступ к своему счету, деньги с него, естественно, исчезают.

До сих пор подобные письма писались исключительно на английском языке, а в первом полугодии этого года появились аналогичные письма на русском языке. А на английском теперь эксплуатируют ситуацию, сложившуюся в российской экономике, в частности арест Михаила Ходорковского и нестабильное положение компании «Юкос». Например, в одном из писем на ломаном английском написано следующее: «... в связи с арестом г. Ходорковского мне необходимо перевести конфиденциально 10 000 000 долларов...».

Относительно новая разновидность спама — это предложения и советы по инвестированию. В большинстве случаев письмо содержит описание «биржевого лидера недели», то есть информацию о компании, которая якобы находится на подъеме стоимости акций. Фактически это попытка повлиять на предпочтения инвесторов и курс акций (очевидно, заказанная игроком фондового рынка).

В международной классификации спама подобные письма относят к мошенничеству (scam), хотя и не запрещенному юридически. Можно предположить, что большинство таких рассылок оплачены держателями акций мелких компаний, желающими, например, поднять стоимость акций до максимума и оперативно продать их, пока они снова не упали в цене.

Еще одна тематическая новинка этого года — предложения антиспамерского ПО.

Строго говоря, первые сообщения такого рода были зафиксированы почти год назад, но тогда они были единичными на фоне общего почтового трафика Рунета. Сейчас их количество стало заметным, хотя и не превышает 1% от общего объема спама.

Спамерскими эти предложения являются как по способу организации рассылки (массовая, анонимная, незапрошенная), так и по сути предложений: большинство ссылок на сайты, где пользователь должен искать антиспамерское ПО, уже недоступны к моменту получения письма или, что гораздо хуже, содержат вирусы.

Открытки «с секретом» — еще один пример тесной консолидации спамеров и создателей вирусов. В первом полугодии 2004 года было зафиксировано как минимум две рассылки с использованием спамерских технологий и спамерского ПО, маскирующихся под сообщения о доставке открытки. Если пользователь совершал переход по ссылке, указанной в сообщении, то есть хотел получить открытку, то на странице такой псевдооткрытки его ждал вирус, который пытался загрузиться на пользовательскую машину3

Основные технологии, используемые спамерами при рассылках, остаются прежними:

использование троянского ПО, установленного незаметно для пользователя на его компьютере

применение настроенных по умолчанию (то есть без пароля или с известным паролем) клиентских устройств доступа — ADSL-модемов, клиентских роутеров, WiFi-устройств, которые позволяют сразу (или после перенастройки злоумышленником) использовать пользовательские мощности для рассылки;

использование старых добрых средств — открытых релеев, CGI-скриптов на сайтах и др., не изменившихся за последние шесть-восемь лет;

NDR-attack (Non Delivery Report) — посылка письма с поддельным отправителем на несуществующий адрес. Отчет о недоставке, содержащий спам-сообщение, будет отправлен поддельному отправителю.

Следует, однако, отметить, что за этот период количественное соотношение описанных методов сильно изменилось. Если в прошлом году и ранее для доставки использовались в первую очередь файлообменные сети (Kazaa и подобные), то сегодня распространение происходит массово — через почтовые вирусы (Bagle, Lovgate) и через дыры в Web-браузерах.

Большинство крупных вирусных и browser-атак в последнее время носят уже явно коммерческий характер: их целью является установка на пользовательской машине троянских компонентов с последующим ее использованием в недобросовестных целях (рассылка спама, кардинг, DoS-атаки). Эти троянские компоненты, в свою очередь, принимают меры для собственной маскировки и для маскировки центра управления. Для управления могут использоваться, в частности, IRC-каналы или же просто сканирование всех поступающих на машину данных — в этом случае команды могут передаваться, например, в потоке спама.

В результате объем мощностей, доступных спамерам, резко увеличился. Сейчас наиболее мощные спамеры могут осуществлять рассылку в несколько миллионов писем в течение всего двух-трех часов, чтобы успеть до того, как среагируют компании, занимающиеся обновлением антиспам-фильтров. Компании — производители фильтров, в свою очередь, увеличивают частоту обновления баз данных.

Из прочих особенностей методов рассылки спама можно отметить пробные рассылки на публичные почтовые адреса, во время которых идет отладка доставки сквозь фильтры в режиме реального времени, и организацию фальшивых, то есть бессодержательных рассылок, которые используются для замусоривания почтового трафика и затруднения работы антиспамерского ПО.

Интересен случай с программой Darkmailer. Как выяснилось, многие спамеры использовали пиратскую версию данной программы для рассылок. А когда в начале марта эта версия перестала

работать, то это привело к резкому сокращению количества спама на довольно продолжительный период7.

2.2. ОБРАТНАЯ СТОРОНА ПРОБЛЕМЫ

Миллионы пользователей, получающих ненужную им рекламу. Это явление их весьма раздражает, но, как правило, нет средств и желания судиться со спамерами - проще удалить письмо.

Тысячи предприятий, у которых просмотр ненужных писем и фильтрация спама забирает огромное количество рабочего времени сотрудников, понижая тем самым доход

Организации, владеющих каналами связи и почтовыми серверами - рассылки спама составляют значительную долю траффика в условиях перегруженного канала, приводят к снижению числа пользователей сервисов, что негативно сказывается на бизнесе.

Отдельные крупные корпорации, занимающиеся разработкой программного обеспечения - для них разработка антиспамерского ПО является выгодным бизнесом.

Группы программистов-энтузиастов, которых спам как явление просто достал.

Представители первой группы не теряют ничего, кроме нервов, предпочитая методы пассивной защиты, которые были описаны выше. Остальные настроены перейти к активной защите:

Ужесточение правил регистрации на бесплатных почтовых серверах, откуда, по статистике, приходит основная часть спама.

Увеличение себестоимости массовых рассылок электронных сообщений, например, введением "электронных сертефикатов" или увеличением времени доставки писем пропорционально вероятности, с которым письмо может считаться спамом.

Принятие законодательных актов, направленных против спама.

Формирование общественного мнения через организацию сайтов, посвященных проблеме спама, распространение среди пользователей сведений о методах защиты от спама.

Создание спамерам психологического дискомфорта, например, подписыванием их на рассылку рекламы в бумажном виде, созданием негативного имиджа предприятиям, использующим такого рода рекламу

Наиболее обозленные хакеры устраивают атаки на почтовые сервера и личные интернет-страницы спамеров, но это уже незаконно.

Законодательство и правоприменени

Для эффективной борьбы со спамом, безусловно, требуется правовая база — иными словами, нужны законы, регулирующие правомерность распространения информации по электронной почте и предусматривающие ответственность за незапрошенные рассылки1.

Отсутствие такого законодательства ведет к ряду негативных явлений, в том числе:

Во-первых, пользователь электронной почты остается беззащитным перед потоком электронного мусора в его почтовом ящике. Он тратит лишнее время на загрузку писем из Интернета, на удаление спама, на поиск действительно нужной корреспонденции. Очень часто спам, рассылаемый без учета возраста получателя, включает в себя материалы для взрослых и прочий сомнительный с точки зрения закона контент. И даже если само содержание спама не противозаконно, все равно неизбежность получения его вызывает раздражение пользователя.

Во-вторых, компании, выступающие против спама, формально являются нарушителями прав спамеров, так как препятствуют фактически незапрещенному законом бизнесу.

До тех пор пока распространение печатных листовок и спама не станет наказуемым, искушение воспользоваться незапрошенной рассылкой сообщений будет для мелкого и среднего бизнеса слишком сильным. Необходимо законодательно зафиксировать, что:

Однако борьба со спамом не должна лишать предпринимателей возможности предлагать свои услуги и выталкивать их с рынка. Она не только не должна наносить ущерб развитию бизнеса, а, наоборот, обязана подталкивать его к эволюции в сторону более цивилизованной практики привлечения клиентов.

спам — незаконен;

фильтрация почты, как платная услуга, является законной;

принуждение провайдеров к фильтрации «по умолчанию» является незаконным

рассылки с соблюдением установленных правил являются законными.

Однако борьба со спамом не должна лишать предпринимателей возможности предлагать свои услуги и выталкивать их с рынка. Она не только не должна наносить ущерб развитию бизнеса, а, наоборот, обязана подталкивать его к эволюции в сторону более цивилизованной практики привлечения клиентов.

Отказ от рассылки незапрошенных рекламных сообщений приведет не только к сокращению числа листовок и объема спама, но и к усилению влияния как традиционных «коллективных» форм рекламы в общественных местах (доски объявлений), так и новых рекламных площадок в Интернете. Вырастет влияние маркетинговых компаний, и продавцам придется искать новые способы завоевания клиента, не раздражая его.

3. МИОРОВАЯ ПРАКТИКА БОРЬБЫ СО СПАСМОМ. ВЫБОР РЕШЕНИЯ ПРОБЛЕМЫ

3.1. ЗАКОН ПРОТИВ СПАМА В США

В декабре 2003 года президент США Дж.Буш-младший подписал закон против спама, который налагает ограничения на рассылку непрошеной электронной почты. Палата представителей США подавляющим большинством голосов утвердила этот закон, что положило конец длящимся уже шесть лет попыткам создать федеральное законодательство, сдерживающее рассылку непрошеных коммерческих сообщений.

Эта мера, грозящая штрафами и тюремным заключением, призвана обуздать массовую рассылку рекламы. За нее проголосовали 392 конгрессмена против 5. «Американцы получают право заявить: „Вычеркните меня из вашего списка, мне это не нужно“», — говорит член республиканской партии Хизер Уилсон. По словам другого законодателя, республиканца Фреда Аптона, законопроект «защищает наших детей от невольного созерцания всего того мусора, который может вывалиться из семейного почтового ящика».

Закон носит официальное название Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM). Министерство юстиции США и Министерство торговли США назвали CAN-SPAM «комплексом технологических, административных, гражданских и уголовных мер», который предоставит потребителям возможность сократить объем нежелательной почты.

CAN-SPAM представляет собой компромиссное решение. Он разрешает Федеральной торговой комиссии США (но не требует) создать реестр «неспамеров», имеет приоритет над многими законами штатов и предоставляет возможность отписки (когда пользователь получает непрошеное письмо и имеет возможность отписаться от дальнейшей рассылки) вместо более строгого требования подписки (когда для рассылки необходимо предварительное согласие пользователя).

CAN-SPAM легализует отдельные виды незапрошенных сообщений. Разрешено отправлять любое количество «коммерческих сообщений электронной почты», если они содержат очевидную рекламу и правильный почтовый адрес США или номер почтового ящика, а также строку unsubscribe (отписаться) в нижней части сообщения.

Корпорация Microsoft работает вместе с представителями государства над применением существующих законов, а также наращивает свои усилия по сотрудничеству с другими интернет-провайдерами в борьбе со спамом.

Фальсификация заголовков электронной почты или использование почтового сервера или открытых почтовых пересылок «для обмана или введения в заблуждение получателей» в отношении источника коммерческого электронного сообщения. Запрещается также регистрация «пяти или более» учетных записей электронной почты или «двух или более имен домена» с ложной информацией, а также их использование для отправки коммерческих электронных сообщений. За первое нарушение предусмотрены наказания вплоть до трехлетнего срока тюремного заключения.

Рассылка коммерческих электронных сообщений с вводящим в заблуждение текстом в строке Subject («Тема»), «который может быть неправильно истолкован получателем».

Рассылка коммерческих электронных сообщений без «действительного обратного адреса» или ссылки на веб-страницу, на которой можно отписаться от рассылки.

Сбор адресов электронной почты путем просмотра веб-узлов и автоматический подбор адресов методом подстановки.

Применение автоматических методов, например скриптов, для использования учетных записей в таких бесплатных службах электронной почты, как Hotmail или Yahoo.

Рассылка коммерческих электронных сообщений с «сексуально ориентированным содержанием», если в них не содержится ссылка на рекомендацию Федеральной торговой комиссии США. Это требование не распространяется на списки подписки. Нарушителям грозит тюремное заключение сроком до пяти лет и штраф в 150 тыс. долл.

Председатель правления и главный архитектор программного обеспечения корпорации Microsoft Билл Гейтс выразил надежду, что закон «поможет потребителям восстановить контроль над своими почтовыми ящиками и поддержит поставщиков услуг электронной почты в их борьбе за обуздание спама». «Microsoft всецело поддерживает строгие законодательные меры, а также запрет на фальсификацию источника электронного сообщения и нелегальные методы сбора адресов — все это поможет провайдерам интернет-услуг найти управу на спамеров», — подчеркнул он.

Microsoft также обращается ко всем пользователям с призывом писать жалобы на спамеров в соответствующие органы власти. Так, письма направляемые в Федеральную торговую комиссию США по адресу uce@ftc.gov будут служить основанием для подачи исков против массовых отправителей мошеннических или вводящих в заблуждение электронных писем.

Рост законотворческой деятельности против спама как в США, так и в мировом масштабе в последнее время внушает оптимизм, в связи с чем Microsoft ожидает огромных успехов в ближайшем будущем.

Что могут сделать сами пользователи?

По мнению Федеральной торговой комиссии США, у пользователей есть пять способов защитить свои адреса электронной почты от программ-сборщиков:

«Замаскировать» свой электронный адрес.

В почтовый адрес пользователя можно вставить слово или выражение, которое обманет компьютерную программу-сборщик, но только не человека. Например, адрес johndoe@myisp (вася@провайдер) можно замаскировать как johndoe@spamaway.myisp (вася@спаму-нет.провайдер).

Использовать отдельное экранное имя в чат-форумах.

Для онлайновых чат-форумов можно создавать экранное имя, не связанное с адресом электронной почты.

Завести отключаемые адреса.

Можно использовать службу отключаемых электронных адресов, которая создает отдельные почтовые адреса, письма с которых пересылаются в постоянный почтовый ящик. Если на один из отключаемых адресов начинает приходить спам, можно ликвидировать этот адрес, не затрагивая постоянный почтовый ящик.

Использовать два электронных адреса.

При работе в компании, которая по роду своей деятельности получает письма от широкого круга лиц, сотрудникам следует организовать для этих целей отдельные почтовые ящики или отключаемые электронные адреса, вместо того чтобы публиковать собственный адрес.

Использовать уникальный почтовый адрес, содержащий буквы и цифры.

Выбор почтового адреса может повлиять на количество получаемого спама, поскольку некоторые спамеры используют атаки со словарем. Они направляют письма по множеству адресов в виде возможных сочетаний имен и фамилий в домене крупного интернет-провайдера или почтовой службы, надеясь найти действующий адрес.

Отказ от рассылки незапрошенных рекламных сообщений приведет не только к сокращению числа листовок и объема спама, но и к усилению влияния как традиционных «коллективных» форм рекламы в общественных местах (доски объявлений), так и новых рекламных площадок в Интернете. Вырастет влияние маркетинговых компаний, и продавцам придется искать новые способы завоевания клиента, не раздражая его.

Оправдаются ли усилия, затраченные на борьбу со спамом?

Поскольку оценки ущерба, наносимого спамом бизнесу и частным пользователям, сильно разнятся, некоторые компании по-прежнему считают это не слишком важной проблемой. Так стоит ли вообще вкладывать средства на борьбу со спамом, создавая различные ассоциации, покупая сложное и недешевое программное обеспечение, размещая дорогостоящую социальную рекламу и т.д.?

Однако существует мнение, что если не начать бороться со спамом, то ситуация может просто выйти из-под контроля. В этом смысле можно сравнить спамеров с обычными преступниками. Государство и общество испокон веков борются с ворами и мошенниками, сажая их в тюрьму, придумывая всевозможные способы защиты и проч. Тем не менее количество воров год от года не уменьшается или уменьшается незначительно. С другой стороны, невозможно даже просто представить, что было бы, если бы борьба с ворами не велась вообще. В этом случае можно прогнозировать, что ситуация в скором времени вышла бы из-под контроля и люди просто боялись бы выходить на улицу. То же самое может случиться и со спамом. Без осознания значимости данной проблемы, как таковой, и объединения усилий представителей ИТ-индустрии и государства ее преодоление будет практически невозможным.

Эффективное противодействие распространению спама предполагает принятие комплексных мер на различных уровнях. Решение данной задачи невозможно без участия всех заинтересованных сторон: разработчиков программного и аппаратного обеспечения, системных интеграторов, провайдеров и органов государственной власти. При этом, однако, следует учитывать тот факт, что никакие меры не смогут гарантировать достижения полной защиты от получения незапрошенных электронных сообщений. В настоящее время речь может идти только о минимизации объемов спама, а не о полном его исключении5.

3.2 РЕШЕНИЯ ДЛЯ БОРЬБЫ СО СПАМОМ НА ПРЕДПРИЯТИИ

Сью Тиббеттс, Продукты второго поколения для защиты электронной почты

Фильтры спама принято располагать на серверах Internet-провайдеров, на шлюзах сети предприятия (например, на DMZ-сервере), на почтовых серверах и настольных компьютерах. Эти подходы, особенно если они объединены в многоуровневом решении, эффективно уменьшают число непрошеных посланий в почтовых ящиках пользователей. Но с увеличением объема спама замедляется обработка сообщений на почтовом сервере и возникает необходимость в дополнительных хранилищах сообщений, отмеченных как потенциальный спам. Поэтому многие компании заменяют программные решения для борьбы со спамом первого поколения специализированными устройствами или возлагают задачи фильтрации спама на хост-службы независимых поставщиков. Данный обзор поможет оценить возможности устройств фильтрации спама и хост-служб и выбрать технологии, обеспечивающие самую надежную защиту электронной почты.

Покупка специализированного устройства

Специализированные устройства представляют собой автономные устройства с собственными операционными системами и предназначены именно для фильтрации спама. Их можно установить во входной точке сети или перед почтовым сервером. Многие устройства поставляются с заранее настроенными правилами, политиками и списками (например, черными списками, белыми списками, собственными списками поставщика) и готовы к работе без дополнительной настройки. Большинство устройств располагает интерфейсом пользователя на базе Web, с помощью которого можно централизованно и дистанционно управлять политиками электронной почты, отыскивать и извлекать сообщения из карантина, а также готовить отчеты в реальном времени и по данным журналов.

Большинство поставщиков устройств ежедневно обновляют правила, чтобы эффективно отражать новые угрозы. Некоторые поставщики предоставляют возможность бесплатного обновления в течение года после покупки устройства; другие предлагают службу обновления по подписке за дополнительную плату. Преимущество устройств — в отсутствии пользовательских лицензий. Компания приобретает устройство, которое обслуживает некоторое количество пользователей электронной почты или усредненное число входящих и исходящих почтовых сообщений в день. В

целом, компании с более чем сотней пользователей более выгодно купить специализированное устройство4.

3.3 ИСПОЛЬЗОВАНИЕ ХОСТ-СЛУЖБЫ

Хост-службы фильтруют сообщения электронной почты, прежде чем те попадут на почтовый сервер компании. Благодаря хост-службе сокращается нагрузка на ресурсы сервера, не требуется покупать дополнительные аппаратные средства или программы, а потенциальный спам хранится на сайте поставщика. Обычно поставщики службы быстро реагируют на новые формы спама. Крупные компании часто выбирают хост-службы из-за дополнительных функций электронной почты, таких как фильтрация и шифрование исходящих сообщений, а также применение политик, но хост-службы могут пригодиться и малым предприятиям с числом сотрудников не более ста, а также компаниям, в которых нет штатного администратора системы обработки почты. Стоимость хост-службы часто определяется числом пользователей электронной почты: чем больше пользователей, тем выше стоимость службы. Многие поставщики служб предоставляют дополнительные услуги, в том числе автоматическое восстановление после аварии и возможность передать функции отказавшего узла исправному, архивирование сообщений в автономном хранилище (ради соответствия законодательным актам и бесперебойной работы компании), обеспечение избыточности данных, защиты системы мгновенного обмена сообщениями (IM) и фильтрации исходящего трафика. Наличие одной или нескольких дополнительных услуг может отразиться на стоимости службы.

Критерии выбора

Основные требования к системе защиты от спама — исчерпывающий план обслуживания или легко устанавливаемое специализированное устройство, которые гарантируют надежное блокирование спама (по меньшей мере, 97%) и минимум выбраковки полезных сообщений. При анализе хост-служб советую обратить внимание на время бесперебойной работы, гарантированное соглашением об уровне обслуживания (SLA), и задержку сообщений. Важно, чтобы хост-служба помещала сообщения в очередь в случае отказа сети компании или линии связи. Кроме того, устройство или служба должны поддерживать почтовые серверы предприятия, быть совместимыми с LDAP и работать с несколькими доменами. Чем больше механизмов защиты (от вирусов, имитации соединений, «шпионов» и фишинга) и технологий фильтрации реализовано в службе или устройстве, тем лучше.

Для эффективной борьбы со спамом предпочтительны продукты и службы с Web-интерфейсом (многоязыковым для пользователей в разных странах), которые обеспечивают дистанционный мониторинг и доступ к отправленным в карантин, блокированным и удаленным нежелательным сообщениям; управление политиками (в частности, настройкой политик для различных доменов, групп пользователей и отдельных пользователей), правилами и списками; администрирование учетных записей пользователей; подготовку отчетов (в некоторых продуктах статистика отображается на приборной панели в реальном времени)6.

ЗАКЛЮЧЕНИЕ

«Лаборатория Касперского», ведущий производитель систем защиты от вредоносного и нежелательного ПО, хакерских атак и спама, представляет очередной отчет по спам-активности за прошедший месяц.

Прогноз, сделанный весной аналитиками «Лаборатории Касперского», оправдался: сезонное падение долевых показателей спама продолжается, такое снижение наблюдается впервые за несколько лет. С января по апрель спам составлял более 86% почтового трафика (в среднем за месяц). Однако в мае доля спама снизилась до 79,1%, и, несмотря на рост этого показателя в июне на 3%, тенденция к ослаблению спамерской активности сохранилась.

Как результат, доля спама в почтовом трафике в июле в среднем составила 78,9%. Самый низкий показатель был отмечен в середине месяца – 16 июля – 66,2%, больше всего спама было зафиксировано 11 числа – 88,9%. Доля графического спама составила 9%.

В июле снизился процент спамовых писем с вредоносными вложениями и фишинговыми ссылками. Письма со ссылками на фишинговые сайты составили 0,58%, что в два раза меньше июньских показателей. Вредоносные файлы содержались в 0,27% всех писем. Спамеры постарались по-своему компенсировать этот спад: во второй половине месяца прошла масштабная рассылка писем со ссылками на сайты, зараженные вредоносными программами. Хакеры взломали десятки сайтов, расположенных в различных доменных зонах. Чтобы пользователь с большей вероятностью проследовал по ссылке, письма сопровождались шокирующими новостными заголовками. Кроме того, в ряде рассылок письма содержали предложение скачать бесплатный антивирус, который на деле оказался разновидностью Trojan-Downloader.

Пятерка лидирующих спам-тематик в июле не претерпела значительных изменений по сравнению с предыдущим месяцем. В нее вошли «Медикаменты; товары и услуги для здоровья» (18%), сезонная тема «Отдых и путешествия» (14%), спам «для взрослых» (12%) и «Реплики элитных товаров» (7%). Кроме того, грядущий учебный год вызвал волну спама на тему «Образование» (8%).

Растущая популярность социальных сетей не может не привлекать внимания спамеров и хакеров, которые использовали все возрастающую славу подобных сайтов в своих целях. При этом спамеры, рекламирующие обычные товары и услуги, пока не эксплуатируют тему социальных сетей, тогда как ссылки на вредоносные программы и предложения хакерского и спамерского ПО уже стали постоянными спутниками подобного спама в электронной почте.

В июле пользователям ресурса Odnoklassniki спамеры предлагали утилиту для автоматического ввода логина и пароля при входе на личную страницу сайта. «Полезная» утилита на самом деле оказалась троянской программой Trojan-PSW.Win32.SocNet.a, которая, действительно, автоматически заполняла форму регистрации, но при этом передавала личные данные владельца на сайт злоумышленников. В середине июля была зафиксирована волна фальшивых извещений о получении сообщения с сайта Odnoklassniki со ссылкой на зараженный сайт. В последние дни месяца прошла рассылка с приглашением зарегистрироваться на портале Friends - якобы от пользователя этой сети. Ссылка в письме не работала, однако можно предположить, что рассылка имела ту же цель, как и письма, имитирующие сообщения с сайта Odnoklassniki. «Лаборатория Касперского» напоминает пользователям о потенциальной опасности приглашений, пришедших с незнакомых адресов.

Спам, не имеющий отношения к социальным сетям, также все чаще носит криминальный характер. Черный PR, компрометирующий ресурсы различной направленности, ссылки на вредоносные программы или на зараженные сайты, реклама поддельных и контрафактных

товаров, предложения услуг криминального характера или ПО для хакерской и спамерской деятельности – все это содержалось в спамовых письмах в июле. И это заставляет говорить о продолжающейся криминализации спама.

Несмотря на незначительное снижение доли спама, аналитики «Лаборатории Касперского» считают, что эта тенденция носит лишь сезонный характер, и с наступлением осени долевые показатели спама вернутся к прежним значениям. Нежелательная корреспонденция по прежнему составляет львиную долю почтового трафика, а содержащиеся в ней опасные вложения, такие как вредоносное ПО и ссылки на зараженные сайты, заставляют относиться к спаму со всей серьезностью6.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

ИНФОРМАТИКА. Практика алгоритмизации и программирования. Интернет-версия издания: Шауцукова Л.З. Информатика 10-11. — М.: Просвещение, 2000 г.

Информатика и программирование (2-е издание)Романченко В.И., Евгений Истомин, Сергей Неклюдов - Андреевский издательский дом, 2008 г.

ЖУРНАЛЫ:

Журнал «Компьютерра» от 27 сентября 2008 г.

Журнал «МОВІ»

Данные официального сайта «Лаборатория Касперского»

Данные официального сайта журнала CHIP

Данные официального сайта «Лаборатория Касперского»