УДК 681.324

С.Г. Семенов, Д.В. Гриньов, О.А. Малишев

Харківський університет Повітряних Сил ім. І. Кожедуба

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД СПАМ

Проведено аналіз основних особливостей СПАМ та методів захисту інформаційних комп'ютерних мереж від нього. Зроблено висновок про неузгодженість в термінології СПАМ і необхідність більш чіткого тлумачення даного терміну. Визначено основні характеристики анонімної, масової, незапитаної розсилок, проведено класифікацію СПАМ. Перелічено та проаналізовано методи захисту інформаційних комп'ютерних мереж від СПАМ. Зроблено висновок про можливі шкідливі наслідки ігнорування методів захисту від СПАМ.

Ключові слова: *СПАМ, інформаційна комп'ютерна мережа, методи захисту від СПАМ, анонімна, масова, незапитана розсилка.*

Вступ

Постановка проблеми. Термін "спам" веде своє походження від старого скетчу британської комік-групи Monty Python Flying Circus, в якому відвідувачі ресторану, що намагаються зробити замовлення, вимушені слухати хор вікінгів, що оспівує м'ясні консерви. СПАМ в сучасних інформаційних комп'ютерних мережах є заняттям, яке в законодавстві низки країн передбачені ті або інші види відповідальності. Наприклад, в США один з найбільших провайдерів Інтернет America Online (AOL) кожен місяць висуває по декілька судових позовів до спамерів.

Аналіз процесу роботи в інформаційних комп'ютерних мережах показав, що користувачі просто не звертають уваги на мережеву рекламу, видаляючи такі повідомлення з своїх поштових скриньок. Насправді згубність таких розсилок полягає в тому, що спамеру це практично нічого не коштує, зате дорого обходиться всім іншим, як одержувачу СПАМ так і його провайдеру. Велика кількість рекламної кореспонденції може привести до зайвого навантаження на канали і поштові сервери провайдера, із-за чого звичайна пошта, яку, можливо, дуже чекають одержувачі, проходитиме значно повільніше. Для того, щоб ефективно боротися із СПАМ, необхідно чітко визначити, що саме мається на увазі під словом "спам".

Аналіз літератури [1 – 4] показав, що нерідко провайдери і власники мереж вважають за краще керуватися "презумпцією винності", відносячи до СПАМ практично всю пошту, яку не запрошував одержувач. За останні півтора роки експерти вивчили всі існуючі види і категорії СПАМ і дійшли висновку, що при огульному віднесенні до СПАМ будь-якого небажаного або рекламного листа виникає велика небезпека втратити ділову пошту. "Побутові" визначення СПАМ як "небажаної пошти" або "незапитаної рекламної розсилки", які можна почути від користувачів, провайдерів або власників комп'ютерних мереж, не витримують критики. Оскільки при фільтрації СПАМ головне – не нашкодити одержувачу пошту, необхідно дати більш зважене визначення.

1. Основні особливості СПАМ

СПАМ – це анонімна, масова, незапитана розсилка. Це визначення досить добре співвідноситься з світовою практикою і визначеннями СПАМ, покладеними в основу американського і європейського законодавства про СПАМ. Крім того, це визначення можна ефективно використовувати на практиці. Поясним його сенс.

Анонімна розсилка: ми всі страждаємо в основному саме від автоматичних розсилок, з прихованою або фальсифікованою зворотною адресою. В даний час не існує спамерів, які не приховували б своєї адреси і місця розсилки [1, 5].

Масова розсилка: саме масові розсилки, і лише вони, є справжнім бізнесом для спамерів і справжньою проблемою для користувачів. Невелика розсилка, зроблена помилково людиною, що не є професійним спамером, може бути небажаною поштою, але не спамом [1, 5].

Непрошена розсилка: очевидно, підписні розсилки і конференції не повинні потрапляти в категорію "СПАМ" (хоча умова анонімності і так значною мірою це гарантує) [6].

СПАМ і цільові комерційні пропозиції. З даного вище визначення виходить, що комерційна пропозиція, явно направлена на адресу одержувача і з реальною зворотною адресою, – це не СПАМ.

Таким чином, ми не рахуємо СПАМом непрошений рекламний лист, наприклад, запрошення на семінар, послане особисто директору фірми. Або пропозицію гірськолижного туру в Шамоні із справжньою зворотною адресою турфірми. Комусь це може показатися обурливим, дивним і нелогічним, але ми вважаємо, що робити цю відмінність необхідно – і теоретично, і практично. Такий лист також може бути небажаним і викликати роздратування. Помітимо, що такі листи у багатьох випадках теж можна розпізнати і відфільтрувати технічно, разом із СПАМ. Наприклад, Kaspersky Anti-Spam має рубрики "Семінари/Конференції", "Туризм" і тому подібні.

Проте перш ніж видаляти листи даних категорій, системному адміністратору варто погоджувати політику обробки СПАМ з відділом маркетингу і PR. Цілком можливо, що їм потрібні подібні листи. Наприклад, комерційні співробітники туристичних фірм часто з цікавістю читають туристичні пропозиції і навіть спам, а організатори семінарів і співробітники кадрових відділів хотіли б одержувати всі запрошення на семінари.

Небажана пошта. Окрім СПАМ і цільових комерційних пропозицій існує ще один вид поштових повідомлень, який часто плутають із СПАМ. Це небажана пошта. В деяких випадках незапитане і непотрібне повідомлення СПАМом не є.

Ось деякі приклади небажаної пошти, яку одержувач не замовляв та/або не бажає одержувати:

Різного роду помилки: помилки автоматичних розсильник – технічний збій служби розсилки, запити на підтвердження підписки на розсилку або якийсь сервіс; помилки людей – наприклад, людина шукає однокурсника, а одержувач має те ж прізвище і схожу адресу. Різноманітна технічна кореспонденція: повідомлення про недоставляння листа і інші помилки; автоматичні повідомлення від антивірусних програм про віруси у відправленому з вашої адреси листі; екстраординарні або рутинні повідомлення від адміністраторів сервісів (наприклад, про те, що поштовий сервіс буде недоступний, або про появу вірусу і ін.). Такі листи для одержувача часто виглядають як незапитані. Нові можливості спілкування і бізнесу: діловий лист від приватної особи (фірми) приватній особі (фірмі). Такий лист часто може служити початком нового контракту, справи, бізнесу. Прямий лист менеджеру корпорації від рекрутінгового агентства – адреса звичайно одержана неофіційно, сам лист справедливо трактується компанією як загроза бізнесу, в той же час такі листи дуже корисні ринку праці і капіталу. І, природно, особисті листи від тих, з ким одержувач ніколи раніше не переписувався: листи від старих знайомих, друзів, агітаторів (наприклад, агітація жителів району проти забруднення парку, і т.п.).

Будь-який з цих листів є незапитаним, бо приймаюча сторона його явно не запрошувала. З іншого боку, викидати подібну пошту без прочитання не можна. З цього виходить, що ознаки масовості і анонімності є необхідними для розпізнавання тих, хто робить бізнес на СПАМ.

Політика поводження із СПАМ і небажаною поштою. Отже, ми розділяємо всі незапитані повідомлення, що потрапили у вашу поштову скриньку, на наступні категорії:

– СПАМ, що має всі ознаки анонімної масової розсилки;

– цільові комерційні пропозиції;

– небажана пошта.

СПАМ, поза сумнівом, потрібно фільтрувати, а потім зберігати в особливих теках або поміщати в карантин, а іноді відразу видаляти – згідно політиці компанії. Другу і третю категорію листів також можливо розпізнавати і фільтрувати, але з ними потрібно поводитися обережніше. У компанії можуть бути різні відділи, які хотіли б одержувати різні категорії непрошеної пошти (адміністраторам потрібні повідомлення від сервісів і антивірусів, кадровикам – запрошення на семінари).

Таким чином, системний адміністратор повинен вводити ретельно продуману політику обробки пошти, що включає не тільки знищення СПАМ, але маршрутизацію і зберігання незапитаної і навіть небажаної пошти.

2. Методи захисту інформаційних комп'ютерних мереж від СПАМ

Існують активні і пасивні методи захисту [1 – 4].

Пасивні методи захисту – це якісь профілактичні заходи, що дозволяють не допустити попадання вашої поштової адреси до спамеру.

Проблеми з рекламними розсилками (СПАМ) у приватного користувача починаються в той момент, коли його email-адреса потрапляє в базу даних до спамерам. Спамери знаходять email-адреси своїх жертв різними способами:

– скануючи веб-сайти;

– скануючи дошки оголошень, форуми, чати, Usenet News і так далі;

– підбираючи "легкі" адреси (jonh@, mary@, alex@, info@, sales@, support@) по словнику імен і частих слів;

– підбираючи "короткі" адреси (aa@, an@, bb@, abc@) простим перебором.

Виходячи з цього, приватному користувачу можна порекомендувати наступні заходи:

1.	Заведіть собі дві адреси – приватний, для листування (приватний і маловідомий, який ви ніколи не публікуєте в загальнодоступних джерелах), і публічний – для публічної діяльності (форумів, чатів і так далі).
2.	Адреса для листування ніколи не повинна публікуватися у відкритому доступі.
3.	Адреса для листування не повинна бути легкою в запам'ятовуванні або "красивою". Ваше ім'я або красиве слово – не підходять. Vasily.M.Pupkin-IV – підходить цілком. Чим довше адреса і чим менш він легкий для читання, тим краще.
4.	Якщо потрібно повідомити свою приватну адресу (у конференції, на сайті) – робіть це способом, непридатним для автоматичного прочитання складальником адрес. "Ivan-точка-Susanin-собака-mail-точка-ру" – хороший спосіб. "Ivan.Susanin at mail.ru" – набагато гірше, Ivan.Susanin@mail.ru - нікуди не годиться. Якщо йдеться про публікацію на сайті, можна опублікувати адресу у вигляді картинки.
5.	Адреса для публікації потрібно наперед вважати тимчасовим. Не варто його жаліти - ви завжди можете завести новий. Як правило, спам починає приходити на нього через декілька днів після публікації. Оскільки цю адресу можуть використовувати не тільки спамери (туди приходитиме і нормальна пошта), слід його періодично переглядати. Ви можете читати пошту, що приходить на нього, раз на тиждень або раз в місяць.

Деякі інтернет-магазини, конференції, форуми і т.п. вимагають реєстрації з вказівкою працюючої електронної пошти. Іноді передані таким чином адреси потрапляють до спамерам. Далеко не завжди це злий намір, але користувачам від цього не легше. Тому:

6.	При реєстраціях завжди указуйте публічну адресу. Він все одно може вважатися втраченим. Можна на кожну реєстрацію заводити нову адресу на безкоштовній пошті – тоді ви знатимете, хто з магазинів і форумів "продав" вашу адресу спамерам.

Якщо СПАМ приходить небагато і з ним ще можна миритися, то слід дотримуватися простих правил:

7.	Ніколи не відповідайте спамеру. Можливо, нічого поганого не відбудеться. Але може трапитися і так, що вашу відповідь прочитає "робот" і помітить вашу адресу як "живу" – в результаті спама приходитиме ще більше.
8.	Не намагайтеся скористатися посиланням "відписатися", якщо ви не упевнені, що вона спрацює. Можливо, вас дійсно відпише даний конкретний розсильник. Але при цьому вашу адресу можуть помітити як діючу і спам стане більше. Дізнатися, що трапиться, можна, тільки спробувавши. Але чи хочете ви цього?

Якщо миритися із СПАМ вже ніяк не можна:

9.	Змініть свою приватну адресу. На деякий час цей допоможе

Якщо ви хочете все-таки мати загальновідому і загальнодоступну адресу, приготуйтеся одержувати туди сотні спам-повідомлень на добу. Якщо не повезе – то тисячі на добу. Якщо від такої адреси ви не хочете відмовлятися, то залишається остання рада:

10.	Використовуйте антиспам-фільтр – або на сервері, вибравши провайдера з послугою фільтрації спама, або у себе на комп'ютері, вибравши засіб, відповідний для вашого поштового клієнта. Сучасні фільтри володіють достатньо високою якістю (відсоток фільтрованого спама у добре настроєних фільтрів досягає 95 – 99%), і їх використання різко понизить гостроту проблеми.

Якщо ж пасивні методи захисту не приносять належного успіху, пора займати активну позицію. Щоб ви могли вести ефективну боротьбу проти спамера, необхідно з'ясувати наступні складові:що рекламує спамер; через якого провайдера йде розсилка СПАМ; справжній електронний ящик спамера.

Висновки

Причина вибухового зростання спам-розсилок в тому, що спамеру розсилка практично нічого не коштує, зате дорого обходиться всім іншим: як одержувачу спама, так і його провайдеру. Спам-повідомлення намагаються бути максимально схожими на нормальну пошту – щоб їх читали. Чим шкідливий СПАМ:

– Пониженням продуктивності компанії.

– Випадковою втратою важливих повідомлень при ручному чищенні електронної пошти.

– Загрозою стабільності роботи поштових серверів.

– Небезпечним змістом: вірусами, троянами, забороненими матеріалами. В даний час приблизно 75 – 80% вхідних повідомлень – СПАМ. Це означає, що три чверті свого дискового простору і процесорної потужності ваш поштовий сервіс витрачає зараз на обслуговування бізнесу спамерів!

– Паразитним трафіком.

– Для провайдерів – витратами на службу підтримки, конфліктами з клієнтами.

Таким чином, СПАМ несе значні ризики для бізнесу як компаній, так і інтернет-провайдерів.

Список літератури

1. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика. Электроинформ, 1997. – 367 с.

2. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В .Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

3. Столингс В. Криптография и защита сетей. Принципы и практика / В. Столингс. – М.: Вільямс, 2001. – 672 с.

4. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика; Электроинформ, 1997. – 367 с.

5. Левин М. Библиотека хакера 2. Книга 1 / М. Левин. – М.: Майор, 2003. – 640 с.

6. Левин М. Библиотека хакера 2. Книга 2 / М. Левин. – М.: Майор, 2003. – 688 с.

Надійшла до редколегії 19.11.2008

Рецензент: д-р. техн. наук, О.В. Лемешко, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ СПАМ

С.Г. Семёнов, Д.В. Гринёв, А.А. Малышев

Проведен анализ основных особенностей СПАМ и методов защиты информационных компьютерных сетей от него. Сделан вывод о несогласованности в терминологии СПАМ и необходимость более четкого толкования данного термина. Определены основные характеристики анонимной, массовой, незапрошенной рассылок, проведена классификация СПАМ. Перечислены и проанализированы методы защиты информационных компьютерных сетей от СПАМ. Сделан вывод о возможных вредных последствиях игнорирования методов защиты от СПАМ.

Ключевые слова: *СПАМ, информационная компьютерная сеть, методы защиты от СПАМ, рассылки.*

RESEARCH OF FEATURES AND METHODS OF DEFENCE OF INFORMATIVE COMPUTER NETWORKS FROM SPAM

S.G. Semenov, D.V. Grinev, A.A. Malyshev

The analysis of basic features of SPAM and methods of defence of informative computer networks is conducted om him. A conclusion is done about inconsistency in terminologies of SPAM and necessity of more clear interpretation of this term. Basic descriptions are certain anonymous, mass, uninquired deliveries, classification of SPAM is conducted. Transferred and analysed methods of defence of informative computer networks om SPAM. A conclusion is done about the possible harmful consequences of ignoring of methods of protecting from SPAM.

Keywords: *SPAM, informative computer network, methods of protecting from SPAM, anonymous, mass, uninquired deliveries.*