# Зомби-генератор в конверте

*Окончание.*
*Начало в №№1(13) и 2(14)*

## Спам: минус деньги плюс проблемы

**Бурное развитие информационных технологий приводит к все большему смещению бизнес-процессов в виртуальную сферу, а значит, к их ускорению и повышению эффективности работы предприятий. Но не все так радужно. Новая среда рождает не только новые возможности, но и новые проблемы. Одна из них — спам, или, попросту говоря, незапрошенная почта. Если не принять решительных мер по ее отфильтровыванию, «эпистолярная река» может не только вымыть из бюджета фирмы за небольшой срок тысячи долларов, но в отдельных случаях и сделать из IT-структуры организации послушный инструмент чужого бизнеса**

## Спамеры с большой дороги

### *(Краткое описание криминальных категорий спама, присутствующих в Рунете)*

#### Фишинг

В 2004 году появилась и начала стремительно расти новая тематическая разновидность спама — фишинг.

Фишинг («ловля на удочку») — это распространение поддельных сообщений от имени банков либо финансовых компаний. Целью такого сообщения является сбор логинов, паролей и пин-кодов пользователей. Обычно такой спам содержит текст с предупреждением об обнаруженных «дырах» в безопасности денежных операций-онлайн, в качестве меры предосторожности предлагается зайти на сайт и подтвердить или сменить пароль доступа к счету или пин-код банковской карты.

Естественно, ссылки в таком письме ведут не на настоящие банковские сайты, а на поддельные — спамерские. Ворованные коды или пароли можно использовать как для доступа к счету, так и для оплаты покупок в интернет-магазинах. К концу 2004 года спамеры перешли на более продвинутые технологии, и теперь фишинг-сообщения могут содержать «шпионский» скрипт, который перехватывает пароли при вводе их на официальном банковском сайте и пересылает спамеру. Причем для активации скрипта достаточно просто открыть сообщение.

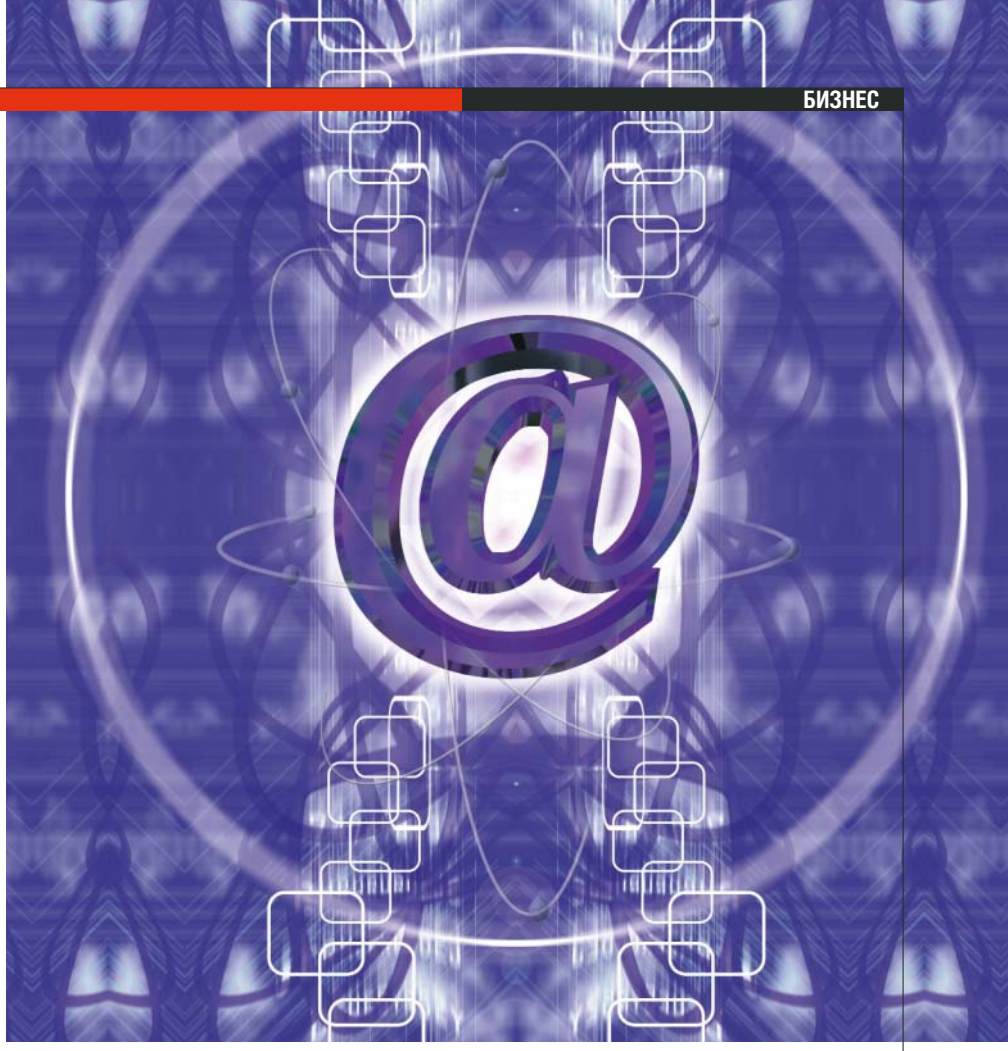
В процентном отношении доля фишинг-сообщений пока не слишком велика, не более 1% от общего потока спама, но пугают темпы роста. В 2003 году такого спама фактически не было, сейчас это уже заметное явление, не понаслышке известное многим пользователям.

Хотя большинство фишинговых писем является англоязычными, пользователей Рунета спамеры тоже не обошли своим вниманием. Особой «любовью» пользуется российский «Ситибанк». Вот пример типичного фишинг-сообщения:

```
From: CityBank
To: Иванов Иван Иванович
Subject: Уведомление о получении платежа
Уважаемый клиент!
На Ваш текущий счет был получен перевод в иностранной валюте на сумму, превышающую USD 2,000. В соответствии с пользовательским соглашением CitiBankR, Вам необходимо подтвердить этот перевод для его успешного зачисления на Ваш счет.
Для подтверждения платежа просим Вас зайти в программу управления Вашим счетом CitiBankR и следовать предложенным инструкциям. Если подтверждение не будет получено в течение 48 часов, платеж будет возвращен отправителю.
Для входа в программу CitiBankR, нажмите сюда >>
С уважением, Служба CitiBankR
```

Своеобразной разновидностью можно считать письма, цель которых — кража паролей от почтовых ящиков. В 2004 году несколько раз проводились подобные рассылки с целью кражи логинов и паролей пользователей Национальной почтовой службы Mail.Ru. Ниже приведен пример спамерского письма, целью которого являлся сбор паролей пользователей Mail.ru:

```
Здравствуйте!
Уважаемый пользователь сервиса @mail.ru, пожалуйста, следуйте всем инструкциям данного письма.
Некто (скорее всего, злоумышленник) только что попытался получить Ваш пароль от e-mail ящика методом MD6 PASSWORD POST.
В целях защиты наш DB робот очистил из базы данных Вашу запись с паролем, и Вы НЕМЕДЛЕННО должны послать на адрес passwriter@mail.ru сообщение данной конструкции: (вместо «password» после } PASSWORD IS . вы должны указать свой настоящий пароль от этого e-mail ящика)
// Password re-write
ADD to * '$username' TABLE * «password»
} PASSWORD IS password // вместо «password» в письме должен быть указан Ваш текущий пароль (без кавычек)
} rewrite with * deleted password /
} end } END of query ;exit
// Password re-write
```



В скором времени мы установим более совершенный способ защиты. Вы немедленно должны отправить данное сообщение, потому что на доступ к вашей персональной DB таблице с правами root обладаете только Вы. На это письмо отвечать не надо, так как оно написано роботом автоматически. Если вы получили несколько копий данного письма, злоумышленник пытался получить ваш пароль несколько раз.

С уважением, администрация почтового сервиса @MAIL.RU

## «Черный пиар» и использование известного бренда

В 2004 году были неоднократно зафиксированы случаи фальсификации рассылок от имени известных фирм, производившиеся с целью испортить имидж данной фирмы и дискредитировать ее в глазах пользователей.

Спам активно используется для «черного пиара», т.е. для создания отрицательного имиджа компании-конкурента и очернения политических деятелей. Участились случаи, когда спамеры, фальсифицируя сведения об отправителях и источниках рассылки, наоборот, пытаются использовать репутацию известной фирмы, чтобы привлечь внимание к рекламируемым товарам и услугам. В конце ноября — декабре 2004 года по Рунету прошла волна спама, замаскированного под рассылки популярного проекта Subscribe.ru. Такие подделки включали не только упоминание Subscribe.ru в тексте спамерского письма, незаконное использование логотипов проекта и т.д.; в фальшивых рассылках также были аккуратно подделаны все технические сведения (заголовки сообщения).

## Продажа контрафакта

Доля рекламы «потрясающе дешевых товаров» — от лекарств до программного обеспечения — к концу 2004 года увеличилась настолько, что превысила долю порнорекламы, которая раньше являлась несомненным лидером спамерских тематик. Между тем большинство подобных товаров либо являются контрафактными (как софт или часы «Ролекс») либо не соответствуют заявленному названию и могут представлять угрозу для жизни и здоровья (как некоторые лекарства и сигареты).

## Социальный инжиниринг

В отдельную категорию можно выделить спамопослания, «играющие» на человеческих эмоциях.

— Однажды на мой ящик на mail.ru пришло очень красивое, можно даже сказать, художественное письмо, — рассказывает Андрей Никишин. — Оно было написано от имени девушки, которая вспоминала, «как мы здорово вчера провели время». «Было все замечательно, — пишет незнакомка, — и ты сам просто чудо. Но... у тебя так дома полы скрипят, милый, не хочешь ли ты сходить, купить пол там-то». То есть мне предлагали купить ламинат! Причем имя как-то подобрали... Письмо было очень грамотно составлено, я не удержался, послал друзьям для коллекции. Нормальное, обычное письмо от девушки молодому человеку. Сходу понять, что это спам, действительно сложно. Признаюсь, оно отняло определенное время. Кто-то отлично поработал. Но составление таких писем — трудоемкий процесс. Поэтому они — редкость.

Методы социального инжиниринга могут быть использованы не только для продвижения товаров, как в последнем примере, но и из чисто инфернальных побуждений. Автор статьи однажды столкнулся с письмом, составители которого пытались использовать эмоции страха, чувства взаимопомощи и доверия. Идея была проста донельзя. В тексте послания предлагалось зайти в системную папку Windows и удалить оттуда определенные файлы, так как по заверению сочинителей письма «они являлись компонентами вредоносной программы замедленного действия, способной стереть все данные с компьютера». Мало того, что людям предлагалось своими же руками разрушить систему, — от них незамедлительно требовали «разослать это письмо друзьям, знакомым и деловым партнерам, дабы предупредить их об опасности.

Понятно, что при пересылке эта информация воспринималась с большим доверием. Таким образом человек брал на себя функции вируса и спамомашины. Причем, как ему казалось, из лучших, благородных побуждений.

*При подготовке статьи был использован «Спам 2004: аналитический отчет» , ЗАО «Ашманов и Партнеры», http://www.spamtest.ru/document?pubid=19223&context=1*