Н. Г. Ляпичева, О. М. Никонова (Москва, ЦЭМИ РАН)**. Современные проблемы почтового сервиса.**

«Времена меняются, и мы меняемся вместе с ними»

Не углубляясь в историю развития атак на почтовый сервис больше чем на 5 лет, можно за этот период обнаружить ряд тенденций, сменяющих друг друга. Общим в них остается направленность на включение сферы нелегитимного использования почтового сервиса в экономические отношения, как в виде относительно легального бизнеса, так и со всеми оттенками серого и черного.

Период массовой рассылки почтовых вирусов, приходящийся на 2004-2007 гг. [1], подготовивший почву для последующего массированного распространения спама, сменился использованием ранее организованных «зомби»-ресурсов и ботнетов для рассылки, результатом чего в первую очередь стало неэффективное расходование сетевых ресурсов Интернета [2].

В отчетах Лаборатории Касперского [3] за 2008 г. также отмечена утрата первенства вирусов массовой рассылки в общей картине распространения вредоносных кодов. Там же выявлена смена роли элетронной почты от прямой рассылки рекламных изделий к более активному использованию различных видов фишинга как для подачи веб-рекламы, так и для реализации криминальных бизнес-планов, от обычного кибермошенничества («Нигерийская вдова») до современных киберпреступлений в сфере электронной торговли и банковской сфере. В частности, электронная почта может использоваться как средство переадресации получателя на сайт-ловушку, организованную в упомянутых целях. Эти периоды иллюстрируются рис. ниже.

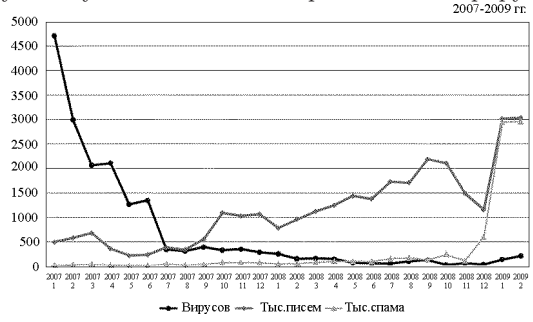

Рис. Смена направленности почтовых атак: 2007–2009 гг.

Давно ожидаемый результат уменьшение спам-нагрузки на почтовый сервис может быть достигнут при снижении эффективности его использования в качестве промежуточного средства других вредоносных воздействий, комплекс методов борьбы с которыми включает широкий набор аппаратно-программных средств защиты.

На основании проведенных исследований было принято решение о внедрении средств удаления входящего спама на почтовом антивирусном/антиспамовом шлюзе [4], в результате чего удаляется около 97% спама (в месяц в сеть пропускается около 85тыс.писем из 3 млн.), причем оставшийся частично отфильтровывается на следующих уровнях защиты почтового сервиса.

СПИСОК ЛИТЕРАТУРЫ

1. *Ляпичева Н. Г.* Анализ вирусной активности в почтовом трафике на узле ЦЭМИ РАН. — Труды Третьей Всероссийской научно-практической конференции «Научное, экспертно-аналитическое и информационное обеспечение стратегического управления, разработки и реализации приоритетных национальных проектов и программ», 31 мая - 1 июня 2007 года, ИНИОН РАН, М: 2007, с. 538–542. http://www.socionet.ru/publication.xml?h=repec:rus:ualhnv:inion2007-1

2. *Ляпичева Н. Г.*, *Никонова О. М.* Математико-статистический анализ объемов спама на узле ЦЭМИ РАН. — Обозрение прикл. и промышл. матем., 2008, т. 15, в. 4, с. 670–671.
3. Kaspersky Security Bulletin. Спам в 2008 г. http://www.spamtest.ru/document.html?context=15948&pubid=208050489
4. Symantec Mail SecurityT for SMTP 5.01 (Premium Antispam). http://www.symantec.com/business/mail-security-for-smtp