Автор: Артур Скальский © Известия.Ру ЗДОРОВЬЕ, МИР 2514 06.08.2003, 10:28 274

Русский червь пугает мир

По мировому Интернету начал стремительно распространяться очередной киберчервь - на этот раз российского производства. Российские продукты по борьбе с вирусами достаточно популярны на Западе - по крайней мере, о них знают пользователи и мировые лидеры рынка ПО. Российские "качественные" вирусы встречаются гораздо реже. При этом и борьба с вирусами в России и на Западе выглядит по-разному - прежде всего в психологическом и эмоциональном плане. К тому же в реальной поимке создателей кибервредителей мало кто заинтересован.

Новый вирус под кодовым названием Mimail входит в топ-листы практически всех компаний, занимающихся борьбой с виртуальными вредителями. Этот вирус является интернет-червем, распространяющимся во вложенных файлах электронных писем. Письма с вирусом приходят с замаскированного адреса и сообщают пользователю, что внутри письма находится важная информация о его электронном адресе. Mimail использует "дыру" в системе безопасности браузера Internet Explorer. Если пользователь открывает письмо, то Mimail незаметно записывает на жесткий диск компьютера и запускает файл-носитель червя FOO.EXE. Затем он копирует себя в директорию Windows под именем VIDEODRV.EXE и далее сам запускает себя при каждой загрузке операционной системы. Также вирус создает свои копии в различных форматах и в заархивированном виде.

Дальнейшее распространение вируса весьма банально - он ищет на жестком диске чужие электронные адреса и начинает незаметно по ним сам себя рассылать. Стоит отметить, что брешь, которую использует данный вирус, была обнаружена еще в марте 2002 года, и компания Microsoft быстро выпустила специальную "заплатку" для Internet Explorer. Однако, как это часто бывает в подобных случаях, эту заплатку многие не стали устанавливать. Новостью в данном случае является то, что скорее всего вирус, входящий в тройку самых распространенных на сегодняшний момент, был создан в России.

Об этом заявили в российской компании "Лаборатория Касперского". При этом "Финансовым Известиям" в компании рассказали, что "прямого" вреда вирус не приносит (например, он не стирает файлы). Однако вред от него может оказаться значительным хотя бы потому, что он будет забивать почтовые ящики по всему миру и мешать нормальной работе почтовых систем. К тому же, как считают в "Лаборатории", в данном случае страдает деловая репутация интернет-пользователя, с чьего адреса вирус продолжает свое путешествие. При этом российские разработчики антивирусных программ оценивают вероятность получения вируса как весьма высокую.

Российское происхождение Mimail в "Лаборатории Касперского" объясняют тем, что код вируса почти полностью совпадает с одно время нашумевшим российским вирусом StartPage. Вот здесь и начинается процесс гадания.

В "Лаборатории Касперского" считают, что доказательством российского происхождения StartPage служит то, что все "сопровождающие" его письма были написаны на чистом русском языке без особых ошибок. Других доказательств происхождения вирусов на сегодняшний день не существует. Причем это касается всех вирусов вообще - например, наличие испанских слов в письменной "оболочке" вируса заставляет всех говорить, что вирус сделан в Испании или в Латинской Америке. Поэтому русский текст писем на самом деле может свидетельствовать как о российском, так и об украинском, белорусском, израильском или "брайтон-бичском" происхождении. Географический разброс в данном случае весьма красноречив - помочь в обнаружении автора вируса такие рассуждения помочь не могут.

Борьба со следствием, а не с причиной

Сейчас в индустрии, производящей программы против вирусов и средства компьютерной безопасности, крутятся миллиарды долларов. При этом компании вынуждены придумывать хитроумные и зачастую дорогостоящие средства лишь для предотвращения непосредственно вирусной атаки или для снижения ущерба от нее. Принципиально решить проблему и навсегда покончить с вирусами эта индустрия не способна. Но в этом не ее вина.

Например, компания Symantec - один из мировых лидеров этой индустрии - создала поистине всемирную структуру по сбору информации о различной вирусной активности. В ключевых регионах мира расположены специальные центры, куда в автоматическом режиме стекается информация от более 19 000 партнеров компании, установивших у себя специальные программы-сенсоры, реагирующие на нестандартные ситуации. Например, информация о Mimail появилась в Symantec 1 августа, и сейчас этому вирусу присвоен балл "3" по пятибалльной шкале, где "5" означает самый высокий уровень опасности. В компании "Финансовым Известиям" рассказали, что сейчас опасность Mimail оценивается выше среднего уровня. Далее - по стандартному алгоритму - при появлении действительно реальной глобальной опасности принимается решение о том, чтобы поставить клиентов в известность и предоставить им алгоритм борьбы с вирусом. По поводу методов своей работы в Symantec заявили: "Мы работаем по всему миру - и тихо. А "Лаборатория Касперского" в России - и громко". Что касается именно российской составляющей этой борьбы, то в Symantec подтвердили, что среди партнеров, поставляющих компании информацию об атаках, есть и российские структуры. Но они традиционно не хотят объявлять свои имена и подтверждать наличие у них проблем с информационной безопасностью. Именно поэтому, по мнению специалистов Symantec, нет российских данных об общем количестве вирусных атак и о финансовых потерях от них, что усложняет борьбу с кибервредителями. Кстати, российское происхождение вируса Mimail в Symantec ставят под сомнение. По крайней мере, подобного рода анализ никогда не проводился, видимо, по причине его неэффективности. К тому же в Symantec считают, что Россия никогда не была влиятельным "поставщиком" серьезных вирусов.

Поиск тайного врага

На первый взгляд для победы над вирусами нужно подойти к проблеме с другого конца - отлавливать их создателей и наказывать. Однако не все так просто. Теоретически даже при всех технических ухищрениях выловить распространителя зараженных писем можно. Особенно тех, чья деятельность имеет коммерческую составляющую: например, некоторые вирусы используются для того, чтобы украсть из компьютера пароли доступа в Интернет или данные о счете пользователя. В "Лаборатории Касперского" сообщили, что были случаи вычисления таких киберпреступников и в России. Однако предписываемое законом наказание - заключение сроком до 7 лет - так никто и не понес. Причина в том, что Интернет - стихийная и саморегулирующаяся система.

Интернет может быть безопасным лишь в том случае, если он безопасен весь. Если найдется хотя бы один провайдер, который не подключится к общим усилиям по поимке преступников, эти усилия будут бессмысленными. Однако, по мнению представителей "Лаборатории Касперского", провайдеры пока не заинтересованы в серьезной борьбе за отслеживание преступников, поскольку провайдерам вся эта вирусная война не приносит больших убытков. Что касается государства, то оно теоретически могло бы упорядочить интернет-жизнь. Однако вольное интернет-сообщество никогда не согласится на такие правила игры. Лишь в Китае государство смогло заставить подчиниться интернетчиков, однако у этого процесса оказалось слишком много побочных эффектов, несовместимых с демократическим устройством общества. Поэтому интернет-свобода и дальше будет распространяться на всех - и на честных интернетчиков, и на создателей вирусов.

Автор: Артур Скальский © Известия.Ру ЗДОРОВЬЕ, МИР 2514 06.08.2003, 10:28 274
URL: https://babr24.com/?ADE=8491 Bytes: 7412 / 7392 Версия для печати

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта