**Вирусные угрозы и проблемы информационной безопасности**

Вирусные угрозы с каждым днем все возрастают. Еще совсем недавно врагом номер один были обычные сетевые черви, которые путешествовали от компьютера к компьютеру, используя уязвимости в клиентском программном обеспечении или неосмотрительность пользователя. Одним из ярких представителей таких червей был Klez. Сегодня все намного сложнее.

Прежде всего, обращает на себя внимание факт появления нового поколения вредоносных кодов — бестелесных червей. Эти вредители способны за несколько минут разрушить современную инфраструктуру интернета. Хотелось бы написать «потенциально способны», но, увы — один из представителей таких червей, Slammer, в конце января 2003 года смог «обездвижить» около 25% интернета! Через 5 минут после начала эпидемии были заражены компьютеры в Южной Корее, Японии, США, Западной Европе. Через 15-20 минут было заражено более 100 тысяч компьютеров!В отличие от классических почтовых червей, бестелесные черви в процессе заражения и распространения не используют ни временных, ни постоянных файлов.

Бестелесные черви впервые появились летом 2001 года, когда была зарегистрирована вспышка эпидемии печально известного CodeRed. Смысл этого класса вредоносных кодов наглядно объясняется их общим названием — «бестелесные». В отличие от классических почтовых червей, бестелесные черви в процессе заражения и распространения не используют ни временных, ни постоянных файлов. Они пробираются на компьютеры через бреши в системах безопасности и существуют исключительно в виде пакетов данных, передаваемых по коммуникационным каналам, или в виде программного кода в памяти зараженного компьютера.

С бестелесными червями очень трудно бороться. Главная проблема заключается в том, что скорость распространения этих вредителей гораздо выше, чем скорость реакции антивирусных компаний. Черви данного типа распространяются со скоростью интернета, то есть такой «замедлитель» распространения вирусных эпидемий как человек не присутствует в цепочке распространения (не надо запускать зараженный файл, не надо кликать по вложению и т. п. — вирус запускает себя сам в момент проникновения на компьютер-жертву). Скорость же реакции разработчиков антивирусных решений — это скорость работы человеческого ума и пальцев, которая значительно уступает молниеносным интернет-эпидемиям бестелесных червей.В конфликт были вовлечены три группировки кибер-преступников: создатели Netsky с одной стороны, разработчики Mydoom и Bagle с другой.

Но бестелесные черви — это не единственная опасность, явившаяся в результате эволюции вирусных угроз. Недавно мы стали свидетелями войны между вирусописателями. Авторы почтовых червей Bagle, Mydoom и Netsky обменивались «любезностями», выпуская все и новые версии своих червей. Всего за 3 часа 3 марта 2004 г. «Лаборатория Касперского» зафиксировала появление сразу 5 новых модификаций печально известных вредоносных программ Bagle (версии i, j), Mydoom (версии f, g) и Netsky (версия f). В конфликт были вовлечены три группировки кибер-преступников: создатели Netsky с одной стороны, разработчики Mydoom и Bagle с другой. Каждая новая модификация червей несла в себе очередное послание к противостоящей группировке, изобилующее нецензурными выражениями.

В этой ситуации больше всего поражает всеобщее бессилие: ни пользователи интернета, ни бизнес-компании, ни правительства, ни спецслужбы — никто не в состоянии помешать горстке технически образованных, но психически неуравновешенных людей играть со всем интернет-сообществом. Данный инцидент является первым звоночком, который обязан привлечь наше внимание. Как вы думаете, если разгорится настоящая война вирусописателей друг с другом, на каком поле боя они будут выяснять отношения, и кто от этого пострадает в первую очередь?

И ещё о войнах. Сегодня главной угрозой национальной безопасности государств является терроризм. Нестабильная ситуация в мире заставляет задуматься: что мешает террористическим и криминальным группировкам устроить кибертеракт или киберограбление? Ведь нет ничего проще, чем взять к себе на службу нескольких хакеров! Компьютерных злоумышленников (например, тех, кто грабит банки) ловят из-за того, что они не умеют скрываться в реальной жизни. Ничто не мешает преступным не виртуальным коллегам поделиться с ними опытом.Террористы планируют вызвать сбои в системах крупнейших экономических и финансовых центров Запада, нарушить работу электросетей, водопровода, промышленных предприятий.

Аналитические центры безопасности США обеспокоены информацией о том, что международные террористические группировки, связанные с исламскими фундаменталистами, готовят беспрецедентную атаку на интернет. Они планируют вызвать сбои в системах крупнейших экономических и финансовых центров Запада, нарушить работу электросетей, водопровода, промышленных предприятий. Последствия террористической атаки в интернете могут быть сравнимы с событиями 11 сентября 2001 года в Нью-Йорке. Если эта информация подтвердится, то сотрудничество террористов и киберпреступников станет неоспоримым фактом и новой, очень серьёзной угрозой.

Еще одним примером вредоносного сотрудничества является объединение спамерских, хакерских и вирусных технологий. Злоумышленники уже сейчас реализовали схему: спам используется для того, чтобы рассылать вирусы пользователям, вирусы поражают компьютеры, которые в дальнейшем служат базой для хакерских атак или рассылки коммерческого спама. Таким образом, злоумышленники заметают следы (противоправные действия совершаются с компьютера невинного пользователя) и в несколько раз повышают эффективность собственных атак (ведь в их распоряжении оказываются мощности многих компьютеров).

Не стоит думать, что описанные угрозы носят гипотетический характер и опасны только крупным известным компаниям. Вне зависимости от того, кем вы являетесь — крупной бизнес-компанией или обычным пользователем интернета — вирусы могут принести огромные финансовые убытки именно вам. Приведем лишь несколько примеров. Бэкдоры предоставляют злоумышленнику удаленный доступ к зараженному компьютеру. Часто вредоносная программа может являться одновременно и сетевым червем и бэкдором.

Одной из тенденций, выявленной в 2003 году «Лабораторией Касперского», явилось увеличение числа бэкдоров (backdoor, программа скрытного удаленного администрирования) среди общего количества вредоносных программ. Бэкдоры предоставляют злоумышленнику удаленный доступ к зараженному компьютеру. Часто вредоносная программа может являться одновременно и сетевым червем и бэкдором. Такой вредитель распространяется в сети по всем направлениям. Попав за периметр корпоративной сети, он сразу же предоставит своему создателю полный контроль над зараженной сетью и подключенными к ней компьютерами. Еще чаще обычный червь сам отсылает пароли и другую важную информацию своему хозяину, тому остается лишь выбрать, чем полакомиться на завтрак, чем на обед, а чем на ужин.

Злой шуткой является вредоносная программа «порно-дилер», которая почти насильно (используя технологии социальной инженерии) выбивает из пользователя разрешение на закачивание порнографических материалов с платных сайтов интернета. Как вы думаете, кому потом приходит счет? Вы не сможете доказать свою непричастность к аморальным поступкам, ведь вредоносная программа заручилась вашим собственным согласием (используя бесчисленное множество психологических трюков). От таких приемов, прежде всего, пострадают обычные пользователи, так как во многих компаниях работа с порноресурсами заблокирована.

Еще одной опасностью для пользователей интернета являются программы-троянцы, ворующие виртуальные деньги. Сейчас широко распространена система электронных платежей (читай денег) — webmoney. Вредоносные программы встраивают свой код в webmoney-клиент, расположенный на вашем жестком диске, или просто предлагают пройти перерегистрацию. После того как злоумышленник или его троянец получат доступ к вашему виртуальному кошельку, они переведут все деньги себе. Владельца компьютера, который ни в чем не виноват, привлекут к суду за те преступления, которые злоумышленник натворил при помощи своего вируса.

Выше уже упоминалось, что вирус может сделать из вашего компьютера базу для предстоящих хакерских налетов. Такое бывает очень и очень часто. Владельца компьютера, который ни в чем не виноват, привлекут к суду за те преступления, которые злоумышленник натворил при помощи своего вируса. Важно также и то, что вирус может легко самоликвидироваться после получения соответствующей команды от своего создателя. В этом случае хозяин компьютера не имеет никакой возможности доказать в суде свою невиновность.

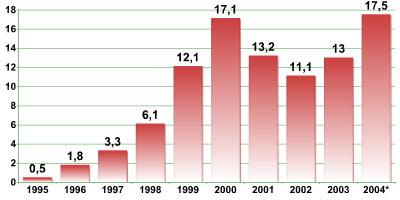
Почему же вирусы так распространены? Почему так часто они поражают, казалось бы, отлично защищенные сети крупных и средних компаний? В чем же здесь дело? Причина кроется вовсе не в плохом антивирусном ПО и слабой поддержке клиентов со стороны антивирусных компаний. Отнюдь! Исследования показывают, что решающую роль играет человеческий фактор. Чаще всего до катастрофы доводит халатность системного администратора. Любые средства защиты становятся бесполезными без своевременного обновления программного обеспечения и установки необходимых патчей. Это все равно, что поставить железную двойную дверь, но открыть балкон и приставить к нему лестницу.

Но причина не в одних лишь системных администраторах. Подавляющее большинство простых пользователей недостаточно осведомлены о проблемах безопасности. Каждый пользователь должен понимать, какую опасность таят в себе вирусы, и знать хотя бы элементарные правила компьютерной гигиены. В противном случае даже самый умный системный администратор и максимально эффективный антивирусный комплекс окажутся бессильными. Новый финский замок и закрытые изнутри окна — это хорошо, но если жильцы сами открывают дверь, кому не попадя, то дом по-прежнему в опасности. Часть пользователей используют нелицензионное программное обеспечение, устанавливают большое количество сомнительного софта, а потом не следят за ним. Сомнительное, пиратское ПО иногда оказывается изначально инфицированным, а также может содержать недокументированные вредоносные функции. Подавляющее большинство простых пользователей недостаточно осведомлены о проблемах безопасности.

Помимо банального нарушения закона, использование нелицензионного антивирусного софта дает ложное ощущение собственной безопасности. Ведь такой пользователь не получает обновлений продукта, часто не имеет возможности обновлять антивирусные базы и лишен всяческих новостей о грозящих эпидемиях и опасностях. Зачастую пиратская антивирусная программа к моменту своего появления на рынке устаревает настолько, что становится бесполезной для борьбы со всеми вирусами, появившимися за последние месяцы.

Приведем немного статистики. По данным Computer Economics в 2000 году ущерб мировой экономике от действий вирусов составил огромную сумму — около 17,5 млрд долларов. Большинство бизнес-компаний тогда пострадало от целой серии скриптовых вирусов и печально знаменитых «любовных» писем (LoveLetter). Чтобы не допустить подобного в будущем, многие представители бизнеса увеличили свои ИТ-бюджеты, в частности ту часть, которая приходилась на информационную безопасность. Это принесло существенные плоды — ущерб снизился до 13,2 млрд долларов. В 2001 году весь мир был потрясен ужасным террористическим актом в США, многие компании снова вложили свои средства в информационную безопасность и, как результат, ущерб снизился еще до 11,1 млрд долларов — это ниже чем в 1999 году. Как часто бывает, у пользователей возникло ложное ощущение безопасности. Многие представители бизнеса, будучи полностью удовлетворенными эффективностью своих вложений в последние два года, урезали бюджеты на ИТ-безопасность. В результате ущерб от вирусов за 2003 год составил порядка 13 млрд долларов, что значительно больше, чем в 2001-2002 годах.

Общемировой ущерб от вирусных эпидемий. млрд USD



Показателен прогноз Computer Economics на 2004 год, ущерб от вирусных эпидемий в котором, предположительно, впервые превысил рекордные показатели 2000 года. Основной ущерб экономике нанесли крупные эпидемии компьютерных червей: Bagle, NetSky, Sasser и Mydoom (в порядке увеличения показателей причиненного ущерба). Учитывая, что во второй половине 2004 года значительных эпидемий не случилось, прогноз можно считать достаточно точным.

Как же бороться с вирусной опасностью? Для того чтобы защитить свои финансы и секретную информацию, а также снизить возможный ущерб от действий вирусов, необходимо, прежде всего, с должным вниманием относиться к информационной безопасности. Проблема не решится сама собой, каждый день появляется около 50 новых модификаций различных вирусов, тысячи антивирусных специалистов постоянно анализируют вредоносные коды и готовят соответствующие кибервакцины. От пользователей, компаний и муниципальных предприятий следует лишь грамотно развернуть антивирусный комплекс в масштабах своей сети, а потом поддерживать его работоспособность.Только последние версии антивирусных продуктов способны надежно защитить пользователей от современных вирусных угроз.

Чтобы поддерживать свою защиту на должном уровне требуется как можно чаще обновлять антивирусные базы. На предприятии это обычно не является проблемой — правильно настроенное антивирусное решение будет скачивать и устанавливать обновления в автоматическом режиме. Совсем другое дело — обновление самого продукта. С каждой новой версией появляются новые антивирусные модули, исправляются мелкие недочеты, а порой и ошибки, в старых модулях. Что еще более важно, в новых версиях реализованы технологии, существенно повышающие эффективность борьбы с новыми видами киберинфекций. Таким образом, только последние версии антивирусных продуктов способны надежно защитить пользователей от современных вирусных угроз. Заметим, что в последнее время на рынке появились компании, которые предлагают профессиональные услуги по установке и поддержанию в рабочем состоянии систем безопасности. По-видимому, небольшим компаниям, не обладающим достаточными ресурсами на самостоятельное управление антивирусной защитой, следует рассмотреть и такой вариант.

Важно помнить, что слабым звеном любой модели безопасности является человек. Поэтому специалистам, отвечающим в компании за компьютерную безопасность, следует проводить просветительскую работу среди своих сотрудников. Это не потребует больших финансовых затрат, а время, потраченное на ликбез, окупится сполна. Необходимо регулярно рассказывать служащим об элементарных правилах компьютерной гигиены, это сформирует у персонала правильный взгляд на проблему информационной безопасности, а вместе с антивирусным комплексом и другими средствами безопасности позволит обеспечить высокий уровень защиты.

На фоне снижения ИТ-бюджетов вообще, приятно отметить, что инвестиции в информационную безопасность в целом растут. Мировое сообщество постепенно осознает необходимость создания эффективной законодательной базы для борьбы с киберпреступлениями. В России, например, постоянно совершенствуется глава 28 (статьи 272-274) УК РФ, посвященная целиком и полностью преступлениям в сфере информационных технологий.Главный союзник хакеров и вирусописателей это несерьезное отношение к самозащите самих пользователей.

Важную роль в решение проблемы информационной безопасности играет просветительская деятельность самих поставщиков продуктов для защиты компьютерных сетей. Своевременное оповещение о вирусных эпидемиях, подробное описание вирусов и методов борьбы с ними — все это не менее важно, чем создание эффективных антивирусных программ.

Информационная безопасность еще долго будет стоять на первом месте среди приоритетов современного бизнеса. Главный союзник хакеров и вирусописателей это несерьезное отношение к самозащите самих пользователей, ленящихся принять ряд мер, позволяющих существенно сократить возможные риски. Поэтому ваша безопасность зависит, в первую очередь, от вашего понимания проблемы, принятия правильных и своевременных решений, а также от использования современного антивирусного программного обеспечения.