**Вирусы против технологии NX в Windows XP SP2**

Идеальных систем не бывает. И что бы в Microsoft ни говорили о курсе на укрепление безопасности своих продуктов, ошибки и критические уязвимости в них будут находить всегда. Установка Service Pack 2 может попортить немало крови даже опытному администратору (См., например, статью Безопасная Windows. А ведь главный "бонус" такой установки - повышение уровня безопасности Windows XP. Так стоит ли овчинка выделки для обычного домашнего пользователя или пока ему вполне можно и подождать?..

**Основные угрозы безопасности**

Взглянем на двадцатку "самых популярных" вредоносных программ минувшего сентября.

Табличку, на самом деле, можно сильно сократить: по большей части она заполнена разнообразными штаммами червей NetSky, Bagle и Mydoom. Одно место досталось венгерскому червю Zafi и еще два занимают представители семейства троянских программ. Все до единого участники "горячей двадцатки" используют только доверчивость и неопытность пользователя: черви распространяются по электронной почте и через P2P-сети в виде исполняемых файлов, а троянцев пользователи вообще подкидывают друг другу сами. А значит, Service Pack 2 на эту ситуацию принципиально не повлияет: "дырки" в головах компьютеровладельцев он, увы, закрыть не в состоянии. Так, может, его и устанавливать не надо?

Проведем простейший эксперимент: подключим ПК со свежеустановленной Windows XP Professional SP1 к Интернету через одного из крупнейших московских провайдеров - "МТУ-Интел" (который вроде бы даже фильтрует в своей сети наиболее известные и опасные вирусы - и уж точно должен был бы фильтровать MSBlast), откроем в IE сайт "Компьютерры" и засечем время. Спустя примерно восемнадцать минут (и скажите еще спасибо, что вам эти 18 минут дали. В студенческих сетях общежитий того же МГУ "время жизни" незащищенной машины составляет не более 3–5 минут компьютер, как и ожидалось, подцепил вирус W32.Blaster.Worm. Так что бросаться из крайности в крайность не стоит: хотя бы наиболее критичные заплатки (в данном случае - KB823980) поставить все-таки необходимо. К тому же MSBlast - всего лишь самый известный червь, проникающий на компьютер без каких-либо действий со стороны пользователя, но есть и гораздо более опасные "незаметные" черви, от которых антивирусы защищают плохо.

Так, много шуму наделала обнаруженная в конце лета уязвимость MS04-28 в стандартной библиотеке GDI+ Windows XP(См. www.microsoft.com/technet/security/bulletin/MS04-028.mspx). Функции этой библиотеки, используемые для просмотра JPEG-файлов, содержат ошибку типа "переполнение буфера" и позволяют при просмотре специально сформированной картинки запустить на компьютере жертвы произвольный код. Библиотеку, включенную во все разновидности Windows XP, используют не только Internet Explorer и Outlook, но и едва ли не каждая вторая программа, которой приходится просматривать картинки этого формата. О масштабах угрозы красноречиво говорят пять (!) выпущенных патчей и список "affected software" на два экрана. А самое печальное, что, даже установив эти патчи, в полной безопасности вы себя все равно не почувствуете, ибо добрые программисты, дабы не терять совместимости своих продуктов с версиями Windows, отличными от XP, и использовать в полной мере преимущества нового графического интерфейса, запросто могли включить в дистрибутивы уязвимую копию GDI+.

К счастью, летом и в начале осени вирусы вели себя на удивление тихо, так что ожидаемая аналитиками эпидемия почтового вируса, использующего эту уязвимость, не состоялась. Пока. Но "потенциал" у JPEG-эксплойта потрясающий, и сомневаться в том, что рано или поздно появится целое семейство соответствующих вирусов, не приходится (в интернете на "клубничных" сайтах уже обнаружились первые "ласточки". Остается лишь порадоваться тому, что хотя информация о MS04-28 появилась только 14 сентября (SP2 вышел двумя неделями раньше), основные заплатки от этой мерзости второй сервис-пак все же содержит (впрочем, это тема для отдельного обсуждения (см., например, материал Мы впишем новую страницу!).

**Data Execution Prevention - защита от еще не существующих эксплойтов**

Впрочем, "недолго музыка играла". Да, из десятка опубликованных с момента выхода SP2 новых уязвимостей большая часть в Windows XP SP2 не работает. Да, на сегодняшний день не существует ни одного хотя бы концептуального эксплойта, на практике доказывающего возможность поражения Windows XP с установленным SP2. Но (возвращаясь к началу статьи) первые соответствующие уязвимости уже найдены и описаны. Например, выпущенный недавно кумулятивный апдейт MS04-038 к Internet Explorer(См. www.microsoft.com/technet/security/Bulletin/MS04-038.mspx) затрагивает и Windows XP SP2 - правда, пока лишь в ранге Important, а не Critical.

Итак, что же получается? SP2 не дает ничего принципиального нового по сравнению с заплаткой KB833987 и подобных ей? Не совсем: счастливые обладатели процессоров AMD Athlon 64/Sempron (Socket 754) и последних степпингов Pentium 4 Prescott/Celeron D, наконец-то получат работающую аппаратную "противовирусную поддержку" в виде специального бита NX в таблицах трансляции виртуальной памяти. Если не вдаваться в подробности (за которыми я отсылаю к статье, упомянутой в предыдущей сноске), благодаря этому биту операционная система может запретить выполнение кода из определенных областей памяти. В случае с SP2 Microsoft попросту запрещает выполнять код из любых областей, для которых явным образом не сказано, что они предназначены именно для кода. И одновременно по умолчанию запрещает запись в страницы, объявленные для хранения кода. Так что какую бы уязвимость в обработке сетевых запросов ни содержала программа, запустить вредоносный код на машине жертвы невозможно: записать вирус в участки памяти, уже занятые программным кодом, нельзя - они защищены от записи. А записывать вирус в любое другое место - в стек или область данных (что и используется во всевозможных уязвимостях с переполнением буфера) - смысла нет, поскольку запустить его оттуда на компьютере с аппаратной поддержкой NX не удастся. Все эти хитрости корпорация называет технологией DEP (Data Execution Prevention).

Честно говоря, вооружившись собственноручно написанной крошечной программкой, проверяющей функционирование DEP, я был несколько обескуражен тем, что на свежеустановленной Windows XP Professional (кстати, кто-нибудь из читателей может объяснить, почему после установки SP2 надпись "Professional" с загрузочного экрана исчезает?) имитация атаки переполнением буфера прошла более чем успешно. Оказалось, что по умолчанию технология Data Execution Prevention в новом сервис-паке включена только для загадочных "наиболее критичных системных приложений". Видимо, Microsoft решила, что вылет приложений по срабатыванию DEP (например, из бенчмарков по DEP "вылетает" Vulpine GLmark) может переполнить чашу терпения пользователей. Однако и выключить DEP совсем, если компьютер ее аппаратно поддерживает, не так-то просто: правка ключей загрузки в файле boot.ini - процедура, конечно, простая, но уж больно "в стиле Unix", а значит, далеко не каждый пользователь туда полезет (не могу удержаться и от подколки в адрес "интуитивно понятного интерфейса" Windows: в лучших традициях Microsoft настройки DEP находятся... в пункте Perfomance Options ("Параметры быстродействия"), доступном со вкладки Advanced ("Дополнительно") диалога System ("Система") из "Панели управления". Впрочем, до верха идиотизма - процесса настройки системы на прием входящих звонков (для установления прямого, так сказать, "нуль-провайдерского" модемного соединения) - эта особенность не дотягивает. Если кто не знает - делается подобная операция только из меню "Дополнительно" штатного "Проводника", причем появляется этот пункт меню только при заходе в папку "Сетевые подключения". Даже с инструкцией на руках я нашел его лишь с третьей попытки - просто не мог представить, что в абсолютно неизменном и никогда не используемом меню Explorer вдруг добавится еще один жизненно необходимый пункт).

Поскольку с эксплойтами к Windows XP SP2 пока не густо, мы испытывали защиту NX "в полевых условиях" на обычных файловых вирусах. Некоторые зловредные программы, в частности Virus.Win32.Jess.a, DEP тоже "хватает за руку" при попытке, например, внедрения своего кода в адресное пространство Internet Explorer. Так что если на вашем компьютере DEP забила тревогу для первого файла... второго... третьего... - есть серьезный повод обеспокоиться. Жаль только, что срабатывание аппаратной защиты по NX равносильно аппаратному прерыванию SEGFAULT, гарантированно убивающему породивший его процесс со стандартно-извиняющимся сообщением Microsoft .

К сожалению, такова особенность защиты, и изменить здесь что-либо невозможно. И поскольку терпеть подобного рода фатальные ошибки можно далеко не всегда, предусмотрена возможность выборочного отключения DEP для конкретных приложений и процессов. Конечно, порой это не слишком удобно, однако безопасность дороже. И хотя я так и не решился поставить SP2 на домашнюю систему (нет ни малейшего желания возиться и перенастраивать или переустанавливать массу привычных и часто использующихся профессиональных программ, в число которых, например, входят два IDE, довольно тесно интегрирующихся с ОС и ревниво относящихся к подобного рода изменениям), но будь у меня компьютер, в котором можно включить аппаратный DEP, я бы поступил иначе. Microsoft, правда, заявляет и некие программные элементы DEP, но ни я, ни специалисты "Лаборатории Касперского" так и не смогли выяснить, в чем это проявляется: эксплойты на подобной системе прекрасно работают (да и удивительно было бы, если б было иначе, - бит NX трудно чем-то заменить). Если захотите проверить, какая у вас поддержка DEP - аппаратная или программная, то после установки SP2 откройте "Свойства системы" - в нижнем правом углу должно быть написано о поддержке режима Physical Address Extension (PAE), поскольку NX является частью AMD64, а для функционирования последней необходимо включить именно этот режим.

Закрытие всех известных дыр и уязвимостей в сочетании с DEP оставляет приятное ощущение надежности. Все работает, проблем почти нет, и даже если неожиданно вылезет очередной JPEG-эксплойт или вирус проникнет со старой версией библиотеки, DEP почти наверняка остановит распространение вредоносных программ. Конечно, аппаратная защита от переполнения буфера - не панацея (есть немало способов обойти и ее, причем даже без участия пользователя), но от самых распространенных и опасных атак она все же защищает. Но что делать, если зараза все-таки пробралась в компьютер?

**Брандмауэр Windows XP SP2**

Зачастую интернет-черви заботятся только о своем выживании - и тогда пользователь лишится незначительной части дискового пространства (которое займут копии червя; Sasser, например, за три часа работы успел абсолютно непреднамеренно наплодить на нашей тестовой машине копий двадцать) и сетевого трафика (128 потоков того же Sasser'а непрерывно сканируют окружающее пространство в поисках жертв). Типичной является также ситуация, когда на машину жертвы "попутно" устанавливается троян, на адрес его автора уходит письмо со всеми паролями пользователя, на сайт какой-нибудь SCO начинается DDoS-атака, или же машина используется как почтовый релей для пересылки спама. Особенно это относится к троянским коням, для которых существуют прекрасные "конфигурационные утилиты", позволяющие собрать троянца по своему вкусу - персонально для чем-то не понравившегося юному "хакеру" пользователя.

Защита от подобных напастей - грамотно настроенный файрволл, который вдобавок выстроит еще одну линию обороны от вторжения в систему без активного участия пользователя. Microsoft во втором сервис-паке серьезно обновила встроенный в Windows XP брандмауэр; так, может быть, здесь можно обойтись и без сторонних решений?

К сожалению, полноценную защиту Microsoft так и не родила. Да, закрыты некоторые ошибки, позволявшие обходить брандмауэр. Но он до сих пор не позволяет вести контроль исходящих соединений, инициируемых уже установленными программами. И в "Лаборатории Касперского" это наглядно продемонстрировали: после засылки на компьютер жертвы того же "Соседа" на специально созданный для этих целей почтовый ящик тут же упало электронное сообщение с файлом паролей пользователя. Так что если действительно заботиться о собственной безопасности, нужно непременно обзавестись файрволлом стороннего производителя. Впрочем, от многих "лобовых" атак и от "прямолинейного" открытия портов троянцем на машине жертвы ("создание backdoor'ов") штатное микрософтовское средство все же спасает.

Правда, Крис Касперски убедительно показал (см. www.insidepro.com/kk/016/016r.shtml), что обойти такую "защиту" совсем не трудно, но спасибо и на том, что пользователю вообще хоть что-то дали. Тем паче и брандмауэры, отслеживающие исходящие соединения, тоже можно обмануть, замаскировавшись под вполне благопристойную программу.

В остальном - брандмауэр вполне прилично справляется с возложенными на него обязанностями: не виснет, не глючит, собственных уязвимостей не имеет и попытки открытия портов "на прослушивание" отслеживает. Скажем так: хуже от его включения уж точно не станет. Тем более что во многих отношениях это вполне приличный файрволл с развитыми настройками, которым опытный администратор найдет полезное применение. Кроме того, научиться работать с этим "средством защиты" сможет даже неопытный пользователь.

**"Шашечки" и общие выводы по безопасности SP2**

К "шашечкам", конечно же, следует отнести появление в Windows XP SP2 Центра безопасности. Это красивое и удобное новшество, а всплывающие подсказочки о неустановленном в системе антивирусе - неплохая забота о пользователе(Меня все эти всплывающие подсказки, откровенно говоря, достали. А как их отключить - я не нашел (правда, особо и не искал). Но реальной надежности или удобства в настройке Центр не добавляет: слишком уж легко его обмануть, сделав вид, что антивирус и сторонний брандмауэр в системе уже установлены.

Традиционного вывода о том, что в Microsoft, как обычно, поработали больше над формой, нежели над содержанием, на сей раз не будет. Надежность Windows XP SP2 действительно заслуживает всяческих похвал: за два месяца - ни одной критической уязвимости, ни одного работоспособного вируса! И дополнительная страховка в виде DEP на будущее. Жаль только, что в погоне за безопасностью серьезно пострадали обычные пользователи. Жаль и того, что в систему не встроили более или менее полноценного файрволла. Так что если не боитесь временных проблем, смело ставьте SP2, добавляйте любой нормальный брандмауэр и антивирус и радуйтесь полностью защищенной системе. А если боитесь - установите наиболее критичные заплатки на SP1, добавьте те же брандмауэр и антивирус и опять-таки радуйтесь защищенной системе. Главное, не забывайте вовремя читать информационные бюллетени Microsoft и антивирусных компаний. Наконец, если у вас неплохой опыт работы с компьютером, а вирусы из почтовых вложений, равно как и незнакомые программы, скачанные из файлообменных сетей, вы не запускаете, то можно воспользоваться и штатным файрволлом и даже, возможно, отказаться от антивируса. Но это - только при наличии полной уверенности в своих силах.