XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.X : С.113-115

УДК 378.33

Н.О.Заручникова (2 курс, каф. ТО), Т.А.Козелецкая, ст. преп.

ОСНОВНЫЕ ВИДЫ И ОСОБЕННОСТИ ВИРУСНЫХ ПРОГРАММ

Существует множество вредоносных программам. В дальнейшем под ними будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

В работе рассмотрены наиболее распространенные виды подобных программ, также последствия, которые они приносят.

К основным программам такого отнесятся: «троянский конь», вирус, «червь», «жадная» программа, «захватчик паролей»:

«Троянский конь» — программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Программы такого типа являются серьезной угрозой безопасности при автоматизированной системе обработке информации (АСОИ).

По характеру угрозы «троянский конь» относится к активным угрозам, реализуемым программными средствами, работающими в пакетном режиме. Наиболее опасным является опосредованное воздействие, когда он действует в рамках полномочий одного пользователя, но в интересах другого пользователя, установить личность которого порой невозможно.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в безвредную исходную программу, которая затем предлагается (дарится, продается, подменяется) пользователям АСОИ. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне). Запустивший такую программу подвергает опасности как себя и свой файлы, так и всю АСОИ в целом.

Характерным примером «Троянского коня» является появившийся в Интернете бесплатно распространяемый Screen Saver, который помимо вывода красивых картинок на экране, осуществляет поиск на компьютере программы-шифровальщика алгоритма DEC. В случае обнаружения программы, Screen Saver ставит под контроль обмен ключами шифрования и пересылает ключи по электронной почте на анонимный сервер.

«Червь» – программа, распространяющаяся через сеть и (в отличие от вируса) не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известный представитель этого класса – вирус Морриса (или, вернее, «червь Морриса»). Наиболее подходящей средой распространения «червя» является сеть, все пользователи которой доверяют друг другу. Отсутствие защитных механизмов как нельзя лучше способствует уязвимости сети.

Вирусы, такие как «троянский конь» и «червь» на сегодняшний день являются одной из самых опасных угроз АСОИ. Радикальным способом защиты от этой угрозы является создание замкнутой среды исполнения программ. В особенности важно разделение внешних сетей (особенно Интернет) и внутренних сетей, по крайней мере, на уровне протоколов, а еще лучше – на физическом уровне. Тогда вероятность внедрения программ подобного рода будет достаточно низкой.

Существуют ещё «жадные» программы – это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода. Многие компьютеры, особенно в исследовательских центрах, имеют фоновые программы, выполняющиеся с низким приоритетом. Они обычно производят большой объем вычислений, а результаты их работы требуются не так часто. Однако при повышении приоритета такая программа может блокировать все остальные. Такая программа и будет «жадной».

Тупиковая ситуация возникает, когда «жадная» программа бесконечна (например, исполняет заведомо бесконечный цикл). Однако во многих операционных системах существует возможность ограничения времени процессора, используемого задачей. Это не относится к операциям, выполняющимся в зависимости от других программ, например, к операциям ввода-вывода, которые завершаются асинхронно к основной программе; время их выполнения не включается в счет времени программы. Перехватывая асинхронное сообщение, о завершении операции ввода-вывода и посылая вновь запрос на новый ввод-вывод, можно добиться по-настоящему бесконечной программы. Такие атаки называют также асинхронными.

Другой пример «жадной» программы – программа, захватывающая слишком большую область оперативной памяти. В оперативной памяти последовательно размещаются данные, например подкачиваемые с внешнего носителя. В конце концов, память может оказаться во владении одной программы, и выполнение других окажется невозможным.

Обычно «жадные» программы осуществляют захват одного из трех основных ресурсов системы: времени процессора, оперативной памяти, каналов ввода-вывода. Однако возможен захват и любых других ресурсов системы: блокирование ее работы, или же использование побочного результата деятельности какой-либо программы (например, вируса). Бороться с захватом ресурсов можно путем введения различных ограничений для выполняемых программ (на время процессора, на количество операций ввода-вывода, на разрешенный объем оперативной памяти и т.д.), а также постоянным операторским наблюдением за их соблюдением.

Захватчики паролей. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, затем они пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом – с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе входа, а не какой-то другой. Кроме того, необходимо неукоснительно придерживаться правил использования паролей и работы с системой. Большинство нарушений происходят не из-за хитроумных атак, а из-за элементарной небрежности. Не рекомендуется покидать рабочее место, не выйдя из системы. Постоянно проверяйте сообщения о дате и времени последнего входа и количестве ошибочных входов. Эти простые действия помогут избежать захвата пароля.

Существуют так же и другие возможности компрометации пароля. Не следует записывать команды, содержащие пароль, в командные процедуры, надо избегать явного объявления пароля при запросе доступа по сети: эти ситуации можно отследить и захватить пароль. Не стоит использовать один и тот же пароль для доступа к разным узлам.