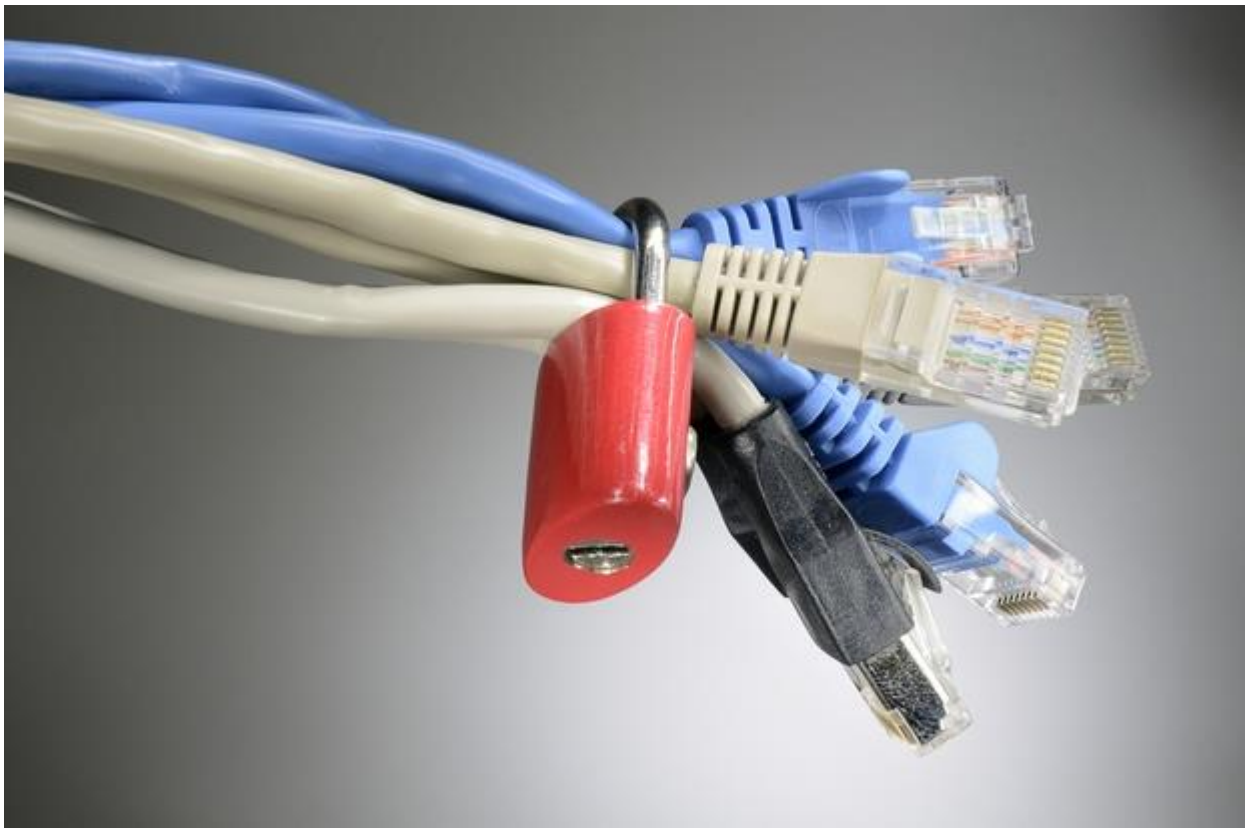
Взгляд под маску, или Как обойти защиту MS Windows

Евгений Родыгин | 20.12.2013



Иногда нам кажется, будто наша информационная система защищена. Иногда — что мудрые администраторы безопасности, разработчики антивирусов и других средств защиты принимают все необходимые меры. Иногда представляется, что мы все делаем правильно. Но это не так...
В один из осенних дней бухгалтер компании А включил АРМ с обновленной ОС Microsoft Windows 7, с установленным антивирусом и другими средствами защиты, проверил целостность файлов СЗИ и банковской программы (ДБО), сформировал платежное поручение на сто тысяч рублей на счет компании Б. Затем убедился, что платежное поручение составлено верно и ушло в банк, подписанное электронной подписью с выполнением всех требований безопасности. На стороне банка была проверена электронная подпись, и платеж был выполнен.

Спустя несколько дней проводилось внутреннее расследование. Основной вопрос состоял в том, почему в банк пришло подписанное поручение на сумму полтора миллиона рублей на никому не известный счет. Расследование показало, что файлы системы ДБО и СЗИ не изменялись, сторонние пользователи не входили в

систему, все средства защиты функционировали как положено. Все говорило о том, что неправильную операцию совершил бухгалтер. Но он этого не делал!
Возможно ли такое? К сожалению, да. Данный способ обхода механизмов защиты, в том числе встроенных в ОС Microsoft Windows подтвержден специалистами нашей компании в процессе анализа и реализации методов динамического контроля программного обеспечения. Особенность способа в том, что он использует уже заложенные в ОС Microsoft Windows механизмы для обхода механизмов защиты самой ОС Windows.

Жесткая подмена
Прежде чем мы раскроем механизм, примененный хакером, рассмотрим причины, которые позволили ему добиться своего. Дело в том, что платформа Microsoft Windows содержит огромные функциональные возможности. Их так много, что создатели средств защиты просто не успевают или не могут учесть их все. Именно такими, пропущенными механизмами ОС Microsoft Windows и могут воспользоваться злоумышленники.
Разработчики ОС Microsoft Windows уделяют серьезное внимание безопасности приложений. Реализовано множество механизмов, не допускающих получение одним прикладным приложением власти над другим. Сами приложения также ограничены в своих возможностях. Для изоляции программ друг от друга компания Microsoft внедрила массу специальных средств — это и защита страниц памяти, и протоколы взаимодействия между процессами, и предотвращение выполнения данных. Но вот мощные отладочные механизмы платформы Microsoft Windows остались без должного внимания.
Отладчиками пользуются разработчики для контроля отлаживаемой программы. При этом приложение «Отладчик» запускает или подключается к отлаживаемой программе и получает над ней полный контроль. Отладчик способен останавливать и продолжать выполнение кода, менять данные и код прямо в работающей программе. И все эти возможности легально и просто предоставляет непосредственно ОС Microsoft Windows. Некоторые функции отладки так же реализованы в центральном процессоре ЭВМ.
Теперь представьте, что хакер создает миниатюрный быстрый и эффективный отладчик-паразит, предназначенный лишь для контроля за приложением-жертвой. Паразит запускает программу-жертву в режиме отладки и полностью контролирует ее работу незаметно для нее самой и ее пользователя. ОС Microsoft Windows

и большинство СЗИ считают, что все в порядке — программист отлаживает код. Пользователь работает с программой-жертвой как обычно и ничего не подозревает. Файлы программы-жертвы не изменяются, контроль целостности проходит без замечаний. Только вот обладая такими возможностями, программа-паразит может подменять данные и код прямо в памяти программы-жертвы во время ее действия, соответственно изменять функционал программы-жертвы и много чего еще. Механизм работает и в последних версиях ОС Windows 8, 8.1.

В семействе ОС Microsoft Windows начиная еще с Windows XP SP2 используется технология Data Execution Prevention (DEP), которая позволяет процессору помечать определенные области памяти как «невыполняемые», а также ASLR.

Если программа-злоумышленник попытается модифицировать свой код в одной из областей памяти или код другого процесса, механизмы защиты ОС Microsoft Windows обнаруживают и предотвращают ее действия. Такие механизмы ОС Microsoft Windows заблаговременно предупреждают выполнение целого класса эксплоитов. Например, приложение получает с веб-страницы данные и в какой-то момент пытается их реализовать как код. DEP ОС Microsoft Windows не позволяет это сделать. Но если приложение работает под контролем программы-отладчика-паразита, то способно перенести данные в страницу кода и выполнить их в контексте приложения-жертвы.

В этой статье мы описали лишь один из возможных сценариев применения механизма, но их множество. Данные о методе реализации официально переданы в компанию Microsoft. Также просим считать нашу статью открытым обращением к антивирусным компаниям и разработчикам средств защиты информации для принятия необходимых мер. На сегодняшний день, по сведениям проекта virustotal.com, только 4 из 45 антивирусов уделяют внимание описанной проблеме.

Как же защитить себя от подобных сценариев? Прежде всего, мы подготовили для вас простую утилиту, которая покажет, актуальна ли в вашей системе описанная угроза. Скачать ее можно по адресу: http://www.wikisec.ru/test_win_01.rar (описание внутри, пароль к архиву: 12345).

Рекомендации по эксплуатации информационных систем:

1. Соблюдать бдительность. Наличие самых современных средств защиты не должно убаюкивать пользователей и службы безопасности.

2. Проводить периодическую инвентаризацию используемого программного обеспечения. Исключить приложения, не относящиеся к деятельности.
3. Применять жесткий контроль каналов, по которым программы могут попасть в АРМ пользователей и сервера.
4. Ни в коем случае не использовать нелицензионное и тем более пиратское (взломанное) программное обеспечение.
5. В случае если представленная утилита показывает наличие угрозы, необходимо для принятия мер обратиться к администратору по безопасности.
==========

Андрей Бешков, менеджер программ ИБ Microsoft в странах СНГ

Есть 10 непреложных законов безопасности (http://technet.microsoft.com/ru-ru/library/cc722487.aspx
По сути, действие описанного в статье образца вредоносного кода схоже с поведением руткитов и буткитов. И те и другие выполняются с высокими привилегиями по отношению к атакуемым процессам или порождают его, а затем скрывают от пользователя реальное положение вещей. Использование режима отладки всего лишь один из методов влияния одного процесса на другой. Начиная с Windows Vista появился еще один механизм — Windows Integrity, предназначенный для разграничения доступа между процессами, запущенными от имени одного пользователя (http://msdn.microsoft.com/en-us/library/bb625957.aspx
Поэтому мы считаем, что данная атака может сработать только в организациях, где не уделяется должного внимания политикам ИБ. Эту и множество других атак можно было бы предотвратить с помощью стандартных средств ОС. Нужно употреблять Software Restriction Policies (SRP) или Applocker для контроля за запускаемыми приложениями и предотвращения запуска, не подписанного сертификатами, или не доверенного кода.

Александр Гостев, главный антивирусный эксперт «Лаборатории Касперского»

В Windows одна программа может контролировать исполнение другой программы, если обе они выполняются под одной учетной записью (или контролирующая программа реализуется под учетной записью администратора). Да, security boundaries в Windows проходят не по границам процессов, а по границам учетных записей. Все разработчики security-продуктов отлично об этом осведомлены. Существуют две ключевые вещи, из-за которых «детектирование» работы в режиме отладчика нецелесообразно.

Во-первых, данный способ не имеет никаких преимуществ по чтению, записи, инжектам и т. д. перед прочими приемами. Нет проблемы с «отладкой», есть проблемы с инжектами как таковыми. И уж главной тут является собственно работа с правами администратора.

Во-вторых, запуск в этом режиме — нормальное явление, подобным методом пользуется множество легальных приложений, например различные протекторы. Реагировать на него при помощи антивирусного решения, особенно персонального продукта, крайне нецелесообразно — как из-за громадного количества ложных срабатываний, так и банального непонимания со стороны пользователя — а что ему с этим, собственно, делать (разрешить/запретить)?

Гарантированно на 100% изолировать какое-то важное приложение от зараженной ОС нельзя, но можно существенно затруднить некоторые действия вредоносных программ.