

Введение

Какие задачи и каким образом должны решать современные системы защиты от вредоносного кода (malware)? Попробуем проследить, каким образом malware проникает на компьютер жертвы и что там происходит потом.

Наиболее распространенные источники malware это:

- **Автозапуск со съемных носителей.** При присоединении к компьютеру съемных носителей (как привило flash-накопители) зловредный код запускается автоматически.
- **Уязвимости ПО.** Злоумышленник использует эксплойт, который загружает модули зловреда на компьютер-жертву, и закрепляет их присутствие в системе, регистрируя на автоматический запуск в ОС. Как правило, код эксплоита минимален, поскольку это связано с определенными трудностями его написания, и его задача, - выполнить базовые действия по закреплению malware в системе. В подавляющем большинстве случаев эксплойт скачивает модуль установки - т.н. dropper, который затем запускает.
- **Социальная инженерия.** Суть данного способа заключается в том, что путем обмана пользователю предлагается самостоятельно запустить некоторое приложение, например проигрыватель неизвестного формата файлов, самораспаковывающийся архив, и т.д. которое, вместо ожидаемых пользователем действий, выполняет установку malware.
- **Инфицирование программ.** В этом случае malware проникает в ОС и выполняется в составе работающего приложения, программ установки и т.п. Этот способ менее распространен, по сравнению с первыми тремя. Однако ущерб от вирусных эпидемий, возникших из инфицированных программ, может быть грандиозным, как это было при массовом распространении Virus.Win32.Virut.

После проникновения на компьютер жертвы наступает следующий этап, когда код **malware** загружается в оперативную память системы и **начинает выполняться**.

Антивирусы

Классические антивирусы контролируют выполнение вредоносного кода, сопоставляя его с имеющимися в базе данных (БД) сигнатурами. Это может быть полезным в лечении уже существующего заражения. Однако, такой подход абсолютно бессилён в противодействии неизвестным угрозам. Классический антивирусный продукт не может защитить пользователя от всего множества вредоносных программ.

HIPS

Подавляющее большинство HIPS систем допускают запуск и ограничивают взаимодействие вредоносного кода с ОС через интерфейс Windows API. При этом malware могут использовать весь диапазон огромного множества функций Windows API. HIPS системы, допускающие выполнение вредоносного кода в ОС, не контролируют весь объем возможных вредоносных действий malware через все имеющиеся в ней функции. Именно неконтролируемые системой защиты области функций интерфейса Windows API логично становятся «парадным входом» для атак злоумышленников. Это неэффективный подход к защите, так как результатом работы этих систем будет модификация ядра ОС, зависимость эффективности защиты от обновлений ОС, снижение ее стабильности, а ошибки программирования модулей, модифицирующих ядро, лишь добавляют возможность краха системы. Более того, система защиты сама по себе ведет к расширению привилегий malware и DOS атакам. К сожалению, существующие HIPS системы несовершенны. Массовый характер найденных ошибок обработки параметров перехваченных системных функций в различных продуктах (Kaspersky, Outpost, DefenceWall, etc) подтверждает это.

Safe'n'Sec 2009

Концепция Safe'n'Sec® V.I.P.O® - **предотвратить инсталляцию malware в операционной системе, как это будет в случае использования социальной инженерии, и запретить запуск malware несанкционированно**

проникнувшего в нее. Это полностью предотвращает выполнение вредоносного кода. Это иной подход к защите.

Технология создания профиля системы позволяет предотвратить выполнение несанкционированно проникнувших в ОС модулей неизвестного кода. А технология V.I.P.O.[®] создает изолированную среду для выполнения неизвестного кода, используя архитектурные возможности Windows линейки NT. Одним из требований к разработке операционных систем линейки NT было то, что они должны отвечать правительственным и промышленным требованиям к безопасности операционных систем. Уровень безопасности определяется по рейтингам безопасности, которые определены национальным центром компьютерной безопасности (National Computer Security Center, NCSC) министерства обороны США. Рейтинг безопасности, повлиявшим на архитектуру защиты Windows, является Trusted Computer System Evaluation Criteria, и соответствует уровню C2 - Controlled Access Protection. «Диалог» Malware и ОС уже невозможен. Нельзя получить доступ к важным данным, которые хранятся в профиле пользователя, устанавливать глобальные перехватчики и получать доступ к буферу обмена (защита от keyloggers). Невозможно изменять код и данные других процессов, несанкционированно модифицировать исполняемые файлы.

В отличие от других HIPS-систем технология Safe'n'Sec V.I.P.O.[®] контролирует весь спектр действий вредоносных программ, сохраняя первоначальную целостность ядра ОС, благодаря модификации маркера защиты процессов (ACCESS_TOKEN) и таблицам избирательного доступа (DACL). Также технология Safe'n'Sec V.I.P.O.[®] защищает от программного ввода (имитация нажатий клавиатуры/мышки), используя безопасное отображение уведомлений для пользователя.

Концепция Safe'n'Sec[®] предполагает работу потенциально уязвимого ПО (browsers, torrents, e-mail clients, etc) с применением налагаемых системой защиты ограничений. Это ПО идентифицируется системой защиты при запуске и выполняется в особой среде, - от имени ограниченного пользователя с наложением ограничений файловой и реестровой активности. Для предотвращения инсталляции нежелательного ПО через уязвимости это имеет немаловажное значение наряду с технологией создания профиля системы. На данный момент Safe'n'Sec идентифицирует и ограничивает права следующих программ:

- Microsoft[®] HTML Help
- BitTorrent
- uTorrent
- Opera Internet Browser
- Mozilla Firefox
- Internet Explorer
- Download Master
- Winamp
- AIMP2
- Windows Media Player
- The KMPlayer
- Light Alloy
- Microsoft Office Outlook
- Microsoft Office Word
- Microsoft Office Excel
- The Bat! E-Mail Client
- Miranda IM
- Quiet Internet Pager
- Skype
- Adobe Reader
- DjVuViewer

Пользователь может в любое время добавить в этот список используемую им программу, чтобы ограничить возможность эксплуатации уязвимостей в ней через интерфейс Safe'n'Sec.

Методология

При тестировании технологии Safe'n'Sec® V.I.P.O® необходимо учесть следующее:

1. Главной задачей Safe'n'Sec® V.I.P.O® является - **заблокировать выполнение любого ПО, его компонентов и модулей, которое инсталлировалось, или пытается инсталлироваться в систему без участия пользователя (администратора).**
2. Если пользователь самостоятельно запускает неизвестное ПО, степень доверия к которому он не может определить, система защиты должна по-умолчанию создать условия, при которых такое ПО не сможет:
 - инсталлироваться в систему (закрепиться в автозапуске, изменить программные модули других приложений и ОС);
 - получить доступ к важным данным пользователя (любая приватная информация, которая хранится в профиле (документах) пользователя, а также обозначенные пользователем файлы и папки);
 - изменять код и данные других процессов, изменять контексты потоков, создавать свои или завершать чужие потоки других процессов;
 - отслеживать клавиатурный ввод, используя глобальные перехватчики, или используя ring-0 модули (драйвера), т.е. защитить от keylogger's;
 - читать и изменять данные из буфера обмена Windows;
 - лишить приложение всех привилегий и прав доступа администратора системы.

Несмотря на вышеперечисленные ограничения, в таком режиме может успешно работать большинство программ пользователя, таких как плееры аудио/видео; просмотрщики картинок и прочий софт, часто используемый в качестве "приманки" в социальной инженерии. Следует отменить особенности работы Safe'n'Sec® V.I.P.O® с программами установки. В состав продукта входит интеллектуальный анализатор, способный обнаруживать инсталляционные пакеты и запускать их в особом режиме – режиме установки. Если инсталляционный пакет ПО имеет цифровую подпись доверенного издателя, его установка происходит прозрачно для пользователя, после чего ПО начинает работать в составе ОС, не беспокоя пользователя вопросами о подозрительной активности, что характерно классическим HIPS-системам. Если инсталляционный пакет не имеет цифровой подписи доверенного издателя, или же такая подпись повреждена, по-умолчанию пользователю будет предложено запуск программы установки в изолированной среде, или запретить запуск совсем. Как дополнительное средство проверки на наличие известных угроз можно применить классический сигнатурный сканер (осуществить проверку прямо при отображении алерта на запуск), но, это не может гарантировать абсолютную безопасность проверяемого объекта. В случае запуска такого ПО в режиме по-умолчанию, пользователь может наблюдать активность приложения, однако возможность нанесения вреда его системе и важным данным сводится к минимуму. В интерфейсе существует возможность включить ведение истории активности таких приложений, что позволит определить степень доверия при первом запуске и осуществить установку этого ПО, или заблокировать его запуск в дальнейшем.

Для проверки работы Safe'n'Sec® V.I.P.O® в действии необходимо:

1. Установить тестируемую ОС, установить необходимое пользователю ПО и систему защиты Safe'n'Sec® V.I.P.O®. Поскольку **система предотвращения вторжений не ставит своей целью лечить уже существующее заражение системы**, предполагается установка системы защиты на свободную от зловредного кода ОС. В связи с тем, что в реальной практике пользователь может устанавливать наш продукт на инфицированную систему, мы применяем классический сигнатурный сканер на этапе создания профиля системы. Однако очень важно понимать, что при этом **мы не гарантируем абсолютное излечение компьютера от malware, поскольку это задача классического антивируса, а не системы предотвращения вторжений.**
2. Используя уязвимости ПО и предполагаемые недостатки работы Safe'n'Sec® V.I.P.O®, протестировать наличие/отсутствие возможности несанкционированной пользователем успешной инсталляции и закрепления зловредного кода на тестируемой системе. Для этого можно имитировать обычную работу пользователя за ПК – посещение ссылок и открытие страниц в Интернете, скачивание

файлов, и прочая активность через глобальную сеть; подключать к тестируемой системе инфицированные съемные носители и т.д.

3. Проверить в действии работу технологии V.I.P.O.[®] - запуск неизвестного приложения в изолированной среде. Для этого можно запускать существующие malware (внесенные после установки Safe'n'Sec[®] V.I.P.O.[®]) на тестируемой системе, и разрешать их запуск в режиме по-умолчанию (т.е. кнопка "разрешить" в окне уведомления). Проверить наличие/отсутствие возможности для:

- инсталляции в систему (закрепиться в автозапуске, изменить программные модули других приложений и ОС);
- кражи важных данных, которые хранятся в профиле пользователя, а также обозначенные пользователем файлы и папки;
- изменения кода и данных других процессов, изменение контекстов потоков, создавать свои или завершать чужие потоки других процессов;
- отслеживать клавиатурный ввод, используя глобальные перехватчики, или используя свои ring-0 модули (keylogging);
- чтения и изменения данных из буфера обмена Windows;
- получение привилегий и прав доступа администратора системы.