Safe'n'Sec 2009: проактивный подход к безопасности

1 апреля, 2009 - 07:30 — Александр Шабанов

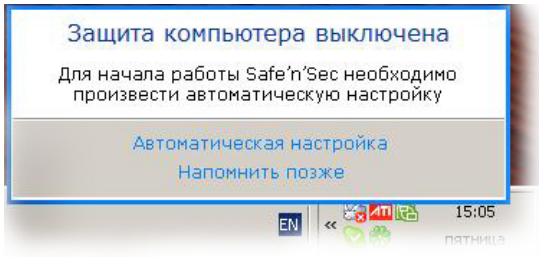
Теги: Домашние пользователи S.N.Safe&Software Safe'n'Sec 2009 HIPS Антивирус

На текущий момент стало совершенно очевидно, что классический сигнатурный подход к персональной защите от вредоносных программ уже не столь эффективен в силу появления тысяч новых вредоносных экземпляров каждые сутки. Наступил этап проактивных технологий, каждый производитель антивирусных систем реализуют их по-разному, предлагая то или иное решение. Недавно мне в руки попал продукт, который делает ставку именно на проактивные технологии и контроль активности - **Safe'n'Sec 2009**.

Смотрите видео ролик!

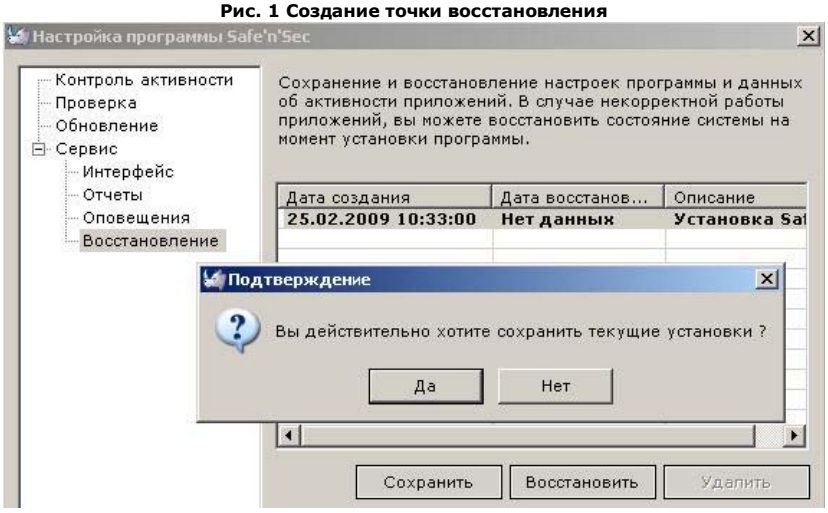
Решение основано на собственной технологии **V.I.P.O. (Valid Inside Permitted Operations)**, которая представляет собой систему предотвращения вторжений (HIPS). Данная технология позволяет контролировать любое изменение целостности компонентов ОС на основе хеш-сумм, а запуск и работа неизвестного приложения, не включенного в БД возможно, только при условии, что такой запуск инициировал сам пользователь. Только пользователь может принять решение о включении нового приложения в качестве компонента его системы, не смогут выполниться и модифицированные компоненты системы, их загрузка будет предотвращена, и пользователь получит информационное сообщение об этом.

После установки Safe'N'Sec 2009 любезно предлагает провести автоматическую настройку, то есть проанализировать текущее состояние операционной системы и создать базу данных процессов и приложений. Процесс этот оказался довольно длительным и занял около получаса на моей рабочей станции, поэтому рекомендуется устанавливать подобного рода системы на «чистую» операционную систему сразу.

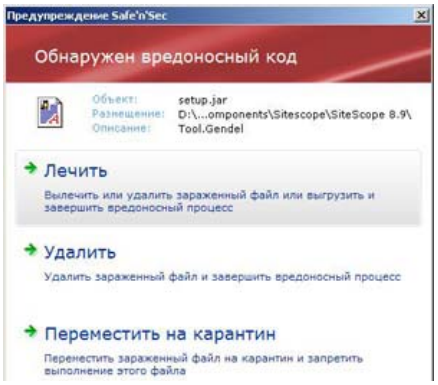


Разработчики Safe'N'Sec позаботились о том, что если что-то пойдет не так и включили функцию резервирования (бекап), путем создания точек восстановления вручную или автоматически (см. рисунок 1).

Рис. 1 Создание точки восстановления



При самостоятельном запуске приложений пользователем появляется уведомление, и дальнейшие действия будут зависеть от решения самого пользователя, а именно следующими путями:



1. **Проверить объект и запустить**. Приложение запускается и может загружать дополнительные модули, не прошедшие контроль целостности по БД. Даже если такое приложение является вредоносным, то оно сможет выполняться только до следующей перезагрузки ОС, поскольку его модули не включены в базу данных.

2. **Запрет запуска приложения.** В этом случае запуск приложения прекращается.

3. **Установка нового приложения**. В этом случае система защиты включает в БД все

новые компоненты устанавливаемого приложения. Загрузка приложения и его компонентов в дальнейшем будет разрешена.

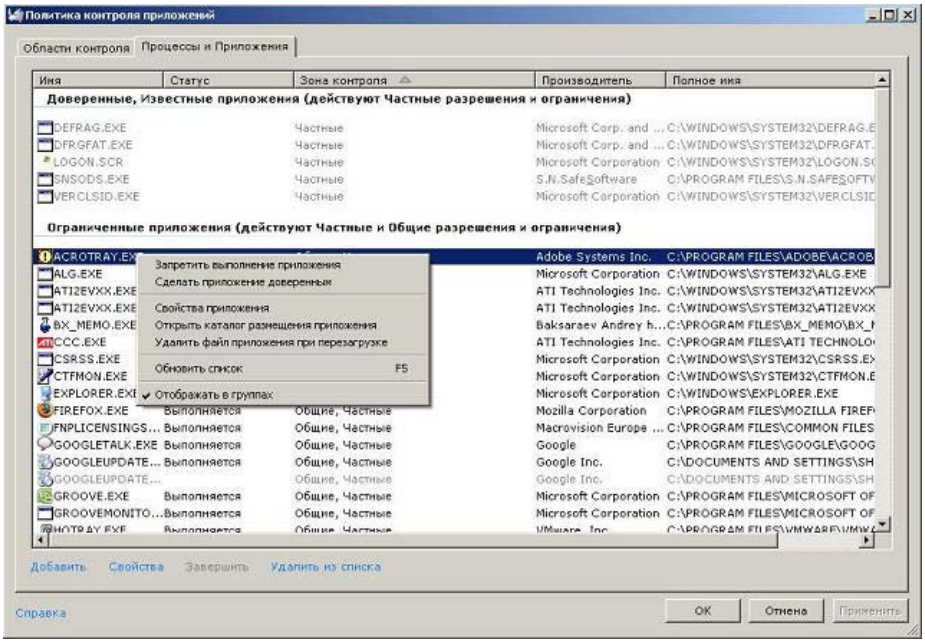
Также существует **«Особый режим»** или режим «слежения загрузки модулей», необходимость которого обуславливается особенностями работу, поскольку при формировании базы данных в нее включаются только одиночные модули, находящиеся на жестком диске, то в нее не попадут модули приложений, которые хранятся в ресурсах, архивах и т.п. Чтобы не нарушить работу таких приложений система защиты должна предоставлять возможность запуска таких приложений в особом режиме.

«Особый режим» необходимо применить один раз для того, чтобы при запуске проблемного приложения включить в базу данных модули, которые будут извлекаться из ресурсов, архивов и т.д. Последующие запуски могут проходить в нормальном режиме без дополнительных действий со стороны пользователя. «Особый режим» выбирается в контекстном меню при клике на проблемном приложении.

В Safe'N'Sec 2009 реализованы механизмы проверки системы по требованию (включая анти-руткит модуль), а также автоматическое обновление, при условии, что пользователь подключен к сети. Итак, перейдем к самому интересному - политикам контроля процессов и приложений.

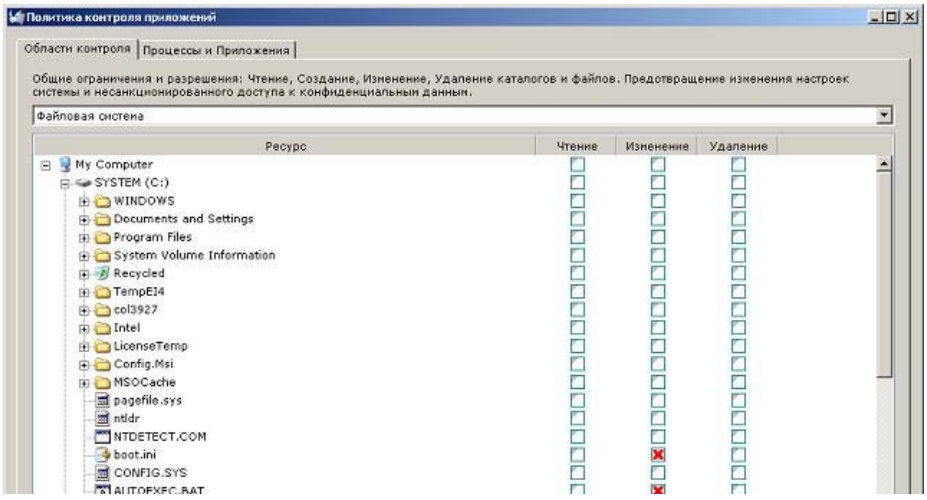
Все приложения делятся на два типа доверенные (известные) и ограниченные (см. рисунок 2). Доверенные выполняются без уведомления пользователя в свободном режиме, а при выполнение ограниченных приложений запрашивается действие пользователя.

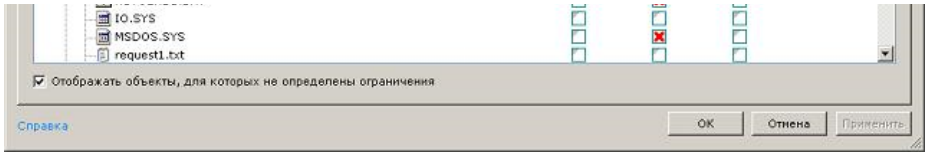
Рис. 2 Процессы и приложения



Каждому процессу в Safe'N'Sec 2009 можно назначить свою политику контроля, состоящую правил на доступ к файловой системе, системному реестру, сети, привилегиям процессов, а также доступу к USB устройствам (см. рисунок 3). В системе организовано два уровня правил: общие и частные. Общие правила распространяются на все приложения и процессы, включая доверенные, а частные правила можно задать дополнительно для каждого приложения отдельно.

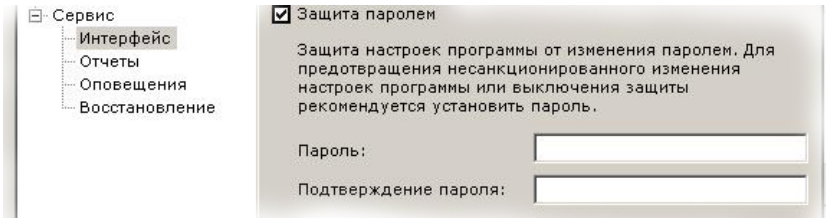
Рис. 3 Назначение общих правил для приложений





Используя возможность ограничивать приложения в доступе к конкретным файлам и USB устройствам в Safe'N'Sec 2009 можно легко организовать защиту своих конфиденциальных данных, дополнительно установив парольную защиту к интерфейсу системы (см. рисунок 4).

Рис. 4 Установка парольной защиты на графический инферфейс



По традиции снял небольшой ролик, который демонстрирует интерфейс и возможную конфигурацию продукта, а также пример реальной работы (в конце ролика демонстрируется запрет на открытие текстового файла Блокнотом):

На мой взгляд, использование систем предотвращения вторжений (HIPS), такой как Safe'N'Sec 2009 (или иных, например DefenseWall HIPS, см. сравнение антивирусов по эффективности защиты от новейших программ), является достойной альтернативой классических антивирусных систем, особенно для опытных пользователей. В завершении хотелось бы сказать, что данный продукт также существует в виде бандлов со встроенным сканером **VBA 32 ("ВирусБлокАда"**) или **Dr.Web ("Доктор Веб")**. Свои комментарии и впечатлеления можно оставить на нашем форуме, где также возможно получить обратную связь от разработчиков продукта. Самому попробовать покрутить продукт можно здесь .

Средняя оценка: 4.4 (голосов: 17)