Визитка

ЭЛЬТАБАРАНЕ МАХМУД АХМЕД,
инженер по техническому сопровождению продаж «Доктор Веб»

Dr.Web Katana Business Edition

Развертывание в корпоративной среде без Active Directory

Когда-то два антивируса на одном компьютере устраивали настоящие войны, не щадя в процессе борьбы ни себя, ни окружающих. Сейчас идея использования двух защитных решений на одной машине уже не вызывает былого шока

Тем более что двойная защита – это дополнительные шансы перехватить вредоносную программу до проникновения через защищенный периметр. А возможность просканировать попавший под подозрение компьютер или сразу всю сеть другим антивирусным движком помогает «лечить» особенно «запущенные» случаи, так что одних только пользователей бесплатной утилиты Dr.Web CureIT! у нас в каждом месяце по несколько миллионов – хотя для корпоративной сети лучше подходит CureNET!.

Конечно, чтобы не вызывать конфликты, второй антивирус должен быть создан особым образом и тщательно протестирован на отсутствие проблем во взаимодействии. Dr.Web Katana достигает этого за счет использования исключительно превентивных технологий, то есть это несигнатурный антивирус, заточенный на обнаружение новейших угроз, например тех же шифровальщиков, которые постоянно модернизируются, перепаковываются или создаются заново на языках вроде Go или вообще встроенном языке программирования 1С, а значит, представляющих серьезную опасность для сигнатурного подхода.

В этом году мы уже писали [1] о том, как развернуть Dr.Web Katana в корпоративной среде на примере использования для этого Active Directory. С тех пор вышла еще более удобная для массовой установки и настройки версия – Dr.Web Katana Business Edition, доработанная специально под массовое корпоративное использование. По большому счету она ставится сама, но для установки продукта на станции необходимо их соответствующим образом подготовить. Например, должны одновременно выполняться следующие пункты:

- ограничения системы контроля учетных записей (UAC) должны быть отключены, если станция работает под управлением Windows Vista или более поздней операционной системы. Если вы работаете под встроенной учетной записью администратора, то данную настройку проводить не нужно. Перейдите к следующему пункту;
- все необходимые для работы сети службы должны быть установлены и настроены;
- параметры общего доступа должны допускать расширенную настройку;
- для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности.

В целом все требования доступны в руководстве администратора (https://download.drweb.ru/doc) и не представляют собой что-то особенное, если Active Directory есть, то задача решается практически моментально.

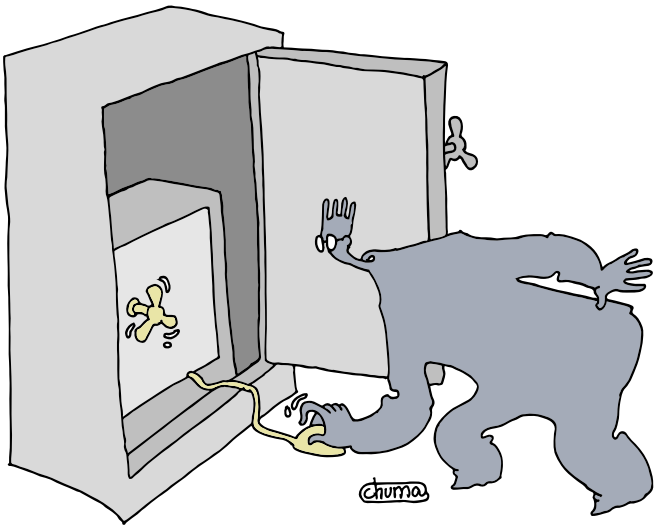
Но что делать, если его нет? Даже десять компьютеров, которые нужно обойти и настроить вручную, могут занять у системного администратора целый день – чего, разумеется, не хотелось бы. Специально для таких случаев мы разработали утилиту для настройки серверов и рабочих станций – для корректной работы Dr.Web CureNet! и Dr.Web KATANA Business Edition. По сути, это просто операции в командной строке, и сделать ее, в теории, мог бы любой системный администратор. Но зачем изобретать велосипед? Тем более несколько раз.

Так, например, выглядит в утилите код получения привилегий:

```
:checkPrivileges
NET FILE 1>NUL 2>NUL
if '%errorlevel%' == '0' ( goto gotPrivileges ) ↵
         else ( goto getPrivileges )

:getPrivileges
if '%1'=='ELEV' (echo ELEV & shift /1 & goto gotPrivileges)
ECHO.
ECHO **************************************
ECHO Invoking UAC for Privilege Escalation
ECHO **************************************

ECHO Set UAC = CreateObject^("Shell.Application"^) > ↵
         "%vbsGetPrivileges%"
ECHO args = "ELEV " >> "%vbsGetPrivileges%"
ECHO For Each strArg in WScript.Arguments >> ↵
         "%vbsGetPrivileges%"
ECHO args = args ^& strArg ^& " "  >> "%vbsGetPrivileges%"
ECHO Next >> "%vbsGetPrivileges%"
ECHO UAC.ShellExecute "!batchPath!", args, "", ↵
         "runas", 1 >> "%vbsGetPrivileges%"
```



Dr.Web Katana Business Edition — удобная для массовой установки и настройки версия, специально под корпоративное использование

```
"%SystemRoot%\System32\WScript.exe" "%vbsGetPrivileges%" %*
exit /B

:gotPrivileges
setlocal & pushd .
cd /d %~dp0
if '%1'=='ELEV' (del "%vbsGetPrivileges%" ↵
        1>nul 2>nul  &  shift /1)
cls
```

Иными словами, ничего сверхъестественного, просто удобный инструмент.

Использовать утилиту можно как в интерактивном, так и в фоновом режиме, а также в конфигурационном, который разумно запускать в первую очередь.

Конфигурационный режим позволяет провести быструю настройку системы для оптимальной работы с продуктами Dr.Web без создания аккаунта DrWebAdmin, а для запуска утилиты в конфигурационном режиме просто дважды щелкните по значку DrWebSysMod.exe, и программа автоматически проведет настройку системы.

Что дальше?

Запуск в фоновом режиме производится элементарно. Он позволяет программе выполнять действия интерактивного режима без участия пользователя. Для работы утилиты в фоновом режиме откройте консоль Windows (cmd), укажите путь к .exe-файлу утилиты и запустите ее командой -s или -S (например, C:\DrWebSysMod.exe -s). Программа начнет работу автоматически без каких-либо команд пользователя.

Интерактивный режим потребует немного больше внимания. По пунктам:

1. Откройте консоль Windows (cmd), укажите путь к exe-файлу утилиты и запустите ее командой -a или -A (например, C:\DrWebSysMod.exe -a).
2. В открывшейся консоли нажмите любую кнопку для начала работы утилиты.
3. Программа начнет поиск Файла Конфигурации. При его наличии программа автоматически возьмет пароль из файлов *.pwd и *.key (пользовательская ОС) или *SRV.pwd и *SRV.key (серверная ОС). При отсутствии Файла Конфигурации утилита предложит ввести пароль вручную.
4. Утилита проверит тип используемой ОС для создания точки восстановления.
   Если ОС является серверной: серверные ОС не поддерживают точки восстановления, пожалуйста, создайте резервную копию системы.
   Если ОС является пользовательской: утилита попытается создать точку восстановления системы. Если функция создания точек восстановления отключена или при создании точки восстановления произошла ошибка, на экран будет выведено соответствующее сообщение.
5. В случае первого запуска утилиты пользователю необходимо создать аккаунт DrWebAdmin, дважды введя новый пароль в строку ввода. Пароль должен состоять из символов {a-z, A-Z и 0-9} и из восьми и более символов. В случае повторных использований утилиты ввод пароля не требуется.
6. Программа проведет проверку системы. В случае успешного завершения проверки утилита сообщает пользователю о готовности машины для работы с продуктами Dr.Web. В случае ошибки на экран выводится соответствующее сообщение с номером ошибки (см. ниже).
7. Нажмите любую кнопку для выхода из программы.

Разумеется, есть проверка на ошибки, куда уж без них, приведу основные:

- **Ошибка 1:** точка восстановления не была создана. Служба может быть отключена или не установлена – недостаточно ресурсов.
- **Ошибка 11:** обнаружена серверная ОС Windows, точка восстановления не может быть создана. Windows Server не поддерживает создание точек восстановления, убедитесь в наличии резервной копии.
- **Ошибка 2:** во время получения пароля из зашифрованных файлов {*.PWD, *.KEY, *SRV.PWD, *SRV.KEY}

drwebconfig.cfg должен находиться в одной директории с утилитой.

> **Ошибка 3:** введенные вами пароли не соответствуют друг другу. Убедитесь, что вы ввели верный пароль дважды. Пароль должен состоять из символов {a-z, A-Z и 0-9} и из восьми и более символов.

Использовать утилиту можно как в интерактивном, так и в фоновом режиме, а также в конфигурационном

> **Ошибка 4:** создание аккаунта DrWebAdmin невозможно. Проверьте Журнал событий системы, права доступа пользователей, настройки GPO (групповая политика).
> **Ошибка 5:** пароль недостаточно сложный. Пароль должен включать в себя символы {a-z, A-Z и 0-9} и состоять из восьми и более символов.
> **Ошибка 6:** служба восстановления системы отключена. Запустите службу восстановления системы.
> **Ошибка 7:** поле «Пароль» не может быть пустым.
> **Ошибка 8:** местонахождение файла утилиты доступно только для чтения, измените права для данного каталога.

Журнал событий находится в (%appdata%\Dr.Web Config Tool\log.txt).

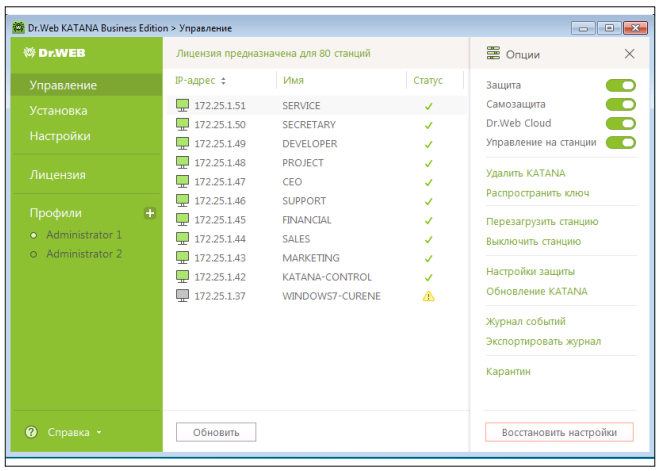
А теперь самое интересное. Как же это работает? Разберем по шагам.

Шаг 1. Запуск консоли управления утилиты.

Шаг 2. Поиск Файла Конфигурации:

> в случае использования версии для рабочих станций пароль будет взят из файлов *.pwd и *.key;
> в случае использования серверной версии пароль будет взят из файлов *SRV.pwd и *SRV.key;
> при отсутствии Файла Конфигурации утилита предложит ввести пароль вручную.

Рисунок 1. Консоль Dr.Web Katana Business Edition



Шаг 3. Проверка типа операционной системы Windows (пользовательская или серверная) для создания точки восстановления.

Если ОС является серверной:

> внимание: серверные ОС не поддерживают точки восстановления, пожалуйста, создайте резервную копию системы.

Если ОС является пользовательской:

> утилита попытается создать точку восстановления системы. При положительном результате, а также в случае, если функция создания точек восстановления отключена или при создании точки восстановления произошла ошибка, на экран будет выведено соответствующее сообщение.

Шаг 4. Проверка наличия Файла Конфигурации и пароля для перехода к следующему шагу.

Шаг 5. Проверка наличия аккаунта DrWebAdmin, в случае положительного результата программа готова для работы по Action-командам.

Если аккаунт DrWebAdmin еще не создан, необходимо создать аккаунт и добавить его в администраторскую группу, после чего утилита готова для работы по Action-командам.

Шаг 6. Проверка наличия аккаунта, точки восстановления системы, журнала событий и папки размещения. При положительном результате утилита продолжит работу по Action-командам.

Action-команды:

> отключение UAC (контроль учетных записей пользователей);
> установка сетевых служб («IPV4 → IPV6 → Клиент Microsoft Network → Общий доступ к файлам и принтерам»);
> изменение настроек общего доступа («Добавление исключений брандмауэра → Запуск общего доступа к файлам → Активация обнаружения сетевых ресурсов»);
> изменение настроек модели совместного доступа и безопасности (на Обычная – локальные пользователи удостоверяются как они сами)
> активация Admin$ Share для пользовательской ОС – проверка Admin$ Share для серверной ОС и активация в случае необходимости.

Шаг 7. Команды Action завершены, пользователю показывается сообщение, говорящее о готовности машины для работы с продуктами Dr.Web.

Пароль и ключ, кстати, шифруются.

Саму утилиту можно скачать по адресу: http://people.drweb.com/people/techtools/private/DrWebCT.exe

Ну а дальше все совсем просто, да еще и с графическим интерфейсом (см. рис. 1).

Все, ваша сеть теперь во всеоружии против вторжений. EOF

[1] Абраменко В. Развертывание Dr.Web Katana в корпоративной среде. //«Системный администратор», №7-8, 2016 г. – С. 52-56 (http://samag.ru/archive/article/3238).