Визитка

*ВЛАДИМИР АБРАМЕНКО,*
*инженер по техническому сопровождению продаж «Доктор Веб»*

# Развертывание Dr.Web Katana
## в корпоративной среде

Защиты много не бывает. Тем более сейчас, когда проникновение вредоносных программ в защищенный периметр, к сожалению, повседневность. Основная причина — компании ошибочно полагают, что используемый ими антивирус должен перехватывать до момента проникновения в локальную сеть все вредоносные программы

В результате, если неизвестная антивирусу вредоносная программа проходит проверку антивирусом, то препятствий к ее запуску пользователем не остается, так как в подавляющем большинстве случаев пользователи работают с правами администратора и у них отсутствуют ограничения на запуск и установку новых приложений. Вариантов построения надежной системы безопасности много, в данной статье мы рассмотрим вариант с установкой двух антивирусов, но в несколько нетрадиционном варианте.

Традиционно два антивируса устанавливаются так, чтобы разнести их по структуре локальной сети. Например, на рабочих станциях устанавливается один, на почтовых серверах и шлюзах – другой, на файловых серверах – третий. Причина понятна – возможная несовместимость двух антивирусных решений при использовании на одном компьютере и двойной расход ресурсов защищаемого устройства.

Есть и минус – если неизвестная вредоносная программа прошла поверки обоих решений, то в дальнейшем обнаружить ее может только одно решение – второму вредоносная программа скорее всего будет недоступна.

К счастью, выход есть всегда. Компания «Доктор Веб» представила несигнатурный антивирус Dr.Web Katana. Решение до момента его релиза было протестировано на совместимость с антивирусами TrendMicro, Symantec, Kaspersky Lab, Mcaffee, ESET, Webroot и может работать одновременно с ними. Развертыванием этого решения мы и займемся.

Непосредственно установка Dr.Web Katana на локальной машине практически не отличается от знакомой многим процедуры установки Dr.Web Security Space или Dr.Web Antivirus, поэтому мы рассмотрим более интересный вариант – развертывание Dr.Web Katana средствами Active Directory Group Policy Object.

Рисунок 1. Добавляем группы Everyone и Domain Computers в перечень пользователей с доступом только на чтение

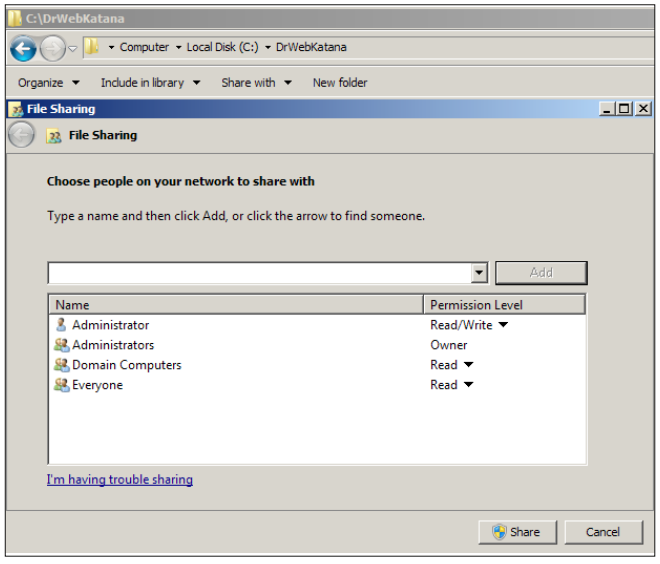
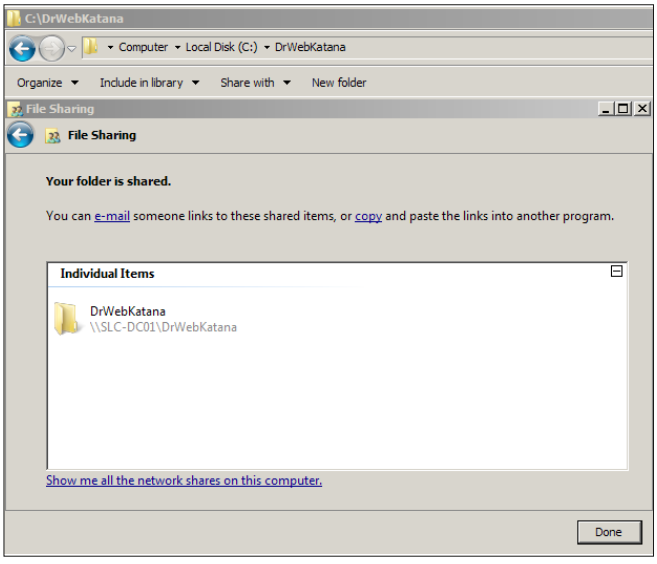



Рисунок 2. Проверяем наличие доступа пользователей к сетевой папке



В качестве первого шага создаем общую сетевую папку, в которой будет расположен MSI-пакет, необходимый для развертывания по сети, с доступом только на чтение и добавляем группы Everyone и Domain Computers в перечень пользователей, которым доступна данная папка (см. рис. 1). Предположим, что сетевой путь к папке будет \\SLC-DC01\DrWebKatana.

Проверяем наличие доступа пользователей к сетевой папке (см. рис. 2).

Извлекаем необходимые для развертывания файлы в сетевую папку. Для этого мы с вами запускаем командную строку (выполняем команду CMD с правами администратора) и выполняем команду, приведенную ниже, указав путь, где находится полученный MSI-файл инсталлятора Dr.Web Katana:

```
msiexec /a C:\drweb-katana-1-201604140-activedirectory.msi ↵
        /qn TARGETDIR=\\SLC-DC01\DrWebKatana
```

здесь:

- **ключ /qn** – параметр отключения графического режима при установке;
- **ключ /a** – запускает развертывание административного пакета;
- **drweb-katana-1-201604140-activedirectory.msi** – название MSI-пакета;
- **TARGETDIR** – созданная сетевая папка.

После выполнения команды необходимые файлы будут помещены на общий сетевой ресурс, указанный в TARGETDIR.

То же действие можно осуществить также и в графическом режиме, выполняем команду:

```
msiexec /a C:\drweb-katana-1-201604140-activedirectory.msi
```

Нажатие клавиши запускает Dr.Web Katana Installer. Нажимаем Next («Далее») (см. рис. 3)

Указываем полный сетевой путь к общей папке, которую создали ранее.

**Внимание!** Обязательно указываем сетевой путь в формате сетевого адреса, даже если папка доступна локально (см. рис. 4).

**Внимание!** До момента выполнения указанной выше команды убедитесь, что созданная сетевая папка пуста – не содержит никаких файлов.

Нажимаем Next («Далее»), и инсталлятор приступает к распаковке необходимых для развертывания файлов на общий сетевой ресурс.

После завершения процесса проверяем общую папку – она должна содержать один MSI-пакет и подпапку Program Files (см. рис. 5). Полученный MSI-пакет мы будем использовать при создании политики AD GPO (Active Directory Group Policy Object.).

Переходим к созданию Group Policy Object.

Рисунок 3. Первый шаг при установке Dr.Web Katana


Рисунок 4. Выбор папки при установке Dr.Web Katana

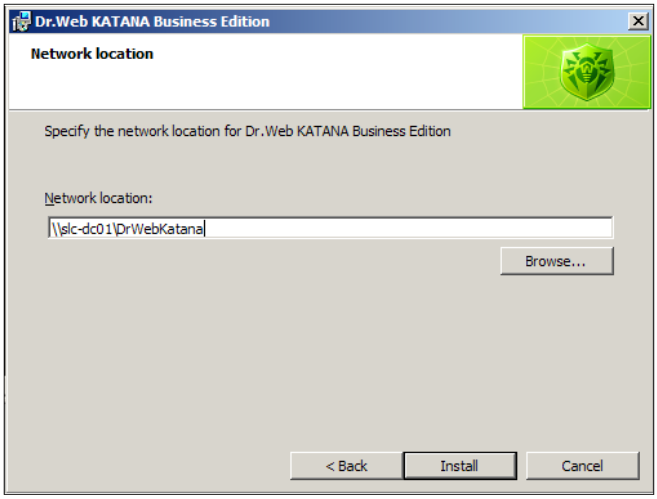



Рисунок 5. Проверяем общую папку – она должна содержать один MSI-пакет и подпапку Program Files

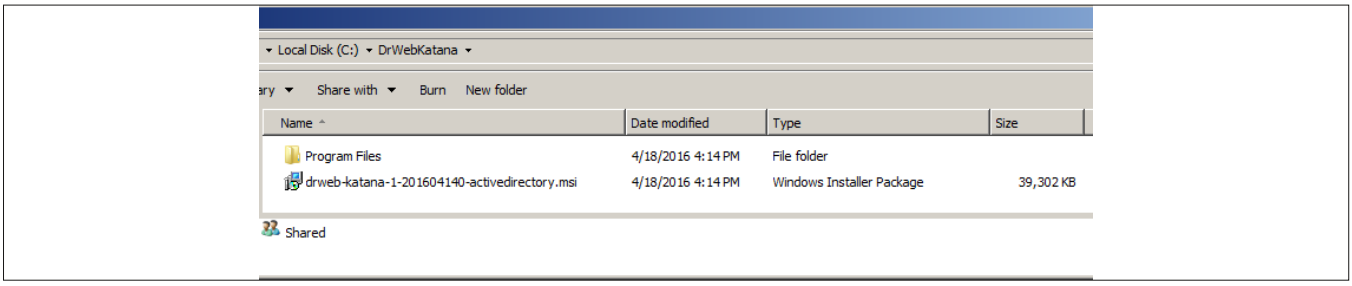


Рисунок 6. Для созданного подразделения (OU) задаем групповую политику

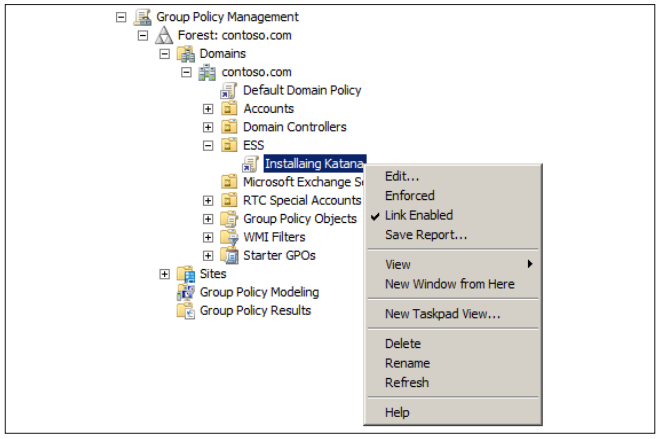



Рисунок 7. В Group Policy management создаем новый пакет

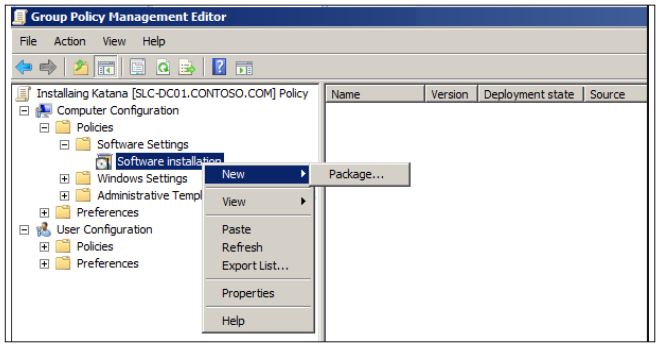



Рисунок 8. Выбираем метод размещения пакета

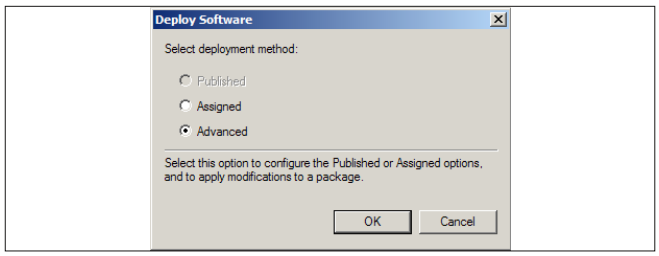
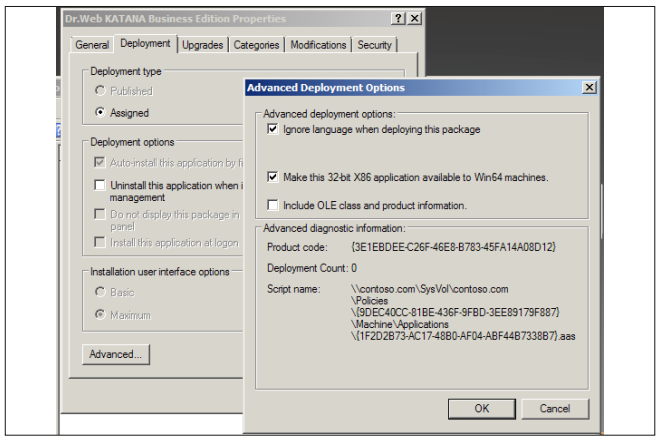



Рисунок 9. Установка дополнительного флага




Запускаем консоль «Active Directory → Пользователи и компьютеры» и создаем новое «Подразделение (OU)» – для нашего примера выберем название ESS. Выбираем «Создать → Подразделение», в открывшемся окне вводим название нового подразделения и нажимаем OK. Включаем в созданное подразделение компьютеры, на которые предполагается устанавливать Dr.Web Katana.

Для созданного подразделения (OU) задаем групповую политику. Для этого запускаем консоль «Редактора управления политиками» (Group Policy Management) («Пуск → Администрирование → Управление групповой политикой»), в контекстном меню созданного подразделения (OU) выбираем пункт «Создать объект GPO» в этом домене и отмечаем пункт Link Enabled (см. рис. 6).

В открывшемся окне задаем название нового объекта групповой политики и нажимаем OK. В контекстном меню новой групповой политики выбираем пункт «Изменить».

В открывшемся окне Group Policy management выбираем элемент «Конфигурация компьютера → Политики → Конфигурация программ → Установка программ», и нажав правую кнопку мыши, выбираем «Создать → Пакет» (см. рис. 7).

Указываем сетевой путь к общей папке (в нашем примере это \\SLC-DC01\DrWebKatana) и находящийся там MSI-пакет. Нажимаем Open («Открыть»). В открывшемся окне выбираем Advanced (см. рис. 8).

Открываем вкладку «Развертывание → Дополнительно» и устанавливаем флаг «Не использовать языковые установки при развертывании» (см. рис. 9).

Дважды нажимаем OK. Установка Dr.Web Katana будет произведена на ПК, которые были добавлены в созданное подразделение (OU), при следующей регистрации машины в домене.

Для того, чтобы проверить корректность выполненной работы запустите CMD на машине, где планируется установка Dr.Web Katana, и выполните команду:

```
gpupdate /force /boot /logoff
```

После применения политики ПК будет перезагружен, во время загрузки вы можете увидеть следующее сообщение (см. рис. 10).

Для того чтобы активировать установленные на компьютерах сети приложения Dr.Web Katana, создаем скрипт PowerShell.

Создаем файл (в данном примере выберем имя файла Key.PS1) со следующим содержимым:

```
# Start-Transcript -Path "C:\Windows\Temp\startup.log"
# to activate logging for windows 10
# making sure script is running on AsADMIN

If (-NOT ([Security.Principal.WindowsPrincipal] ↵
    [Security.Principal.WindowsIdentity]::GetCurrent()). ↵
    IsInRole([Security.Principal.WindowsBuiltInRole] ↵
    "Administrator")){
$arguments = "& '" + $myinvocation.mycommand.definition + "'"
Start-Process "$psHome\powershell.exe" -Verb runAs ↵
    -ArgumentList $arguments
break
}

# Files to Check
$KatanaKey="C:\Program Files\DrWeb\agent.key"
```

```
$SpiderAgent="C:\Program Files\DrWeb\spideragent.exe"

If (Test-Path $SpiderAgent ){

If(test-path $KatanaKey){}

Else {
    # Add your key File location over the network
        $from = "\\slc-dc01\Key\agent.key"
            # leave this as Default
    $destinationFolder = "C:\Program Files\DrWeb\"

    if (!(Test-Path -path $destinationFolder)) ↵
        {New-Item $destinationFolder -Type Directory}
    copy-item $from -destination $destinationFolder -Force

    if ($?) {"Successfully copied '$from' ↵
        to '$destinationFolder'"}
    Start-Sleep -Seconds 5
    # Stop-Transcript - remove # to activate logging
    # for windows 10}
    Restart-Computer
}}
```

В строке:

```
$from = "\\slc-dc01\Key\agent.key"
```

указываем сетевой путь к ключевому файлу (в нашем примере agent.key). Сам файл должен находиться в ранее созданной сетевой папке.

Для того, чтобы проверить наличие поддержки PowerShell, на машине где планируется активация агента, в меню «Пуск → Выполнить» запустите powershell.exe от имени администратора и выполните команду:

```
Set-ExecutionPolicy Unrestricted
```

**Внимание!** PowerShell Script поддерживается только для MS Windows 7 и выше.

**Внимание!** После активации Dr.Web Katana отключите поддержку скриптов PowerShell и удалите политику.

Для добавления скрипта, запустите Group Policy Management, выберите Script Startup («Конфигурация компьютера → Политики → Конфигурация Windows → Script (Startup/Shutdown)», см. рис. 11).

Перейдите на вкладку PowerShell Scripts (см. рис. 12). Нажмите кнопку Add («Добавить») и укажите сетевой путь к PowerShell-скрипту. Дополнительные параметры указывать не надо (см. рис. 13).

Выберите последовательность запуска скрипта согласно скриншоту, приведенному ниже. Должен быть выбран вариант Run Windows PowerShell scripts first (см. рис. 14).

При следующей регистрации машины в домене Dr.Web Katana будет активирована (см. рис. 15).

Dr.Web Katana может быть активирована и иным способом – с помощью BAT-файла. Для этого создаем файл (в данном примере будем использовать имя Key.BAT), имеющий следующее содержимое:

```
@echo off
:: BatchGotAdmin

:-------------------------------------
REM --> Check for permissions
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" ↵
```

Рисунок 10. Сообщение при загрузке системы


Рисунок 11. Создание Startup Script

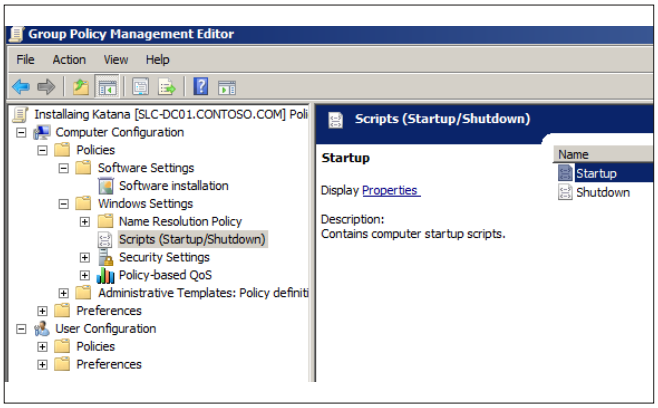



Рисунок 12. Добавление PowerShell Script

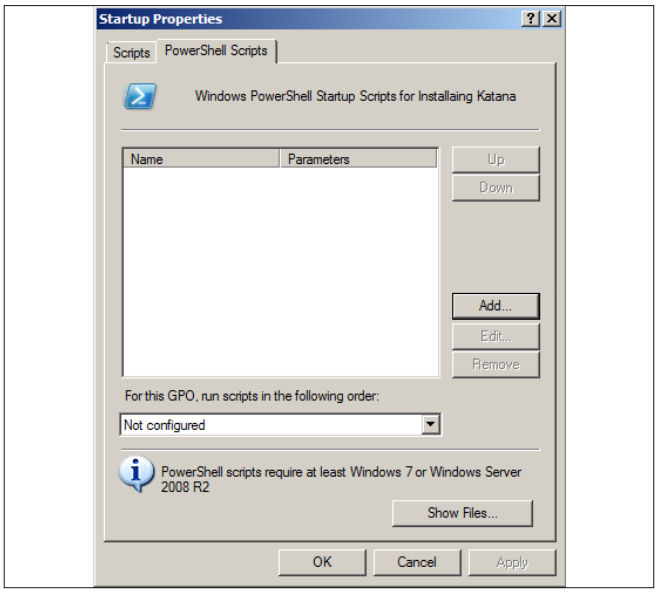



Рисунок 13. Указываем сетевой путь

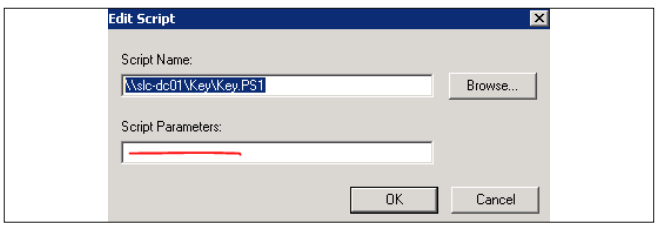


Рисунок 14. Выбираем последовательность запуска скрипта

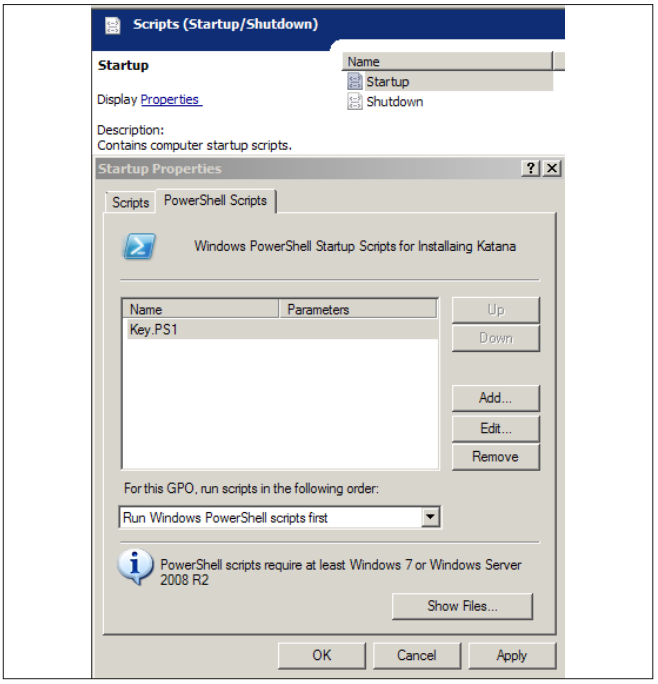



Рисунок 15. Лицензия активирована

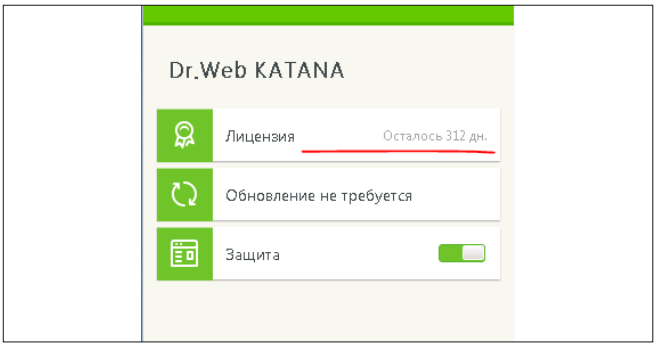
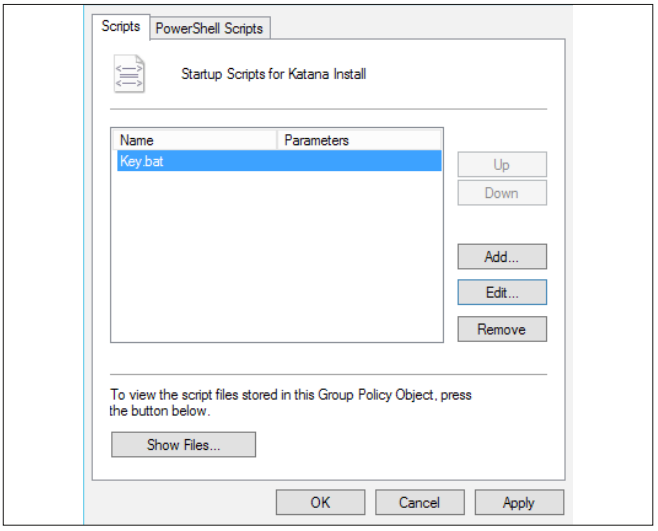



Рисунок 16. Добавление BAT-файла




```
        "%SYSTEMROOT%\system32\config\system"

REM --> If error flag set, we do not have admin.
if '%errorlevel%' NEQ '0' (
echo Requesting administrative privileges...
goto UACPrompt
) else ( goto gotAdmin )

:UACPrompt
echo Set UAC = CreateObject^("Shell.Application"^) > ↵
        "%temp%\getadmin.vbs"
set params = %*:"=""

echo UAC.ShellExecute "%~s0", "%params%", "", "runas", 1 >> ↵
        "%temp%\getadmin.vbs"
"%temp%\getadmin.vbs"
exit /B

:gotAdmin
if exist "%temp%\getadmin.vbs" ( del "%temp%\getadmin.vbs" )
pushd "%CD%"
CD /D "%~dp0"

:--------------------------------------
TIMEOUT /T 10 /NOBREAK
Echo off

:Start
IF EXIST "C:\Program Files\DrWeb\spideragent.exe" ↵
         (GOTO CheckKey) ELSE (GOTO End1)

:CheckKey
IF EXIST "C:\Program Files\DrWeb\agent.key" (GOTO End) ↵
         Else (GOTO CopyKey)

:CopyKey
copy "\\slc-dc01\Key\agent.key" "C:\Program Files\DrWeb\"
IF EXIST "C:\Program Files\DrWeb\agent.key" (GOTO End) ↵
         Else (GOTO Key2)
goto End2

:End
echo Both Agent and key already exist.
goto FINISH

:End1
echo DrWebKatana is not installed
goto FINISH

:End2
echo DrWebKatana Key is copied Please restart to activate
goto FINISH

:Key2
echo DrWebKatana Key copying received ACCESS DENIED ERROR

:FINISH
```

В строке:

```
copy "\\slc-dc01\Key\agent.key" "C:\Program Files\DrWeb\"
```

указываем сетевой путь к ключевому файлу (в нашем примере agent.key). Сам файл должен находиться в ранее созданной сетевой папке.

Дальнейшие наши действия не отличаются от действий при активации с использованием PowerShell-скрипта. Разница состоит только в закладке, на которой нам следует указать BAT-файл (необходимо выбрать первую вкладку Script, вместо PowerShell Script, как в указанном выше первом примере) (см. рис. 16).

При следующей регистрации машины в домене ключ будет скопирован на локальную машину. Для активации Dr.Web Katana потребуется повторная перезагрузка. EOF