Построение системы корпоративной антивирусной защиты смартфонов на базе Kaspersky Endpoint Security for Smartphone

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Сегодня применение мобильных устройств в корпоративных сетях становится все шире и шире. Соответственно появляется проблема защиты от вирусов всего этого «зоопарка» устройств. В данной статье я не буду касаться вопросов управления и поддержки данных устройств, мы с вами сосредоточимся на гораздо более узкой задаче – обеспечение антивирусной защиты парка смартфонов.

Введение

Сегодняшняя ситуация на рынке мобильных вирусов характеризуется следующими факторами:

1. ОС Android уверенно завоевывает популярность, оставив позади Windows Mobile. Операционные системы iOS и Blackberry также увеличили свое присутствие на рынке, а вот Symbian продолжает терять позиции, хотя в мировом масштабе по-прежнему остается лидером.
2. Произошли изменения в списке платформ, для которых появляются вредоносные программы. К ним добавились iOS (ОС для iPhone/iPod Touch/iPad) и Android. Появившееся вредоносное ПО для iOS может заразить только «разлоченные» (jailbroken) смартфоны.
3. В целом вредоносное ПО и атаки стали намного сложнее
4. Большинство вредоносного ПО для смартфонов нацелено на кражу денег пользователя.
5. Корпоративные смартфоны, кроме того, нуждаются в защите информации в случае кражи

Исходя из этого, возникает необходимость разворачивания централизованной антивирусной защиты смартфонов. Рассмотрим разворачивание такой защиты на базе Kaspersky Work Space Security.

В состав данного продукта входит антивирус для защиты смартфонов Kaspersky Endpoint Security 8 for Smartphone Maintenance Pack 1, который можно загрузить по адресу http://products.kaspersky-labs.com/russian/special/kesmobile/

Kaspersky Endpoint Security 8 for Smartphone Maintenance Pack 1 включает в себя следующие версии:

- 8.0.0.37 (Microsoft Windows Mobile);
- 8.1.39 (Symbian OS);
- 8.1.27 (BlackBerry OS);

- 8.1.71 (Android OS);
- 9.0.57.0 (Kaspersky Administration Kit Plugin);

Новинки:

- Поддержана работа программы на устройствах с Android OS. Реализованы следующие функции для версии программы, которая устанавливается на устройства с Android OS: Антивирус, Анти-Спам, Личные контакты, Анти-Вор.
- Поддержана возможность удаленного администрирования устройств с Android OS через Kaspersky Administration Kit.
- Добавлена поддержка устройств фирмы Nokia с Symbian^3.
- Добавлена поддержка устройств с Blackberry OS версии 6.0.

Описание

Kaspersky Endpoint Security 8 for Smartphone предназначен для обеспечения комплексной защиты мобильных устройств. Возможности программы:

- антивирусная проверка файлов при их открытии, сохранении и запуске (кроме мобильных устройств с BlackBerry OS);
- перехват и проверка всех входящих сообщений MMS и файлов, которые передаются следующими способами: с использованием беспроводных соединений (инфракрасный порт, Bluetooth), при синхронизации с персональным компьютером, при загрузке файлов через веб-браузер или через другие каналы;
- проверка файловой системы устройства по требованию пользователя или по расписанию на наличие вирусов и других вредоносных программ (кроме мобильных устройств с BlackBerry OS);
- возможность отправлять зараженные файлы в карантин, а также лечить некоторые из них (кроме мобильных устройств с BlackBerry OS);
- обновление антивирусных баз программы по требованию пользователя или по расписанию через GPRS-Internet, Wi-Fi, через Microsoft ActiveSync для устройств с Microsoft Windows Mobile или EDGE (кроме мобильных устройств с BlackBerry OS);
- блокирование нежелательных входящих вызовов и SMS;
- получение текущего номера телефона при смене SIM-карты;
- возможность дистанционного блокирования устройства в случае его кражи или потери;
- возможность дистанционного удаления информации пользователя с устройства в случае его кражи или потери;
- возможность дистанционного определения местоположения устройства;
- отправка SMS-команд на другие устройства с установленной программой Kaspersky Endpoint Security 8 for Smartphone (или Kaspersky Mobile Security 9) для дистанционного блокирования устройства, удаления данных, определения местоположения устройства, скрытия конфиденциальной информации пользователя;
- защита мобильного устройства от сетевых атак по протоколам TCP/IP (кроме мобильных устройств с Blackberry OS и Android OS);
- хранение файлов в зашифрованном виде (кроме мобильных устройств с Blackberry OS и Android OS);
- временное скрытие информации и событий для конфиденциальных номеров, выбранных пользователем (кроме мобильных устройств с BlackBerry OS).

- поддержка работы программы со следующими системами удаленного администрирования: Kaspersky Administration Kit, MS SCMDM, Sybase Afaria;
- установка программы на мобильное устройство и ее активация с помощью систем удаленного администрирования;
- удаление программы с устройств через MS SCMDM;
- синхронизация устройства с системами удаленного администрирования;
- настройка параметров работы программы как для нескольких устройств сразу, так и индивидуально для каждого отдельного устройства, применение политик с помощью систем удаленного администрирования;
- передача отчетов о состоянии защиты мобильных устройств и событиях программы в Kaspersky Administration Kit.

Внимание! Программа устанавливается только в основную память мобильного устройства.

Kaspersky Endpoint Security 8 for Smartphone включает следующие компоненты:

- Антивирус (кроме мобильных устройств с BlackBerry OS);
- Анти-Спам;
- Анти-Вор;
- Сетевой экран (кроме мобильных устройств с BlackBerry OS и Android OS);
- Шифрование (кроме мобильных устройств с BlackBerry OS и Android OS);
- Личные Контакты (кроме мобильных устройств с BlackBerry OS).

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Программа предназначена только для тех мобильных устройств, которые поддерживают прием и передачу SMS и работают на следующих операционных системах:

- Symbian OS 9.1, 9.2, 9.3, 9.4 Series 60 UI, Symbian^3 (только мобильные устройства фирмы Nokia).
- Microsoft Windows Mobile 5.0, 6.0, 6.1, 6.5.
- BlackBerry OS 4.5, 4.6, 4.7, 5.0, 6.0
- Android OS 1.5, 1.6, 2.0, 2.1, 2.2, 2.3.

Система удаленного администрирования должна удовлетворять следующим минимальным требованиям:

- Kaspersky Administration Kit версии 8.0.2112 и выше.
- Mobile Device Manager Software Distribution Microsoft Corporation Version: 1.0.4050.0000 (SP).
- System Center Mobile Device Manager Microsoft Corporation Version: 1.0.4050.0000.
- Sybase Afaria 6.50.4607.0.

Разворачивание Kaspersky Administration Kit не представляет никакого труда, поэтому останавливаться на нем подробно не имеет смысла.

Управление программой с помощью Kaspersky Administration Kit

Управление смартфонами и установленной на них программой Kaspersky Endpoint Security 8.0 for Smartphone осуществляется аналогично управлению клиентскими компьютерами с

установленными на них продуктами «Лаборатории Касперского». Администратор при этом должен создать группы, в состав которых он включит мобильные устройства, а после этого создать политику для KES.

Особенностью KES является то, что все параметры работы программы, включая лицензию, расписание обновления баз и проверки устройств, определяются с помощью политики.

Необходимо учесть, что при установке Сервера администрирования должен быть установлен компонент для управления защитой мобильных устройств. При установке данного компонента создается сертификат Сервера администрирования для мобильных устройств. Он используется для аутентификации мобильных устройств при обмене данными с Сервером администрирования. Без сертификата для мобильных устройств установить соединение между Сервером администрирования и мобильными устройствами невозможно. Средний объем передаваемых при одной синхронизации данных составляет 20-40 КБ.

Согласно документации данный компонент должен находиться в папке Plugin вашего Administration Kit. На самом деле все немного не так. Данный компонент вы должны загрузить с сайта по следующей ссылке http://www.kaspersky.com/downloads/productupdates/downloads-endpoint-security-smartphone , затем разархивировать и скопировать в папку Plugin вашего пакета Administration Kit, а затем установить его на рабочем месте администратора антивирусной сети.

После этого вам необходимо развернуть Сервер администрирования, указав при этом что вам нужна Поддержка мобильных устройств. При этом создается сертификат для мобильных устройств, который хранится в папке установки программы Kaspersky Administration Kit во вложенной папке Cert. При первой синхронизации мобильного устройства с Сервером администрирования копия сертификата доставляется на устройство и сохраняется на нем в специальной папке.

Кроме того, вам необходимо загрузить инсталляционный пакет KES8_forAdminKit_ru.exe, находящийся по адресу http://www.kaspersky.com/downloads/productupdates/downloads-endpoint-security-smartphone (о чем в документации также, увы, нет ни слова).

Далее вы можете настраивать все, как написано в документации.

Обновление антивируса

Если ваши смартфоны будут обновляться с серверов «Лаборатории Касперского», то проблем у вас не возникнет никаких. Если же вы хотите, чтобы они обновлялись с внутреннего сервера, вам придется указать его адрес.

Для того чтобы обновления производились с серверов обновлений «Лаборатории Касперского», в поле Адрес сервера обновлений введите KLServers.

При использовании для обновления баз программы какого-либо другого сервера обновлений в блоке Источник обновлений указывается HTTP-сервер, локальная или сетевая папка. Например, http://domain.com/index/.

Структура папок в источнике обновлений должна совпадать с аналогичной структурой на серверах обновлений «Лаборатории Касперского».

По адресу, указанному в политике, KES будет искать папку index и в ней файл mobile.xml. Файл mobile.xml должен быть аналогичен вот этому: http://ftp.kaspersky.com/index/mobile.xml.

Для WM нужен только узел с ComponentID=»KMS90WM». Параметр RelativeSrvPath должен указывать на папку, где лежат базы, относительно адреса, указанного в политике АК в качестве источника обновлений. Параметр Filename должен указывать на имя файла баз, параметр FileDate должен содержать дату и время.

Таким образом, если клиент указывает на адрес http://mycompany.com, то KMS будет искать файл http://mycompany.com/index/mobile.xml.

А сами базы можно брать, например, отсюда:
http://ftp.kaspersky.com/bases/av/avc/symbian/kms90.avc

Вывод

Как видите, несмотря на то, что задача кажется весьма скромной, на самом деле придется повозиться, однако полученный результат стоит того! Удачи вам, друзья!