Превентивная защита ПК от Petya.C

Новый вирус, который уже успели окрестить и NoPetya и NotPetya, официально носит название Petya.C. Этот вирус модифицирует MBR (Master Boot Record – главная загрузочная запись), прописывает в него свой код и при перезагрузке шифрует файлы, требуя выкуп. Но еще он “научился” распространяться по локальной сети и использовать существующие уязвимости. Подробнее можно почитать в статье компании Майкрософт, где рассматривается случай с распространением через обновление бухгалтерского ПО MeDoc.

Как же спасти свой ПК от заражения подобным вирусом? Можно ли защитить MBR от перезаписи или запретить удаленный запуск приложений на ПК под управлением ОС Windows? Короткий ответ – можно.

Защита MBR

MBRFilter – это драйвер от компании Cisco, который запрещает изменение загрузчика программами если Виндовс работает в обычном, а не безопасном режиме (Safe Mode).

Для установки скачайте драйвер в зависимости от разрядности вашей ОС, распакуйте архив, кликните правой клавишей на файле MBRFilter.inf (файл меньшего размера) и выберите в меню пункт “Установить”. Виндовс потребует перезагрузки, перезагрузите ОС и все готово. От вирусов в целом вас это не спасет, но спасти данные от злобных шифровальщиков – вполне поможет.

Запрет удаленного запуска программ

Здесь вам придется воспользоваться командной строкой. Запустите cmd с правами администратора:

- Нажмите значок поиска на Панели задач или кнопку Пуск
- В строке поиска напечатайте cmd

- В результатах поиска нажмите правую кнопку мыши на классическом приложении Командная строка
- В открывшемся меню выберите пункт Запустить от имени администратора

Дальше наберите команду:

sc.exe sdshow scmanager

Вам выведется строчка из кучи разных непонятных букв, что-то типа D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU) и т.д. Это формат записи флагов и прав на файлы – SDDL. Вам нужно сохранить эту строчку! Чтобы ее скопировать: выделите весь текст, кликните правой клавишей, текст будет в буфере обмена. Далее вставьте этот текст в ваш любимый текстовый редактор. Т.к. строчка длинная, в командной оболочке она была разбита на две или три строки, в текстовом редакторе отредактируйте ее так, чтобы это была одна строчка, без переводов строки.

Как вариант, можете выполнить следующий код:

sc.exe sdshow scmanager > c:\scm.backup.txt

Т.о. строчка сохранится в файл c:\scm.backup.txt

Далее сделайте копию файла, в строчку после D: добавьте следующее:

(D;;GA;;;NU)

Чтобы начало строчки у вас выглядело так:

D:(D;;GA;;;NU)(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)

Далее всю длинную строчку вставьте после команды:

sc.exe sdset scmanager D:(D;;GA;;;NU)(A;;CC;;;AU)(A;;C.....(все остальные буквы)

И проверьте правильность (если не выдало ошибок):

sc.exe sdshow scmanager

Начало строки может выглядеть вот так:

D:(D;;KA;;;NU)(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)

Это нормально, не переживайте. Главное, чтобы все остальные буквы совпадали.

Теперь хакер или вирус не сможет при помощи *psexec* запустить вирус или программу на вашем ПК под управлением ОС Виндовс.

Источник