Вирус Little.exe

«*Little*» - таково название у вируса, который распространяется на съемных носителях в скрытой папке «*portable*». Написан этот вирус на Visual Basic и имеет размер в 188 КБ.

Может быть и не стоило тратить время на изучение этого вируса, написанного каким-то школьником на факультативных занятиях информатики, но нужно отдать должное создателю вируса: злоумышленник освоил новый раздел реестра *[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]*. До этого, юные вирусописатели знали только о существовании раздела автозагрузки программ: *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]*. Позже, школьники догадались использовать ключ «*Shell*» для старта вирусов вместе с программой «*explorer.exe*».

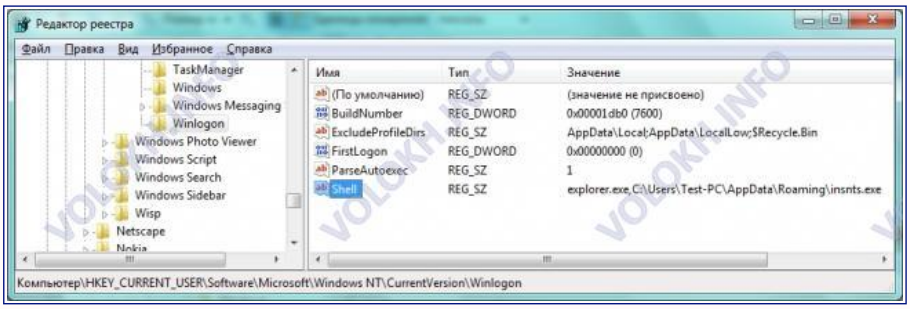
Таким образом, вирус Little.exe при запуске копируется в директорию «*C:\Users\Test-PC\AppData\Roaming*», где исполняемому файлу присваивается имя «*insnts.exe*». Стоит отметить, такое поведение вируса свойственно запуску в операционной системе Windows 7. В Windows XP путь к файлу будет иным, так как по умолчанию в Windows XP пользователь работает под правами администратора, соответственно, вирус получит больше полномочий. Тем не менее, данный вирус запустился под правами обычного пользователя в Windows 7 и прописался для запуска в доступном ему разделе системного реестра.

Обнаружив вирус в системе, я тут же попытался его удалить и забыть про него, но вирус просто так сдаваться не собирался. В списке процессов вирус не отображался, но не позволял себя удалить простым удалением, так как использовался другим процессом, а точнее «explorer.exe».

Второе, что я попробовал предпринять – это редактирование ключа «Shell» ветви реестра [HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon], но вирус снова добавлял путь к исполняемому файлу вируса в ключ реестра «Shell».

Конечно же, если попытаться выгрузить из списка процессов «explorer.exe», то файл вируса «insnts.exe» можно удалить без проблем, но можно поступить более интересным способом, о чем я расскажу чуть ниже.

Как мы уже выяснили, при запуске вирус прописывается в системном реестре в разделе [HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]:



Вредоносная программа изменила параметр ключа системного реестра «Shell» с «explorer.exe» на «**explorer.exe,C:\Users\Test-PC\AppData\Roaming\insnts.exe**», то есть помимо запуска «explorer.exe» при старте компьютера загрузится также вирус. «*Test-PC*» здесь означает имя учетной записи, логичным будет предположить, что имя учетной записи у вас будет отличаться, но суть от этого не изменится.

Если вы не знаете, под какой учетной записью вы работаете или где найти ключ «Shell», то откройте системный реестр следующим образом: нажмите сочетание клавиш «Win+R» и появится окно «Выполнить».

Введите в этом окне команду «regedit» и нажмите «OK». Теперь последовательно раскрывайте ветви реестра [HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon] и, выделив ветвь «Winlogon», справа вы увидите ключ реестра «Shell».

Можете поэкспериментировать с удалением или изменением параметра ключа «Shell», однако вирус будет проверять наличие в параметре ключа строки «C:\Users\Test-PC\AppData\Roaming\insnts.exe». Если вы попытаетесь изменить или добавить какую-либо букву или символ в эту строку, то вирус немедленно продублирует в параметр ключа «Shell» путь к исполняемому файлу вируса. При удалении ключа «Shell», вирус моментально создает его снова. Что же тогда делать, если невозможно отредактировать нужный нам ключ?

Давайте напишем простой Bat-файл. Итак, открывайте Блокнот и напишите в нем следующие две строчки:

```
attrib -s -h -r C:\Users\Test-PC\AppData\Roaming\insnts.exe

 del C:\Users\Test-PC\AppData\Roaming\insnts.exe
```

Теперь сохраняйте напечатанное под любым именем, например «DelLittle» с расширением «**.bat**». Немного позже, мы узнаем, что значат эти строки, а сейчас взгляните на параметр ключа «Shell» и подумайте, что можно в нем исправить. Если ничего не приходит в голову, то измените параметр ключа «Shell» следующим образом: «**D:\DelLittle.bat,explorer.exe,/C:\Users\Test-PC\AppData\Roaming\insnts.exe**». Только не забудьте изменить «Test-PC» на имя учетной записи, под которой вы работаете.

Давайте разберемся с нашим измененным параметром. В кавычках у нас находится путь к написанному нами Bat-файлу. Далее после запятой идет запуск программы «explorer.exe», затем снова идет запятая и прямой слеш, а уже только после него путь к вирусу «Little.exe».

Что же здесь происходит и почему вирус теперь ничего не изменяет? Ответ прост: перед путем к исполняемому файлу мы добавили прямой слеш, и вирус не заметил никаких изменений.

Вот теперь пришло время разобрать написанный нами Bat-файл. В первой строке мы изменяем атрибуты нашего вируса. Для этого используется команда «*attrib*» с дополнительными параметрами «*-s -h -r*». Знак тире перед сокращениями «Hidden», «System» и «Read» снимает атрибуты с файла «insnts.exe», соответственно, знак плюса «+» установит заданные атрибуты для файла. Мы как бы говорим: *убрать атрибуты: «системный», «скрытый» и «только для чтения» у файла «insnts.exe», который располагается по адресу «C:\Users\Test-PC\AppData\Roaming\»*.

Вторая строка уже удаляет файл, с которого мы убрали атрибуты. Удаление происходит с помощью команды «del». Чтобы компьютер знал, какой именно файл требуется удалить, команде «del» мы сообщаем полный путь к файлу.

Если сейчас запустить наш файл «DelLittle.bat», то ничего не произойдет, так как файл занят приложением «explorer.exe». Поэтому мы изменили параметр ключа «Shell» таким образом: «D:\DelLittle.bat,explorer.exe,/C:\Users\Test-PC\AppData\Roaming\insnts.exe».

При старте компьютера сначала запустится созданный нами «DelLittle.bat» и только потом «explorer.exe», а файл вируса не запустится, так как мы поставили прямой слеш после запятой. Будьте внимательны, если вы поставите слеш перед запятой, то программа «explorer.exe» не запустится, и вы увидите только черный экран. Хотя ничего страшного не произойдет, вирус будет удален. Поэтому важно правильно поставить

Archive notes

2017

January February March
April May June
July

2016 2015 2014 2013 2012 2011

Tags notes

OpenSource Microsoft
Swindle Linux
Apple Security
Technology Volokh
Programming Humor
Army Live
Books Review
Internet Telecommunication
Article Hardware
Other Computer
Phone Virus
Software Project

прямой слеш, чтобы вирус не смог запуститься, а так как все что находится справа от слеша, будет считаться дополнительным параметром. Разумным будет предположить, что у программы «explorer.exe» нет параметра «C:\Users\Test-PC\AppData\Roaming\insnts.exe», значит, ничего и не произойдет.

После этих манипуляций перезагружаем компьютер. После включения компьютера мы можем убедиться в отсутствии файла «insnts.exe» в папке «C:\Users\Test-PC\AppData\Roaming\». Нам остается только подправить параметры ключа «Shell» должным образом. Удаляйте все кроме «explorer.exe». Это значит, что в параметре ключа не должны быть никакие запятые, никакие слеши, а только программа Проводник «**explorer.exe**».

На этом можно поставить огромную точку, точнее нажать кнопку «Enter» после редактирования параметра ключа «*Shell*».

2011-10-28 14:44