УДК 004.056.57

ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ КОМПЬЮТЕРА ПОСЛЕ ПОРАЖЕНИЯ ВИРУСОМ-БЛОКИРОВЩИКОМ

Халиман Н.П., Рябцев В.Г.
Черкасский филиал Европейского университета, Украина

Рассматриваются вопросы информационной безопасности, в частности, методы восстановления операционной системы Windows персонального компьютера после ее поражения вредоносными программами типа Trojan Winlock, блокирующих доступ к системе. Рекомендуется восстановление системы с помощью набора программ ERD Commander.

Введение

Семейство вредоносных программ ***Trojan.Winlock (Винлокер)*** блокирует или затрудняет работу операционной системы и требует перечисления денег злоумышленникам за восстановление работоспособности компьютера [1]. При включении компьютера появляются сообщения типа: «Вы получили временный бесплатный доступ к сайту для взрослых, необходимо оплатить продолжение его использования», либо тем, что «на Вашем компьютере обнаружена нелицензионная копия Windows» (рис. 1).

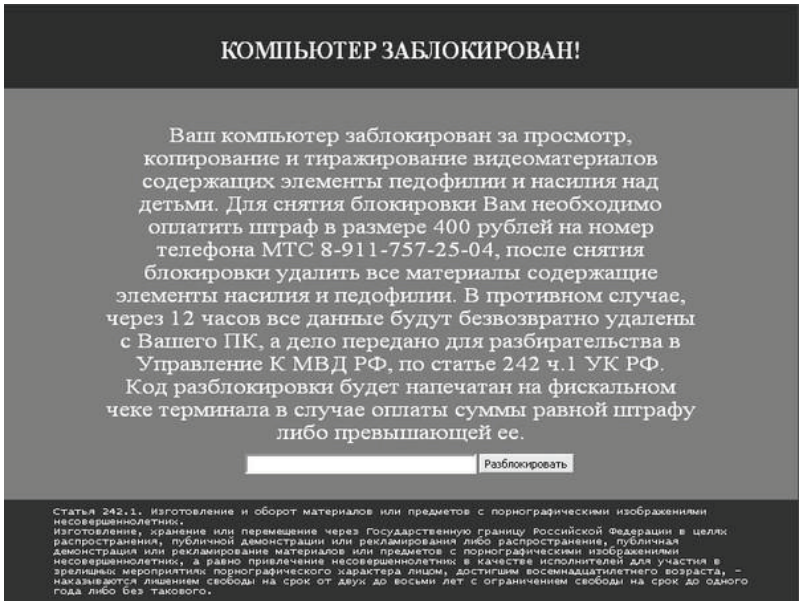

Рисунок 1. Пример сообщения, выдаваемого вирусом

Пути распространения Trojan.Winlock и подобных вирусов разнообразны, зачастую инфицирование происходит через уязвимости браузеров при просмотре зараженных сайтов.

Целью работы является изучение методов разблокирования компьютера, зараженного вирусом-блокировщиком.

Актуальность поставленной задачи подтверждается тем, что в данное время существуют тысячи различных видов винлокеров, которые активно атакуют незащищенные системы, выводя их из рабочего состояния. Далее будут рассмотрены основные методы борьбы с этим видом вредоносных программ.

1 Метод восстановления системы подбором ответного кода

Если есть возможность доступа в Интернет с другого компьютера, то ответные коды самых

распространенных винлокеров есть на сайтах компаний Dr.Web [2] и Kaspersky Lab [3]. После деактивации сообщения необходимо проверить систему антивирусом.

2 Вход в систему с помощью Live CD ERD Commander

ERD Commander - это набор программ, работающих в среде WindowsPE. WindowsPE позволяет выполнить загрузку системы со съемного носителя, что дает возможность запустить компьютер даже в случае тотального повреждения его файлов существующей на диске ОС, жизненно необходимых для ее старта. Являясь «почти настоящей» 32-битовой Windows, WinPE обеспечивает полный доступ к NTFS-томам, системному реестру, параметрам настройки и драйверам [4].

Для загрузки с Live CD необходимо в настройках BIOS установить загрузку из CD-ROM, затем надо выбирать директорию, где установлена операционная система Windows XP, обычно это *«C:\ WINDOWS»,* и нажимать *OK*.

Первый вариант удаления вируса возможен через «откат системы». Это вернет состояние компьютера на тот момент, когда вируса еще не было, и возможно будет нормально загрузиться, а затем продолжать удалять вирус из операционной системы. Для этого нужно выбрать команду: *Start -> System tools -> System Restore* (рис. 2). Вызванный таким способом мастер восстановления системы производит возврат к той контрольной точке, когда система еще была работоспособна. Если контрольные точки отсутствуют, необходимо найти место в реестре, где прописан вирус. Для редактирования реестра необходимо войти в редактор реестра при помощи команды: *Start -> Administrative tools -> Registry Editor.*

Рисунок 2. Вызов мастера восстановления системы

В древовидной системе реестра нужно переместиться в ветку *HKEY_LOCAL_MACHINE Software\Microsoft\WindowsNT\CurrentVersion\Winlogon*.

В строке *Value Data* пункта *Shell* должен быть прописан только файл *Explorer.exe,* если там размещено еще какое-нибудь странное название, это и есть наш вирус. Его необходимо удалить, нажав по пункту *Shell* и изменив его значение (*Value data*) на *«C:\Windows\Explorer.exe*» без кавычек (рис. 3).

Затем необходимо посмотреть пункт *Userinit*: в нем должно быть прописано *C:\Windows\ System32\userinit.exe.* После этого необходимо перезагрузить компьютер и проверить систему антивирусом.

Выводы

Использование данных методов должно помочь сохранить работоспособность и безопасность операционной системы без потерь информации и финансовых средств.

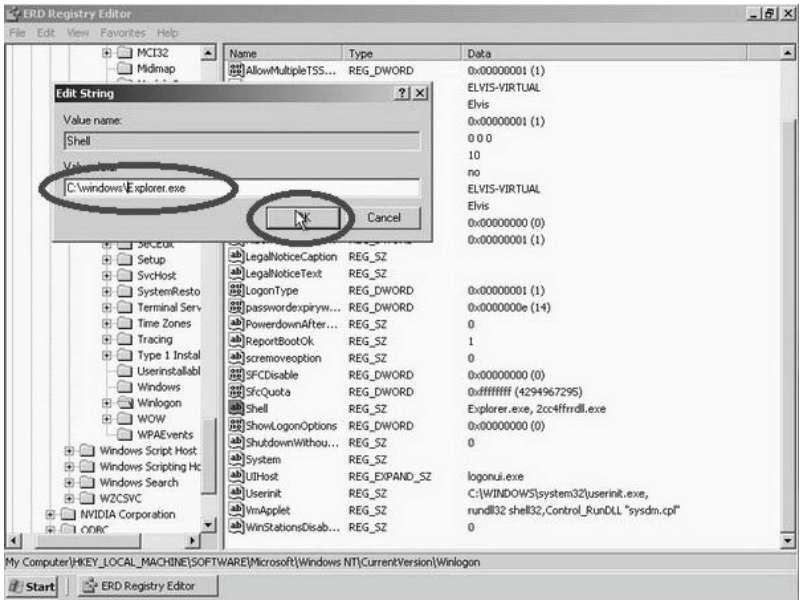

Рисунок 3. Изменение значения *Shell*

Литература

[1] Trojan.Winlock. Материал из Википедии – свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/Trojan.Winlock/

[2] Бесплатный разблокировщик Dr.Web от Trojan.Winlock . Материал из сайта Dr.Web. Электронный ресурс. Режим доступа: http://www.drweb.com/unlocker/index/

[3] Удаление баннера с рабочего стола, разблокировка Windows. Материал из сайта службы технической поддержки Kaspersky Lab . Электронный ресурс. Режим доступа: http://support.kaspersky.ru/viruses/deblocker

[4] ERD Commander. Материал из сайта Windows FAQ.ru. Электронный ресурс. Режим доступа: http://www.windowsfaq.ru/content/view/659/46/