УДК 004.491.42

Нейтрализация вредоносных последствий вирусов семейства Trojan.Winlock

© Ю.В. Елисина, А.М. Губарь

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Описаны особенности проявления заражения вирусами семейства Trojan.Winlock в операционной системе (ОС). Рассмотрены последствия внедрения Trojan.Winlock в ОС. Предложен алгоритм нейтрализации этих последствий в зависимости от того, существует ли возможность загрузки ОС в безопасном режиме, установлена ли на зараженном персональном компьютере другая ОС, а также имеется ли другая учетная запись. Для случая невозможности загрузки с действующей ОС описан способ решения проблемы с использованием внешней ОС.

Ключевые слова: *операционная система, вирус, блокировка, Trojan.Winlock, реестр Windows.*

Введение. Trojan.Winlock (наименование вирусов согласно терминологии ООО «Доктор Веб») — семейство вредоносных программ, блокирующих или затрудняющих работу с операционной системой и требующих перечисления денег злоумышленникам за восстановление работоспособности компьютера. Trojan.Winlock — частный случай программ-вымогателей. Впервые они появились в конце 2007 г. Широкое распространение вирусы-вымогатели получили зимой 2009–2010 гг., оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета. Второй всплеск активности этого вредоносного программного обеспечения пришелся на май 2010 г. К сожалению, и на данный момент вероятность инфицирования этим видом трояна очень высока.

Ранее для перевода денег обычно использовались короткие премиум-номера, в настоящее время подобные программы также могут требовать перечисления денег на электронные кошельки (например, «Яндекс.Деньги», «WebMoney») или на баланс мобильного номера. Необходимость перевести деньги часто объясняется так: «Вы получили временный бесплатный доступ к сайту для взрослых, необходимо оплатить продолжение его использования» либо «на Вашем компьютере обнаружена нелицензионная копия Windows». Возможен также вариант сообщения «за просмотр, копирование и тиражирование видео с насилием над детьми и педофилией» (рис. 1).

Пути распространения Trojan.Winlock и подобных вирусов разнообразны, в значительной части случаев инфицирование происхо-

дит через уязвимые места браузеров при просмотре зараженных сайтов, скачивании различного программного обеспечения с неблагонадежных ресурсов, на которых посредством дистрибутивов распространяются вирусы.

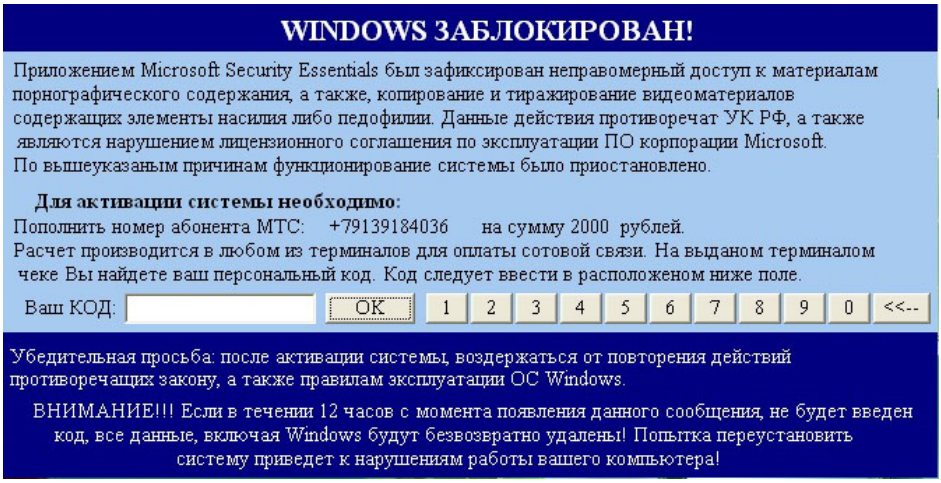

Рис. 1. Баннер, созданный Trojan.Winlock.6011 (орфография и пунктуация «авторов» баннеров сохранены)

1. Нейтрализация последствий Trojan.Winlock с помощью специального программного обеспечения. Модификаций данного вируса огромное множество, причем визуально изображения «баннеров» могут и не отличаться (меняются только телефонные номера). Эти модификации классифицируются как разные угрозы из-за механизма воздействия, однако алгоритм решения единственный.

Проанализировав последствия внедрения вируса и его внутреннюю структуру, предлагаем следующий алгоритм нейтрализации последствий этого вида троянов.

1.1. ***Нейтрализация при существовании кода/способа разблокировки.*** Для большинства старых модификаций существуют так называемые коды разблокировки по номеру телефона, указанному на «баннере» (в настоящее время кодов почти нет). Они доступны, например, в разделе «Разблокировка Windows (Trojan.Winlock)» на официальном сайте компании «Доктор Веб». Имеются инструкции для разблокировки, например: «для разблокировки кликнуть в область, обозначенную розовым прямоугольником», «7 раз кликнуть по строке с текстом "корпорации Microsoft", затем кликнуть по фразе "Для активации системы необходимо"».

1.2. ***Нейтрализация при частичной блокировке системы.*** Возможны два варианта частичной блокировки системы:

1) заблокирован «рабочий стол» только одной учетной записи;

2) «баннер» закрывает центр экрана, однако в незакрытой области можно выполнять действия.

В этих случаях можно запустить любые утилиты сканирования, вручную обнаружить файл трояна, отредактировать реестр и т. д. Возможности решения проблемы почти неограниченны. Например, можно использовать сканер, не требующий установки, Dr.Web CureIT (бесплатная утилита).

1.3. ***Нейтрализация при полной блокировке системы.*** Различают три варианта полной блокировки системы:

1) есть возможность загрузить ПК в безопасном режиме ОС;

2) отсутствует возможность загрузки ОС в безопасном режиме, на ПК установлено несколько ОС;

3) нет возможности загрузить ПК в безопасном режиме ОС, на ПК нет других ОС.

Если удается загрузить систему в безопасном режиме, можно выполнять все действия из п. 1.2. Бывает, что не удается загрузиться в каком-то определенном режиме, тогда нужно обязательно проверить все режимы, чаще всего «безопасный режим с поддержкой командной строки» работает.

Существуют следующие виды безопасного режима загрузки ОС:

- безопасный режим;
- безопасный режим с загрузкой сетевых драйверов;
- безопасный режим с поддержкой командной строки.

В зависимости от дальнейших действий необходимо выбрать тот или иной режим. Например, если требуется использование сети Интернет, то обязательна загрузка сетевых драйверов.

При наличии такой возможности загружаем другую ОС и выполняем действия из п. 1.2. В данном случае мы «лечим» винчестер (логический диск) с «зараженной» ОС как съемное устройство.

В случае отсутствия других ОС единственным решением является загрузка с внешнего диска (загрузка с другой ОС). Например, можно использовать диски аварийного восстановления Dr. Web LiveCD|LiveUSB — необходимо записать загрузочные диски для запуска на зараженном ПК. При использовании LiveUSB необходимо предварительно убедиться, что версия BIOS поддерживает загрузку с USB-устройств. Подробную информацию можно найти в документации к ПК или к материнской плате.

На многих дисках восстановления уже имеются встроенные программы для сканирования ОС. Если сканирование не принесло положительных результатов, троян придется искать вручную.

2. Ручной способ удаления вируса. Чтобы удалить вирус семейства Trojan.Winlock вручную, нужно ликвидировать созданные им записи из реестра и сами вирусы.

Для просмотра и редактирования содержимого реестра нужно скопировать файлы:

C:\Windows\System32\config\software;

ntuser.dat:

Для пользователей Windows XP файл ntuser.dat необходимо копировать из каталога *\Documents and Settings_ВАШЕ_ИМЯ_ПОЛЬЗОВАТЕЛЯ_*.

Для пользователей Windows Vista/Windows 7 файл ntuser.dat необходимо копировать из каталога *\Users_ВАШЕ_ИМЯ_ПОЛЬЗОВАТЕЛЯ_*.

Для загрузки «куста» (файла, раздела) реестра и доступа к реестру неактивной или не загружающейся системы можно использовать стандартный редактор реестра (regedit.exe) на любой ОС Windows. Для этого, запустив редактор, необходимо выбрать одну из корневых веток: HKEY_LOCAL_MACHINE или HKEY_USERS, после чего в меню «Файл» станет активной опция «Загрузить куст»/«Load hive».

2.1. ***Анализ файла software.*** В файле software необходимо проверить следующие ветви:

1. *Microsoft\Windows NT\CurrentVersion\Winlogon*:

• параметр *Shell* должен быть равен *Explorer.exe*. Если перечислены любые другие файлы, необходимо записать их названия и полный путь к ним, затем удалить все лишнее и задать значение Explorer.exe;

• параметр *userinit* должен быть равен *C:\Windows\system32\user init.exe*, (именно так, с запятой на конце, где *C* — имя системного диска). Если указаны файлы после запятой, то нужно записать их названия и удалить все, что указано после первой запятой.

Возможны ситуации, когда присутствует схожая ветвь с названием *Microsoft\Windows NT\CurrentVersion\winlogon*. Если эта ветвь существует, ее необходимо удалить.

2. *Microsoft\Windows\CurrentVersion\Run.* Эта ветвь содержит настройки объектов автозапуска.

Попав на компьютер, вирус должен в первую очередь где-либо записать свои файлы, откуда он потом будет запускаться и действовать. В основном вирусы размещают себя в следующих местах:

• в корневых папках дисков, чаще всего C:\;

• в профиле пользователей ПК (C:\Documents and Settings\ в Windows XP и C:\Users\ в Windows Vista и Windows 7);

• во временных папках (C:\Windows\Temp, C:\Documents and Settings\Temp, C:\Users\Temp);

• в папке операционной системы, как правило, C:\WINDOWS\, и вложенных в нее папках (часто C:\WINDOWS\system\, C:\WINDOWS\system32\, C:\WINDOWS\system32\drivers\, C:\WINDOWS\Temp).

Особенно внимательно следует отнестись к наличию в указанных папках объектов, отвечающих следующим критериям:

• имена напоминают системные процессы, но программы запускаются из других папок, например, C:\Documents and Settings\Dima\svchost.exe;

• имена вида vip-porno-1923.avi.exe;

• приложения запускаются из временных папок;

• неизвестные приложения запускаются из системных папок, например C:\Windows\system32\install.exe;

• имена состоят из случайных комбинаций букв и цифр, например C:\Documents and Settings\Dima\094238387764\094238387764.exe.

Если подозрительные объекты замечены, их имена и пути необходимо записать, а соответствующие им записи удалить из автозагрузки. Имена параметров могут быть различными, часто «load», «explorer», «userinit».

3. *Microsoft\Windows\CurrentVersion\RunOnce* — тоже ветвь автозагрузки, ее следует проанализировать аналогичным образом. Завершив анализ, необходимо нажать на имя загруженного раздела и выполнить «*Файл» → «Выгрузить куст»*.

2.2. ***Анализ файла ntuser.dat.*** В файле ntuser.dat необходимо проверить следующие ветви:

1. *Software\Microsoft\Windows\CurrentVersion\Run*.

2. *Software\Microsoft\Windows\CurrentVersion\RunOnce*, задающие объекты автозагрузки.

Необходимо проанализировать их на наличие подозрительных объектов, как указано выше.

3. *Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.* Эту ветвь необходимо анализировать по аналогии с файлом software. Особое внимание следует обратить на параметр *Shell* в ветке *Software\Microsoft\WindowsNT\CurrentVesion\Winlogon,* он должен иметь значение *Explorer.exe*. Если такой ветки нет вообще — все в порядке.

Надо помнить, что часто вирусы имеют названия, схожие или идентичные с названиями системных файлов, поэтому необходимо обращать особое внимание на каталог, в котором они расположены.

Примечание. При наличии возможности и желания целесообразно снять винчестер с «зараженной» ОС и подключить к другому ПК как съемное устройство. Лечение аналогично указанному в п. 1.2.

Заключение. Вирусы семейства Trojan.Winlock имеют большое количество модификаций и представляют опасность для любой ОС на платформе Windows. Для правильной разблокировки компьютера необходимо удалить как исполняемый файл, так и записи о нем в реестре, однако в реальности достаточно удалить только исполняемый файл, в реестре остаются записи («ссылки» на троян). Блокировки системы уже не будет, но данный способ не является корректным.

Аналогично, если убрать параметры в реестре, созданные трояном, блокировки не будет, хотя сам вредоносный файл все еще будет присутствовать в ОС. В этом случае файл представляет потенциальную опасность, так как при его повторном запуске блокировка ОС возобновится.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Елисина Ю.В., Губарь А.М. Нейтрализация вредоносных последствий вирусов семейства Trojan.Winlock. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1006.html

Елисина Юлия Владимировна родилась в 1989 г. Студентка 6-го курса кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана, специалист отдела технической поддержки ООО «Доктор Веб». e-mail: elisina.yulia @gmail.com

Губарь Александр Михайлович родился в 1946 г., окончил МВТУ им. Н.Э. Баумана в 1970 г. Канд. техн. наук, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана. Автор около 50 печатных работ в области вычислительной техники. e-mail: gam46@inbox.ru