Винлок — Lurkmore

A long time ago, in a galaxy far, far away...

События и явления, описанные в этой статье, были давно, и помнит о них разве что пара-другая олдфагов. Но Анонимус не забывает!

I see what you did there.

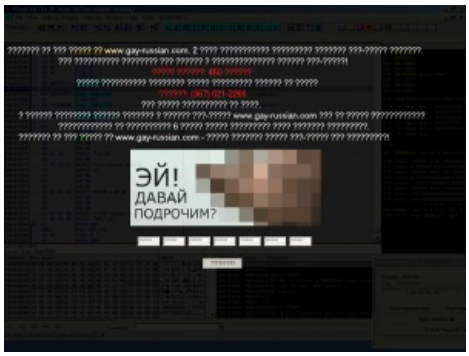
Информация в данной статье приведена по состоянию на конец нулевых. Возможно, она уже безнадёжно устарела и заинтересует только слоупоков.

Винлок (англ. *Winlock*) — троян-вымогатель, актуальная беда рядовых юзеров и прочих нубов, начиная с конца 2007 года. С 2012 года винлок был заменён на трояны-шифровальщики. Для большинства возникает ВНЕЗАПНО и самостоятельно очень сложно выводится — большинство винлоков имеют довольно хорошую защиту от дурака, да и, собственно, недалёкость реципиента и есть основа прибыли создателей этой подставы.

Минималистичный SFW-вариант

Что это?

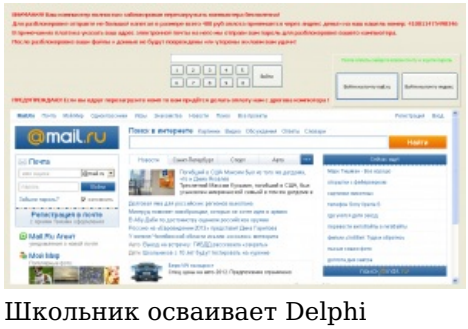
Внешне выглядит как окошко, в котором вам пытаются втюхать какую-то фигню и заставить вас отправить СМС (недешевое, разумеется), дабы разблокировать ваш комп. После отправки, якобы, придёт код активации, или же будет напечатан на чеке qiwi, который разблокирует комп.



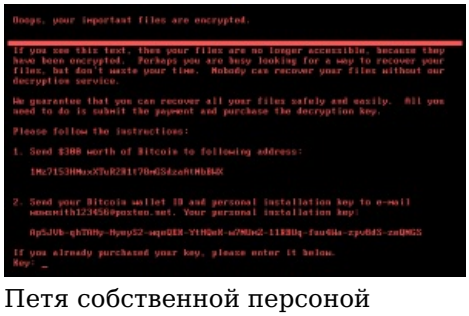
Codepage fail

Винлок развивался долго:

- Сначала это был простенький троян, который заменял файл hosts и защищал его от записи, что приводило к замене некоторых страниц на уютный сайтик вымогателя. Самые первые версии выглядели скорее шуткой, так как ничего не вымогали, а просто блокировали рабочий стол, показывая на весь экран что-то вроде большой волосатой задницы.
- Затем это был баннер, который, как правило, полностью состоял из прона и распространялся как гуглояндексовый бар. «Прикреплялся» к браузеру и вне его не распространялся.
- Затем этот баннер «научился» перекрывать рабочий стол и диспетчер задач. Опытный юзер быстро побеждал этот вирус путём разных хитростей типа regedit'а и разных известных сочетаний клавиш.
- Вирусописатели в ответ доработали троян напильником. Теперь он полностью загораживает рабочий стол, завершает explorer, перекрывает доступ почти ко всему и запрещает диспетчер задач.
- Есть даже винлоки со всякой хуитой в виде анимации и звукового сопровождения (Win32.Gaara(wrm), в народе — «вирус с японских порносайтов», видео с пруфом было найдено в 2010 году). Обычно это рожа анимешного перса, которая требует отправить деньги, но вместо простой блокировки вызывает BSOD. Окна антивирусов об угрозе эти винлоки просто закрывают.
- Последние версии (MBR-Locker'ы) и вовсе устанавливаются как отдельный загрузчик и стартуют ещё ДО загрузки венды, не оставляя пушистой жертве ни единого шанса.
- Теоретически и практически можно заразить Биос, например, в материнской плате AWARD, и сразу при включении компьютера будет появляться сообщение «Заплатите выкуп», если троян изменит программный код Биоса (сам Биос — это программа, начальный загрузчик). Но трояноописатели нынче ленивые, и такой фигней не страдают. Да и материнские платы у всех разные, и Биосы разные, так что эпидемии троянов-вымогателей, заражающих Биос, скорее всего не будет.



Школьник осваивает Delphi



Петя собственной персоной

Также можно в программу, которая обновляет Биос, засунуть трояна (троян тоже является обычной

программой, но вредоносной), который всё и заблокирует. Если идиот скачает программу для обновления Биос чёрт знает откуда.

- Следующей ступенью развития заразы стал CryptLock (он же SMSLock, Cryzip, PGPlock). После внедрения криптлок шифрует все содержимое на всех дисках, и сетевых тоже (если разрешена запись в файлы), кроме exe, dll и т. д., после чего вывешивает уже всем знакомое окошко с требованием отправить смс на номер для получения пароля дешифровки. От прочих пионерских поделок отличался особой трудностью в истреблении (пароль дешифровки представлял собой длинную мешанину из букв разного регистра и символов) и лечился только подсовыванием серверу фейковой команды подтверждения оплаты; в наше время его знает большинство солидных антивирусов.
- Нынешние трояны-шифровальщики совсем охуели, и используют ассиметричное шифрование, а закрытый ключ находится у мудаков-вымогателей. И можно было бы перехватить этот ключ, когда троян отправляет ключ на сервер мудаков-вымогателей, но он передаётся в зашифрованном виде, и хуй ты там что перехватишь. Всё это не оставляет никакого шанса для расшифровки. К счастью, ублюдки-вымогатели соображают, что дешифратор надо высылать, и часто его высылают за охуенные бабки.
- Дальнейший шаг — закрытый ключ для шифрования файлов генерируется на машине жертвы, и сохраняется на ней зашифрованным через открытый ключ вымогателей. После оплаты, вымогатели расшифровывают этот закрытый ключ жертвы у себя. Таким образом, основной закрытый ключ вымогателей вообще не передаётся по сети.
- Следующий этап — червь-шифровальщик под названием WannaCry/WCry/WanaCrypt0r 2.0. Использует дыру в маздае, от пользователя телодвижений не требует, запускается самостоятельно. Сканирует 139-й и 445-й порты, если они открыты и не стоит обновление — атакует. За один день поразил over9000 компьютеров. Также ставит руткит (чтобы мало не показалось).
- Некоторые кулхацкеры додумались всунуть в MBRLocker шифровальщик (Trojan.Ransom.Petya). Но оказалось, что у создателей трояна последняя стадия рукожопости, и поэтому Петя расшифровать твой прон не сможет, а с последующими версиями его удаляет.

Где скачать?

Скачать винлок не составляет труда. Достаточно просто побродить по интернету некоторое время. Винлок сам найдёт вас. Вы даже не заметите, как он скачается и установится в вашу систему. Нет, серьёзно, всё так и есть, особенно если вы шляетесь по всяким сетевым аналогам общественных сортиров при дефолтном браузере и без отключения скриптов. Винлок может попасть к вам на комп с любого брошенного или порно-сайта, кулхацкеры могут заразить им часто посещаемый форум или сайт, а также вы сами по-старинке можете скачать его под видом «нового мега-ПО». Есть версии под Макось и называются маклоками. Мойте руки перед едой!

Существует распространённое заблуждение, что эта напасть касается только пользователей Windows XP, и что юзеры Висты, Семёрки или Макоси могут спать спокойно. Разумеется, это типичный нубский миф. Не менее года существуют и активно приносят доход ушлым людям версии под Seven и Макось. И даже самая залатанная контрацепция, в конечном итоге, не спасает безликие массы Анонимусов от простуды в виде винлока.

Также, чтобы найти троян-шифровальщик, достаточно открывать вложения в спаме.

Пользователи линупса: просто двиньте вперёд, эта статья не для вас и не про вас.

Как это работает?

Работает это элементарно: после скачивания винлок запускается и прописывает себя в AutoRun (Автозагрузку), (см. ниже про борьбу с напастью, вкратце: запущенный из-под ограниченной учётки винлок не сможет прописать себя в авторан куста HKLM, а только в пользовательский куст HKCU — почистить же пользовательский куст труда не составляет). Соответственно, после перезагрузки (а в последних версиях — прямо тут же), пользователь увидит перед собой этот баннер. Выключить его почти невозможно — он блокирует заветные сочетания Ctrl+Alt+Del (начиная с Висты, это сочетание обрабатывается ядром системы), Alt+F4, Winkey+R, а также завершает эксплорер путём подмены пути к нему в реестре на файл вируса. Последнее поколение винлоков вылезает даже в безопасном режиме, поэтому их удаление ещё более затруднено. Также, они могут представлять собой DLL-библиотеку, которая будет генерировать случайный exe-файл с этим самым винлоком.

Естественно, незнающий чайник с выпученными глазами побежит оплачивать выписанный счёт (теряя кучу денег), либо начнет звонить в Скорую компьютерную помощь (и опять-таки лишится пары тысяч деревянных), либо прибежит к знакомому компьютерщику (придётся потратиться на пузырь водки), причём бегать начнет сразу же — ибо дедлайн в 24 (2, 3, 5, 12) часа, написанный на баннере, после чего все файлы с компа пропадут.

Но изначально винлоки ориентированы на офисный планктон, так как вылезшее на весь экран (гей-)порно (в особо коварных модификациях винлок скачивает (гей-)порноролик, запускает, делает скриншот экрана и ставит обоями) вызывает тонны лулзов у коллег и ненужные вопросы у начальства — хомячок сделает

все что угодно, чтобы убрать эту мерзопакость с экрана.

Само собой, никто не гарантирует, что после отправки заветного СМС придет не менее заветный код. Но тем не менее, иногда-таки приходит, и некоторые винлоки имеют систему самоудаления с компьютера с подчищением всех хвостов. Кстати, хоть про удаление всех данных винлоки и привирают для убыстрения работы хомячкова нервного ганглия, однако зашифровать содержимое ФС вполне себе способны.

Путём многочасовой половой ебли на заражённых машинах выяснено, что некоторые модификации winlock'а прописывают значения, используя символы (буквы) из разных алфавитов! Пример: *C:\WINDOWS\system32\userinit.exe*, значение *\us**е**rinit.exe* написано с использованием православной кириллической Е. Посему, оптимальное решение — перезаписать ручками значения важных параметров! Однако новая версия антивируса Данилова (возможно, и другие антивирусы) полностью блокирует данные кусты реестра от редактирования (как пользователем, так и вирусами), конечно, если юзверь выставит соответствующие галки в настройках, которые по-обыкновению спрятаны в самые далёкие ебеня. После перезагрузки и входа в систему трояна можно удалить вручную по уже известному пути. Этот способ хоть и эффективен, но подходит только для опытных пользователей.

Обнаружено, что последние и самые совершенные модификации винлока действуют немного по-другому. Можно попасть на вирус, который НЕ меняет пути в реестре, а модифицирует непосредственно файлы explorer.exe и/или userinit.exe. Считается, что надо загрузить PE-систему типа ERD Commander или Alkid Live CD, найти у друга/подруги/кошки/соседа оригинальные файлы виндуза, снять с них хэш MD5, снять хэш со своих файлов (если манипуляции с реестром не принесли успеха). При несовпадении хэша есть смысл свои родные заменить на скопированные и принесенные от друга/подруги/кошки/соседа файлы. Опять же, не проверялось, есть ли разница в хеш-суммах при разных вариантах виндуза (наличие сервис паков, обновлений и т. д.). При наличии диска с дистрибутивом винды делаем команду `sfc /scannow`. Другого способа, кажется, больше нет. Впрочем, остаётся ещё незабвенная переустановка винды.

Как лечить?

Итак, %username%, внезапно ты включил комп и точно также внезапно узнал, что оказывается, ты смотришь гей-порнуху и теперь за это должен. Что делать? Знай: удалить винлок можно. Есть даже несколько разных способов на выбор.

- **Способ нулевой, неожиданный**: Некоторые вирусописатели прячут код разблокировки в середине стостраничного пользовательского соглашения, открывающегося по незаметной гиперссылке где-то в окне вируса. Рассчитывать на это, естественно, не стоит, а проверить нужно. В особо веселых случаях после ввода этого кода вирус полностью самоудаляется.

- **Способ первый, радикальный**: самый простой — переустановить Шindoшs ~~и форматнуть винты~~. Не стоит обращать внимание на уловки вирусописателей, BIOS они не удалят, файлы тоже. Но переустанавливать винду, если, конечно, ты не пользуешься portable-версиями программ — это та ещё еботня. Пользователей поумнее спасет заблаговременно выполненное резервное копирование (WIM, Acronis, Symantec Ghost и прочие), но большинству делать регулярный бэкап системного раздела лень, а хранить его на жестком диске не позволяет жаба. Еще вариант, при создании разделов на новом винте отформатировать небольшой кусок под операционку, а 95% оставшейся памяти — под все данные. В этом случае переустановка винды с форматированием одного маленького диска не будет вызывать никаких серьезных проблем с потерей музычки, кинца, рефератов и любимой порнухи.

  > Сюда же совершение локального виндекапца и переход на незагаженные ОСи. Берегись синдрома утёнка!

- **Способ второй, мануальный**. Заходим с безопасного режима (если висит и там, то быстро, решительно переходим к другому методу). Находим в реестре (run → regedit.exe) папки автозапуска и удаляем мерзопакость оттуда:
  1. Воспользоваться откатом системы.
  2. HKLM — software — microsoft — windows NT (для ХРюши) — current version — winlogon. Там смотрим значения Shell и Userinit. В Shell должна быть только строка Explorer.exe, в Userinit — C:\WINDOWS\system32\userinit.exe**,** (обязательно с запятой в конце).
  3. HKLM — Software — microsoft — windows — current version — run. Там смотрим строку Shell.
  4. HKLM — Software — microsoft — windows — current version — runonce. Некоторые пользуются веткой разового запуска, переписывая её каждый раз.
     - Сейчас вирус пользуется обоими путями. В шеле и юзерините будут прописаны пути к файлу вируса, удалите файлы, пропись в реестре к ним и, скорее всего, в комп вы попадёте. Проверьте папки, в которых находятся explorer.exe (WINDOWS) и userinit.exe (\WINDOWS\system32). Не исключено, что вирус создал там файлы с внешне таким же названием, но с кирилической буквой «е» в нем. Тогда ссылки в ветке winlogon внешне будут корректными. Затем подчищайте антивирусом систему.
     - После зачистки в свойствах безопасности вышеозначенных веток очищаете access-лист, заводите пользователя «Все», ставите галочку «Только на чтение», создаёте себе учётку, запрещаете ей изменять права на данный куст. Всё. С этого момента можно забыть про винлок

до конца своих дней и идти дальше разглядывать, как педобир сношает занзибарских младенцев.

- **Способ второй, мануальный, модифицированный, самый надёжный**. Никаких откатов не требуется. Если троян блокирует обычный безопасный режим, то при нажатии клавиши F8 необходимо выбрать безопасный режим с поддержкой командной строки. На данный момент времени большинство винлокеров не способны его заблокировать. После загрузки надо запустить редактор реестра при помощи команды regedit и искать там подозрительные записи. В первую очередь необходимо проверить ветку HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, в частности в параметре Shell должно быть написано explorer.exe**,** а в параметре Userinit — C:\WINDOWS\system32\userinit.exe**,** (обязательно с запятой). Если там всё в порядке, необходимо проверить этот же путь, но в ветке HKEY_CURRENT_USER. Также желательно проверить ветки, в которых прописаны автозагружаемые программы, например HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (и runonce). В случае обнаружения подозрительных записей, их необходимо заменить на стандартные значения (в случае с автозагрузкой удалить). Для надёжности можно вручную вбить explorer.exe и userinit.exe для уверенности, что ссылки корректны и ведут к нужным файлам. Также необходимо очистить папки C:\Windows\Temp, C:\Documents and Settings\%Username%\Local Settings\Temporary Internet Files, кеш Оперы и ФайерФокса и обратить внимание на папку C:\Documents and Settings\%Username%\Application data — в ней не должно быть никаких исполняемых файлов (exe, com, bat, cmd).
  Чтобы избежать вышеприведенной еботни с реестром, можно воспользоваться тем же ERD Commander'ом.

- **Способ третий, по-соседски** — чистим систему из другой системы.
  - Если на одном компе уже установлена не одна ОС (например, Linux + Windows, Windows + Hackintosh, Windows XP + Windows 7, Windows 7 + Windows 10), то убираете винлок, зайдя с другой системы.
  - Вынимаем свой жесткий диск и несем его к доброму другу со свежим антивирусом. Цепляемся к его компьютеру и при помощи антивируса чистим свой хард. Желательно проверить не одним антивирусом. Есть небольшая вероятность посадить заразу на компьютер доброго друга, так что надёжней использовать его компьютер для поддержки при других методах.
  - Через LiveCD, лучше на основе Windows. Исполняемые файлы вируса ищем обычным поиском по дате создания, записи в реестре трем руками. Все интересующие нас ветки лежат в Windows\System32\config и подгружаются в виде куста в обычный RegEdit из командной строки. Можно использовать и линукс без установки, но при этом придется (если повезет, то недолго) шариться по пользовательским папкам и вручную выгребать авгиевы конюшни кэша браузера и т. п. При относительно прямых руках вся процедура лечения занимает минут 15. Процесс может упростить/ускорить применение бесплатной утилиты Autoruns (бывший Sysinternals, теперь Microsoft). Тулза позволяет редактировать ключи автозапуска, в том числе и в офлайн-системе.
  - Автоматизированный вариант — идем сюда, качаем образ для домашнего использования AntiWinLockerLiveCD, записываем на болванку, загружаем и радуемся жизни.
  - По сети. Для исполнения этого метода надо провести предварительную подготовку, а именно создать пользователя с паролем и админскими правами (можно просто нарезать пароль пользователю «Админ»). Ну и заиметь локальную сеть с кем-нибудь. После получения вируса идем к доброму соседу, открываем командную строку и пользуем команды tasklist и taskkill, для начала запустить их с ключом «/?», чтобы лицезреть справку и (при наличии некоторого количества серого вещества) понять, как их запустить на своем больном компе, и выпилить нахрен вирус из списка запущенных процессов. Дальше — антивирус и чистка реестра уже у себя дома.
  - В случае, если вирус модифицирует непосредственно файлы explorer.exe и/или userinit.exe, находим оригинальные пригодные для системы и заменяем их в соответствующих папках. Для этого можно взять эти файлы с другого компьютера с такой же системой, скачать из интернета или извлечь их из установочного диска системы. У Windows XP они вместе с другими хранятся в папке i386 с расширениями с замененной последней буквой (в сжатом виде, распаковывается программой extrac32, лежащей там же). У Windows Vista, Windows 7, Windows 8/8.1 и Windows 10 в архиве install.wim в папке sources. Надобность в подобном варианте определяется по отсутствию подозрительных ссылок в вышеописанных ветках реестра. В качестве предварительного контроля можно зайти в соответствующие папки и проверить размер файлов и их дату.

- **Четвёртый способ** — создать любой документ — в блокноте, Ворде, пэйнте, да чём угодно; внести в него пару изменений а затем — нажать на компе или клавиатуре кнопку Power. Начнётся выключение компа, часть процессов завершится — в том числе и Винлок, однако, созданный нами документ не закроется, а выдаст окно: «сохранить изменения? — да, нет, отмена». Жмём отмена, что заодно означает отмену выключения компа. Итог: винлок завершён, комп работает. Можно спокойно править системные файлы. Увы, в последних версиях вируса способ может не сработать.

- **Пятый способ** — записываем на бумажку, чего возжелало неумолимое поделие (какую и куда отправлять смс, на какой номер положить деньги etc), бежим к ближайшему здоровому ПК с интернетом, заходим на страничку поиска кодов разблокировки от Dr. Web или от Касперского.

Читаем, вставляем, вводим, ищем картинку со «своим» винлоком, получаем с сайта код разблокировки. Радостно бежим домой. Вводим. Облегчённо вздыхаем. Если получилось не облегчённо, а обречённо, значит, вы гордый первооткрыватель нового штамма сифилиса, и, скорее всего, разблокировка кодом вообще не предусмотрена, чистый развод.

- **Способ шестой, телефонно-матершинный:**
  1. Звоним оператору сотовой связи и при помощи длительной эмоциональной и щедро сдобренной матом речи выясняем, какому провайдеру принадлежит короткий номер, на который просят отправить.
  2. Пишем этому самому провайдеру гневное послание — мол, ваши действия квалифицируются как сговор с мошенниками, содействие вредителям и т. д., — блокировка компьютеров нашего предприятия нанесла нам материальный ущерб, и мы намерены обращаться в полицию, прокуратуру и суд по месту регистрации фирмы-провайдера.
  3. Через час получаем звонок от милой барышни из провайдера с извинениями и продиктованным кодом разблокировки.
  4. Делаем некоторые выводы об «отсутствии» каких-либо связей между мошенниками и провайдером.
  5. После разблокировки все же вычищаем говно при помощи калёного антивируса.

- **Седьмой способ** — ребут, и по загрузке системы СРАЗУ ЖЕ открываем «Диспетчер задач». Можно заранее установить альтернативный диспетчер задач Process Explorer, который чаще всего неизвестен винлокерам. Поскольку винлок грузится не моментально, то будет 2-3 секунды на то, чтобы пробежать список запущенных приложений и найти подозрительный процесс (что-нибудь вроде Win.exe, запущенный не под SYSTEM, а под %USERNAME%). Затем винлок наконец включается и блокирует диспетчер задач. Снова ребут, снова сразу же открываем диспетчер задач, и держим один палец на клавише с первой буквой названия процесса, второй — на Del, третий на Enter. Непрерывно долбим кнопку с первой буквой названия процесса, чтобы как только винлок начинает грузиться, строка с названием его процесса стала активной. Дальше быстро жмем Del и Enter, убивая процесс не дожидаясь его полной загрузки. Если не получилось, а с первой попытки скорее всего и не получится, ребут и снова повторяем те же манипуляции. Можно просто зажать клавишу Shift при загрузке Винды — все процессы пользователя в автозапуске по ветке Run не запустятся! *(спойлер:* К сожалению, начиная с Windows Vista данный способ больше не работает. При нажатии и удержании клавиши Shift во время запуска Windows Vista, Windows 7 и более поздних версий Windows процессы в автозапуске (в том числе и винлок) по-прежнему продолжают запускаться. Как следствие, под Вистой, Семёркой, Восьмёркой и Десяткой удаление винлока ещё более затруднено по сравнению с Windows XP.*)* Чем больше процессов стартует при запуске системы, тем легче успеть выпилить винлок. Если в компе стоит несколько плашек оперативы, то можно облегчить себе задачу, оставив только самую малоемкую плашку и вытащив все остальные. После отключения винлока переключаемся в диспетчере задач на вкладку «Приложения», жмём «Новая задача» и вбиваем **explorer.exe**. Дальше ручками сносим винлок из автозагрузки (какие ключи проверять уже написано выше), палим его местонахождение и удаляем, после чего для пущего спокойствия сканируем ПК антивирусом.

- **Восьмой способ** — для тех локеров, которые прописывают себя в MBR. Нужен загрузочный диск той самой винды — грузимся с него, заходим в консоль восстановления и пишем команду fixmbr, нажимаем Y, нажимаем Enter. Всё, перезагружаемся, радуемся. Если у Вас Vista и старше — нужна утилита bootsect.exe (входит в WAIK) — грузимся с загрузочного диска и вводим в командную строку:

```
bootsect /nt60 c: – восстанавливаем загрузчик Vista и выше.
bootsect /nt52 c: – восстанавливаем загрузчик XP.
```

- **Девятый способ** — купить болванку и записать rescue disc Кашпировского или доктора Паука, вставить и проверить ПК. К некоторым иногда можно применить отключение питания компьютера, но новых этим не обманешь.

  У Каспера в составе Kaspersky Rescue Disk есть утилита разблокировки (сама лечит реестр, заменяет повреждённые системные файлы на новые), которая запускается командой windowsunlocker из терминала. Каспер также предлагает залить свое поделие на флэшечку, чтобы можно было загрузиться с нее на случай судного дня.

- **Десятый способ** — попробуйте нажать Ctrl+Alt+Del (Ctrl+Shift+Esc). Часть локеров его не блокирует. Если удалось, попробуйте сменить пользователя — при перезапуске винлок самоубивается. Как вариант: найти на вкладке «процессы» процесс Explorer.exe и завершите его. На предупреждение венды о том, что завершение какого-то процесса вызовет ёбаный пиздец, ответьте положительно (нажмите ДА), после чего, не закрывая диспетчер задач, идём по такому пути: файл -> Новая задача (выполнить…). Вводим слово «Explorer», жмём Enter. Теперь компьютер свободен от баннера. Далее следует выполнить откат к более раннему состоянию системы. Ну, и не помешает, конечно же, прочистить свой ПК антивирусным ПО.

  Можно попробовать еще комбинацию Win+U. Она имеет высокий приоритет, и большинство локеров ее не блокирует. Откроется окошко специальных возможностей. Там тыркаем помощь, дальше на сайт поддержки Microsoft, и, если локер не очень крут, откроется браузер. Скачиваем диспетчер задач, убиваем локер и чистим реестр.

Профилактика

Чтобы раз и навсегда забыть про веселый баннер или по крайней мере свести шансы его появления к минимуму, нужно соблюдать простые правила:

- В качестве превентивных мер начни с повседневной работы в винде под юзером с ограниченными правами, а не под админом — признай уже, ты никакой не профессионал и не спец в компах и уследить за всем всё равно не сможешь, да и админские права каждый день ни к чему. Кажущееся неудобство — глупость: так, виста и семёрка практически на любое действие, требующее повышенных прав, научились запрашивать логин/пароль админа. В XP можно использовать «запуск от имени», сидя в админской учётке (то есть explorer с правами админа уже есть, остальное запускаем с правами пользователя), а лучше сидеть в ограниченной и запускать от имени администратора только те программы, которые этого действительно требуют. В семёрке же надо отключить говноUAC и сидеть в учётке «обычный доступ», ибо с отключённым UAC винлок запустится с правами пользователя. Почему поможет? Потому что криворукие пионерские поделки, называемые винлоками, прописывают себя в авторан в кусте реестра HKLM, в папки windows, system32, program files, а также меняют системные файлы. Ко всем этим ресурсам учётная запись обычного пользователя не имеет прав на запись, изменение, удаление — таким образом, винлок, запустившийся под пользователем с ограниченными правами, просто не сможет ничего сделать с твоей системой.

- Учётке админа задай пароль позаковыристей, чтобы винлок с зайчатками интеллекта не смог за две минуты подобрать его тупым перебором. Это главное!

- Только после понижения прав своей учётке и задания пароля админу имеет смысл использовать Firefox с дополнением NoScript (или иной браузер с параноидальными аддонами) — в настройках браузера выставь вычищение кэша после сеанса, запрещать исполнение файлов из временных папок браузера и т. д.

- Можно заранее запастись LiveCD (LiveUSB). Скачать его можно на любом торренте (но лучше на проверенном, а то какой-нибудь другой троян уже будет ждать тебя внутри). Про LiveCD можно всё прочитать в интернете: как лечить и как чинить. Ещё лучше — запастись всякими аварийными виндоуз-коммандерами, они чуть попроще в исполнении.

- После установки винды спрячь установочный диск в коробку и всегда держи его под рукой: при помощи родного образа и опыта работы с командной строкой можно легко починить покорёженную винлоком систему путём замены жизненно важных файлов на исходные. По этой же причине стоит раз и навсегда забыть про сборки: кривую пионерскую поделку реанимировать куда труднее, чем оригинальную систему.

- Не забывай хотя бы раз в месяц создавать контрольную точку восстановления, чтобы после песца локального значения не почувствовать себя Марти МакФлаем, откатив систему на полгода-год назад (или не имея возможности откатить вообще).

- Также подойдёт старый способ, хорошо защищающий и от троянов: запускать любой подозрительный софт — кейгены, кряки, обнулители триала, etc — под виртуальным ПК (подойдёт любая программа, хоть бы и тот же VirtualBox). При этом от винлока пострадает только виртуальная ось, которую легко можно реанимировать средствами оболочки виртуального ПК. Алсо, некоторые шифровщики научились детектить то, что они в виртуальной системе и поэтому не будут показывать разрушительные действия будучи запущенными под виртуалкой.

- От троянов-шифровальщиков защитит только резервное копирование на внешний диск. Также, можно запретить запись в файлы подозрительным программам. Еще можно запретить выход в сеть, и троян скорее всего не будет шифровать файлы (ключ он не сможет передать на сервер ублюдков-вымогателей). Но есть и хитрожопые трояны — они внедряют код в доверенный процесс, доверенный для системы предотвращения вторжений, то есть для HIPS (например, создает поток в процессе explorer.exe), после этого процесс explorer.exe весело бегает по всему диску шифруя всё, что можно. И ничего не заметишь, видимых окон у ебаной троянской программы нет.

Есть хорошая и плохая новость. Хорошая — лаборатория касперского заявляет, что компонент «Мониторинг активности» в их антивирусе обнаруживает, что ебаный троян шифрует файлы, и грохает его, а потом из резервных копий восстанавливает файлы (до того, как файл зашифрован, создается копия).

Доктор веб тоже это умеет (превентивная защита). Также у Доктор веба есть охуенная защита от потери данных.

Плохая новость — ебаный шифровальщик, используя новый алгоритм, может обойти защиту (алгоритмы для обнаружения шифровальщиков, заложенные в HIPS), крутые антивирусы ничего не заметят и все файлы будут зашифрованы. Но если стоял Доктор веб, и была включена Защита от потери данных — все файлы будут восстановлены.

Винлокер и спермерка

Прописывание винлокера в кусте реестра HKLM на Win 7 не принесет результата, так как shell грузится из локальной записи пользователя. Для тех, у кого семерка не starter и есть возможность создания второго пользователя, можно заблаговременно сделать второго админа и при подхвате заразы просто зайти под ним и вычистить комп или удалить зараженного пользователя вместе с его файлами и создать еще одного. Этот способ работает и на хрюше, так как в последнее время быдлокодеры перешли исключительно на прописывание запуска только в профайле, а не в общем HKLM-кусте.

Примеры кривых пионерских поделок

















См. также

- SMS-лохотрон
- BSOD
- Винлок — это не только троян!

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель

Профит

$регистрация 1000 мелочей 2 в 1 25-й кадр Bitcoin Biz By design Deadline Embrace, extend and extinguish Enlarge your penis Extreme Advertising Fine print Forex HYIP Kirby Kontora Lockerz.com Made in China Opulence, I has it Product placement QNet SAP Second-hand SEO SMS-лохотрон SMS-шпион The Asylum Wazzup Роман Абрамович Автошкола Акция Алексей Бабушкин Алименты Амеро Бабло БАДы Баянист Тамада Услуги Березовский Бизнес-пакеты Биокатализатор топлива Биржа Благотворительность Блат Бобби Котик Брачный аферизм Бренд Букмекерская контора Буржуй Бутик Быдлодевайс Быстро, качественно, недорого Вазелин Вахтовый метод Вентиляторный завод Видеокурсы Виктор Петрик Винлок Вирусный маркетинг Волшебная таблетка Всемирная история, банк «Империал» Выборы Генномодифицированная вода Гешефт Глобальное потепление Голливуд Гомеопатия Горд Грабовой Дисбактериоз Дойная корова Дональд Трамп Донат Ебай Залогово-кредитный аукцион Заработок в интернете Звёздные войны Звонилка Золото Игровые автоматы ИКЕА Иммуномодулятор Иннова Интернет-магазин Кадровые агентства Карательная психиатрия Кардинг Карликовое государство Кликбейт Копираст Коробка из-под ксерокса Корпоративная культура Красная ртуть Кредит Лёгкий голод Лас-Вегас Литрес Лох Лохотрон Лохоугадайка Макдоналдс

w:Trojan.Winlock