

«Практическая работа: *Лабораторная работа №1 Изучение путей распространения и форм проявления компьютерных вирусов*»

Выполнили:

студент группы 1ИСП11-18

Белякова А.А.

Ищенко Т.С.

Проверил:

Возвахов Д.А.

Москва

2022

**Цель работы и содержание:** изучить пути распространения и формы проявление компьютерных вирусов.

**Trojan Winlock**

Баннеры «Windows заблокирован — для разблокировки отправьте СМС» и их многочисленные вариации безмерно любят ограничивать права доступа вольных пользователей ОС Windows. При этом зачастую стандартные способы выхода из неприятной ситуации – корректировка проблемы из Безопасного режима, коды разблокировки на сайтах ESET и DR Web, как и перенос времени на часах BIOS в будущее далеко не всегда срабатывают.

**Пути распространения Trojan.Winlock**

В большинстве случаев заражение происходит в связи с уязвимостью браузера. Зона риска – все те же “взрослые” ресурсы. Классический вариант заражения – юбилейный посетитель с ценным призом. Еще один традиционный путь инфицирования – программы, маскирующиеся под авторитетные инсталляторы, самораспаковывающиеся архивы, обновления – Adobe Flash и пр. Интерфейс троянов красочен и разнообразен, традиционно используется техника маскировки под окна антивирусной программы, реже — анимация и др.

**Вредные привычки Trojan.Winlock**

Для обеспечения распространения и автозапуска вирусы семейства Trojan.Winlock модифицируют ключи реестра:  
  
-[...\Software\Microsoft\Windows\CurrentVersion\Run] 'svhost' = '%APPDATA%\svhost\svhost.exe'  
-[...\Software\Microsoft\Windows\CurrentVersion\Run] 'winlogon.exe' = '<SYSTEM 32>\winlogon.exe'  
  
С целью затруднения обнаружения в системе вирус блокирует отображение срытых файлов, создает и запускает на исполнение:

* %APPDATA%\svhost\svhost.exe

Запускает на исполнение:

* <SYSTEM 32>\winlogon.exe
* %WINDIR%\explorer.exe
* <SYSTEM 32>\cmd.exe /c """%TEMP%\uAJZN.bat"" "
* <SYSTEM 32>\reg.exe ADD «HKCU\Software\Microsoft\Windows\CurrentVersion\Run» /v «svhost» /t REG\_SZ /d "%APPDATA%\svhost\svhost.exe" /f

Завершает или пытается завершить системный процесс:

* %WINDIR%\Explorer.EXE

Вносит изменения в файловую систему:  
  
Создает следующие файлы:

* %APPDATA%\svhost\svhost.exe
* %TEMP%\uAJZN.bat

Присваивает атрибут 'скрытый' для файлов:

* %APPDATA%\svhost\svhost.exe

Ищет окна:

* ClassName: 'Shell\_TrayWnd' WindowName: ''
* ClassName: 'Indicator' WindowName: ''

**Лечение. Способ 1.** Поиск нужного кода разблокировки по изображению в базе данных сервиса Dr.Web

На другой странице сайта авторы представили еще один вариант выбора — готовую базу кодов разблокировки для распространенных версий Trojan.Winlock, классифицируемых по изображениям.

Аналогичный сервис поиска кодов представлен антивирусной студией ESET, где собрана база из почти 400 000 тысяч вариантов кодов разблокировки и лабораторией Касперского, предложившей не только доступ к базе кодов, но и собственную лечащую утилиту — Kaspersky WindowsUnlocker.

**Лечение. Способ 2.** Утилиты – разблокировщики.

Сплошь и рядом встречаются ситуации, когда из-за активности вируса или сбоя системы Безопасный режим с поддержкой командной строки, позволяющий провести необходимые оперативные манипуляции оказывается недоступным, а откат системы по каким-то причинам также оказывается невозможным. В таких случаях Устранение неполадок компьютера и Диск восстановления Windows оказываются бесполезны, и приходится задействовать возможности восстановления с Live CD.

Для разрешения ситуации рекомендуется использовать специализированную лечащую утилиту, образ которой потребуется загрузить с компакт диска или USB-накопителя. Для этого соответствующая возможность загрузки должна быть предусмотрена в BIOS. После того, как загрузочному диску с образом в настройках БИОС будет задан высший приоритет, первыми смогут загрузиться CD-диск или флэшка с образом лечащей утилиты.

В общем случае зайти в БИОС на ноутбуке чаще всего удается при помощи клавиши F2, на ПК – DEL/DELETE, но клавиши и их сочетания для входа могут отличаться (F1, F8, реже F10, F12…, сочетания клавиш Ctrl+Esc, Ctrl+Ins, Ctrl+Alt, Ctrl+Alt+Esc и др.). Узнать сочетание клавиш для входа можно, отслеживая текстовую информацию в нижней левой области экрана в первые секунды входа. Подробнее о настройках и возможностях BIOS различных версий можно узнать здесь.

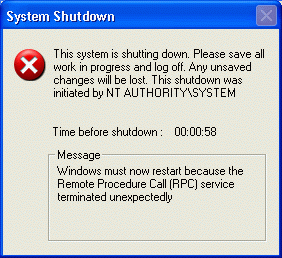
Поскольку работу мышки поддерживают только поздние версии BIOS, перемещаться вверх и вниз по меню вероятнее всего придется при помощи стрелок “вверх” – “вниз”, кнопок “+” “–“, ”F5” и ”F6”.

**«Lovesan», «Lovsan», «Blaster», «Msblast», «Poza»**

Все эти имена относятся к одной вредоносной программе, но используются разными антивирусными компаниями. В терминологии «Лаборатории Касперского» этот червь называется «Lovesan». На данный момент известны три модификации червя, которым некоторыми разработчиками присвоены индексы «a», «b» и «c».

**Признаками заражения компьютера являются:**

* Наличие файлов «MSBLAST.EXE», «TEEKIDS.EXE» или «PENIS32.EXE» в системном каталоге Windows (обычно WINDOWSSYSTEM32)
* Внезапная перезагрузка компьютера после соединения с интернетом каждые несколько минут
* Многочисленные сбои в работе программ Word, Excel и Outlook
* Сообщения об ошибках, вызванных файлом «SVCHOST.EXE»
* Появление на экране окна с сообщением об ошибке (RPC Service Failing)



«Lovesan» не несет существенной опасности непосредственно для зараженного компьютера. Червь не удаляет, не изменяет и не похищает данные. Его угроза состоит в нарушении нормальной работы интернета в целом, что происходит из-за перегрузки каналов передачи данных рассылкой вирусного кода. Кроме того, начиная с 16 августа «Lovesan» атакует web-сайт windowsupdate.com, на котором содержатся обновления для операционной системы Windows. В результате этого web-сайт может выйти из строя, и пользователи окажутся отрезанными от этой важной информации.

**Уязвимые ОС**

Червь заражает компьютеры под управлением Windows NT, Windows 2000, Windows XP. Полный список уязвимых операционных систем приведен ниже:

* Windows NT 4.0 Server
* Windows NT 4.0 Terminal Server Edition
* Windows 2000
* Windows XP 32 bit Edition
* Windows XP 64 bit Edition
* Windows Server 2003 32 bit Edition
* Windows Server 2003 64 bit Edition

**Защита**

Существует несколько способов защиты от «Lovesan». Во-первых, необходимо загрузить последние обновления антивируса и ни в коем случае не отключать антивирусный монитор во время работы с интернетом. Во-вторых, используйте межсетевой экран (firewall) для блокировки портов 135, 69 и 4444. Наконец, установите обновление для Windows, закрывающее брешь, через которую «Lovesan» проникает на компьютеры. Последний способ является наиболее эффективным, поскольку предотвращает заражение не только «Lovesan», но также всеми его разновидностями и другими подобными червями, использующими описанную брешь Windows.

**Что такое межсетевой экран и где его взять?**

Межсетевой экран (англ. Firewall) — это специальная программа, которая защищает от хакерских атак, контролируя потоки данных между интернетом и компьютером. Она допускает только безопасные соединения с сетью, фильтрует вредоносные пакеты данных и предотвращает доступ в интернет неавторизованных приложений.

Существуют два типа межсетевых экранов: для защиты сетей и рабочих станций. Для защиты домашних компьютеров мы рекомендуем воспользоваться Kaspersky Anti-Hacker.

**Не могу загрузить обновление с сайта Microsoft — компьютер постоянно перегружается.**

Внезапная перезагрузка компьютера — одно из проявлений «Lovesan». Для обеспечения передачи обновления с сайта Microsoft мы рекомендуем найти файл TFTP.EXE (в системном каталоге Windows, обычно WINDOWSSYSTEM32, и скрытом каталоге WINDOWSSYSTEM32DLLCACHE) и переименовать его. После окончания загрузки и установки обновления можно вернуть файлу оригинальное название.

**Что мне делать, если вирус уже заразил мой компьютер?**

Для этого достаточно использовать установленный на вашем компьютере антивирус. Перед этим убедитесь, что антивирус содержит последние обновления базы данных.

Также вы можете воспользоваться бесплатной утилитой для защиты от «Lovesan», предлагаемой «Лабораторией Касперского». Данная программа обнаруживает активную копию червя в памяти компьютера, деактивирует ее, удаляет зараженные файлы с жесткого и сетевых дисков, восстанавливает системный реестр Windows. После завершения работы утилиты перезагрузите компьютер и запустите антивирусный сканер с последними обновлениями базы данных.

**Virus.Win9x.CIH**

|  |  |
| --- | --- |
| Дата обнаружения | **20/11/2002** |
| Класс | [Virus](https://threats.kaspersky.com/ru/class/Virus/) |
| Платформа | [Win9x](https://threats.kaspersky.com/ru/platform/Win9x/) |
| Описание | Technical Details Также известен как “Чернобыль”. Резидентный вирус, работает только под Windows95/98 и заражает PE-файлы (Portable Executable). Имеет довольно небольшую длину – около 1Кб. Был обнаружен “в живом виде” на Тайване в июне 1998 – автор вируса заразил компьютеры в местном университете, где он (автор вируса) в то время проходил обучение. Через некоторое время зараженные файлы были (случайно?) разосланы в местные Интернет-конференции, и вирус выбрался за пределы Тайваня: за последующую неделю вирусные эпидемии были зарегистрированы в Австрии, Австралии, Израиле и Великобритании. Затем вирус был обнаружен и в нескольких других странах, включая Россию.  Примерно через месяц зараженные файлы были обнаружены на нескольких американских Web-серверах, распространяющих игровые программы. Этот факт, видимо, и послужил причиной последовавшей глобальной вирусной эпидемии. 26 апреля 1999 года (примерно через год после появления вируса) сработала “логическая бомба”, заложенная в его код. По различным оценкам, в этот день по всему миру пострадало около полумиллиона компьютеров – у них оказались уничтожены данные на жестком диске, а на некоторых плюс к тому испорчено содержимое микросхем BIOS на материнских платах. Данный инцидент стал настоящей компьютерной катастрофой – вирусные эпидемии и их последствия никогда до того не были столь масштабными и не приносили таких убытков.  Видимо, по тем причинам, что 1) вирус нес реальную угрозу компьютерам во всем мире и 2) дата срабатывания вируса (26 апреля) совпадает с датой аварии на Чернобыльской атомной электростанции, вирус получил свое второе имя – “Чернобыль” (Chernobyl).  Автор вируса, скорее всего, никак не связывал Чернобыльскую трагедию со своим вирусом и поставил дату срабатывания “бомбы” на 26 апреля по совсем другой причине: именно 26 апреля в 1998 году он выпустил первую версию своего вируса (которая, кстати, так и не вышла за пределы Тайваня) – 26 апреля вирус “CIH” отмечает подобным образом свой “день рождения”. Как вирус работает При запуске зараженного файла вирус инсталлирует свой код в память Windows, перехватывает обращения к файлам и при открытии PE EXE-файлов записывает в них свою копию. Содержит ошибки и в некоторых случаях завешивает систему при запуске зараженных файлов. В зависимости от текущей даты стирает Flash BIOS и содержимое дисков.  Запись в Flash BIOS возможна только на соответсвующих типах материнских плат и при разрешающей установке соответственного переключателя. Этот переключатель обычно установлен в положение “только чтение”, однако это справедливо не для всех производителей компьютеров. К сожалению Flash BIOS на некоторых современных материнских платах не может быть защищена переключателем: одни из них разрешают запись в Flash при любом положении переключателя, на других защита записи в Flash может быть отменена программно.  После успешного стирания Flash-памяти вирус переходит к другой деструктивной процедуре: стирает информацию на всех установленных винчестерах. При этом вирус использует прямой доступ к данным на диске и тем самым обходит встроенную в BIOS стандартную антивирусную защиту от записи в загрузочные сектора.  Известно три основные (“авторские”) версии вируса. Они достаточно похожи друг на друга и отличаются лишь незначительными деталями кода в различных подпрограммах. Версии вируса имеют различные длины, строки текста и дату срабатывания процедуры стирания дисков и Flash BIOS:    Длина Текст Дата срабатывания Обнаружен “в живом виде”  1003 CIH 1.2 TTIT 26 апреля Да  1010 CIH 1.3 TTIT 26 апреля Нет  1019 CIH 1.4 TATUNG 26 каждого месяца Да – во многих странах Технические детали При заражении файлов вирус ищет в них “дыры” (блоки неспользуемых данных) и записывает в них свой код. Присутствие таких “дыр” обусловлено структурой PE-файлов: позиция каждой секции в файле выравнена на определенное значение, указанное в PE-заголовке, и в большинстве случаев между концом предыдущей секции и началом последующей есть некоторое количество байт, которые не используются программой. Вирус ищет в файле такие неиспользуемые блоки, записывает в них свой код и увеличивает на необходимое значение размер модифицированной секции. Размер заражаемых файлов при этом не увеличивается.  Если в конце какой-либо секции присутствует “дыра” достаточного размера, вирус записывает в нее свой код одним блоком. Если же такой “дыры” нет, вирус дробит свой код на блоки и записывает их в конец различных секций файла. Таким образом, код вируса в зараженных файлах может быть обнаружен и как единый блок кода, и как несколько несвязанных между собой блоков.  Вирус также ищет неиспользуемый блок данных в PE-заголовке. Если в конце заголовка есть “дыра” размером не менее 184 байт, вирус записывает в нее свою startup-процедуру. Затем вирус изменяет стартовый адрес файла: записывает в нее адрес своей startup-процедуры. В результате такого приема структура файла становится достаточно нестандартной: адрес стартовой процедуры программы указывает не в какую-либо секцию файла, а за пределы загружаемого модуля – в заголовок файла. Однако Windows95 не обращает внимания на такие “странные” файлы, грузит в память заголовок файла, затем все секции и передает управление на указанный в заголовке адрес – на startup-прецедуру вируса в PE-заголовке.  Получив управление, startup-процедура вируса выделяет блок памяти VMM-вызовом PageAllocate, копирует туда свой код, затем определяет адреса остальных блоков кода вируса (расположенных в конце секций) и дописывает их к коду своей startup-процедуры. Затем вирус перехватывает IFS API и возвращает управление программе-носителю.  С точки зрения операционной системы эта процедура наиболее интересна в вирусе: после того, как вирус скопировал свой код в новый блок памяти и передал туда управление, код вируса исполняется как приложение Ring0, и вирус в состоянии перехватить AFS API (это невозможно для программ, выполняемых в Ring3).  Перехватчик IFS API обрабатывает только одну функцию – открытие файлов. Если открывается файл с расширением EXE, вирус проверяет его внутренний формат и записывает в файл свой код. После заражения вирус проверяет системную дату и вызывает процедуру стирания Flash BIOS и секторов диска (см. выше).  При стирании Flash BIOS вирус использует соответствующие порты чтения/записи, при стирании секторов дисков вирус вызывает VxD-функцию прямого обращения к дискам IOS\_SendCommand. Известные варианты вируса Автор вируса не только выпустил копии зараженных файлов “на свободу”, но и разослал исходные ассемблерные тексты вируса. Это привело к тому, что эти тексты были откорректированы, откомпилированы и вскоре появились модификации вируса, имевшие различные длины, однако по функциональности они все соответствовали своему “родителю”. В некоторых вариантах вируса была изменена дата срабатывания “бомбы”, либо этот участок вообще никогда не вызывался.  Известно также об “оригинальных” версиях вируса, срабатывающих в дни, отличные от 26 [апреля]. Данный факт объясняется тем, что проверка даты в коде вируса происходит по двум константам. Естественно, что для того, чтобы поставить таймер “бомбы” на любой заданный день, достаточно поменять лишь два байта в коде вируса. |

**Контрольные вопросы**

**1.** Где можно взять описание работы компьютерных вирусов (конкретные примеры)?

<https://vms.drweb.ru/search/>

<https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html>

[htt http://www.securelist.com/ru/descriptions http://www.kaspersky.ru/rss/technews http://www.securitylab.ru/\_Services/Export/RSS/ http://www.viruslist.com/ru/rss/latestvirusdescriptions http://www.viruslist.com/ru/rss/virusalerts http://www.viruslist.com/ru/rss/latestnews http://news.drweb.com/list/?c=10 http://www.kaspersky.com/viruswatch3ps://www.virustotal.com/gui/home/upload](https://www.virustotal.com/gui/home/upload)

**2.** Какие есть пути распространения компьютерных вирусов ?

* **Письма со спамом** - Авторы вредоносных программ часто пытаются обманным умыслом скачать вредоносные файлы. Это может быть письмо с вложенным файлом, который описывается как уведомление о доставке, возврат налогового платежа или счет по купленному билету. В письме может быть сказано, что необходимо открыть вложение, чтобы получить отправление или деньги.
* **Вредоносные Office макрос** - Microsoft Office включает в себя мощный язык сценариев, позволяющий разработчикам создавать дополнительные инструменты, которые помогут вам работать продуктивнее. К сожалению, злоумышленники также могут использовать этот язык для создания вредоносных сценариев, которые устанавливают вредоносные программы или делают другие плохие вещи.
* **Зараженные съемные носители** - Многие вредоносные программы распространяются, заражая съемные носители, такие как USB-устройства флэш-памяти или внешние жесткие диски. Вредоносная программа может автоматически установиться при подключении зараженного носителя к компьютеру
* **Вместе с другим программным обеспечением** - Некоторые вредоносные программы могут устанавливаться одновременно с другими скачанными программами. К таким программам относится программное обеспечение со сторонних веб-сайтов или файлы, передаваемые через одноранговые сети.
* **Взломанные или скомпрометированные веб-страницы** - Вредоносные программы могут использовать известные программные уязвимости для заражения компьютера. Уязвимость — это брешь в программном обеспечении, через которую вредоносные программы могут получить доступ к компьютеру.
* **Другие вредоносные программы** - Некоторые типы вредоносных программ могут загружать на компьютер другие угрозы. После установки этих угроз на компьютере они продолжат загружать дополнительные угрозы.

**3.** Какие есть формы проявления компьютерных вирусов?

* **Черви — Worm.** Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.
* **Вирусы-маскировщики — Rootkit**. Эти вирусы используются для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.
* **Вирусы – шпионы — Spyware.** Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация — адреса, пароли, данные кредитных карт).
* **Зомби — Zombie**. Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть —бот-нет) и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может даже не догадываться, что его компьютер зомбирован и используется злоумышленником.
* **Рекламные вирусы — Adware**. Программы-рекламы, без ведома пользователей встраиваются в различное программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.
* **Вирусы – блокировщики — Winlock**. Такие программы блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно, в котором пользователя обвиняют в скачивании нелицензионного контента или нарушении авторских прав.  И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или пополнить его счет. Естественно, после перевода денег на счет злоумышленника, баннер никуда не пропадает.
* **Троянские вирусы — Trojan**. Троянская программа является самым опасным типом вирусов, так как она маскируется в других безвредных программах. И до того момента как пользователь не запустит эту самую безвредную программу, троян не несет никакой опасности и обнаружить его нелегко. Троянская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления личных данных пользователя. Отличительной особенностью вируса-трояна является то, что он не может самостоятельно размножаться.

**4.** Какие формы проявления компьютерных вирусов наиболее незаметны для пользователя?

* Вирус загрузочного сектора
* Вирус перезаписи
* Полиморфный вирус
* Червь
* Троян