

***Избавление от
тroyанов-вымогателей
и разблокировка
Windows***

Борисов В.А.

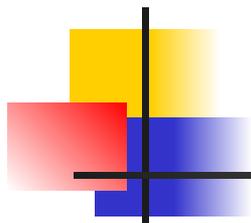
КАСК – филиал ФГБОУ ВПО РАНХ и ГС

Красноармейск 2013 г.

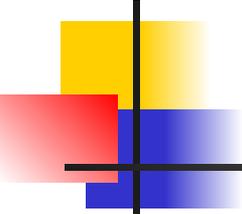


Оглавление

- Голыми руками
- Простые меры
- Хитростью
- По старинке
- Операция
- Борьба на ранней стадии
- Отвертка
- Общие правила безопасности



Голыми руками

- 
-
- Для некоторых троянов действительно существует код разблокировки.
 - В редких случаях они даже честно удаляют себя полностью после ввода верного кода.
 - Узнать его можно на соответствующих разделах сайтов антивирусных компаний.

Сервис разблокировки Windows компании «Доктор Веб»

Dr.WEB® Антивирус

Для дома Для бизнеса Скачать Магазин Поддержка Обучение Партнеры

Поиск по номеру
Поиск по изображению

Настроить вывод результатов

Количество элементов на странице: 10

Показать номера кошельков/телефонов:

Скрыть вирусы, для которых нет кода разблокировки:

[Обновить](#)

Рассказать о сервисе друзьям:

[B](#) [f](#) [t](#) [g+](#) [v](#) [e](#) [+](#) [45](#)

- Инструкция по разблокировке Windows
- Пришлите код разблокировки
- ИМХО
- Ты можешь помочь
- Правовой уголок
- Горячая лента угроз
- Бесплатная лечащая утилита Dr.Web CureIt!
Даже если систему удалось разблокировать, необходимо удалить из нее следы пребывания троянца. Это можно сделать с помощью Dr.Web CureIt!

Сервис разблокировки компьютеров

Введите номер кошелька/телефона

9179525609

Искать коды

Результаты поиска для кошелька/телефона № 9179525609

Trojan.Winlock.2741

Коды разблокировки:

- 16342131
- 70000004

Trojan.Winlock.3256

Коды разблокировки:

- 99885522

Сервис разблокировки Windows компании «Лаборатория Касперского»



Deblocker

Удаление баннера с рабочего стола, разблокировка Windows

3649

Например, 9051234567 или 7015:wowdl70 (смс на короткий номер)

[Как искать?](#)

Коды разблокировки для 3649:



2548125

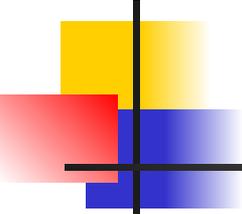


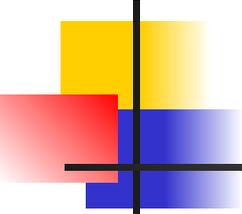
himydarling
159753789

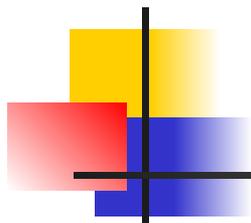


Выполните следующие действия:

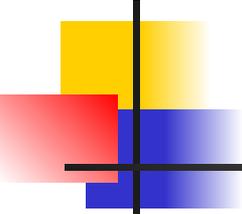
1. Нажмите **Ctrl+Alt+Delete**
2. В открывшемся окне Диспетчера Задач завершите процесс вредоносной программы.
3. Проведите полную проверку при помощи **AVPTool** ([скачать здесь](#)).

- 
-
- Зайти в специализированные разделы сайтов [«Доктор Веб»](#) Зайти в специализированные разделы сайтов «Доктор Веб», [«Лаборатории Касперского»](#) и других разработчиков антивирусного ПО можно с другого компьютера или телефона.

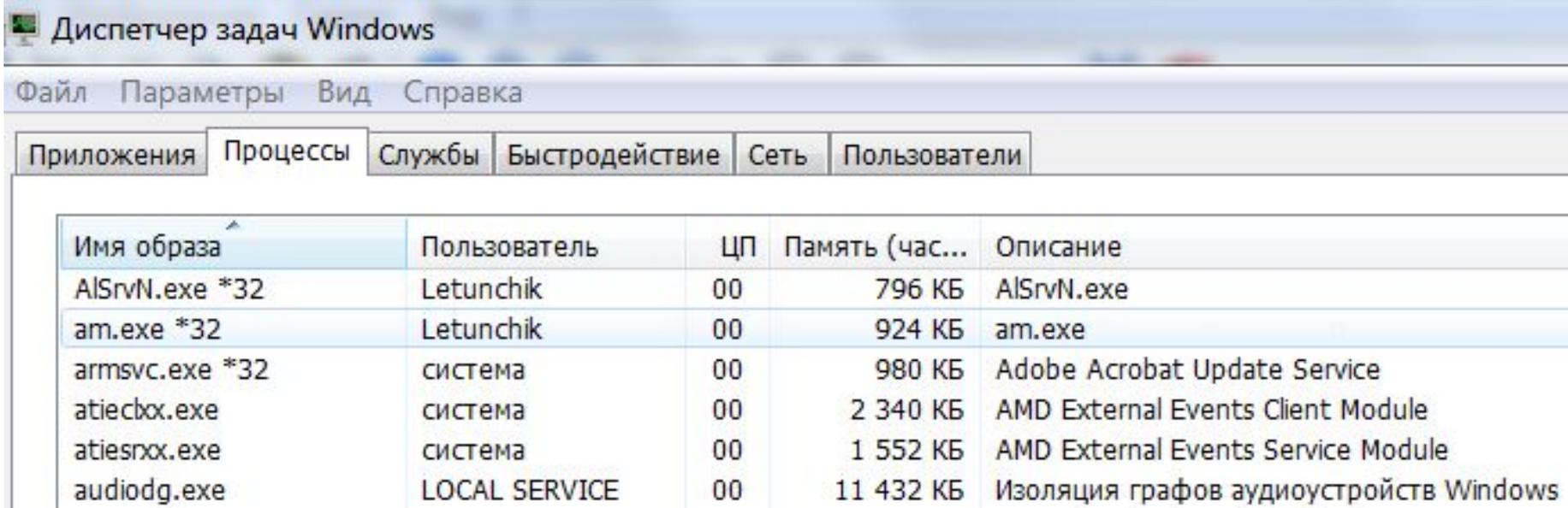
- 
-
- После разблокировки не радуйтесь преждевременно и не выключайте компьютер.
 - Скачайте любой бесплатный антивирус и выполните полную проверку системы. Для этого воспользуйтесь, например, утилитой [Dr.Web CureIt!](#) Скачайте любой бесплатный антивирус и выполните полную проверку системы. Для этого воспользуйтесь, например утилитой Dr Web CureIt! или



Простые меры

- 
-
- Прежде чем использовать сложные методы и спецсофт, попробуйте обойтись имеющимися средствами.
 - Вызовите диспетчер задач комбинацией клавиш {CTRL}+{ALT}+{DEL} или {CTRL}+{SHIFT}+{ESC}.
 - Если получилось, то мы имеем дело с примитивным трояном, борьба с которым не доставит проблем. Найдите его в списке процессов и принудительно завершите.

Подозрительный процесс в диспетчере задач

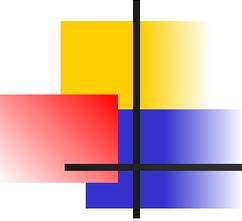


Диспетчер задач Windows

Файл Параметры Вид Справка

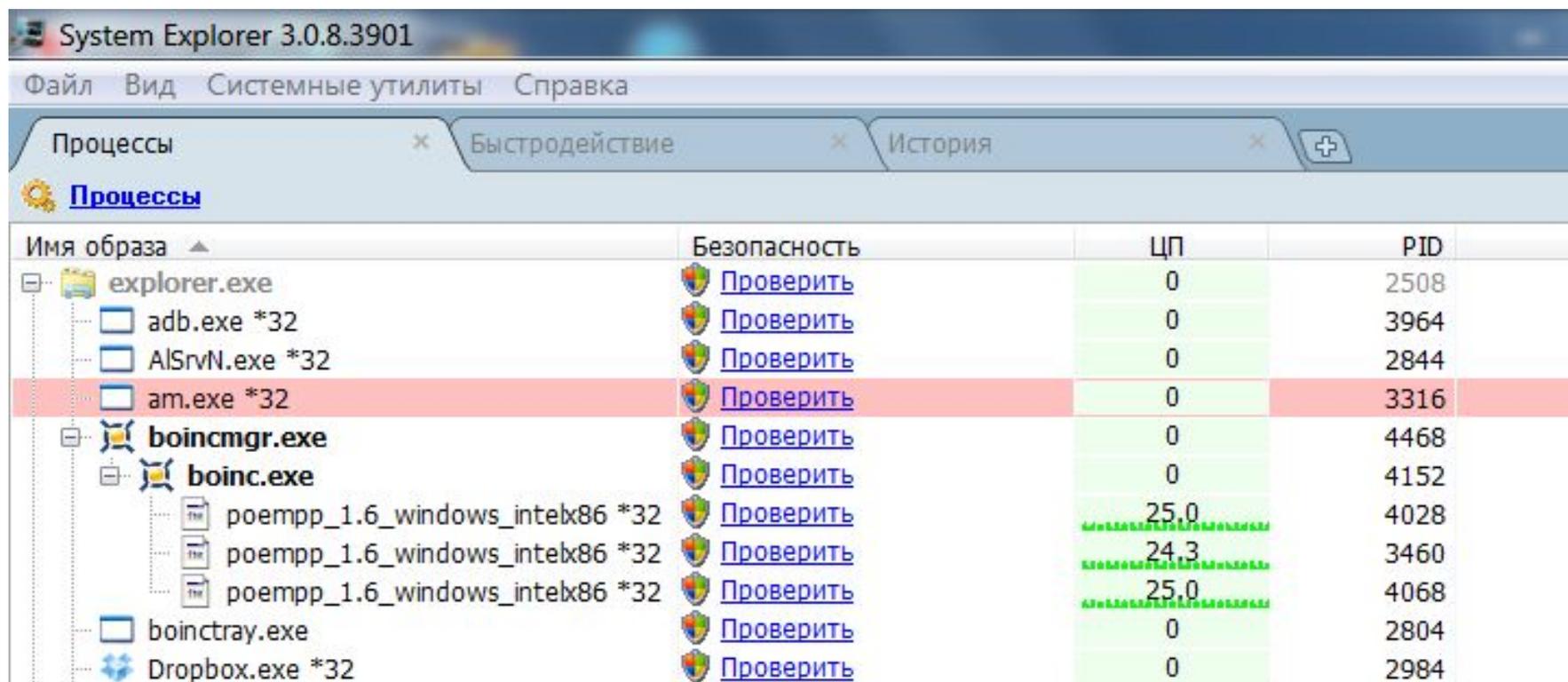
Приложения Процессы Службы Быстродействие Сеть Пользователи

Имя образа	Пользователь	ЦП	Память (час...	Описание
ALsrvN.exe *32	Letunchik	00	796 КБ	ALsrvN.exe
am.exe *32	Letunchik	00	924 КБ	am.exe
armsvc.exe *32	система	00	980 КБ	Adobe Acrobat Update Service
atiecbx.exe	система	00	2 340 КБ	AMD External Events Client Module
atiesrxx.exe	система	00	1 552 КБ	AMD External Events Service Module
audiodg.exe	LOCAL SERVICE	00	11 432 КБ	Изоляция графов аудиоустройств Windows

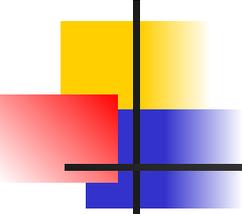
- 
-
- Посторонний процесс выдаёт невнятное имя и отсутствие описания.
 - Если сомневаетесь, просто поочерёдно выгружайте все подозрительные до исчезновения баннера.

- 
-
- Если диспетчер задач не вызывается, попробуйте использовать сторонний менеджер процессов через команду «Выполнить», запускаемую нажатием клавиш {Win}+{R}.

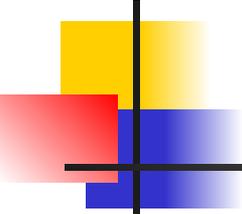
Подозрительный процесс в System Explorer

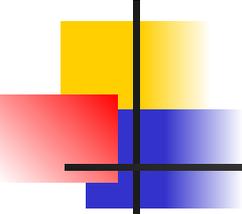


Имя образа	Безопасность	ЦП	PID
explorer.exe	Проверить	0	2508
adb.exe *32	Проверить	0	3964
ALSRvN.exe *32	Проверить	0	2844
am.exe *32	Проверить	0	3316
boincmgr.exe	Проверить	0	4468
boinc.exe	Проверить	0	4152
poempp_1.6_windows_intelx86 *32	Проверить	25,0	4028
poempp_1.6_windows_intelx86 *32	Проверить	24,3	3460
poempp_1.6_windows_intelx86 *32	Проверить	25,0	4068
boinctray.exe	Проверить	0	2804
Dropbox.exe *32	Проверить	0	2984

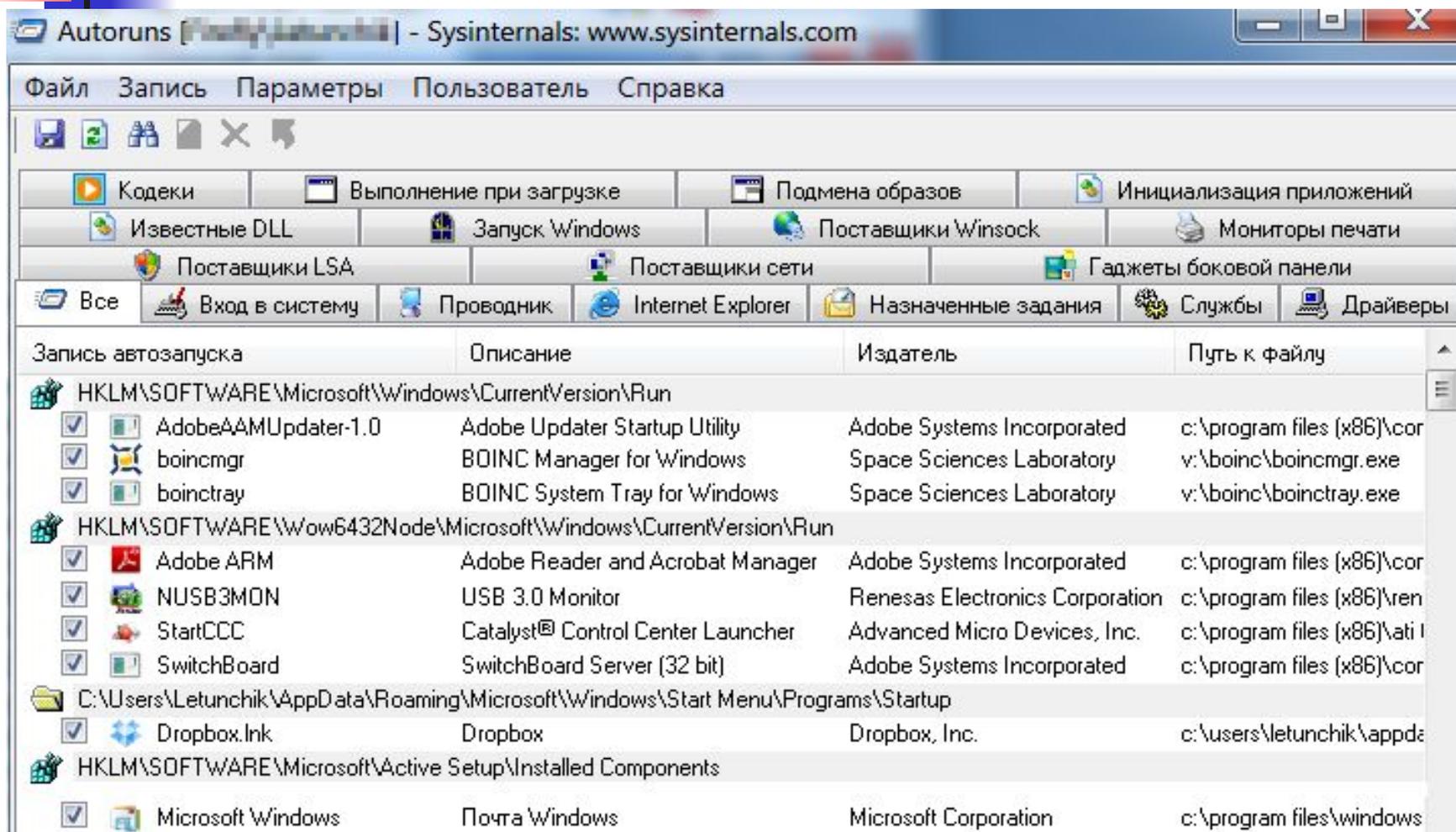
- 
-
- Скачать программу можно с другого компьютера или даже с телефона. Она занимает всего пару мегабайт.
 - По ссылке «проверить» происходит поиск информации о процессе в онлайн-базе данных, но обычно и так всё понятно.

- 
-
- После закрытия баннера часто требуется перезапустить «Проводник» (процесс explorer.exe).
 - В диспетчере задач нажмите: Файл -> Новая задача (выполнить) -> c:\Windows\explorer.exe.

- 
-
- Когда троян деактивирован на время сеанса, осталось найти его файлы и удалить их.
 - Это можно сделать вручную или воспользоваться бесплатным антивирусом.

- 
-
- Типичное место локализации трояна – каталоги временных файлов пользователя, системы и браузера.
 - Целесообразно всё же выполнять полную проверку, так как копии могут находиться где угодно, а беда не приходит одна.

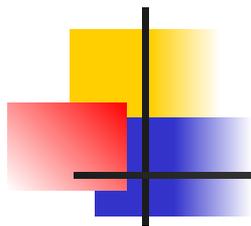
AutoRuns покажет все объекты автозапуска



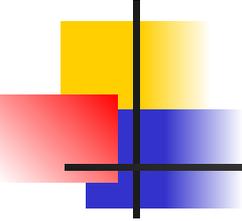
The screenshot shows the Autoruns utility window from Sysinternals. The window title is "Autoruns [File Edit View Options Help] - Sysinternals: www.sysinternals.com". The menu bar includes "Файл", "Запись", "Параметры", "Пользователь", and "Справка". The toolbar contains icons for file operations and navigation. Below the toolbar is a grid of category buttons: "Кодеки", "Выполнение при загрузке", "Подмена образов", "Инициализация приложений", "Известные DLL", "Запуск Windows", "Поставщики Winsock", "Мониторы печати", "Поставщики LSA", "Поставщики сети", and "Гаджеты боковой панели". A row of application icons includes "Все", "Вход в систему", "Проводник", "Internet Explorer", "Назначенные задания", "Службы", and "Драйверы".

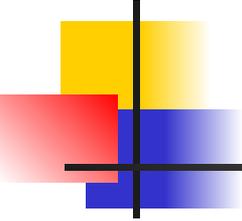
The main area displays a table of auto-starting programs with the following columns: "Запись автозапуска", "Описание", "Издатель", and "Путь к файлу".

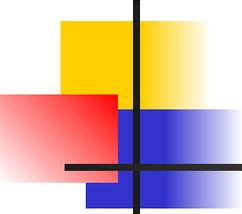
Запись автозапуска	Описание	Издатель	Путь к файлу
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/>	AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	c:\program files (x86)\cor
<input checked="" type="checkbox"/>	boincmgr	BOINC Manager for Windows	v:\boinc\boincmgr.exe
<input checked="" type="checkbox"/>	boinc tray	BOINC System Tray for Windows	v:\boinc\boinc tray.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/>	Adobe ARM	Adobe Reader and Acrobat Manager	c:\program files (x86)\cor
<input checked="" type="checkbox"/>	NUSB3MON	USB 3.0 Monitor	c:\program files (x86)\ren
<input checked="" type="checkbox"/>	StartCCC	Catalyst® Control Center Launcher	c:\program files (x86)\ati
<input checked="" type="checkbox"/>	SwitchBoard	SwitchBoard Server (32 bit)	c:\program files (x86)\cor
C:\Users\Letunchik\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
<input checked="" type="checkbox"/>	Dropbox.lnk	Dropbox	c:\users\letunchik\appda
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/>	Microsoft Windows	Почта Windows	c:\program files\windows

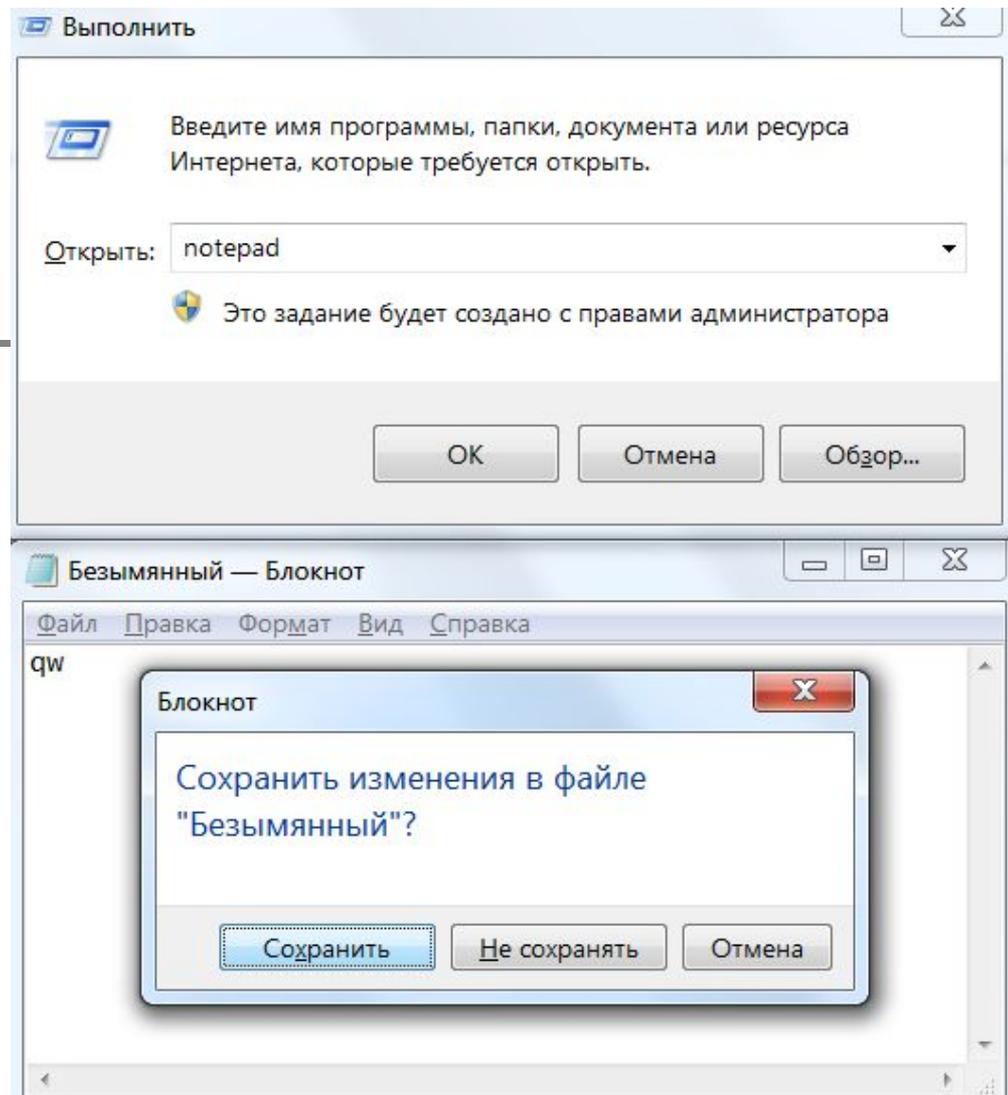


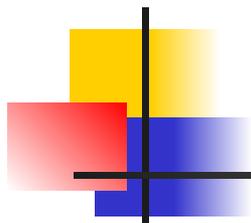
Хитростью

- 
-
- Справиться с трояном на первом этапе поможет особенность в поведении некоторых стандартных программ.
 - При виде баннера попробуйте запустить «вслепую» Блокнот или WordPad.

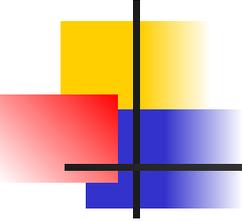
- 
-
- Нажмите {WIN}+{R}, напишите notepad и нажмите {ENTER}.
 - Под баннером откроется новый текстовый документ.
 - Наберите любую абракадабру и затем коротко нажмите кнопку выключения питания на системном блоке.
 - Все процессы, включая троянский, начнут завершаться, но выключения компьютера не произойдёт.

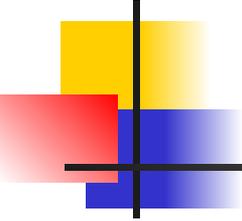
- 
- Останется диалоговое окно «Сохранить изменения в файле?».
 - С этого момента на время сеанса мы избавились от баннера и можем добить трояна до перезагрузки.

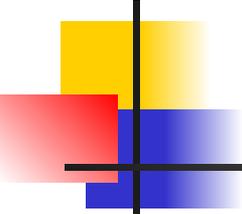




По старинке

- 
-
- Более продвинутые версии троянов имеют средства противодействия попыткам избавиться от них.
 - Они блокируют запуск диспетчера задач, подменяют другие системные компоненты.

- 
-
- В этом случае перезагрузите компьютер и удерживайте клавишу {F8} в момент загрузки Windows.
 - Появится окно выбора способа загрузки.
 - Нам требуется «Безопасный режим с поддержкой командной строки».

- 
-
- После появления консоли пишем explorer и нажимаем {ENTER} – запустится проводник.
 - Далее пишем regedit, нажимаем {ENTER} и видим редактор реестра.
 - Здесь можно найти созданные трояном записи и обнаружить место, откуда происходит его автозапуск.

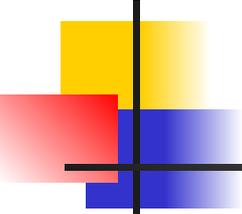
Ключи реестра, часто модифицируемые троянами семейства Winlock

Registry Editor

File Edit View Favorites Help

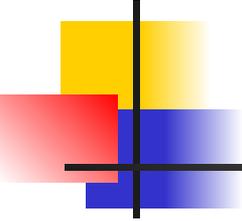
Name	Type	Data
AllowMultipleTSSessions	REG_DWORD	0x00000001 (1)
AltDefaultDomainName	REG_SZ	WINDOWSXPSP3
AltDefaultUserName	REG_SZ	Andrew
AutoRestartShell	REG_DWORD	0x00000001 (1)
Background	REG_SZ	0 0 0
cachedlogonscount	REG_SZ	10
DebugServerCommand	REG_SZ	no
DefaultDomainName	REG_SZ	WINDOWSXPSP3
DefaultUserName	REG_SZ	Andrew
forceunlocklogon	REG_DWORD	0x00000000 (0)
HibernationPreviouslyEnabled	REG_DWORD	0x00000001 (1)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
LogonType	REG_DWORD	0x00000001 (1)
passwordexpirywarning	REG_DWORD	0x0000000e (14)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
SfcDisable	REG_DWORD	0xffffffff (4294967197)
SfcQuota	REG_DWORD	0xffffffff (4294967295)
Shell	REG_SZ	<u>Explorer.exe</u>
ShowLogonOptions	REG_DWORD	0x00000000 (0)
ShutdownWithoutLogon	REG_SZ	0
System	REG_SZ	
UIHost	REG_EXPAND_SZ	logonui.exe
Userinit	REG_SZ	<u>C:\WINDOWS\system32\userinit.exe,</u>
WmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
WinStationsDisabled	REG_SZ	0

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

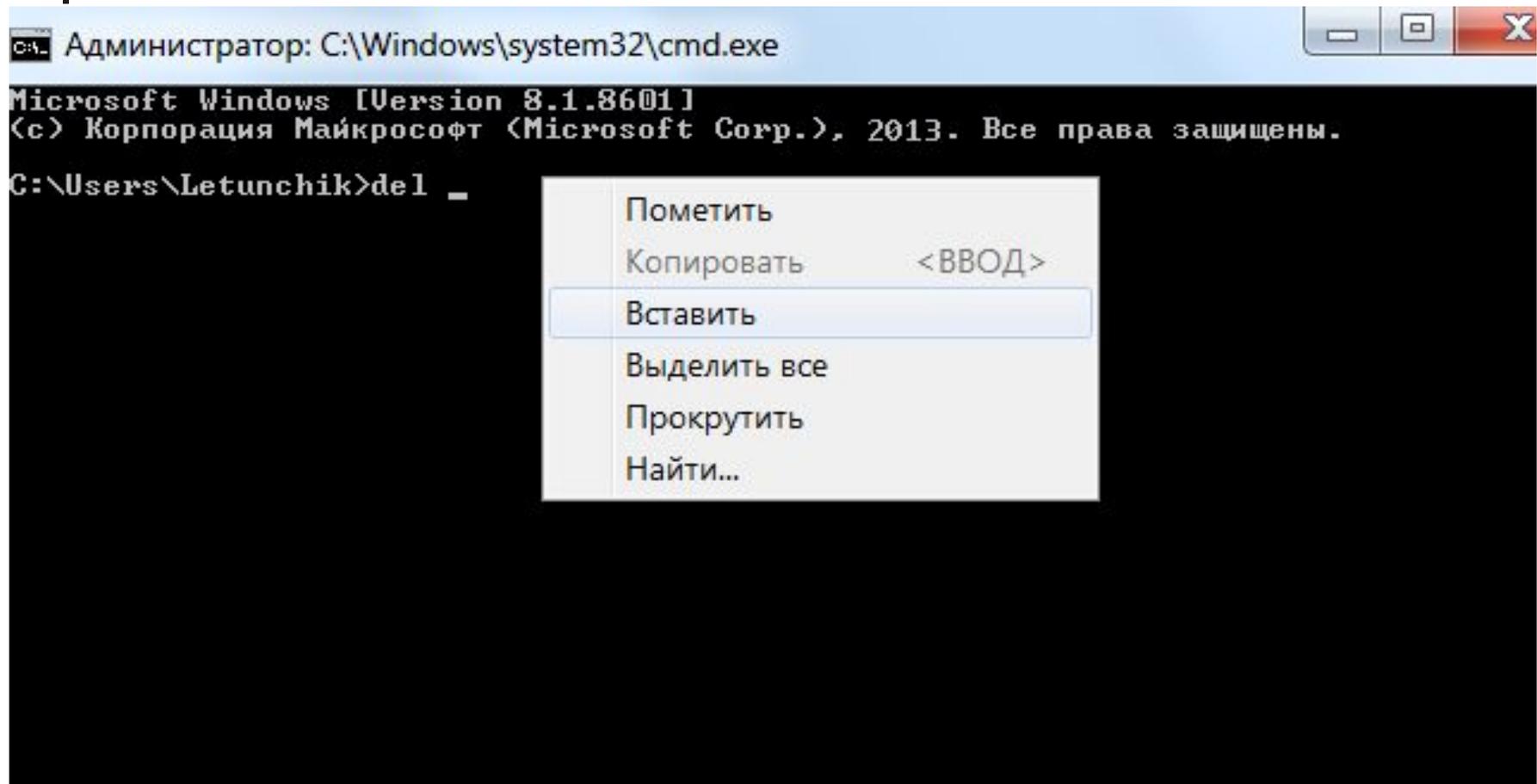
- 
-
- Чаще всего вы увидите полные пути к файлам трояна в ключах Shell и Userinit в ветке

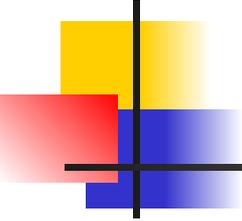
HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon

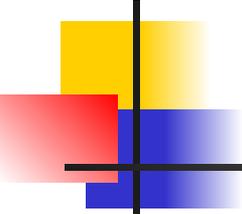
- В «Shell» троян записывается вместо explorer.exe, а в «Userinit» указывается после запятой.

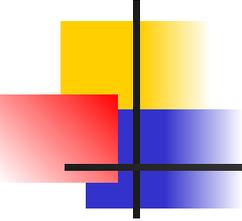
- 
-
- Копируем полное имя троянского файла в буфер обмена из первой обнаруженной записи.
 - В командной строке пишем del, делаем пробел и вызываем правой клавишей мыши контекстное меню.

Удаление трояна из консоли

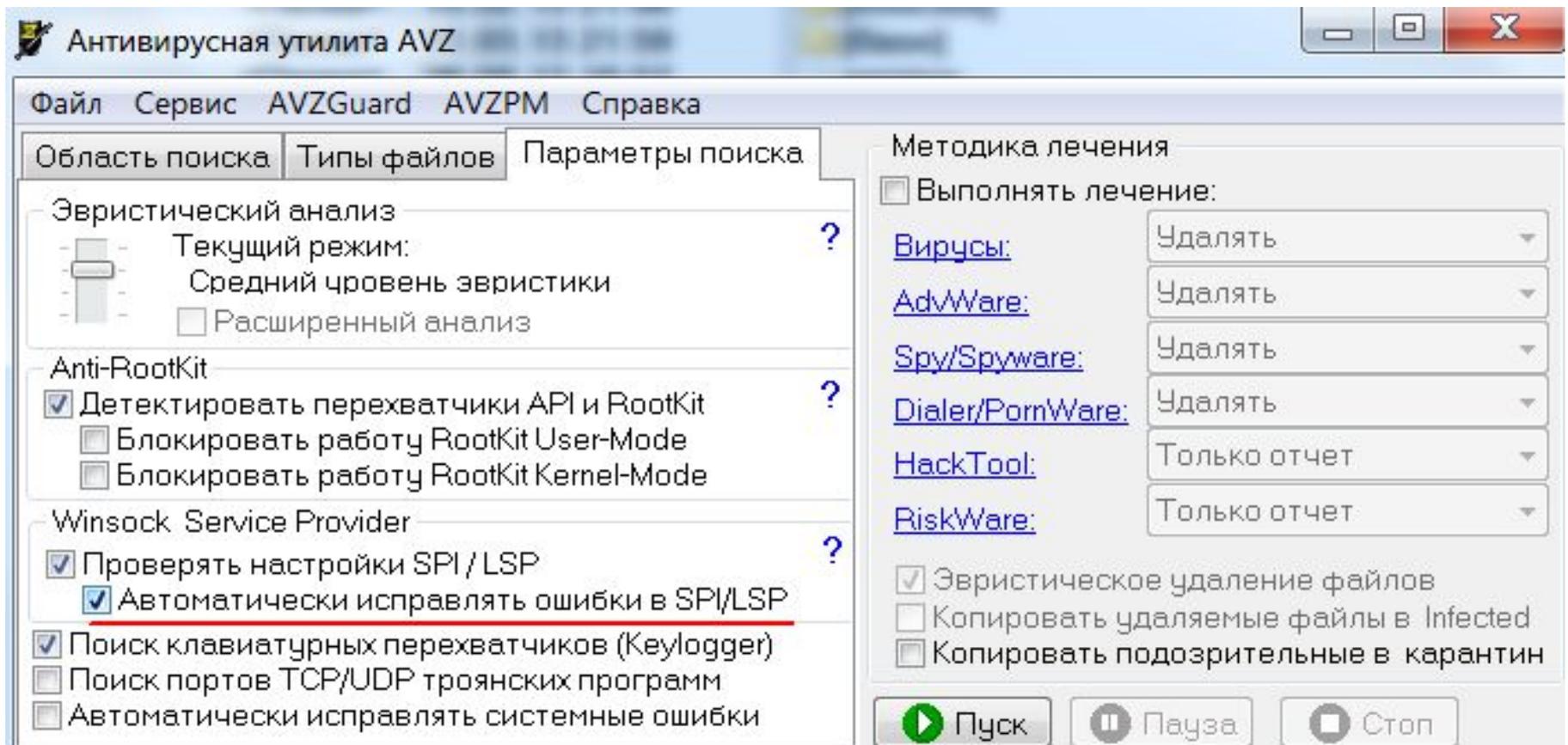


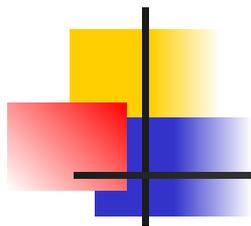
- 
-
- Выбираем команду «вставить» и нажимаем {ENTER}.
 - Один файл трояна удалён, делаем тоже самое для второго и последующих.

- 
-
- Затем выполняем в реестре поиск по имени файла трояна, внимательно просматриваем все найденные записи и удаляем подозрительные.
 - Очищаем все временные папки и корзину.
 - Даже если всё прошло идеально, не поленитесь затем выполнить полную проверку любым антивирусом.

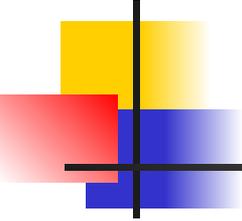
- 
-
- Если из-за трояна перестали работать сетевые подключения, попробуйте восстановить настройки Windows Sockets API утилитой AVZ.

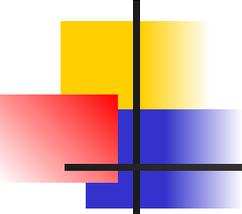
Восстановление сетевых сервисов с помощью AVZ



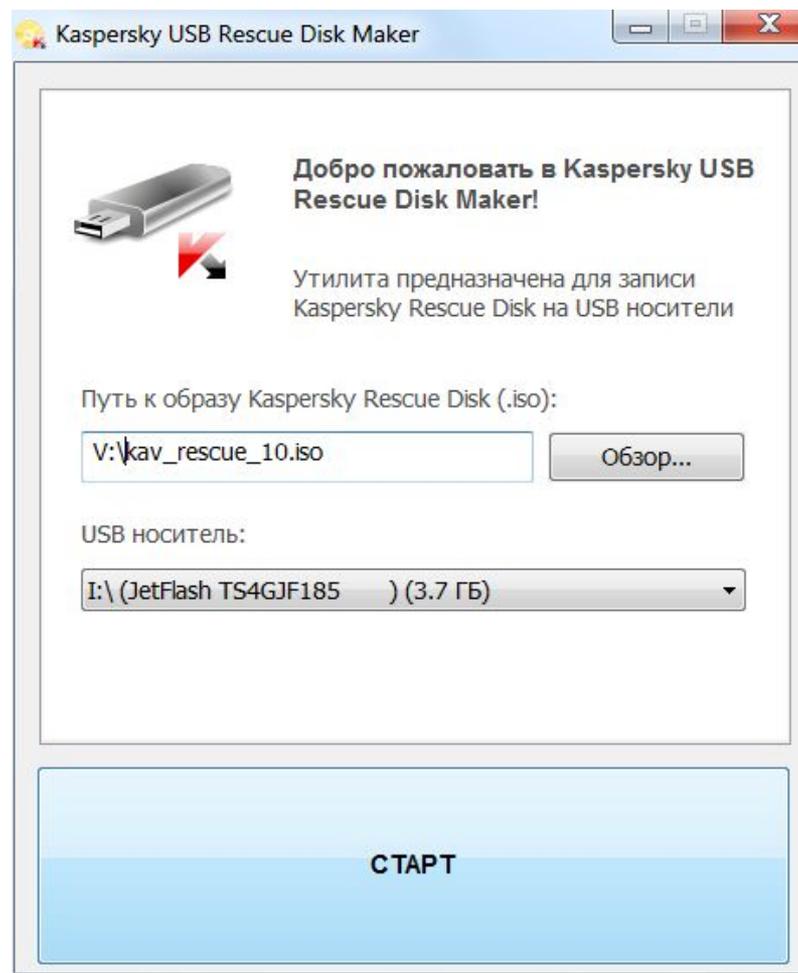


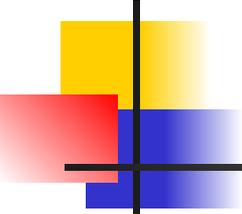
Операция

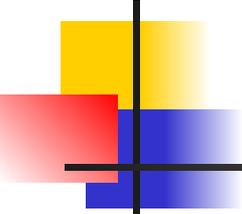
- 
-
- В случаях серьёзного заражения бесполезно бороться из-под инфицированной системы.
 - Логичнее загрузиться с заведомо чистой и спокойно вылечить основную.

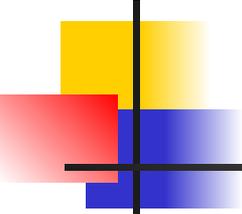
- 
-
- Существуют десятки способов сделать это, но один из самых простых – воспользоваться бесплатной утилитой Kaspersky WindowsUnlocker, входящей в состав Kaspersky Rescue Disk Существуют десятки способов сделать это, но один из самых простых – воспользоваться бесплатной утилитой Kaspersky WindowsUnlocker, входящей в состав Kaspersky Rescue Disk. Как и **DrWeb LiveCD**,³⁸

Создание загрузочной флэшки из образа Kaspersky Rescue Disk



- 
-
- При включении заражённого компьютера удерживайте клавишу для входа в BIOS.
 - Обычно это {DEL} или {F2}, а соответствующее приглашение отображается внизу экрана.
 - Вставьте Kaspersky Rescue Disk или загрузочную флэшку.

- 
-
- В настройках загрузки выберите первым загрузочным устройством привод оптических дисков или флэшку (иногда она может отображаться в раскрываемом списке HDD).
 - Сохраните изменения {F10} и выйдите из BIOS.

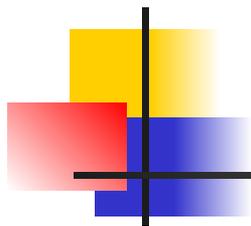
- 
-
- Современные версии BIOS позволяют выбирать загрузочное устройство на лету, без входа в основные настройки.
 - Для этого требуется нажать {F12}, {F11} либо сочетание клавиш – подробнее смотрите в сообщении на экране, в инструкции к материнской плате или ноутбуку.
 - После перезагрузки начнётся запуск Kaspersky Rescue Disk.

Загрузка Kaspersky Rescue Disk

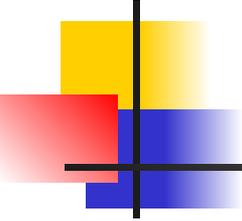


Kaspersky Rescue Disk в графическом режиме





Борьба на ранней стадии

- 
-
- Отдельный подкласс составляют трояны, поражающие главную загрузочную запись (MBR).
 - Они появляются до загрузки Windows, и в секциях автозапуска вы их не найдёте.

Троян семейства Winlock, заразивший MBR



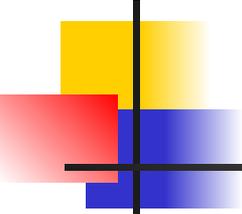
AMIBIOS (C) 2011 American Megatrends, Inc
ASRock G41M-S3 ACPI BIOS Revision 3086
CPU : Intel core 2 duo 2.99 GHz
Speed : 2.99 GHz

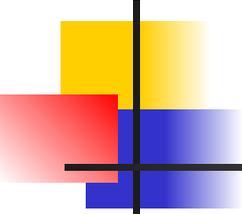
DDR3 DIMM, 800 - 1333 Mhz, Dual-Channel, Liner Mode
Checking NURAM..
1024 MB OK

Ваш BIOS заблокирован за установку Нелицензионного Программного обеспечения и использования поддельного ключа активации Windows!!! Для разблокировки BIOS, Вам необходимо оплатить покупку оригинального ключа активации. После оплаты, Вам будет направлена SMS с кодом разблокировки. Полученный код необходимо ввести в поле Enter Code и нажать клавишу Enter.
Все подробности на сайте xaluye.net, раздел "Оплаты"

Enter Code:

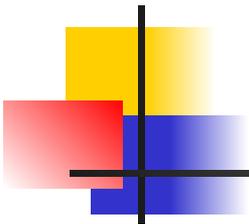
Press DEL to run Setup
Press <F8> for BBS POPUP

- 
-
- Первый этап борьбы с ними заключается в восстановлении исходного кода MBR.
 - В случае XP для этого загружаемся с установочного диска Windows, нажатием клавиши {R} вызываем консоль восстановления и пишем в ней команду fixmbr.
 - Подтверждаем её клавишей {Y} и выполняем перезагрузку.

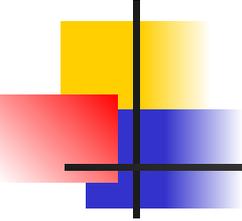
- 
-
- Для Windows 7 аналогичная утилита называется BOOTREC.EXE, а команда fixmbr передаётся в виде параметра:

Bootrec.exe/FixMbr

- После этих манипуляций система вновь загружается. Можно приступить к поиску копий трояна и средств его доставки любым антивирусом.

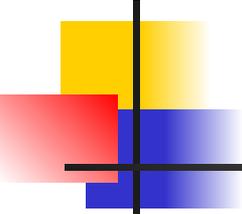


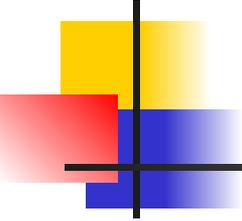
Отвертка

- 
-
- На маломощных компьютерах и особенно ноутбуках борьба с троянами может затянуться, так как загрузка с внешних устройств затруднена, а проверка выполняется очень долго. В таких случаях просто извлеките заражённый винчестер и подключите его для лечения к другому компьютеру. Для этого удобнее воспользоваться боксами с

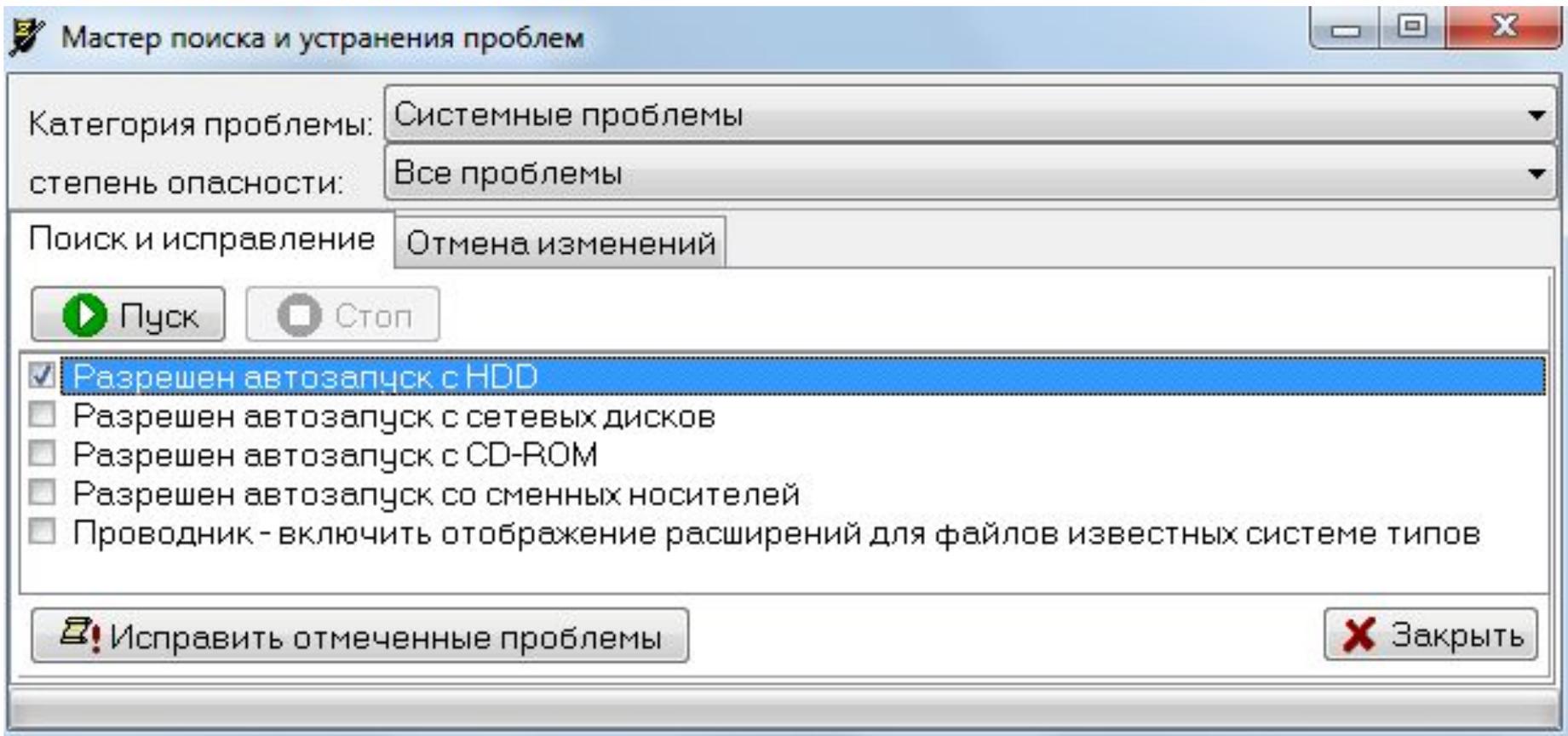
Антивирусная проверка жёстких дисков на другом компьютере

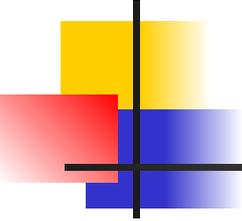


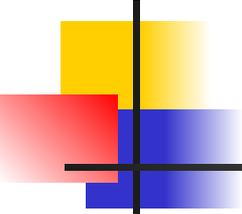
- 
-
- Чтобы не разносить заразу, предварительно отключаем на «лечащем» компьютере автозапуск с HDD (да и с других типов носителей не мешало бы).
 - Сделать это удобнее всего бесплатной утилитой AVZ, но саму проверку лучше выполнять чем-то другим.

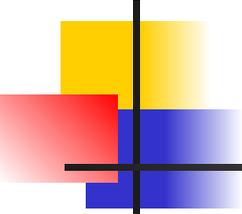
- 
-
- Зайдите в меню «Файл», выберите «Мастер поиска и устранения проблем».
 - Отметьте «Системные проблемы», «Все» и нажмите «Пуск».
 - После этого отметьте пункт «Разрешён автозапуск с HDD» и нажмите «Исправить отмеченные проблемы».

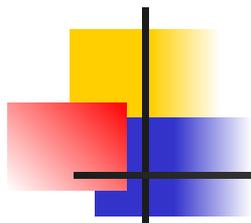
Отключение автозапуска с помощью AVZ



- 
-
- Перед подключением заражённого винчестера стоит убедиться, что на компьютере запущен резидентный антивирусный мониторинг с адекватными настройками и есть свежие базы.

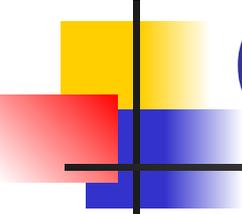
- 
-
- Если разделы внешнего жёсткого диска не видны, зайдите в «Управление дисками».
 - Для этого в окне «Пуск» -> «Выполнить» напишите `diskmgmt.msc` и затем нажмите {ENTER}.
 - Разделам внешнего жёсткого диска должны быть назначены буквы.
 - Их можно добавить вручную командой «изменить букву диска...».
 - После этого проверьте внешний винчестер целиком.

- 
-
- Для предотвращения повторного заражения следует установить любой антивирус с компонентом мониторинга в режиме реального времени и придерживаться общих правил безопасности.



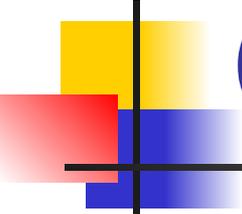
Общие правила безопасности

Общие правила безопасности



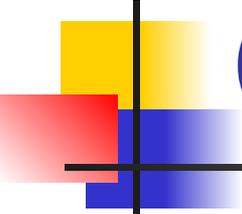
- старайтесь работать из-под учётной записи с ограниченными правами;
- пользуйтесь альтернативными браузерами – большинство заражений происходит через Internet Explorer;
- отключайте Java-скрипты на неизвестных сайтах;

Общие правила безопасности

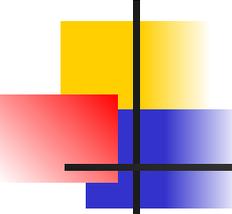


- отключите автозапуск со сменных носителей;
- устанавливайте программы, дополнения и обновления только с официальных сайтов разработчиков;
- всегда обращайтесь внимание на то, куда на самом деле ведёт предлагаемая ссылка;

Общие правила безопасности



- блокируйте нежелательные всплывающие окна с помощью дополнений для браузера или отдельных программ;
- своевременно устанавливайте обновления браузеров, общих и системных компонентов;
- выделите под систему отдельный дисковый раздел, а пользовательские файлы храните на другом.



Ресурсы

- <http://www.computerra.ru/59610/trojan-windows-unlocking/>
- <http://support.kaspersky.ru/viruses/solutions?qid=208637133>
- <http://hardisoft.ru/soft/borba-s-programmami-vymogat-elyami/>
- <http://kzncomputer.ru/articles/14-how-to-delete-the-banner>
- <http://mes-blog.com.ua/virusy/virus-blokiruet-windows.html>
- <http://todostep.ru/DelBanner.html>