Anti-Malware
Anti-Malicious Software

Результаты теста антивирусов на лечение активного заражения (Тест №3 от 10.2008)

http://www.anti-malware.ru/

Таблица 1: Итоговые результаты лечения

Антивирус	Награда	% вылеченных
Dr.Web Anti-Virus 4.44.5.8080	 **Platinum Malware Treatment Award**	100%
Kaspersky Anti-Virus 2009 8.0.0.357	 **Gold Malware Treatment Award**	80%
Avast! Professional Edition 4.8.1229		
Agnitum Outpost Antivirus Pro 6.5.2358.316.0607	 **Bronze Malware Treatment Award**	53%
Norton AntiVirus 2009		
Panda Antivirus 2009		40%
BitDefender Antivirus 2009 12.0.10.1	**Тест провален**	33%
Trend Micro Antivirus plus Antispyware 2008 16.10.1182		
McAfee VirusScan 2008 12.1.110		
F-Secure Anti-Virus 2009		
AVG Anti-Virus & Anti-Spyware 8.0.0.2		
Avira AntiVir PE Premium 8.1.0.367		20%
Sophos Anti-Virus 7.3.4		13%
Eset NOD32 Antivirus 3.0.669.0		0%
VBA32 Antivirus 3.12.8.6		

Таблица 2а: Результаты лечения активного заражения различными антивирусными продуктами

Антивирус \ вредоносное ПО *	Avast! Professional Edition 4.8.1229	AVG Anti-Virus & Anti-Spyware 8.0.0.2	Avira AntiVir PE Premium 8.1.0.367	BitDefender Antivirus 2009 12.0.10.1	Dr.Web Anti-Virus 4.44.5.8080	Eset NOD32 Antivirus 3.0.669.0	F-Secure Anti-Virus 2009	Kaspersky Anti-Virus 2009 8.0.0.357
Adware. Win32.NewDotNet	+	-	-	+	+	-	-	+
Backdoor.Win32.Sinowal.ce	+	-	-	-	+	-	-	+
Email-Worm.Win32.Scano.bd	-	-	-	-	+	-	-	+
Rootkit.Win32.Agent.ea	+	-	-	+	+	-	-	-
Rootkit.Win32.Podnuha.a	+	-	-	-	+	-	-	+
Trojan-Dropper.Win32.Agent.vug	+	+	+	-	+	-	+	+
Trojan-Dropper.Win32.Mutant.e	+	-	-	-	+	-	+	+
Trojan-Proxy.Win32.Saturn.cu	+	-	-	-	+	-	-	-
Trojan-Proxy. Win32.Xorpix.dh	+	+	-	-	+	-	+	+
Trojan-Spy.Win32.Zbot.bsa	+	+	+	+	+	-	-	+
Trojan.Win32.Agent.lkz	+	+	-	+	+	-	+	+
Trojan.Win32.Monderb.gen	+	+	+	+	+	-	+	+
Trojan.Win32.Pakes.cuh	+				+	-		-
Trojan.Win32.Small.yc	-	-	-	-	+	-	-	+
Virus.Win32.Rustock.a	-	-	-	-	+	-	-	+
Вылечено/Всего	12/15	5/15	3/15	5/15	15/15	0/15	5/15	12/15

* Названия вредоносных программ указано по классификации Лаборатории Касперского

Таблица 2б: Результаты лечения активного заражения различными антивирусными продуктами

Антивирус \ вредоносное ПО	McAfee VirusScan 2008 12.1.110	Outpost Antivirus Pro 6.5.2358.316.0607	Panda Antivirus 2009	Sophos Anti-Virus 7.3.4	Norton AntiVirus 2009	Trend Micro Antivirus plus Antispyware 2008 16.10.1182	VBA32 Antivirus 3.12.8.6
Adware. Win32.NewDotNet	+	+	+	+	+	+	-
Backdoor.Win32.Sinowal.ce	+	-	-	-	-	-	-
Email-Worm.Win32.Scano.bd	-	-	-	-	+	-	-
Rootkit.Win32.Agent.ea	-	-	-	-	-	-	-
Rootkit.Win32.Podnuha.a	-	-	-	-	-	-	-
Trojan-Dropper.Win32.Agent.vug	-	+	+	-	+	+	-
Trojan-Dropper.Win32.Mutant.e	+	-	-	-	+	-	-
Trojan-Proxy.Win32.Saturn.cu	-	+	-	-	-	-	-
Trojan-Proxy. Win32.Xorpix.dh	-	+	+	-	+	+	-
Trojan-Spy.Win32.Zbot.bsa	+	+	+	-	+	-	-
Trojan.Win32.Agent.lkz	+	+	+	-	+	+	-
Trojan.Win32.Monderb.gen	-	+	+	-	+	+	-
Trojan.Win32.Pakes.cuh	-	+	-	-	-	-	-
Trojan.Win32.Small.yc	-	-	-	+	-	-	-
Virus.Win32.Rustock.a	-	-	-	-	-	-	-
Вылечено/Всего	5/15	8/15	6/15	2/15	8/15	5/15	0/15

+	- антивирус успешно устранил активное заражение, работоспособность системы восстановлена (не нарушена).
-	- антивирус не смог устранить активное заражение или была серьезно нарушена работоспособность системы.

Таблица 4: Описания вредоносных программ, используемых в тесте

Полное имя вируса по классификации Лаборатории Касперского	Краткое описание	Способ противодействия своему обнаружению/удалению	Информация о подобных модификациях малвар в сети Интернет
Adware. Win32.NewDotNet	Рекламная программа-шпион. После ее инсталляции имеются следующие исполняемые файлы: \WINDOWS\NDNuninstall6_38.exe, \Program Files\NewDotNet\newdotnet6_38.dll и \Program Files\NewDotNet\uninstall6_38.exe. Все файлы и каталог NewDotNet имеют атрибут "скрытый". Библиотека регистрируется в системном реестре - HKLM\...\Run. Системный процесс rundll32.exe постоянно восстанавливает ключ автозагрузки, в случае его удаления. Так же библиотека регистрируется как Winsock Providers (4 поставщика транспортных протоколов и 1 поставщик пространства имен). В случае отсутствия файла newdotnet6_38.dll (удаление его антивирусом), но наличия ключей Winsock - будет отсутствовать доступ в Интернет.	Регистрация в системном реестре как Winsock Providers	http://www.symantec.com/security_response/writeup.jsp?docid=2004-020511-0558-99&tabid=1

Backdoor.Win32.Sinowal.ce	Троянская программа-шпион. При запуске модифицирует главную загрузочную запись (MBR) жесткого диска с целью загрузки своего драйвера еще до старта ОС. Перехватывает IRP обработчики disk.sys и cdrom.sys с целью блокировки чтения/изменения антивирусными продуктами главной загрузочной записи.	KernelMode (модификация машинного кода ядра - сплайсинг) CLASSPNP.SYS ClassInitialize IRP-hooks Cdrom IRP_MJ_CREATE Cdrom IRP_MJ_CLOSE Cdrom IRP_MJ_READ Cdrom IRP_MJ_WRITE Cdrom IRP_MJ_FLUSH_BUFFERS Cdrom IRP_MJ__CONTROL Cdrom IRP_MJ_INTERNAL__CONTROL Cdrom IRP_MJ_SHUTDOWN Cdrom IRP_MJ_POWER Cdrom IRP_MJ_SYSTEM_CONTROL Cdrom IRP_MJ_PNP Disk IRP_MJ_CREATE Disk IRP_MJ_CLOSE Disk IRP_MJ_READ Disk IRP_MJ_WRITE Disk IRP_MJ_FLUSH_BUFFERS Disk IRP_MJ__CONTROL Disk IRP_MJ_INTERNAL__CONTROL Disk IRP_MJ_SHUTDOWN Disk IRP_MJ_POWER Disk IRP_MJ_SYSTEM_CONTROL Disk IRP_MJ_PNP	http://www.symantec.com/security_response/writeup.jsp?docid=2008-010718-3448-99&tabid=1

Email-Worm.Win32.Scano.bd	Почтовый червь. При инсталляции создает свою копию в \WINDOWS\csrss.exe и регистрирует в системном реестре отладчиком explorer.exe (Image File Execution Options\explorer.exe\ параметр - Debugger). Запускает три системных процесса (один svchost.exe и два services.exe) и создает в них троянские потоки, которые и восстанавливают файл и ключ автозагрузки в случае их удаления. Если антивирус удаляет тело червя, но не удаляет ключ его автозагрузки, то при старте системы не загрузится Explorer.exe, что не позволит работать с ПК.	Регистрация в реестре как отладчик системного процесса. Пересоздание своих ключей и файлов в случае их удаления	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SCANO.AB&VSect=P
Rootkit.Win32.Agent.ea	Троянская программа. Является KernelMode руткитом. При инсталляции создает драйвер в \WINDOWS\system32\drivers с произвольным именем. Троян маскирует свой ключ автозагрузки перехватом функций с помощью модификации машинного кода ядра, а так же маскирует себя на диске перехватом IRP-обработчиков драйвера файловой системы. Драйвер загружается непосредственно после ядра и его зависимостей.	KernelMode (модификация машинного кода ядра - сплайсинг) NtEnumerateKey NtOpenKey IRP-hooks Ntfs IRP_MJ_CREATE Ntfs IRP_MJ_DIRECTORY_CONTROL	http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99&tabid=1
Rootkit.Win32.Podnuha.a	Троянская программа. Является KernelMode руткитом. При инсталляции создает драйвер в \WINDOWS\system32\drivers и библиотеку в \Windows\system32\ с произвольным именем. Dll зарегистрирована как расширение Winlogon (Winlogon\Notify), как BHO (Explorer\Browser Helper Objects) и как сервис (Name_service\Parametres\ServiceDll). Доступ к драйверу заблокирован, так же как и возможность удалять ключи автозагрузки в реестре. Библиотека защищена от переименования/удаления.	KernelMode (модификация машинного кода ядра - сплайсинг) ObOpenObjectByName	http://research.sunbelt-software.com/threatdisplay.aspx?name=Rootkit.Win32.Podnuha.a&threatid=153388
Trojan-Dropper.Win32.Agent.vug	Троянская программа. Является KernelMode руткитом. Инсталлирует драйвер в \WINDOWS\system32\drivers с произвольным именем. Маскирует себя на диске перехватом IofCompleteRequest модификацией машинного кода ядра, в реестре и в памяти по DKOM методике.	KernelMode (модификация машинного кода ядра - сплайсинг) IofCompleteRequest DKOM	http://research.sunbelt-software.com/threatdisplay.aspx?name=Trojan-Dropper.Win32.Agent.vug&threatid=390054

Trojan-Dropper.Win32.Mutant.e	Троянская программа-спамбот. Является KernelMode руткитом. При инсталляции создает драйвер с рандомным именем в \Windows\system32\drivers и WinCtrl32.dll в \Windows\system32\. Драйвер руткита блокирует к себе доступ перехватом IRP обработчиков драйвера файловой системы и защищает свои ключи от удаления установкой колбеков на работу с реестром. WinCtrl32.Dll пересоздается драйвером в случае удаления антивирусом.	IRP-hooks Ntfs IRP_MJ_CREATE FastFat IRP_MJ_CREATE CmRegisterCallback	http://www.bitdefender.com/VIRUS-1000297-en--Trojan.Dropper.Cutwail.D.html
Trojan-Proxy.Win32.Saturn.cu	Троянская программа. Является KernelMode руткитом. При инсталляции создает драйвер с рандомным именем в \Windows\system32\config и расширением Evt. Регистрирует себя в системном реестре под именем asc3550(рандомно a-z) без параметра ImagePath и использует ключ отложенного перемещения/переименования для перемещения своего драйвера из каталога config в drivers на ранней стадии загрузки системы. После загрузки asc3550(a-z) в память он удаляется с диска. Свой файл драйвера в config защищает перехватом в ядре, подсовывая содержимое системного файла SysEvent.Evt, а ключи маскирует установкой колбеков на работу с реестром.	KernelMode (модификация машинного кода ядра - сплайсинг) IofCallDriver CmRegisterCallback	http://www.symantec.com/security_response/writeup.jsp?docid=2007-082818-0250-99
Trojan-Proxy. Win32.Xorpix.dh	Троянская программа. Является библиотекой - \documents and settings\all users\Documents\settings\partnership.dll, открытой с монопольным доступом. Имеет атрибут "скрытый" вместе с каталогом в котором находится. Библиотека зарегистрирована для автоматического запуска в системном реестре - Winlogon\Notify. В случае удаления ключа автозагрузки, он моментально пересоздается.	Монопольное открытие файла и пересоздание своего ключа автозагрузки	http://www.viruslist.com/ru/viruses/encyclopedia?virusid=138399

Trojan-Spy.Win32.Zbot.bsa	Троянская программа-шпион. Перехватывает множество функций в UserMode с целью маскировки и шпионажа (перехват методом подмены адресов). При инсталляции создает файл ntos.exe в системном каталоге и регистрирует в реестре (Winlogon\ параметр Userinit), с целью загрузки его при каждом старте системы. В случае удаления пути к своему файлу в значении параметра Userinit, он тут же дописывает путь к себе (восстанавливает свой ключ автозагрузки). Троян блокирует доступ к себе с помощью созданных им троянских потоков в системных процессах.	UserMode (подмена адреса) ntdll.dll:NtQueryDirectoryFile Блокировка своего файла от открытия, восстановление ключей автозагрузки	http://www.avira.com/en/threats/section/fulldetails/id_vir/4233/tr_spy.zbot.dkx.html
Trojan.Win32.Agent.lkz	Троянская программа. Является KernelMode руткитом. При инсталляции создает в \Windows\system32\drivers драйвер clbdriver.sys и в \Windows\system32\ библиотеку clbdll.dll. Маскируется на диске, в памяти и в реестре.	KernelMode (модификация машинного кода ядра - сплайсинг) NtEnumerateKey NtQueryDirectoryFile DKOM	http://ru.mcafee.com/virusInfo/default.asp?id=description&virus_k=132847
Trojan.Win32.Monderb.gen	Троянская программа. Является библиотекой. При инсталляции регистрирует себя в системном реестре - Winlogon\Notify, Explorer\ShellExecuteHooks, Explorer\Browser Helper Objects. Данные ключи постоянно перепроверяются и в случае отсутствия - восстанавливаются. Библиотека расположена в системном каталоге. Имя выбирается произвольное в момент инсталляции. Банальное удаление не возможно, т.к. она используется системными процессами. Вредоносный код мониторит создания ключа отложенного перемещения/переименования и, в случае обнаружения имени своей библиотеки в значении параметра этого ключа, удаляет его.	Пересоздание своих ключей автозагрузки и удаление ключа отложенного перемещения/переименования, который используют антивирусы для удаления вредоносных файлов.	http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?lst=vis&idvirus=53087&sitepanda=particulares

Trojan.Win32.Pakes.cuh	Троянская программа-спамбот. Является KernelMode руткитом. При инсталляции создает драйвер в системном каталоге с произвольным именем. Блокирует доступ к своему файлу перехватом IRP обработчиков драйвера файловой системы, подсовывая вместо содержимого своего файла содержимое системного файла sfc_os.dll. Блокирует свой ключ реестра перехватом в ядре.	KernelMode (правка адресов в KiST) NtCreateKey NtOpenKey NtTerminateProcess IRP-hooks Ntfs IRP_MJ_CREATE KOH Key object-->ParseProcedure	http://www.symantec.com/security_response/writeup.jsp?docid=2006-070513-1305-99
Trojan.Win32.Small.yc	Троянская программа. При инсталляции создает base*32.dll (* - произвольные символы) в системном каталоге и изменяет значение параметра Windows в Session Manager\SubSystems таким образом, чтобы csrss.exe загружал dll вредоносной программы, а не системную basesrv.dll. Если в ходе лечения системы удаляется файл вредоносной программы, а ключ windows не восстанавливается в первоначальное состоянии, то система будет постоянно падать в BSOD при загрузке. Загрузка с последней удачной конфигурации не поможет сделать систему рабочей, т.к. вредоносная программа изменяет параметр Windows во всех кустах ControlSet.	Регистрация в автозапуске изменением ключа windows	http://research.sunbelt-software.com/threatdisplay.aspx?name=Trojan.Inject.GF&threatid=222395

Virus.Win32.Rustock.a	Файловый вирус с функцией рассылки спама. Является KernelMode руткитом. Заражает системные драйвера, расположенные в \Windows\system32\drivers (в произвольный момент времени заражен один файл). Зараженный драйвер маскируется перехватом IRP обработчиков драйвера файловой системы. Руткит на лету подсовывает содержимое дизинфецированного системного драйвера при обращении к зараженному файлу. Внедряет из памяти библиотеку в winlogon.exe с целью использования системного процесса для рассылки спама. Библиотека в памяти защищается и маскируется перехватами ядре.	KernelMode (модификация машинного кода ядра - сплайсинг) NtCreateThread NtDelayExecution NtDuplicateObject NtOpenThread NtProtectVirtualMemory NtQuerySysteminformation NtReadVirtualMemory NtResumeThread NtTerminateProcess NtTerminateThread NtWriteVirtualMemory IRP-hooks (сплайс) Ntfs IRP_MJ_CLOSE Ntfs IRP_MJ_CREATE Ntfs IRP_MJ_DIRECTORY_CONTROL Ntfs IRP_MJ_QUERY_INFORMATION Ntfs IRP_MJ_READ Ntfs IRP_MJ_SET_INFORMATION Ntfs IRP_MJ_WRITE Ntfs IRP_MJ_DISPATCHWAIT	http://www.eset.com/download/whitepapers/Yet_Another_Rustock_Analysis.pdf

Agnitum Outpost Antivirus Pro 6.5.2358.316.0607

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Не может удалить файл червя - он постоянно восстанавливается. При старте системы пропадает рабочий стол (заблокирован запуск вредоносной программы).
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	+
Trojan-Dropper.Win32.Mutant.e	-	Детектирует библиотеку. Драйвер не обнаружен.
Trojan-Proxy.Win32.Saturn.cu	+	Остался ключ автозагрузки.
Trojan-Proxy. Win32.Xorpix.dh	+	+
Trojan-Spy.Win32.Zbot.bsa	+	+
Trojan.Win32.Agent.lkz	+	Остался ключ автозагрузки.
Trojan.Win32.Monderb.gen	+	+
Trojan.Win32.Pakes.cuh	+	+
Trojan.Win32.Small.yc	-	Антивирус блокирует загрузку троянской библиотеки. Система не загружается, постоянно падает в BSOD.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

http://www.anti-malware.ru/

Avast! Professional Edition 4.8.1229

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	Выводится сообщение с ошибкой при старте системы, т.к остался ключ автозапуска в реестре.
Backdoor.Win32.Sinowal.ce	+	+
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
Rootkit.Win32.Agent.ea	+	+
Rootkit.Win32.Podnuha.a	+	Остались ключи автозапуска.
Trojan-Dropper.Win32.Agent.vug	+	+
Trojan-Dropper.Win32.Mutant.e	+	Остались ключи автозапуска.
Trojan-Proxy.Win32.Saturn.cu	+	Остался ключ автозапуска.
Trojan-Proxy. Win32.Xorpix.dh	+	Остался ключ автозапуска.
Trojan-Spy.Win32.Zbot.bsa	+	Остался ключ автозапуска.
Trojan.Win32.Agent.lkz	+	Остался ключ автозапуска.
Trojan.Win32.Monderb.gen	+	Остались ключи автозапуска.
Trojan.Win32.Pakes.cuh	+	+
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.*
Virus.Win32.Rustock.a	-	Детектирует зараженный драйвер, но не может лечить. Имеется возможность удалять или помещать в карантин.**

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

http://www.anti-malware.ru/

* - исход лечения зависит от способа проверки. При бут-сканировании и лечении система будет повреждена и не сможет загрузиться. Если же при инсталляции отказаться от бут-сканирования и пролечиться из-под загруженной ОС сканером, то система будет вылечена.

** - исход лечения зависит от того, какой драйвер в момент лечения был заражен. Если это будет критически важный драйвер - система станет нерабочей, если же будет заражен не жизненно необходимый для работы системы драйвер, то он будет удален и после загрузки восстановлен самой операционной системой.

AVG Anti-Virus & Anti-Spyware 8.0.0.2

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	-	Выводится сообщение с ошибкой при старте системы, остались ключи автозапуска в реестре. Пропал доступ в Интернет.
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Не загружается Explorer после перезагрузки. Удаленный файл постоянно появляется.
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозапуска.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует библиотеку. Драйвер не обнаружен.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	+	Остался ключ автозапуска.
Trojan-Spy.Win32.Zbot.bsa	+	Остались ключи автозапуска в реестре.
Trojan.Win32.Agent.lkz	+	Остался ключ автозапуска.
Trojan.Win32.Monderb.gen	+	Остались ключи автозапуска в реестре.
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Avira AntiVir PE Premium 8.1.0.367

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	-	Выводится сообщение с ошибкой при старте системы, остались ключи автозапуска в реестре. Пропал доступ в Интернет.
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Не загружается Explorer после перезагрузки. Удаленный файл постоянно появляется.
Rootkit.Win32.Agent.ea	-	Зависает при сканировании.
Rootkit.Win32.Podnuha.a	-	Обнаруживает и удаляет библиотеку. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозагрузки.
Trojan-Dropper.Win32.Mutant.e	-	Обнаруживает все файлы вредоносной программы. Библиотеку удаляет (после перезагрузки драйвер ее снова создает), но при попытки удалить драйвер приложение завершается с ошибкой.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	-	Наличие трояна не обнаружено.
Trojan-Spy.Win32.Zbot.bsa	+	Остался ключ автозагрузки.
Trojan.Win32.Agent.lkz	-	Детектирует файлы вредоносной программы, но не предлагает их удалить.
Trojan.Win32.Monderb.gen	+	Остались ключи автозапуска в реестре.
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

BitDefender Antivirus 2009 12.0.10.1

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
Rootkit.Win32.Agent.ea	+	+
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	-	Детектируется только родительский файл.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует библиотеку. Драйвер не обнаружен.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	-	Наличие трояна не обнаружено.
Trojan-Spy.Win32.Zbot.bsa	+	+
Trojan.Win32.Agent.lkz	+	Остался ключ автозапуска.
Trojan.Win32.Monderb.gen	+	+
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Dr.Web Anti-Virus 4.44.5.8080

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	+	+
Email-Worm.Win32.Scano.bd	+	+
Rootkit.Win32.Agent.ea	+	+
Rootkit.Win32.Podnuha.a	+	+
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозапуска.
Trojan-Dropper.Win32.Mutant.e	+	Остался ключ автозапуска.
Trojan-Proxy.Win32.Saturn.cu	+	Остался ключ автозапуска.
Trojan-Proxy. Win32.Xorpix.dh	+	+
Trojan-Spy.Win32.Zbot.bsa	+	+
Trojan.Win32.Agent.lkz	+	+
Trojan.Win32.Monderb.gen	+	+
Trojan.Win32.Pakes.cuh	+	Остался ключ автозапуска.
Trojan.Win32.Small.yc	+	+
Virus.Win32.Rustock.a	+	+

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

http://www.anti-malware.ru/

Eset NOD32 Antivirus 3.0.669.0

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	-	Детектируется только родительский файл.
Backdoor.Win32.Sinowal.ce	-	Детектирует наличие буткита в памяти. Лечение невозможно.
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	-	Наличие трояна не обнаружено.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует библиотеку. Драйвер не обнаружен.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	-	Наличие трояна не обнаружено.
Trojan-Spy.Win32.Zbot.bsa	-	Наличие трояна не обнаружено.
Trojan.Win32.Agent.lkz	-	Детектирует и переименовывает библиотеку. Драйвер не обнаружен.
Trojan.Win32.Monderb.gen	-	Детектирует, но не может удалить библиотеку.
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Детектируется только родительский файл.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

http://www.anti-malware.ru/

F-Secure Anti-Virus 2009

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	-	Длительная загрузка ОС после лечения. Пропал доступ в Интернет.
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
Rootkit.Win32.Agent.ea	-	Зависает при сканировании.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозапуска.
Trojan-Dropper.Win32.Mutant.e	+	Остался ключ автозапуска.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	+	+
Trojan-Spy.Win32.Zbot.bsa	-	Детектирует файл вредоносной программы, но не предлагает удалить.
Trojan.Win32.Agent.lkz	+	Остался ключ автозапуска.
Trojan.Win32.Monderb.gen	+	Остались ключи автозапуска в реестре.
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Kaspersky Anti-Virus 2009 8.0.0.357

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	+	+
Email-Worm.Win32.Scano.bd	+	+
Rootkit.Win32.Agent.ea	-	Зависает при сканировании.
Rootkit.Win32.Podnuha.a	+	Остались ключи автозапуска в реестре.
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозагрузки.
Trojan-Dropper.Win32.Mutant.e	+	+
Trojan-Proxy.Win32.Saturn.cu	-	Детектирует трояна в памяти, но не может найти на диске.
Trojan-Proxy. Win32.Xorpix.dh	+	+
Trojan-Spy.Win32.Zbot.bsa	+	Остался ключ автозагрузки.
Trojan.Win32.Agent.lkz	+	Остался ключ автозагрузки.
Trojan.Win32.Monderb.gen	+	Остались ключи автозапуска в реестре.
Trojan.Win32.Pakes.cuh	-	После установки продукт не работает.
Trojan.Win32.Small.yc	+	+
Virus.Win32.Rustock.a	+	+

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

http://www.anti-malware.ru/

McAfee VirusScan 2008 12.1.110

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	Остался ключ NSP.
Backdoor.Win32.Sinowal.ce	+	+
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозагрузки).
Rootkit.Win32.Agent.ea	-	Детектирует вредоносную программу, но не может удалить.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	-	Наличие трояна не обнаружено.
Trojan-Dropper.Win32.Mutant.e	+	Остались ключи автозагрузки.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	-	Наличие трояна не обнаружено.
Trojan-Spy.Win32.Zbot.bsa	+	+
Trojan.Win32.Agent.lkz	+	Остался ключ автозапуска.
Trojan.Win32.Monderb.gen	-	Детектирует, но не может удалить библиотеку.
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Norton AntiVirus 2009

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	-	Не устанавливается антивирус. Зависает на этапе установки.
Email-Worm.Win32.Scano.bd	+	+
Rootkit.Win32.Agent.ea	-	Зависает сканирование в процессе поиска вредоносных программ.
Rootkit.Win32.Podnuha.a	-	Обнаруживает и удаляет библиотеку. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	+
Trojan-Dropper.Win32.Mutant.e	+	Остался ключ автозагрузки.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	+	+
Trojan-Spy.Win32.Zbot.bsa	+	+
Trojan.Win32.Agent.lkz	+	Остался ключ автозагрузки.
Trojan.Win32.Monderb.gen	+	+
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Детектируется только родительский файл.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Panda Antivirus 2009

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозагрузки).
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозагрузки.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует файлы вредоносной программы, но не может удалить.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	+	Остался ключ автозагрузки.
Trojan-Spy.Win32.Zbot.bsa	+	Остался ключ автозагрузки.
Trojan.Win32.Agent.lkz	+	Остался ключ автозагрузки.
Trojan.Win32.Monderb.gen	+	Остались ключи автозапуска в реестре.
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Детектируется только родительский файл.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Sophos Anti-Virus 7.3.4

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Не может удалить файл червя - он постоянно восстанавливается.
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	-	Наличие трояна не обнаружено.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует только библиотеку и не может ее удалить. Доступ к драйверу для проверки не может получить. При попытке удаления библиотеки, падает процесс winlogon.exe и система падает в BSOD
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	-	Наличие трояна не обнаружено.
Trojan-Spy.Win32.Zbot.bsa	-	Наличие трояна не обнаружено.
Trojan.Win32.Agent.lkz	-	Обнаруживает библиотеку, но ничего с ней сделать не может.
Trojan.Win32.Monderb.gen	-	Не может удалить троянский файл. При попытке лечения падает процесс winlogon.exe и система падает в BSOD
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	+	+
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

Trend Micro Antivirus plus Antispyware 2008 16.10.1182

Название вируса	Вердикт	Подробности
Adware. Win32.NewDotNet	+	+
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Не может удалить файл червя - он постоянно восстанавливается.
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Обнаруживает и удаляет библиотеку. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	+	Остался ключ автозагрузки.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует библиотеку. Драйвер не обнаружен.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	+	+
Trojan-Spy.Win32.Zbot.bsa	-	Наличие трояна не обнаружено.
Trojan.Win32.Agent.lkz	+	Остался ключ автозагрузки.
Trojan.Win32.Monderb.gen	+	+
Trojan.Win32.Pakes.cuh	-	Наличие трояна не обнаружено.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.

VBA32 Antivirus 3.12.8.6

Название вируса	Вердикт	
Adware. Win32.NewDotNet	-	Не может удалить файл рекламной программы.
Backdoor.Win32.Sinowal.ce	-	Наличие трояна не обнаружено.
Email-Worm.Win32.Scano.bd	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозагрузки).
Rootkit.Win32.Agent.ea	-	Наличие трояна не обнаружено.
Rootkit.Win32.Podnuha.a	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Dropper.Win32.Agent.vug	-	Наличие трояна не обнаружено.
Trojan-Dropper.Win32.Mutant.e	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan-Proxy.Win32.Saturn.cu	-	Наличие трояна не обнаружено.
Trojan-Proxy. Win32.Xorpix.dh	-	Наличие трояна не обнаружено.
Trojan-Spy.Win32.Zbot.bsa	-	Наличие трояна не обнаружено.
Trojan.Win32.Agent.lkz	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Trojan.Win32.Monderb.gen	-	Детектирует, но не может удалить библиотеку.
Trojan.Win32.Pakes.cuh	-	Не может удалить файл трояна - он постоянно восстанавливается.
Trojan.Win32.Small.yc	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
Virus.Win32.Rustock.a	-	Наличие трояна не обнаружено.

"Наличие трояна не обнаруживается" означает, что файл вируса не обнаруживается в зараженной системе, при этом родительский файл (дистрибутив) детектируется.