Anti-Malware
Anti-Malicious Software

Результаты теста антивирусов на лечение активного заражения (Тест №4 от 02.2010)

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

Таблица 1: Итоговые результаты лечения

Антивирус	Награда	% вылеченных
Dr.Web Anti-Virus 5.00.10.11260		81%
Kaspersky Anti-Virus 2010 (9.0.0.736)	**Gold Malware Treatment Award**	
Avast! Professional Edition 4.8.1229		63%
Microsoft Security Essentials 1.0.1611.0	**Silver Malware Treatment Award**	
Norton AntiVirus 2010 (17.0.0.136)		56%
F-Secure Anti-Virus 2010 10.00 build 246	**Bronze Malware Treatment Award**	44%
Panda Antivirus 2010 (9.01.00)	**Тест провален**	38%
AVG Anti-Virus & Anti-Spyware 9.0.716		31%
Avira AntiVir PE Premium 9.0.0.75		
Sophos Anti-Virus 9.0.0		
Trend Micro Antivirus plus Antispyware 2010 (17.50.1366)		
BitDefender Antivirus 2010 13.0.18.345		25%
Eset NOD32 Antivirus 4.0.474.0		
McAfee VirusScan Plus 2010 (13.15.113)		19%
Comodo Antivirus 3.13.121240.574		13%
Outpost Antivirus Pro 2009 (6.7.1 2983.450.0714)		
VBA32 Antivirus 3.12.12.0		6%

Таблица 2a: Результаты лечения активного заражения различными антивирусными продуктами

Антивирус \ вредоносное ПО	Avast! Professional Edition 4.8.1229	AVG Anti-Virus & Anti-Spyware 9.0.716	Avira AntiVir PE Premium 9.0.0.75	BitDefender Antivirus 2010 13.0.18.345	Comodo Antivirus 3.13.121240.574	Dr.Web Anti-Virus 5.00.10.11260	Eset NOD32 Antivirus 4.0.474.0	F-Secure Anti-Virus 2010 10.00 build 246	Kaspersky Anti-Virus 2010 (9.0.0.736 (a.b))
AdWare.Virtumonde (Vundo)	+	+	+	+	+	+	+	+	+
Rustock (NewRest)	+	-	-	-	-	+	-	-	-
Sinowal (Mebroot)	-	-	-	-	-	-	-	-	-
Email-Worm.Scano (Areses)	-	-	-	-	-	+	-	+	-
TDL (TDSS, Alureon, Tidserv)	+	+	-	-	-	+	-	+	+
TDL2 (TDSS, Alureon, Tidserv)	-	+	-	-	-	-	-	-	+
Srizbi	+	-	-	+	-	+	-	-	+
Rootkit.Podnuha (Boaxxe)	+	-	-	-	-	+	-	-	+
Rootkit.Pakes (synsenddrv)	+	+	+	-	+	+	+	+	+
Rootkit.Protector (Cutwail, Pandex)	+	-	+	-	-	+	-	-	+
Virus.Protector (Kobcka, Neprodoor)	-	-	-	-	-	+	-	-	+
Xorpix (Eterok)	+	-	+	-	-	+	+	+	+
Trojan-Spy.Zbot	+	+	+	+	-	+	+	+	+
Win32/Glaze	+	-	-	+	-	-	-	+	+
SubSys (Trojan.Okuks)	-	-	-	-	-	+		-	+
TDL3 (TDSS, Alureon, Tidserv)	-	-	-	-	-	+	-	-	+
Вылечено/Всего	10/16	5/16	5/16	4/16	2/16	13/16	4/16	7/16	13/16

Таблица 2б: Результаты лечения активного заражения различными антивирусными продуктами

Антивирус \ вредоносное ПО	McAfee VirusScan Plus 2010 (13.15.113)	Microsoft Security Essentials 1.0.1611.0	Norton AntiVirus 2010 (17.0.0.136)	Outpost Antivirus Pro 2009 (6.7.1.2983.450 .0714)	Panda Antivirus 2010 (9.01.00)	Sophos Anti-Virus 9.0.0	Trend Micro Antivirus plus Antispyware 2010 (17.50.1366)	VBA32 Antivirus 3.12.12.0
AdWare.Virtumonde (Vundo)	+	+	+	+	+	+	+	-
Rustock (NewRest)	-	+	+	-	+	-	-	-
Sinowal (Mebroot)	-	-	-	-	-	-	-	-
Email-Worm.Scano (Areses)	-	-	+	-	-	-	-	-
TDL (TDSS, Alureon, Tidserv)	-	-	+	-	-	+	+	-
TDL2 (TDSS, Alureon, Tidserv)	-	+	+	-	-	-	-	-
Srizbi	-	-	-	-	-	-	-	-
Rootkit.Podnuha (Boaxxe)	-	+	-	-	-	-	-	-
Rootkit.Pakes (synsenddrv)	-	+	+	-	+	+	+	-
Rootkit.Protector (Cutwail, Pandex)	-	+	-	-	-	-	-	-
Virus.Protector (Kobcka, Neprodoor)	-	+	-	-	-	-	-	-
Xorpix (Eterok)	-	+	+	-	+	-	-	-
Trojan-Spy.Zbot	+	+	+	-	+	+	+	-
Win32/Glaze	-	+	+	+	+	-	+	+
SubSys (Trojan.Okuks)	+	-	-	-	-	+	-	-
TDL3 (TDSS, Alureon, Tidserv)	-	-	-	-	-	-	-	-
Вылечено/Всего	3/16	10/16	9'/16	2/16	6/16	5/16	5/16	1/16

+	- 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	Алиасы
AdWare.Win32.Virtumonde.nmz	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 с произвольным именем. Файл постоянно открыт, что не позволяет его удалить/переименоваать. Вредоносный код мониторит создания ключа отложенного перемещения/переименования и, в случае обнаружения имени своей библиотеки в значении параметра этого ключа, удаляет его.	Файл постоянно держится открытым, пересоздание своих ключей автозагрузки и удаление ключа PendingFileRenameOperations, который используют антивирусы для удаления вредоносных программ.	AdWare.Virtumonde (Vundo)
Backdoor.Win32.NewRest.z	Троянская программа-спамбот. Является KernelMode руткитом. При инсталляции создает драйвер в каталоге Drivers с произвольным именем. Блокирует доступ к своему файлу перехватом IRP обработчиков драйвера файловой системы, постоянно пересоздает свой файл. Блокирует свой ключ реестра от чтения и удаления перехватами в ядре.	KernelMode (правка адресов в KiST) NtCreateKey NtOpenKey NtTerminateProcess IRP-hooks Ntfs IRP_MJ_CREATE DKOH Key object (ParseProcedure)	Rustock (NewRest)
Backdoor.Win32.Sinowal.fkp	Троянская программа-шпион. При запуске модифицирует главную загрузочную запись (MBR) жесткого диска с целью загрузки своего драйвера еще до старта ОС. Драйвер хранится в неразмеченной области диска. Перехватывает IRP обработчики драйвера, распологающегося в стеке вслед за устройством \Device\Harddiskx\DRx с целью блокировки чтения/изменения антивирусными продуктами главной загрузочной записи.	KernelMode IRP-hooks IRP_MJ_INTERNAL_DEVICE_CONTROL	Sinowal (Mebroot)

Email-Worm.Win32.Scano.ao	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). Создает в системных процессах троянские потоки, которые 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	Email-Worm.Scano (Areses)
Packed.Win32.TDSS.z	Троянская программа. Является KernelMode руткитом. При инсталляции создает драйвер в \WINDOWS\system32\drivers с именем aliserv3.sys и библиотеку alil.dll в системном каталоге. Драйвер руткита является фильтром драйвера файловой системы, чем и достигается маскировка на диске. Блокирует открытие тома. Маскируется в реестре перехватами в ядре и в памяти DKOM-методом. Использует функцию LockFile с целью блокировки чтения своих файлов.	KernelMode (модификация машинного кода ядра - сплайсинг) NtFlushInstructionCache NtEnumerateKey Driver-Filter DKOM	TDL (TDSS, Alureon, Tidserv)
Packed.Win32.TDSS.z	Троянская программа. Является KernelMode руткитом. При инсталляции создает драйвер в \WINDOWS\system32\drivers\gasfky*.sys и две dll в системном каталоге. Вредоносная программа маскируется на диске, в реестре и памяти. Блокирует открытие диска, чтение тома, пересоздает свои ключи автозагрузки и файлы в случае удаления. Снимает права доступа к своим ключам. Переустанавливает свои перехваты в случае их снятия.	KernelMode (модификация машинного кода ядра - сплайсинг) NtFlushInstructionCache NtEnumerateKey NtSaveKey NtSaveKeyEx IofCallDriver IofCompleteRequest DKOM	TDL2 (TDSS, Alureon, Tidserv)

Trojan.Win32.Srizbi.cb	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	Srizbi
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\Parameters\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	Rootkit.Podnuha (Boaxxe)
Rootkit.Win32.Pakes.zp	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.	KernelMode (модификация машинного кода ядра - сплайсинг) IofCompleteRequest stealth SSDT hooks (KTHREAD modification)	Rootkit.Pakes (synsenddrv)
Rootkit.Win32.Protector.cd	Троянская программа-спамбот. Является KernelMode руткитом. При инсталляции создает драйвер в \Windows\system32\drivers\Ati*.sys. Драйвер руткита блокирует к себе доступ перехватом IRP обработчиков драйвера файловой системы и защищает свой ключ от удаления установкой колбеков на работу с реестром. Спамбот переустанавливает свои IRP-перехваты в случае их снятия.	KernelMode IRP-hooks Ntfs IRP_MJ_CREATE FastFat IRP_MJ_CREATE CmRegisterCallback	Rootkit.Protector (Cutwail, Pandex)

Virus.Win32.Protector.b	Троянская программа-спамбот. Является KernelMode руткитом. При инсталляции заражает системный драйвер ndis.sys и хуком на IofCallDriver маскируется от обнаружения, подсовывая при чтении зараженного файла оригинальное его содержимое. Инфектор создает свою копию в системном каталоге с именем reader_s.exe, прописывается в ключе Run, инжектится в создаваемый процесс svchost сцелью рассылки спама. Рутикит компонента также инжектится в svchost и рассылает спам.	KernelMode (модификация машинного кода ядра - сплайсинг) IofCallDriver	Virus.Protector (Kobcka, Neprodoor)
Trojan.Win32.Agent.xlg	Троянская программа. Является библиотекой - \documents and settings\all users\Documents\settings\abc32.dll, открытой с монопольным доступом. Имеет атрибут "скрытый" вместе с каталогом в котором находится. Библиотека зарегистрирована для автоматического запуска в системном реестре - Winlogon\Notify. На ключа Notify права на чтение оставляет только у группы System. В случае удаления ключа автозагрузки, он моментально пересоздается.	Монопольное открытие файла и пересоздание своего ключа автозагрузки	Xorpix (Eterok)
Trojan-Spy.Win32.Zbot.gen	Троянская программа-шпион. Перехватывает множество функций в UserMode с целью маскировки и шпионажа (перехват методом подмены адресов). При инсталляции создает файл sdra64.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 монопольным открытием и маскируется на диске перехватом ntdll.dll:NtQueryDirectoryFile.	UserMode (подмена адреса) ntdll.dll:NtQueryDirectoryFile Блокировка своего файла от открытия, восстановление ключей автозагрузки	Zbot
Trojan-PSW.Win32.Ambera.n	Троянская программа-шпион. При запуске создает файл xas32.dll в системной директории и регистрирует его в реестре для автоматической загрузки как Winsock Providers. В случае отсутствия файла xas32.dll (удаление его антивирусом), но наличия ключей Winsock - будет отсутствовать доступ в Интернет.	Регистирация в системном реестре как Winsock Providers	Win32/Glaze

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	SubSys (Trojan.Okuks)
Trojan.Win32.Cosmu.cyq	Троянская программа. Является KernelMode руткитом. При инсталляции заражает системный порт или мини-порт драйвер (например, atapi.sys) таким образом, что его размер не изменяется и позволяет загрузить в память драйвер, расположенный в последних секторах жесткого диска на виртуальной шифрованной файловой системе. При чтении зараженного файла руткит подсовывает оригинальное содержимое файла до заражения.	KernelMode DKOM	TDL3 (TDSS, Alureon, Tidserv)

Avast! Professional Edition 4.8.1368

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска.
Rustock (NewRest)	+	+
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	-	Детектирует библиотеку. Драйвер не обнаружен.
Srizbi	+	+
Rootkit.Podnuha (Boaxxe)	+	Остались ключи автозапуска.
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	+	+
Virus.Protector (Kobcka, Neprodoor)	-	Удаляет зараженный системный файл вместе с сервисом. Пропадает сеть.
Xorpix (Eterok)	+	Остался ключ автозапуска.
Trojan-Spy.Zbot	+	+
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.*
TDL3 (TDSS, Alureon, Tidserv)	-	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/

* - 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.

2. AVG Anti-Virus & Anti-Spyware 9.0.716

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	-	Наличие трояна не обнаружено.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	+	Остался ключ автозапуска.
TDL2 (TDSS, Alureon, Tidserv)	+	Остался ключ автозапуска.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Обнаруживает и удаляет библиотеку. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозапуска.
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	-	Невозможно установить на зараженную систему.
Trojan-Spy.Zbot	+	Остался ключ автозапуска.
Win32/Glaze	-	Файл удален. Пропал доступ в Интернет.
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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/

Avira AntiVir PE Premium 9.0.0.75

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	-	Обнаруживает, но не может удалить файл.
Sinowal (Mebroot)	-	Детектирует наличие руткита, но не лечит систему.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
Srizbi	-	Зависает при попытке проверить файл руткита.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозагрузки.
Rootkit.Protector (Cutwail, Pandex)	+	Остался ключ автозагрузки.
Virus.Protector (Kobcka, Neprodoor)	-	Невозможно установить на зараженную систему.
Xorpix (Eterok)	+	Остался ключ автозагрузки.
Trojan-Spy.Zbot	+	Остался ключ автозагрузки.
Win32/Glaze	-	Детектирует файл, но не удаляет его.
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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 2010 13.0.18.345

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	-	Наличие трояна не обнаружено.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
Srizbi	+	+
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	-	Наличие трояна не обнаружено.
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	-	Наличие трояна не обнаружено.
Trojan-Spy.Zbot	+	+
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.

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

Comodo Antivirus 3.13.121240.574

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	-	Наличие трояна не обнаружено.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Детектирует библиотеку. Драйвер не обнаружен.
TDL2 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозагрузки.
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	-	Наличие трояна не обнаружено.
Trojan-Spy.Zbot	-	Наличие трояна не обнаружено.
Win32/Glaze	-	Файл удален. Пропал доступ в Интернет.
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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 5.00.10.11260

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	+	+
Sinowal (Mebroot)	-	Перезагрузка системы при запуске сканера.
Email-Worm.Scano (Areses)	+	+
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	-	Не позволяет запустить собственые компоненты.
Srizbi	+	+
Rootkit.Podnuha (Boaxxe)	+	+
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	+	+
Virus.Protector (Kobcka, Neprodoor)	+	+
Xorpix (Eterok)	+	+
Trojan-Spy.Zbot	+	+
Win32/Glaze	-	Файл удален. Пропал доступ в Интернет.
SubSys (Trojan.Okuks)	+	+
TDL3 (TDSS, Alureon, Tidserv)	+	+

"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 4.0.474.0

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	-	Детектирует наличие руктита, но ничего не может сделать.
Sinowal (Mebroot)	-	Детектирует наличие руктита, но ничего не может сделать.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска)
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Детектирует библиотеку. Драйвер не обнаружен.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозагрузки.
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	+	Остался ключ автозагрузки.
Trojan-Spy.Zbot	+	Остался ключ автозагрузки.
Win32/Glaze	-	Файл удален. Пропал доступ в Интернет.
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	Детектирует наличие руктита, но ничего не может сделать.

"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 2010 10.00 build 246

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	-	Детектирует наличие руткита, после чего система циклически перезагружается в ходе своей загрузки.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	+	+
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	-	Детектирует наличие руткита, но не лечит систему.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	+	+
Trojan-Spy.Zbot	+	Остался ключ автозагрузки.
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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 2010 (9.0.0.736 (a.b))

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	-	После установки продукт не работает.
Sinowal (Mebroot)	-	Постоянно падает процесс антивируса.
Email-Worm.Scano (Areses)	-	Зависает при обнаружении.
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	+	+
Srizbi	+	+
Rootkit.Podnuha (Boaxxe)	+	+
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	+	+
Virus.Protector (Kobcka, Neprodoor)	+	+
Xorpix (Eterok)	+	+
Trojan-Spy.Zbot	+	+
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	+	+
TDL3 (TDSS, Alureon, Tidserv)	+	+

"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 Plus 2010 (13.15.113)

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	-	Наличие трояна не обнаружено.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Детектирует наличие руткита, но не лечит систему.
Srizbi	-	Детектирует наличие руткита, но не лечит систему.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку и переименовывает ее. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	-	Наличие трояна не обнаружено.
Rootkit.Protector (Cutwail, Pandex)	-	Детектирует наличие руткита, но не лечит систему.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	-	Наличие трояна не обнаружено.
Trojan-Spy.Zbot	+	+
Win32/Glaze	-	Файл удален. Пропал доступ в Интернет.
SubSys (Trojan.Okuks)	+	+
TDL3 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.

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

Microsoft Security Essentials 1.0.1611.0

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	+	Остался ключ автозагрузки.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Не может удалить файл червя - он постоянно восстанавливается.
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	+	Остался ключ автозагрузки.
Srizbi	-	Зависает при попытке проверить файл руткита
Rootkit.Podnuha (Boaxxe)	+	Остались ключи автозагрузки.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозагрузки.
Rootkit.Protector (Cutwail, Pandex)	+	Остался ключ автозагрузки.
Virus.Protector (Kobcka, Neprodoor)	+	+
Xorpix (Eterok)	+	Остался ключ автозагрузки.
Trojan-Spy.Zbot	+	Остался ключ автозагрузки.
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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 2010 (17.0.0.136)

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	+	+
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	+	+
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	+	+
Srizbi	-	Зависает при попытке проверить файл руткита.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку и переименовывает ее. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	+	+
Trojan-Spy.Zbot	+	+
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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/

Outpost Antivirus Pro 2009 (6.7.1 2983.450.0714)

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	-	Наличие трояна не обнаружено.
Sinowal (Mebroot)	-	Невозможно установить на зараженную систему.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Детектирует библиотеку. Драйвер не обнаружен.
Srizbi	-	BSOD
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	-	Наличие трояна не обнаружено.
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Детектирует наличие руктита, но ничего не может сделать.
Xorpix (Eterok)	-	Наличие трояна не обнаружено.
Trojan-Spy.Zbot	-	Наличие трояна не обнаружено.
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Детектирует трояна,но не может удалить.
TDL3 (TDSS, Alureon, Tidserv)		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 2010 (9.01.00)

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остались ключи автозапуска в реестре.
Rustock (NewRest)	+	Остался ключ автозагрузки.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Детектирует наличие руткита, но не лечит систему.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку и удаляет ее. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозагрузки.
Rootkit.Protector (Cutwail, Pandex)	-	Детектирует наличие руткита, но не лечит систему.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	+	Остался ключ автозагрузки.
Trojan-Spy.Zbot	+	Остался ключ автозагрузки.
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	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 9.0.0

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	-	Обнаруживает, но не может удалить файл.
Sinowal (Mebroot)	-	Детектирует наличие руткита, но не лечит систему.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	-	Детектирует наличие руткита, но не лечит систему.
Srizbi	-	Детектирует наличие руткита, но не лечит систему.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	-	Обнаруживает, но не может удалить файл.
Virus.Protector (Kobcka, Neprodoor)	-	Удаляет зараженный системный файл. Пропадает сеть.
Xorpix (Eterok)	-	Детектирует библиотеку, но не может с ней ничего сделать.
Trojan-Spy.Zbot	+	+
Win32/Glaze	-	Файл удален. Пропал доступ в Интернет.
SubSys (Trojan.Okuks)	+	+
TDL3 (TDSS, Alureon, Tidserv)	-	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/

Trend Micro Antivirus plus Antispyware 2010 (17.50.1366)

Название вируса	Вердикт	Подробности
AdWare.Virtumonde (Vundo)	+	Остался ключ автозагрузки.
Rustock (NewRest)	-	Обнаруживает, но не может удалить файл.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Не может удалить файл червя - он постоянно восстанавливается.
TDL (TDSS, Alureon, Tidserv)	+	Остался ключ автозагрузки.
TDL2 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку, но не может с ней ничего сделать. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	+	Остался ключ автозагрузки.
Rootkit.Protector (Cutwail, Pandex)	-	Обнаруживает, но не может удалить файл.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	-	Детектирует библиотеку, но не может с ней ничего сделать.
Trojan-Spy.Zbot	+	Остался ключ автозагрузки.
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Наличие трояна не обнаружено.
TDL3 (TDSS, Alureon, Tidserv)	-	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/

VBA32 Antivirus 3.12.12.0

Название вируса	Вердикт	
AdWare.Virtumonde (Vundo)	-	Детектирует, но не может удалить библиотеку.
Rustock (NewRest)	-	Наличие трояна не обнаружено.
Sinowal (Mebroot)	-	Наличие трояна не обнаружено.
Email-Worm.Scano (Areses)	-	Файл удален, но при старте системы пропадает рабочий стол (не удален ключ автозапуска).
TDL (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
TDL2 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.
Srizbi	-	Наличие трояна не обнаружено.
Rootkit.Podnuha (Boaxxe)	-	Детектирует библиотеку и переименовывает ее. Драйвер не обнаружен.
Rootkit.Pakes (synsenddrv)	-	Наличие трояна не обнаружено.
Rootkit.Protector (Cutwail, Pandex)	-	Наличие трояна не обнаружено.
Virus.Protector (Kobcka, Neprodoor)	-	Обнаруживает и удаляет инфектора. Зараженный драйвер не обнаружен.
Xorpix (Eterok)	-	Детектирует заражение, но не может открыть файл.
Trojan-Spy.Zbot	-	Наличие трояна не обнаружено.
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	-	Систему невозможно загрузить, падает в BSOD т.к. остался ключ автозагрузки.
TDL3 (TDSS, Alureon, Tidserv)	-	Наличие трояна не обнаружено.

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