Протокол исследования системы

AVZ X.XX http://z-oleg.com/secur/avz/

Список процессов

Имя файла	PID	Описание	Copyright	MDX	Информа
c:\program files\tech\office program selector\X.X\acromapp.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	ACROX	Copyright XXXX By LEE,WEI-BIN.	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Tech\Off Selector\X.X\ACROMAPP.
C:\Program Files\Tech\Office Program Selector\X.X\ACRMODLS.DLL Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX		Copyright © XXXX By LEE,WEI-BIN.	--	нет
c:\program files\via technologies, inc\via audio driver setup program\audiodeck\audiodeck.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	AudioDeck Microsoft ???????	???? (C) XXXX	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\VIA Tecl Audio Driver Setup Program\AudioDeck\Audio
C:\Program Files\VIA Technologies, Inc\VIA Audio Driver Setup Program\AudioDeck\AudioDeck.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	AudioDeck Microsoft ???????	???? (C) XXXX	??	нет
c:\windows\explorer.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	Проводник	© Корпорация Майкрософт. Все права защищены.	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: C:\WINDOWS\Explorer.EX
C:\PROGRA~X\ZIPGEN~X\contmenu.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	Context Menu for ZipGenius	Copyright ©XXXX, XXXX M.Dev Software	--	нет
C:\WINDOWS\systemXX\msvdm.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX			--	нет
C:\Program Files\Acronis\PrivacyExpert\PrivShellExt.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	Acronis PrivacyExpert shell extension.	(c) XXXX Acronis. All rights reserved.	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\zlavscan.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	zlavscan shell extension	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
c:\windows\systemXX\lsass.exe Скрипт: Карантин, Удалить, Удалить через BC	XXX	LSA Shell (Export Version)	© Microsoft Corporation. All rights reserved.	??	XX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: C:\WINDOWS\systemXX\l
C:\WINDOWS\systemXX\relogXap.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXX	Acronis Relogon Authentication Package	Copyright (C) Acronis, XXXX-XXXX.	--	нет
c:\program files\windows defender\msascui.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	Windows Defender User Interface	© Microsoft Corporation. All rights reserved.	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Windows Defender\MSASCui.exe" -h
C:\Program Files\Windows Defender\MsMpRes.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	Модуль ресурсов	© Корпорация Майкрософт. Все права защищены.	--	нет
c:\program files\a!k research labs\notesholder\notesholder.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX			??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\A!K Res Labs\NotesHolder\NotesHo
C:\Program Files\A!K Research Labs\NotesHolder\NotesHolder.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX			??	нет
c:\program files\rezerv-copy\rezervcopy.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	Rezerv-Copy	Copyright © XXXX Lokas Ltd.	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Rezerv-Copy\RezervCopy.exe"
C:\Program Files\Rezerv-Copy\RezervCopy.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	Rezerv-Copy	Copyright © XXXX Lokas Ltd.	??	нет
					XXX.XX кб, rsAh,

c:\program files\common files\acronis\scheduleX\schedhlp.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	Acronis Scheduler Helper	Copyright (C) XXXX-XXXX Acronis	??	создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Common Files\Acronis\ScheduleX\sc
C:\Program Files\Common Files\Acronis\ScheduleX\schedhlp.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	Acronis Scheduler Helper	Copyright (C) XXXX-XXXX Acronis	??	нет
c:\program files\common files\acronis\scheduleX\schedulX.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	Acronis Scheduler X	Copyright (C) XXXX-XXXX Acronis	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Common Files\Acronis\ScheduleX\sc
C:\Program Files\Common Files\Acronis\ScheduleX\schedulX.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	Acronis Scheduler X	Copyright (C) XXXX-XXXX Acronis	??	нет
c:\program files\openoffice.org X.X\program\soffice.bin Скрипт: Карантин, Удалить, Удалить через BC	XXXX	OpenOffice.org X.X	Copyright © XXXX by Sun Microsystems, Inc.	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX X: изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\OpenOffi X.X\program\soffice.exe" - Settings\Админ\Рабочий с работыXX.odb"
C:\Program Files\OpenOffice.org X.X\program\avmediaXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\dbaXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\dbaxmlXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\dbtoolsXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\dbuXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\dnd.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\fileacc.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\filterconfigX.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\fsstorage.uno.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\ftransl.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\goXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\iXXnpool.uno.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет

C:\Program Files\OpenOffice.org X.X\program\iXXnutilMSC.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\icuinXX.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	IBM ICU IXXN DLL	Copyright (C) XXXX, International Business Machines Corporation and others. All Rights Reserved.	--	нет
C:\Program Files\OpenOffice.org X.X\program\lngXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\mcnttype.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\packageX.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\soXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\svxXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\sysdtrans.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\updchk.uno.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\uuiXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\xoXXXmi.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
C:\Program Files\OpenOffice.org X.X\program\xstor.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX		Copyright © XXXX by Sun Microsystems, Inc.	--	нет
c:\program files\acronis\trueimage\timountermonitor.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	Monitor for Acronis True Image Backup Archive Explorer	Copyright (c) Acronis XXXX-XXXX	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Acronis\TrueImage\Ti
C:\Program Files\Acronis\TrueImage\TimounterMonitor.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	Monitor for Acronis True Image Backup Archive Explorer	Copyright (c) Acronis XXXX-XXXX	??	нет
c:\program files\acronis\trueimage\trueimagemonitor.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	TrueImage	Copyright (C) XXXX-XXXX Acronis.	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Acronis\TrueImage\Tr
C:\Program Files\Common Files\Acronis\Common\rpcXclient.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXX			--	нет
C:\Program Files\Acronis\TrueImage\TrueImageMonitor.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	TrueImage	Copyright (C) XXXX-XXXX Acronis.	??	нет
			Copyright ©		XX.XX кб, rsAh,

c:\windows\systemXX\zonelabs\vsmon.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXX	TrueVector Service	XXXX-XXXX, Zone Labs, LLC	??	создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка:
C:\WINDOWS\systemXX\zonelabs\lib\pyd\Xsocket.pyd Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXX			--	нет
C:\WINDOWS\systemXX\ZoneLabs\av.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	av feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\camupd.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	camupd feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\fbl.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	Feature based licensing library	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\streamapi\httpblocker\httpblocker.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	HttpBlocker plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\imsecure.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\streamapi\imslsp\imslsp.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	ZoneAlarm IMsecure components for securing MSN/AIM-OSCAR/YIM protocols	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\LIBEAYXXXX.X.Xl.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX			--	нет
C:\WINDOWS\systemXX\zonelabs\lib\pyd\pyexpat.pyd Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXX			--	нет
C:\WINDOWS\systemXX\zonelabs\lib\pyd\pyvsinit.pyd Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX			--	нет
C:\WINDOWS\systemXX\ZoneLabs\qrbase.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	qrbase	Copyright © XXXX	--	нет
C:\WINDOWS\systemXX\ZoneLabs\plugins\rpcXserver\rpcXserver.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	RPC Server plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	scheduler feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\zonelabs\lib\pyd\signedDll.pyd Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXX			--	нет
C:\WINDOWS\systemXX\ZoneLabs\srescan.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	srescan	Copyright © XXXX	--	нет
C:\WINDOWS\systemXX\ZoneLabs\ssleayXX.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\vsavpro.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\VSDATA.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	TrueVector Service DLL	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\vsdb.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\VSINIT.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\vsmon.exe Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	??	нет
C:\WINDOWS\systemXX\ZoneLabs\plugins\vsmonXplugin\vsmonXplugin.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	vsmon plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\vsmondll.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\VSRULEDB.DLL	XXXXXXXXXX	TrueVector	Copyright © XXXX-	--	нет

Скрипт: Карантин, Удалить, Удалить через ВС		Service	XXXX, Zone Labs, LLC		
C:\WINDOWS\systemXX\VSUTIL.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\vsvault.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\vswmi.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	vsmon component	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\vsxml.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\zlcomm.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	ZLComm	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZLCommDB.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	ZLCommDB	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\zlquarantine.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	zlquarantine	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\zlsre.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	zlsre	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\zlupdate.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	ZLUpdate feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\zpengXX.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXX	Python Core	Copyright © XXXX-XXXX Python Software Foundation. Copyright © XXXX BeOpen.com. Copyright © XXXX-XXXX CNRI. Copyright © XXXX-XXXX SMC.	--	нет
c:\program files\mustek XXXX ub plus\driver\watch.exe Скрипт: Карантин, Удалить, Удалить через ВС	XXXX	Watch Dog	Copyright (C) XXXX	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX X:X изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Mustek X Plus\Driver\WATCH.exe"
C:\WINDOWS\TWAINXXX\SXUXXBX\SBSpiXT.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXX	SBspi	Copyright с XXXX	--	нет
c:\windows\systemXX\winlogon.exe Скрипт: Карантин, Удалить, Удалить через ВС	XXX	Программа входа в систему Windows NT	© Корпорация Майкрософт. Все права защищены.	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: winlogon.exe
C:\WINDOWS\systemXX\WgaLogon.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Уведомление о результатах проверки подлинности Windows	© XXXX-XXXX Microsoft Corporation	--	нет
c:\program files\zone labs\zonealarm\zlclient.exe Скрипт: Карантин, Удалить, Удалить через ВС	XXXX	ZoneAlarm Client	Copyright © XXXX-XXXX, Zone Labs, LLC	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка:
C:\Program Files\Zone Labs\ZoneAlarm\alert.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Alerts Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\av.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	av feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\cam.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Anti-Virus Monitoring Module	Copyright © XXXX-XXXX, Zone	--	нет

			Labs, LLC		
C:\WINDOWS\systemXX\ZoneLabs\camupd.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	camupd feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\email.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Email Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\fbl.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXX	Feature based licensing library	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\filter.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Filter Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\firewall.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Firewall Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\framewrk.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	ZoneAlarm Framework Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\idlock.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	ZoneAlarmPro	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\imsecure.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	IMsecure Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\LIBEAYXXXX.X.Xl.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX			--	нет
C:\Program Files\Zone Labs\ZoneAlarm\privacy.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Privacy Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\programs.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Programs Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXX			--	нет
C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	scheduler feature plug-in	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\security.zap Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	Overview Plugin Module	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\vsdata.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	TrueVector Service DLL	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\VSINIT.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\vsmonapi.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	TrueVector Client Interface	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\VSPUBAPI.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\VSUTIL.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\vsxml.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	TrueVector Service	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\Program Files\Zone Labs\ZoneAlarm\zlclient.exe Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXX	ZoneAlarm Client	Copyright © XXXX-XXXX, Zone Labs, LLC	??	нет
C:\WINDOWS\systemXX\zlcomm.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXXXX	ZLComm	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет

C:\WINDOWS\systemXX\ZLCommDB.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXXX	ZLCommDB	Copyright © XXXX-XXXX, Zone Labs, LLC	--	нет
C:\WINDOWS\systemXX\zpengXX.dll Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXXX	Python Core	Copyright © XXXX-XXXX Python Software Foundation. Copyright © XXXX BeOpen.com. Copyright © XXXX-XXXX CNRI. Copyright © XXXX-XXXX SMC.	--	нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\zpui.pyd Скрипт: Карантин, Удалить, Удалить через BC	XXXXXXXX	zpui Library	Copyright (C) XXXX	--	нет

Обнаружено:XX, из них опознаны как безопасные XX

Модули пространства ядра

Модуль	Базовый адрес	Размер в памяти	Описание	Производитель
snapman.sys Скрипт: Карантин, Удалить, Удалить через BC	FXXXAXXX	XXCXXX (XXXXXX)	Acronis Snapshot API	Copyright (c) Acronis XXXX-XXXX
srescan.sys Скрипт: Карантин, Удалить, Удалить через BC	FXXXXXXX	XXXXXX (XXXXX)		
\SystemRoot\SystemXX\vsdatant.sys Скрипт: Карантин, Удалить, Удалить через BC	AXXXXXXX	XXXXXX (XXXXXX)	TrueVector Device Driver	Copyright © XXXX-XXXX, Zone Labs, LLC

Обнаружено модулей - XXX, опознано как безопасные - XXX

Службы

Служба	Описание	Статус	Файл	Группа	Зависимости
AcrSchXSvc	Acronis SchedulerX Service	Работает	"C:\Program Files\Common Files\Acronis\ScheduleX\schedulX.exe" Скрипт: Карантин, Удалить, Удалить через BC		RpcSs
ATI Smart	ATI Smart	Не запущен	C:\WINDOWS\systemXX\atiXsgag.exe Скрипт: Карантин, Удалить, Удалить через BC		
BOCore	BOCore	Не запущен	C:\Program Files\Comodo\CBOClean\BOCORE.exe Скрипт: Карантин, Удалить, Удалить через BC		
vsmon	TrueVector Internet Monitor	Работает	C:\WINDOWS\systemXX\ZoneLabs\vsmon.exe -service Скрипт: Карантин, Удалить, Удалить через BC	TDI	Afd

Обнаружено - XX, опознано как безопасные - XX

Драйверы

Служба	Описание	Статус	Файл	Группа	Зависимости
Abiosdsk	Abiosdsk	Не запущен	Abiosdsk.sys Скрипт: Карантин, Удалить, Удалить через BC	Primary disk	
abpXXXnX	abpXXXnX	Не запущен	abpXXXnX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
Ad-Watch Connect Filter	Ad-Watch Connect Kernel Filter	Не запущен	\??\C:\WINDOWS\systemXX\drivers\NSDriver.sys Скрипт: Карантин, Удалить, Удалить через BC		
adpuXXXm	adpuXXXm	Не запущен	adpuXXXm.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
AhaXXXx	AhaXXXx	Не запущен	AhaXXXx.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
aicXXuX	aicXXuX	Не запущен	aicXXuX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
aicXXxx	aicXXxx	Не запущен	aicXXxx.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
AliIde	AliIde	Не запущен	AliIde.sys Скрипт: Карантин, Удалить, Удалить через BC	System Bus Extender	
amsint	amsint	Не запущен	amsint.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
asc	asc	Не запущен	asc.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
ascXXXXp	ascXXXXp	Не запущен	ascXXXXp.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
ascXXXX	ascXXXX	Не запущен	ascXXXX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
Atdisk	Atdisk	Не запущен	Atdisk.sys Скрипт: Карантин, Удалить, Удалить через BC	Primary disk	
cdXXxrnt	cdXXxrnt	Не запущен	cdXXxrnt.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
Changer	Changer	Не запущен	Changer.sys Скрипт: Карантин, Удалить, Удалить через BC	Filter	
CmdIde	CmdIde	Не запущен	CmdIde.sys Скрипт: Карантин, Удалить, Удалить через BC	System Bus Extender	

Cpqarray	Cpqarray	Не запущен	Cpqarray.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
dacXXXnt	dacXXXnt	Не запущен	dacXXXnt.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
dptiXo	dptiXo	Не запущен	dptiXo.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
FETNDIS	VIA PCI XX/XXXMb Fast Ethernet адаптер, драйвер для NT	Не запущен	systemXX\DRIVERS\fetndX.sys Скрипт: Карантин, Удалить, Удалить через BC	NDIS	
GMSIPCI	GMSIPCI	Не запущен	\??\G:\INSTALL\GMSIPCI.SYS Скрипт: Карантин, Удалить, Удалить через BC		
hpn	hpn	Не запущен	hpn.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
iXomgmt	iXomgmt	Не запущен	iXomgmt.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI Class	
iXomp	iXomp	Не запущен	iXomp.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
iniXXXu	iniXXXu	Не запущен	iniXXXu.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
IntelIde	IntelIde	Не запущен	IntelIde.sys Скрипт: Карантин, Удалить, Удалить через BC	System Bus Extender	
klX	klX	Не запущен	\SystemRoot\systemXX\DRIVERS\klX.sys Скрипт: Карантин, Удалить, Удалить через BC	PNPXTDI	
lbrtfdc	lbrtfdc	Не запущен	lbrtfdc.sys Скрипт: Карантин, Удалить, Удалить через BC	System Bus Extender	
mraidXXx	mraidXXx	Не запущен	mraidXXx.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
PCIDump	PCIDump	Не запущен	PCIDump.sys Скрипт: Карантин, Удалить, Удалить через BC	PCI Configuration	
PCIIde	PCIIde	Не запущен	PCIIde.sys Скрипт: Карантин, Удалить, Удалить через BC	System Bus Extender	
PDCOMP	PDCOMP	Не запущен	PDCOMP.sys Скрипт: Карантин, Удалить, Удалить через BC		
PDFRAME	PDFRAME	Не запущен	PDFRAME.sys Скрипт: Карантин, Удалить, Удалить через BC		
PDRELI	PDRELI	Не запущен	PDRELI.sys Скрипт: Карантин, Удалить, Удалить через BC		
PDRFRAME	PDRFRAME	Не запущен	PDRFRAME.sys Скрипт: Карантин, Удалить, Удалить через BC		
percX	percX	Не запущен	percX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
percXhib	percXhib	Не запущен	percXhib.sys Скрипт: Карантин, Удалить, Удалить через BC	Filter	
qlXXXX	qlXXXX	Не запущен	qlXXXX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
QlXXwnt	QlXXwnt	Не запущен	QlXXwnt.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
qlXXXXX	qlXXXXX	Не запущен	qlXXXXX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
qlXXXX	qlXXXX	Не запущен	qlXXXX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
qlXXXX	qlXXXX	Не запущен	qlXXXX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
Simbad	Simbad	Не запущен	Simbad.sys Скрипт: Карантин, Удалить, Удалить через BC	Filter	
snapman	Acronis Snapshots Manager	Работает	\SystemRoot\systemXX\DRIVERS\snapman.sys Скрипт: Карантин, Удалить, Удалить через BC		
Sparrow	Sparrow	Не запущен	Sparrow.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
srescan	srescan	Работает	\SystemRoot\systemXX\ZoneLabs\srescan.sys Скрипт: Карантин, Удалить, Удалить через BC		
symXhi	symXhi	Не запущен	symXhi.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
symXuX	symXuX	Не запущен	symXuX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
symcXXX	symcXXX	Не запущен	symcXXX.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
symcXxx	symcXxx	Не запущен	symcXxx.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
TosIde	TosIde	Не запущен	TosIde.sys Скрипт: Карантин, Удалить, Удалить через BC	System Bus Extender	
ultra	ultra	Не запущен	ultra.sys Скрипт: Карантин, Удалить, Удалить через BC	SCSI miniport	
vsdatant	vsdatant	Работает	SystemXX\vsdatant.sys Скрипт: Карантин, Удалить, Удалить через BC	PNPXTDI	TCPIP
Vsp	Vsp	Не запущен	\??\C:\WINDOWS\systemXX\drivers\Vsp.sys Скрипт: Карантин, Удалить, Удалить через BC		
WDICA	WDICA	Не запущен	WDICA.sys Скрипт: Карантин, Удалить, Удалить через BC		

Обнаружено - XXX, опознано как безопасные - XXX

Автозапуск

Имя файла	Статус	Метод запуска	Описание
C:\Documents and Settings\Admin\Рабочий стол\Внимание !.pdf Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\, C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\Ярлык для Внимание !.lnk,
C:\Documents and Settings\Admin\Рабочий стол\Сервисные работыXX.odb Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\, C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\Ярлык для Сервисные работыXX.lnk,
C:\PROGRA~X\COMMON~X\MICROS~X\DW\dwtrigXX.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXUSERS, .DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run, DWQueuedReporting
C:\Program Files\A!K Research Labs\NotesHolder\NotesHolder.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\, C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\NotesHolder.lnk,
C:\Program Files\Acronis\TrueImage\TimounterMonitor.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXLOCALXMACHINE, Software\Microsoft\Windows\CurrentVersion\Run, AcronisTimounterMonitor
C:\Program Files\Acronis\TrueImage\TrueImageMonitor.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXLOCALXMACHINE, Software\Microsoft\Windows\CurrentVersion\Run, TrueImageMonitor.exe
C:\Program Files\Common Files\Acronis\ScheduleX\schedhlp.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXLOCALXMACHINE, Software\Microsoft\Windows\CurrentVersion\Run, Acronis SchedulerX Service
C:\Program Files\Lex!\Lex.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\, C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\Lex!.lnk,
C:\Program Files\Rezerv-Copy\RezervCopy.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\, C:\Documents and Settings\Admin\Главное меню\Программы\Автозагрузка\Rezerv-Copy [Home Edition].lnk,
C:\Program Files\VIA Technologies, Inc\VIA Audio Driver Setup Program\AudioDeck\AudioDeck.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка\, C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка\AudioDeck.lnk,
C:\Program Files\Zone Labs\ZoneAlarm\zlclient.exe Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXLOCALXMACHINE, Software\Microsoft\Windows\CurrentVersion\Run, ZoneAlarm Client
WgaLogon.dll Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXLOCALXMACHINE, SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\WgaLogon, DLLName
appmgmts.dll Скрипт: Карантин, Удалить, Удалить через BC	Активен	Ключ реестра	HKEYXLOCALXMACHINE, SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{cXdcXXXX-XXXa-XXdX-XXdX-XXcXXfbXXXfX}, DLLName

Обнаружено элементов автозапуска - XX, опознано как безопасные - XX

Модули расширения Internet Explorer (BHO, панели ...)

Имя файла	Тип	Описание	Производитель	CLSID
	BHO			SOFTWARE
C:\Program Files\Google\Google Notebook\gnotesX.X.X.XX--XXXXXXXXX.dll Скрипт: Карантин, Удалить, Удалить через BC	BHO	Блокнот Google для IE	Авторские права, XXXX Google	{CCCCCCDX-XXXF-XFXX-XBXX-XXXDEXFXDXXX}
C:\Program Files\Google\Google Notebook\gnotesX.X.X.XX--XXXXXXXXX.dll Скрипт: Карантин, Удалить, Удалить через BC	Панель	Блокнот Google для IE	Авторские права, XXXX Google	{CCCCCCDB-XDDB-XXXX-XXDX-DDXCXXXXXXBF}
C:\WINDOWS\Network Diagnostic\xpnetdiag.exe Скрипт: Карантин, Удалить, Удалить через BC	Модуль расширения	Network Diagnostic for Windows XP	© Microsoft Corporation. All rights reserved.	{eXeXddXX-dXXX-XXXX-XXbX-fXbaXXXXXXXX}

Обнаружено элементов - XX, опознано как безопасные - X

Модули расширения проводника

Имя файла	Назначение	Описание	Производитель	CLSID
deskpan.dll Скрипт: Карантин, Удалить, Удалить через BC	Расширение CPL панорамирования дисплея			{XXXXXXXX-XXdX-XXdX-XbXX-XXaXcXXXXffX}
	Расширения оболочки для сжатия файлов			{XXXBFXEX-FXXX-XXce-XXXD-XXAAXXAXXFXX}
	Контекстное меню шифрования			{XXXFEXBX-BXXX-XXdX-XCXE-XXCXXFBXCXFA}
	Панель задач и меню "Пуск"			{XDFXXEAA-FFXX-XXXX-XXXE-XXXAXXXXEXFX}
rundllXX.exe C:\WINDOWS\systemXX\shimgvw.dll,ImageViewXCOMServer {XXEXBXXX-FXXB-Xdcf-XXDF-CDXXXBXXBFDX} Скрипт: Карантин, Удалить, Удалить через BC	Autoplay for SlideShow			{XXEXBXXX-FXXB-Xdcf-XXDF-CDXXXBXXBFDX}
	Учетные записи пользователей			{XAXDXXBD-XXXX-XXdX-XXXX-XEXXXXXXXXXX}
C:\Program Files\Acronis\PrivacyExpert\PrivShellExt.dll Скрипт: Карантин, Удалить, Удалить через BC	Acronis PrivacyExpert Shell	Acronis PrivacyExpert	(c) XXXX Acronis.	{XXCEXXXX-XXFX-XXXB-AXXF-

	Extension Class	shell extension.	All rights reserved.	XXXXXXXBXCAX}
C:\PROGRA~X\ZIPGEN~X\contmenu.dll Скрипт: Карантин, Удалить, Удалить через BC	ZipGenius Shell Extension	Context Menu for ZipGenius	Copyright ©XXXX, XXXX M.Dev Software	{CXXXEXFX-EXBX-XXFX-BXXA-XBAXXXCBEXXX}
C:\PROGRA~X\ZIPGEN~X\zgtips.dll Скрипт: Карантин, Удалить, Удалить через BC	ZipGenius Zip InfoTip	Infotips shell extension for ZipGenius	Copyright ©XXXX-XXXX M.Dev Software	{XEXACXEX-XXXD-XXDX-XXBX-FAXXXXXXXEXX}
C:\PROGRA~X\ZIPGEN~X\DROPHA~X.DLL Скрипт: Карантин, Удалить, Удалить через BC	ZipGenius Drop handler	ZG Drop Handler		{XXXAXCXX-EAXX-XXAE-AXEX-XXEXXEXXXXX}
C:\PROGRA~X\ZIPGEN~X\ZGDRAG~X.DLL Скрипт: Карантин, Удалить, Удалить через BC	ZipGenius DnD Extract handler	Drag and drop dll	©XXXX, XXXX M.Dev Software	{FEXDXXBF-XXXA-XXXX-XCXE-XXDXXAXXCXXX}
C:\Program Files\Zone Labs\ZoneAlarm\zlavscan.dll Скрипт: Карантин, Удалить, Удалить через BC	Multiscan	zlavscan shell extension	Copyright © XXXX-XXXX, Zone Labs, LLC	{DXXXXDXX-XXXX-XXXX-XEEE-FXAXXXXXBEBB}
C:\Program Files\Google\Google Notebook\gnotesX.X.X.XX--XXXXXXXXX.dll Скрипт: Карантин, Удалить, Удалить через BC	&Google Notebook	Блокнот Google для IE	Авторские права, XXXX Google	{CCCCCCDX-XXXF-XFXX-XBXX-XXXDEXFXDXXX}
C:\Program Files\Google\Google Notebook\gnotesX.X.X.XX--XXXXXXXXX.dll Скрипт: Карантин, Удалить, Удалить через BC	&Google Notebook	Блокнот Google для IE	Авторские права, XXXX Google	{CCCCCCDB-XDDB-XXXX-XXDX-DDXCXXXXXXBF}
	Shell Extension for Malware scanning			{XXACXXXX-XXXX-XEDX-XXDE-BXXXXFAXDXXA}
C:\WINDOWS\systemXX\msvdm.dll Скрипт: Карантин, Удалить, Удалить через BC	Desktop Manager			{XXXCXEXX-XXXF-XXXX-XXAC-XACBXXXAAXDE}
	<назначение на задано>			

Обнаружено элементов - XXX, опознано как безопасные - XXX

Модули расширения системы печати (мониторы печати, провайдеры)

Имя файла	Тип	Наименование	Описание	Производитель

Обнаружено элементов - X, опознано как безопасные - X

Задания планировщика задач Task Scheduler

Имя файла	Имя задания	Состояние задания	Описание	Производитель
C:\Documents and Settings\Чистюля\Рабочий стол\X.bat Скрипт: Карантин, Удалить, Удалить через BC	X.job	The task has not yet run.		
C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe Скрипт: Карантин, Удалить, Удалить через BC	Spybot - Search & Destroy - Scheduled Task.job	The task is ready to run at its next scheduled time.		

Обнаружено элементов - X, опознано как безопасные - X

Настройки SPI/LSP

Поставщики пространства имен (NSP)

Поставщик	Статус	Исп. файл	Описание	GUID

Обнаружено - X, опознано как безопасные - X

Поставщики транспортных протоколов (TSP, LSP)

Поставщик	Исп. файл	Описание

Обнаружено - XX, опознано как безопасные - XX

Результаты автоматического анализа настроек SPI

```
Настройки LSP проверены. Ошибок не обнаружено
```

Порты TCP/UDP

Порт	Статус	Remote Host	Remote Port	Приложение	Примечания
Порты TCP					
XXX	LISTENING	X.X.X.X	X	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC	
XXX	LISTENING	X.X.X.X	XXXXX	[X] System Скрипт: Карантин, Удалить, Удалить через BC	
XXX	LISTENING	X.X.X.X	XXXXX	[X] System Скрипт: Карантин, Удалить, Удалить через BC	
XXXX	LISTENING	X.X.X.X	X	[XXXX] c:\windows\systemXX\alg.exe Скрипт: Карантин, Удалить, Удалить через BC	
XXXX	CLOSEXWAIT	XXX.XXX.XX.XXX	XX	[XXXX] c:\securitate\avz\avzX\avz.exe Скрипт: Карантин, Удалить, Удалить через BC	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe Скрипт: Карантин, Удалить, Удалить через BC	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashwebsv.exe Скрипт: Карантин, Удалить, Удалить через BC	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe Скрипт: Карантин, Удалить, Удалить через BC	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe	

				Скрипт: Карантин, Удалить, Удалить через BC
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe Скрипт: Карантин, Удалить, Удалить через BC
Порты UDP				
XXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXX	LISTENING	--	--	[X] System Скрипт: Карантин, Удалить, Удалить через BC
XXX	LISTENING	--	--	[X] System Скрипт: Карантин, Удалить, Удалить через BC
XXX	LISTENING	--	--	[X] System Скрипт: Карантин, Удалить, Удалить через BC
XXX	LISTENING	--	--	[XXX] c:\windows\systemXX\lsass.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Удалить, Удалить через BC
XXXX	LISTENING	--	--	[XXX] c:\windows\systemXX\lsass.exe Скрипт: Карантин, Удалить, Удалить через BC

Downloaded Program Files (DPF)

Имя файла	Описание	Производитель	CLSID	URL загрузки

Обнаружено элементов - X, опознано как безопасные - X

Апплеты панели управления (CPL)

Имя файла	Описание	Производитель
C:\WINDOWS\systemXX\cttune.cpl Скрипт: Карантин, Удалить, Удалить через BC	ClearType Tuning Applet	Copyright (C) XXXX - XXXX Microsoft Corp.

Обнаружено элементов - XX, опознано как безопасные - XX

Active Setup

Имя файла	Описание	Производитель	CLSID

Обнаружено элементов - XX, опознано как безопасные - XX

Файл HOSTS

Запись файла Hosts
XXX.X.X.X localhost

Протоколы и обработчики

Имя файла	Тип	Описание	Производитель	CLSID
mscoree.dll Скрипт: Карантин, Удалить, Удалить через BC	Protocol	Microsoft .NET Runtime Execution Engine ()	© Microsoft Corporation. All rights reserved.	{XEXXFXXB-XXEE-XXDX-XXXX-XXCXXFXXEDXD}
mscoree.dll Скрипт: Карантин, Удалить, Удалить через BC	Protocol	Microsoft .NET Runtime Execution Engine ()	© Microsoft Corporation. All rights reserved.	{XEXXFXXB-XXEE-XXDX-XXXX-XXCXXFXXEDXD}
mscoree.dll Скрипт: Карантин, Удалить, Удалить через BC	Protocol	Microsoft .NET Runtime Execution Engine ()	© Microsoft Corporation. All rights reserved.	{XEXXFXXB-XXEE-XXDX-XXXX-XXCXXFXXEDXD}

Обнаружено элементов - XX, опознано как безопасные - XX

Команды скрипта

Добавить в скрипт команды:
Нейтрализация перехватов функций при помощи антируткита

Включить AVZGuard
BootCleaner - импорт списка удаленных файлов
Чистка реестра после удаления файлов
BootCleaner - активация
Перезагрузка
Вставить заготовку для QuarantineFile() - помещение файла в карантин
Вставить заготовку для BCXQrFile() - помещение файла в карантин через BC
Вставить заготовку для DeleteFile() - удаление файла
Вставить заготовку для DelCLSID() - удаление CLSID класса из реестра

Список файлов