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 Скриит: <u>Карантин, Уланить через ВС</u>	XXXX	ACROX	Copyright XXXX By LEE,WEI- BIN.	??	XXX.XX кб, rsAh, coздан: 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 Скрыпт: Каранты, Удалить через ВС	xxxxxxx		Copyright © XXXX By LEE,WEI- BIN.		нет
c:\program files\via technologies, inc\via audio driver setup program\audiodeck\audiodeck.exe Скриит: <u>Карантии. Улалить. через ВС</u>	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 Cspum: Kapaurus. Yaanuri. sepei BC	XXXXXXX	AudioDeck Microsoft ???????	???? (C) XXXX	??	нет
с:\windows\explorer.exe Скрипт: Карантин. Удалить. через ВС	xxxx	Проводник	© Корпорация Майкрософт. Все права защищены. Copyright	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX XX изменен: XX.XX.XXXX X Командная строка: C:\WINDOWS\Explorer.E>
<u>C:\PROGRA~X\ZIPGEN~X\contmenu.dll</u> Скрипт: <u>Карантии. Удалить. Удалить через ВС</u>	XXXXXXX	Context Menu for ZipGenius	©XXXX, XXXX M.Dev Software		нет
<u>C:\WINDOWS\systemXX\msvdm.dll</u> Скрипт: <u>Карантии, Удалить, Удалить через ВС</u>	XXXXXXXX				нет
C:\Program Files\Acronis\PrivacyExpert\PrivShellExt.dll Скрипт: Каранты, Удалить, удалить через ВС	xxxxxxxx	Acronis PrivacyExpert shell extension.	(c) XXXX Acronis. All rights reserved.		нет
C:\Program Files\Zone Labs\ZoneAlarm\zlavscan.dll Скринт: Карантии. Удалить. через ВС	xxxxxxxxx	zlavscan shell extension	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
c:\windows\systemXX\lsass.exe Скрипт: <u>Карантии. Удалить. Удалить. через ВС</u>	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 Ckpinr: Kapairriu. Yaaauris, Yaaauris, sepen BC	xxxxxxxx	Acronis Relogon Authentication Package	Copyright (C) Acronis, XXXX- XXXX.		нет
c:\program files\windows defender\msascui.exe Скрытт: <u>Каранты, Удалить через ВС</u>	xxxx	Windows Defender User Interface	© Microsoft Corporation. All rights reserved.	??	XXX.XX кб, rsAh, coздан: XX.XX.XXXX X изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Windows Defender\MSASCui.exe" -h
C:\Program Files\Windows Defender\MsMpRes.dll Скрипт: Карантны, Удаанть, Чарет ВС	xxxxxxxxx	Модуль ресурсов	© Корпорация Майкрософт. Все права защищены.		нет
c:\program files\a!k research labs\notesholder\notesholder.exe Скрытт: <u>Карантин, Удалить через ВС</u>	xxxx			??	XXX.XX кб, rsAh, создан: XX.XX.XXXX X изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\A!K Resa Labs\NotesHolder\NotesHo
<u>C:\Program Files\A!K Research Labs\NotesHolder\NotesHolder.exe</u> Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	XXXXXXX			??	нет
c:\program files\rezerv-copy\rezervcopy.exe Скриит: <u>Карантии, Удалить, Удалить, через ВС</u>	xxxx	Rezerv-Copy	Copyright © XXXX Lokas Ltd.	??	XXXX.XX кб, rsAh, создан: XX.XX.XXXX X изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Rezerv- Copy\RezervCopy.exe"
C:\Program Files\Rezerv-Copy\RezervCopy.exe Скрипт: Карантин, Удалить через ВС	XXXXXXX	Rezerv-Copy	Copyright © XXXX Lokas Ltd.	??	нет
					XXX.XX кб, rsAh,

c:\program files\common files\acronis\scheduleX\schedhlp.exe	XXXX	Acronis Scheduler Helper	Copyright (C) XXXX- XXXX Acronis	??	создан: XX.XX.XXXX XX изменен: XX.XX.XXX X Командная строка: "C:\Program Files\Common Files\Acronis\ScheduleX\sc
C:\Program Files\Common Files\Acronis\ScheduleX\schedhlp.exe Скриит: Карантин, Удалить, Удалить черен ВС	XXXXXXX	Acronis Scheduler Helper	Copyright (C) XXXX- XXXX Acronis	??	нет
c:\program files\common files\acronis\scheduleX\schedulX.exe Скринт: <u>Карантии. Узалить. Узалить через ВС</u>	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 Cspurr: Kapaurus, Удалить, через ВС	XXXXXXX	Acronis Scheduler X	Copyright (C) XXXX- XXXX Acronis	??	нет
c:\program files\openoffice.org X.X\program\soffice.bin	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\OpenOffice.exe" - с Settings\Ддмин\Рабочий ст работыXX.odb"
C:\Program Files\OpenOffice.org X.X\program\avmediaXXXmi.dll Cxpurr: Kapantrus, Узаанть, Уданть через ВС	xxxxxxxx	x	Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\dbaXXXmi.dll Скринт: Карантин, Удалить, Удалить через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.	,	нет
C:\Program Files\OpenOffice.org X.X\program\dbaxmlXXXmi.dll Скриит: Карантин, Удаанть, Удаанть, через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.	,	нет
C:\Program Files\OpenOffice.org X.X\program\dbtoolsXXXmi.dll Скринт: Карантин, Удалить через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.	,	нет
C:\Program Files\OpenOffice.org X.X\program\dbuXXXmi.dll	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\dnd.dll Съринт: Караатни, Удалить, через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\fileacc.dll Cspum: Kapantus, Yasantus, Yas	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\filterconfigX.dll Cspum: Kapaurus, Yasaurus, Yasaurus, sepen BC	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\fsstorage.uno.dll Скринт: Карантия, Улаванть, Удаванть через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\ftransl.dll Скринт: Карантин, Удалить, Удалить через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.	,	нет
C:\Program Files\OpenOffice.org X.X\program\goXXXmi.dll Скринт: Карантин. Удалить. Удалить через ВС	xxxxxxxx	X	Copyright © XXXX by Sun Microsystems, Inc.	,	нет
C:\Program Files\OpenOffice.org X.X\program\iXXnpool.uno.dll Скринт: Карантин. Удаанть черен ВС	xxxxxxxx	x	Copyright © XXXX by Sun Microsystems, Inc.	,	нет

<u>C:\Program Files\OpenOffice.org X.X\program\iXXnutilMSC.dll</u> Съринт: <u>Карантии, Удалить, Через ВС</u>	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\icuinXX.dll Скрипт: Карантин, Удалить, через ВС	xxxxxxxxxx ¹	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 Скринт: Карантин, Удалить, Чарет ВС	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
<u>C:\Program Files\OpenOffice.org X.X\program\mcnttype.dll</u> Скрыт: <u>Каранты. Удалить. Удалить через ВС</u>	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
<u>C:\Program Files\OpenOffice.org X.X\program\packageX.dll</u> Скриит: <u>Карантии, Удалить, через ВС</u>	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
<u>C:\Program Files\OpenOffice.org X.X\program\soXXXmi.dll</u> Скрипт: <u>Карантин. Удалить. через ВС</u>	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
<u>C:\Program Files\OpenOffice.org X.X\program\svxXXXmi.dll</u> Скринт: <u>Карантин. Удалить. Через ВС</u>	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\sysdtrans.dll	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\updchk.uno.dll Скринт: Карантин. Улалить. через вС	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\uuiXXXmi.dll Скринт: Карантин. Удалить. Через ВС	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
C:\Program Files\OpenOffice.org X.X\program\xoXXXmi.dll Скрипт: Карангин, Удалить, Через ВС	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
<u>C:\Program Files\OpenOffice.org X.X\program\xstor.dll</u> Скриит: <u>Карантин. Улалить. Удалить через ВС</u>	xxxxxxxxx		Copyright © XXXX by Sun Microsystems, Inc.		нет
c:\program files\acronis\trueimage\timountermonitor.exe Скриит: <u>Карантии. Удалить. Удалить через ВС</u>	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 Скринт: Карантын. Удалить через ВС	XXXXXXX	Monitor for Acronis True Image Backup Archive Explorer	Copyright (c) Acronis XXXX- XXXX	??	нет
c:\program files\acronis\trueimage\trueimagemonitor.exe Скриит: <u>Карантия. Уладить. Уладить через ВС</u>	XXXX	ГrueImage	Copyright (C) XXXX- XXXX Acronis.	??	XXXX.XX кб, rsAh, создан: XX.XXXXXX XX изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Acronis\TrueImage\Tr
C:\Program Files\Common Files\Acronis\Common\rpcXclient.dll Cspurr: Kapaurus. Узаанть. 9cpc. BC	XXXXXXXXX				нет
C:\Program Files\Acronis\TrueImage\TrueImageMonitor.exe Ckpunt: Kapautus. Удалить. через ВС	XXXXXXX	ΓrueImage	Copyright (C) XXXX- XXXX Acronis.	??	нет
			Copyright ©		XX.XX кб, rsAh,

c:\windows\systemXX\zonelabs\vsmon.exe	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	XXXXXXXX		Laos, ELC		нет
Ceputri: Kapatrini. Yaaniris. Janaris Jeneri BC C:\WINDOWS\systemXX\ZoneLabs\av.dll Ceputri: Kapatrini. Yaaniris. Janaris seperi BC	xxxxxxx	av feature plug-in	Copyright © XXXX-XXXX, Zone		нет
C:\WINDOWS\systemXX\ZoneLabs\camupd.dll Cspurr: Kapaarrus, Yanaurts, Spaarrus, Spaarru	xxxxxxxxx	camupd feature	Labs, LLC Copyright © XXXX- XXXX, Zone		нет
C:\WINDOWS\systemXX\ZoneLabs\fbl.dll	xxxxxxxx	Feature based	Labs, LLC Copyright © XXXX-	_	нет
Скрипт: Карантин, Улалить, Улалить через ВС	AAAAAAA	licensing library	XXXX, Zone Labs, LLC Copyright © XXXX-		nei
C:\WINDOWS\systemXX\ZoneLabs\streamapi\httpblocker\httpblocker.dll	XXXXXXX	HttpBlocker plug-in	XXXX, Zone Labs, LLC Copyright ©		нет
C:\WINDOWS\systemXX\ZoneLabs\imsecure.dll Скрипт: <u>Карантин. Удалить. Удалить. через ВС</u>	xxxxxxxxx	Service	XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\streamapi\imslsp\imslsp.dll Скринт: Карантин, Узаанть, Узаанть, через ВС	xxxxxxx	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. Удаашть, Удаашть, через ВС	XXXXXXX				нет
C:\WINDOWS\systemXX\zonelabs\lib\pyd\pyexpat.pyd Скрипт: Карантин, Удаанть, Удаанть, через ВС	XXXXXXXX				нет
C:\WINDOWS\systemXX\zonelabs\lib\pyd\pyvsinit.pyd Скрипт: Карантин. Удаанть, Удаанть через ВС	XXXXXXX				нет
C:\WINDOWS\systemXX\ZoneLabs\qrbase.dll Скрипт: Карантин, Улалить, Удалить, через ВС	XXXXXXX	qrbase	Copyright © XXXX Copyright ©		нет
C:\WINDOWS\systemXX\ZoneLabs\plugins\rpcXserver\rpcXserver.dll Cspurr: Kapairriu, Yaaairris, Yaaairris veper BC	XXXXXXX	RPC Server plug- in	XXXX- XXXX, Zone Labs, LLC Copyright ©		нет
C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll Cspunr: Kapanrun, Yaaanrus vepen BC	xxxxxxxxx	scheduler feature plug-in	XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\zonelabs\lib\pyd\signedDll.pyd	XXXXXXXX				нет
C:\WINDOWS\systemXX\ZoneLabs\srescan.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX	srescan	Copyright © XXXX Copyright ©		нет
C:\WINDOWS\systemXX\ZoneLabs\ssleayXX.dll Cspum: Kapaurus, Yaaaurus, Yaaaurus, Sepesi RC	xxxxxxxxx	TrueVector Service	XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\vsavpro.dll	XXXXXXX	TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\VSDATA.dll Скрипт: Карантин, Удалить, Удалить, через ВС	xxxxxxx	TrueVector Service DLL	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\vsdb.dll Скрипт: Карантии, Удалить, Удалить через ВС	xxxxxxx	TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\VSINIT.dll Скрипт: Карантин, Удалить, Удалить, через ВС	xxxxxxx	TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\vsmon.exe	xxxxxxx	TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC	??	нет
C:\WINDOWS\systemXX\ZoneLabs\plugins\vsmonXplugin\vsmonXplugin.dll	xxxxxxx	vsmon plug-in	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\vsmondll.dll Скрипт: <u>Карантин</u> , <u>Удалить, Удалить через ВС</u>	xxxxxxx	TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\VSRULEDB.DLL	xxxxxxxxx	TrueVector	Copyright © XXXX-		нет

Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>		Service	XXXX, Zone Labs, LLC		
C:\WINDOWS\systemXX\VSUTIL.dll Скринт: Карантин. Удалить. Удалить. через ВС	xxxxxxxxx	X TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\vsvault.dll Скринт: Карантин, Удалить, Удалить, через ВС	xxxxxxxxx	X TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\vswmi.dll Скринт: Карантин. Удалить. Через ВС	xxxxxxxx	vsmon component	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\vsxml.dll Скрипт: Карантин. Удалить. через ВС	xxxxxxx	TrueVector Service	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\zlcomm.dll Csphitt: Kapantun. Yaanitta. 42pen BC	xxxxxxxxx	X ZLComm	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZLCommDB.dll Скриит: Карантин. Удалить, Удалить через ВС	XXXXXXXXX	X ZLCommDB	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\zlquarantine.dll Скриит: Карантии. Удалить, Удалить через ВС	xxxxxxx	zlquarantine	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\zlsre.dll Скриит: <u>Карантин, Удалить через ВС</u>	xxxxxxx	zlsre	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\zlupdate.dll Скрипт: Карантин. Удалить. Удалить через ВС	xxxxxxx	ZLUpdate feature plug-in	Copyright © 2 XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\zpengXX.dll Скрипт: Карантия, Удалить, через ВС	xxxxxxxx	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	XXXX	Watch Dog	Copyright (C)	??	XXX.XX кб, rsAh, создан: XX.XX.XXXX X:2 изменен: XX.XX.XXXX X Командная строка: "C:\Program Files\Mustek 2 Plus\Driver\WATCH.exe"
C:\WINDOWS\TWAINXXX\SXUXXBX\SBSpiXT.dll Cephtit: Kapantini. Yanantis. Sepes BC	xxxxxxxx	SBspi	Copyright c XXXX		нет
c:\windows\systemXX\winlogon.exe Скриит: <u>Карантин. Улаанть. через ВС</u>	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 Скриит: Карантин. Удалить. Удалить через ВС	xxxxxxx	Уведомление о результатах проверки подлинности Windows	© XXXX- XXXX Microsoft Corporation		нет
c:\program files\zone labs\zonealarm\zlclient.exe Скриит: <u>Карантии, Удалить, Удалить через ВС</u>	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	xxxxxxx	Alerts Plugin Module	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\av.dll Скритт: Карантин. Удалить. Удалить через ВС	xxxxxxx	av feature plug-in	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\cam.zap Серинт: <u>Карантин. Улалить. Удалить через ВС</u>	XXXXXXX	Anti-Virus Monitoring Module	Copyright © XXXX- XXXX, Zone		нет

C:\WINDOWS\systemXX\ZoneLabs\camupd.dll Скрипт: Карантин, Удалить, Удалить через ВС	xxxxxxxxx	camupd feature	Labs, LLC Copyright © XXXX- XXXX, Zone		нет
<u>C:\Program Files\Zone Labs\ZoneAlarm\email.zap</u> Скриит: <u>Карантии, Удалить удалить через ВС</u>	xxxxxxxx	Email Plugin Module	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\fbl.dll Серипт: Карантии. Улалить. Улалить через ВС	xxxxxxx	Feature based licensing library	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\filter.zap	XXXXXXX	Filter Plugin Module	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\firewall.zap	xxxxxxx	Firewall Plugin Module	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\framewrk.dll Серипт: Карантин. Удалить. Удалить через ВС	xxxxxxxxx	ZoneAlarm Framework Module	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\idlock.zap	xxxxxxxxx	ZoneAlarmPro	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\imsecure.zap	xxxxxxxxx	IMsecure Plugin Module	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\WINDOWS\systemXX\LIBEAYXXXX.X.XI.dll Скрипт: Карантин, Удалить, Удалить через ВС	XXXXXXXX				нет
C:\Program Files\Zone Labs\ZoneAlarm\privacy.zap Скрыпт: Карантин. Удалить. Удалить через ВС	xxxxxxxx	Privacy Plugin Module	Copyright © XXXX- XXXX, Zone Labs, LLC		нет
C:\Program Files\Zone Labs\ZoneAlarm\programs.zap	XXXXXXX	Programs Plugin Module	Copyright © XXXX-XXXX, Zone		нет
Capatin, gaanta, gaanta sees DC		Wioduic	Labs, LLC		
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd	xxxxxxxx	Wodulc			нет
		scheduler feature plug-in	Labs, LLC		нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd Cepum: Kapartini. Yaanitis. Yaanitis seper BC C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll		scheduler feature	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright ©		
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd Серинг: Карантин. Удалить. через ВС С:\WINDOWS\systemXX\ZoneLabs\scheduler.dll Серинг: Карантин. Удалить. Удалить. через ВС С:\Program Files\Zone Labs\ZoneAlarm\security.zap	xxxxxxxxx	scheduler feature plug-in Overview Plugin	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX- XXXX, Zone		нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd Cc:\WINDOWS\systemXX\ZoneLabs\scheduler.dll С:\WINDOWS\systemXX\ZoneLabs\ZoneAlarm\security.zap C:\Program Files\Zone Labs\ZoneAlarm\security.zap C:\WINDOWS\systemXX\vsdata.dll	xxxxxxxxx	scheduler feature plug-in Overview Plugin Module TrueVector	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone	-	нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd Съринт: Карантин. Удалить. Удалить через ВС C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll Съринт: Карантин. Удалить. Удалить через ВС C:\Program Files\Zone Labs\ZoneAlarm\security.zap Съринт: Карантин. Удалить. Удалить через ВС C:\WINDOWS\systemXX\vsdata.dll Съринт: Карантин. Удалить. Удалить через ВС C:\WINDOWS\systemXX\vsdata.dll	xxxxxxxxx xxxxxxxx xxxxxxxx	scheduler feature plug-in Overview Plugin Module TrueVector Service DLL TrueVector	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © Copyright © Copyright © Copyright © Copyright ©	-	нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd С:\WINDOWS\systemXX\ZoneLabs\scheduler.dll Серинг: Карантин. Удалить. Удалить черел ВС С:\Program Files\Zone Labs\ZoneAlarm\security.zap Серинг: Карантин. Удалить. Удалить черел ВС С:\WINDOWS\systemXX\vsdata.dll Серинг: Карантин. Удалить. Удалить черел ВС С:\WINDOWS\systemXX\vsINIT.dll Серинг: Карантин. Удалить. Удалить. черел ВС	xxxxxxxx xxxxxxx xxxxxxx xxxxxxx	scheduler feature plug-in Overview Plugin Module TrueVector Service DLL TrueVector Service TrueVector Client	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone		нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll С:\WINDOWS\systemXX\ZoneLabs\ZoneAlarm\security.zap C:\WINDOWS\systemXX\vsdata.dll C:\WINDOWS\systemXX\vsdata.dll C:\WINDOWS\systemXX\vsINIT.dll C:\WINDOWS\systemXX\vsINIT.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	scheduler feature plug-in Overview Plugin Module TrueVector Service DLL TrueVector Service TrueVector Client Interface	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone		нет нет нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll C:\WINDOWS\systemXX\ZoneAlarm\security.zap C:\WINDOWS\systemXX\vsdata.dll C:\WINDOWS\systemXX\vsdata.dll C:\WINDOWS\systemXX\vsINIT.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vspeaBC	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	scheduler feature plug-in Overview Plugin Module TrueVector Service DLL TrueVector Service TrueVector Client Interface TrueVector Service TrueVector Service	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labx, LLC Copyright © XXXX- XXXX, Zone		нет нет нет нет
C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\pyexpat.pyd C:\WINDOWS\systemXX\ZoneLabs\scheduler.dll С:\WINDOWS\systemXX\ZoneAlarm\security.zap C:\WINDOWS\systemXX\vsdata.dll С:\WINDOWS\systemXX\vsdata.dll C:\WINDOWS\systemXX\vsinit.dll C:\WINDOWS\systemXX\vsinit.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vsmonapi.dll C:\WINDOWS\systemXX\vspea BC C:\WINDOWS\systemXX\vspea BC C:\WINDOWS\systemXX\vspea BC C:\WINDOWS\systemXX\vspea BC	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	scheduler feature plug-in Overview Plugin Module TrueVector Service DLL TrueVector Client Interface TrueVector Service TrueVector TrueVector Service TrueVector TrueVector TrueVector TrueVector Service	Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labs, LLC Copyright © XXXX- XXXX, Zone Labx, LLC Copyright © XXXX- XXXX, Zone		нет нет нет нет

C:\WINDOWS\systemXX\ZLCommDB.dll

XXXXXXXXX ZLCommDB

Copyright © XXXXнет

XXXX, Zone Labs, LLC

нет

Copyright © XXXX-XXXX Python Software

Foundation.

C:\WINDOWS\systemXX\zpengXX.dll

XXXXXXXX Python Core

Copyright © XXXX BeOpen.com. Copyright © XXXX-XXXX CNRI. Copyright © XXXX-XXXX SMC.

C:\WINDOWS\systemXX\ZoneLabs\lib\pyd\zpui.pyd

XXXXXXXX zpui Library Copyright (C)

нет XXXX

Обнаружено:XX, из них опознаны как безопасные XX

Модули пространства ядра

Описание Базовый адрес Размер в памяти Производитель Модуль snapman.sys Скрипт: <u>Карантин</u>, FXXXAXXX XXCXXX (XXXXXX) Acronis Snapshot API Copyright (c) Acronis XXXX-XXXX

srescan.sys Скрипт: Каранти

FXXXXXXX XXXXXX (XXXXX)

\SystemRoot\SystemXX\vsdatant.sys AXXXXXXXXXXXXX (XXXXXX) TrueVector Device Driver Copyright © XXXX-XXXX, Zone Labs, LLC

Обнаружено модулей - XXX, опознано как безопасные - XXX

Службы

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

Обнаружено - XX, опознано как безопасные - XX

Драйверы

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

Cpqarray	Cpqarray	Не	Cpqarray.sys	SCSI miniport	
dacXXXnt	dacXXXnt	запущен Не	Скрипт: <u>Карантин, Улалить. Улалить через ВС</u> dacXXXnt.sys	SCSI miniport	
		запущен Не	Скрипт: <u>Карантин. Удалить. Удалить через ВС</u> dptiXo.sys	•	
dptiXo	dptiXo VIA PCI XX/XXXMb Fast Ethernet	запущен Не	Скрипт: Карантин, Удалить, Удалить через ВС	SCSI miniport	
FETNDIS	адаптер, драйвер для NT	запущен	systemXX\DRIVERS\fetndX.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	NDIS	
GMSIPCI	GMSIPCI	Не запущен	\??\G:\INSTALL\GMSIPCI.SYS Скрипт: Карантин, Улалить. Улалить через ВС		
hpn	hpn	Не запущен	hpn.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
iXomgmt	iXomgmt	Не запущен	iXomgmt.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI Class	
iXomp	iXomp	Не запущен	<u>iXomp.sys</u> Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
iniXXXu	iniXXXu	Не запущен	iniXXXu.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
IntelIde	IntelIde	He запущен	IntelIde.sys Скрипт: Карантин, Удалить, Удалить через ВС	System Bus Extender	
klX	klX	He запущен	\SystemRoot\systemXX\DRIVERS\kIX.sys	PNPXTDI	
lbrtfdc	lbrtfdc	Не запущен	lbrtfdc.sys Скрипт: Карантин, Удалить, Удалить через ВС	System Bus Extender	
mraidXXx	mraidXXx	Не	mraidXXx.sys Скрипт: Карантин, Удалить, Удалить через ВС	SCSI miniport	
PCIDump	PCIDump	запущен Не	PCIDump.sys	PCI Configuration	1
PCIIde	PCIIde	запущен Не	Скрипт: <u>Карантин, Удалить, Удалить через ВС</u> <u>PCIIde.svs</u>	System Bus	
PDCOMP	PDCOMP	запущен Не	Скрипт: <u>Карантин, Удалить, Удалить через ВС</u> PDCOMP.sys	Extender	
		запущен Не	Скрипт: <u>Карантин. Удалить. Удалить через ВС</u> PDFRAME.sys		
PDFRAME	PDFRAME	запущен Не	Скрипт: Карантин, Улалить, Улалить через ВС PDRELI.sys		
PDRELI	PDRELI	запущен Не	Скрипт: <u>Карантин</u> , <u>Удалить</u> , <u>Удалить через ВС</u>		
PDRFRAME	PDRFRAME	запущен	PDRFRAME.sys Скрипт: Карантин, Улалить, Улалить, через ВС		
percX	percX	Не запущен	<u>percX.sys</u> Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
percXhib	percXhib	Не запущен	percXhib.sys Скрипт: <u>Карантин, Улалить, Улалить через ВС</u>	Filter	
qlXXXX	qlXXXX	Не запущен	<u>qlXXXX.sys</u> Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
QlXXwnt	QlXXwnt	Не запущен	QlXXwnt.sys Скрипт: <u>Карантин</u> , <u>Удалить</u> , <u>Удалить через ВС</u>	SCSI miniport	
qlXXXXX	qlXXXXX	Не запущен	<u>qlXXXXX.sys</u> Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
qlXXXX	qlXXXX	Не запущен	qlXXXX.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
qlXXXX	qlXXXX	He запущен	qlXXXX.sys Скрипт: <u>Карантин, Улалить, Улалить через ВС</u>	SCSI miniport	
Simbad	Simbad	He запущен	Simbad.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	Filter	
snapman	Acronis Snapshots Manager	Работает	\SystemRoot\systemXX\DRIVERS\snapman.sys Скрипт: Карантин, Улалить, Улалить через ВС		
Sparrow	Sparrow	Не запущен	Sparrow.sys Скрипт: Карантин, Удалить, Удалить через ВС	SCSI miniport	
srescan	srescan	Работает	\SystemRoot\systemXX\ZoneLabs\srescan.sys		
symXhi	symXhi	Не запущен	symXhi.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
symXuX	symXuX	Не запущен	symXuX.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
symcXXX	symcXXX	He запущен	symcXXX.sys Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	SCSI miniport	
symcXxx	symcXxx	Не	symcXxx.sys Скрипт: Карантин, Удалить, Удалить через ВС	SCSI miniport	
TosIde	TosIde	запущен Не	ТosIde.sys Скрипт: Карантын, Удалить, Удалить через ВС	System Bus	
ultra	ultra	запущен Не	ultra.sys	Extender SCSI miniport	
vsdatant	vsdatant	запущен Работает	Скрипт: <u>Карантин, Удалить удалить через ВС</u> <u>SystemXX\vsdatant.sys</u> Скрипт: <u>Карантин, Удалить удалить через ВС</u>	PNPXTDI	TCPIP
Vsp	Vsp	Не	\??\C:\WINDOWS\systemXX\drivers\Vsp.sys	·	
WDICA	WDICA	запущен Не	Скрипт: <u>Карантин, Удалить, Удалить через ВС</u> WDICA.sys		
	жыса X, опознано как безопасные - XXX	запущен	Скрипт: Карантин, Удалить, <u>Удалить через ВС</u>		
* -					

Автозапуск

Имя файла	Статус	Метод запуска	Описание
C:\Documents and Settings\Админ\Рабочий стол\Внимание !.pdf	Активен	Ярлык в папке автозагрузки	С:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка\Ярлык для Внимание !.lnk,
C:\Documents and Settings\Админ\Рабочий стол\Сервисные работыXX.odb Скрипт: Карантин, Удалить, удалить через ВС	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка\Ярлык для Сервисные работыХХ.lnk,
C:\PROGRA~X\COMMON~X\MICROS~X\DW\dwtrigXX.exe	Активен	Ключ реестра	$HKEYXUSERS, \\ .DEFAULT lem:lem:lem:lem:lem:lem:lem:lem:lem:lem:$
C:\Program Files\A!K Research Labs\NotesHolder\NotesHolder.exe Cspiiir: Карангин, Удалить, Удалить через ВС	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка\NotesHolder.lnk,
C:\Program Files\Acronis\TrueImage\TimounterMonitor.exe Cspuur: Карангин, Уавангъ, Удаангъ, через ВС	Активен	Ключ реестра	$\label{eq:hkeyxlocalxmachine} HKEYXLOCALXMACHINE, \\ Software \ \ Microsoft \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
C:\Program Files\Acronis\TrueImage\TrueImageMonitor.exe Cspurr: Карангин. Удалить. Удалить. через BC	Активен	Ключ реестра	$\label{eq:hamiltonian} HKEYXLOCALXMACHINE, \\ Software \ \ Microsoft \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
C:\Program Files\Common Files\Acronis\ScheduleX\schedhlp.exe Скринт: Карантин. Удалить. Удалить через ВС	Активен	Ключ реестра	$\label{thm:line} HKEYXLOCALXMACHINE, \\ Software \ Microsoft \ Windows \ Current \ Version \ Run, \ Acronis \ Scheduler X \\ Service$
C:\Program Files\Lex!\Lex.exe Скрипт: Карантин, Удалить, Удалить через ВС	Активен		C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка\Lex!.lnk,
C:\Program Files\Rezerv-Copy\RezervCopy.exe	Активен	Ярлык в папке автозагрузки	C:\Documents and Settings\Админ\Главное меню\Программы\Автозагрузка C:\Documents and Settings\Админ\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 через ВС	Активен		C:\Documents and Settings\All Users\Главное меню\Программы\Aвтозагрузка C:\Documents and Settings\All Users\Главное меню\Программы\Aвтозагрузка\AudioDeck.Ink,
C:\Program Files\Zone Labs\ZoneAlarm\zlclient.exe Cspurr: Kapanrius. Узавить. чрез ВС	Активен	Ключ реестра	HKEYXLOCALXMACHINE, Software\Microsoft\Windows\CurrentVersion\Run, ZoneAlarm Client
WgaLogon.dll Copuit: <u>Kapantini. Удалить. удалить через ВС</u>	Активен	Ключ реестра	HKEYXI OCALXMACHINE SOFTWARE\Microsoft\Windows
appmgmts.dll Скрипт: <u>Карантии, Удаанть, удаанть через ВС</u>	Активен		$HKEYXLOCALXMACHINE, SOFTWARE \ Microsoft \ Windows \ NT \ Current \ Version \ Winlogon \ GPExtensions \ \{cXdcXXXX-XXXA-XXdX-XXcXXfbXXXfX\}, DLL \ Name$

Обнаружено элементов автозапуска - XX, опознано как безопасные - XX

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

Имя файла	Тип	Описание	Производитель	CLSID
	ВНО			SOFTWARE
C:\Program Files\Google\Google Notebook\gnotesX.X.X.XXXXXXXXXX.dll Скрипт: Кариттин, Удалить, Удалить через ВС	ВНО	Блокнот Google для IE	Авторские права, XXXX Google	{CCCCCDX-XXXF-XFXX-XBXX-XXXDEXFXDXXX}
C:\Program Files\Google\Google Notebook\gnotesX.X.XX-XXXXXXXXXX.dll Ckpun:: Карантин, Удалить через ВС	Панель	Блокнот Google для IE	Авторские права, XXXX Google	$ \{ CCCCCCDB\text{-}XDDB\text{-}XXXX\text{-}XXDX\text{-}DDXCXXXXXXBF} \}$
C:\WINDOWS\Network Diagnostic\xpnetdiag.exe	Модуль расширения	Network Diagnostic for Windows XP	© Microsoft Corporation. All rights reserved.	{eXeXddXX-dXXX-XXXX-XXbX-fXbaXXXXXXXX}
Обнаружено элементов - XX, опознано как безопа	асные - Х			

Модули расширения проводника

Имя файла	Назначение	Описание	Производитель	CLSID
deskpan.dll Скрипт: <u>Карантии, Удалить через ВС</u>	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 [XXEXBXXXX-FXXB-Xdcf-XXDF-CDXXXBXXBFDX] Copum: Kapaurus, Yaanurs, yeep 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 ВС	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 Скринт: Карантин. Улалить. Улалить через ВС	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 Csparr: Kaparrin, Yaaniris, Vaaniris sepe: 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 Cspairt: Каранты, Удалить, через ВС	ZipGenius Drop handler	ZG Drop Handler		{XXXAXCXX-EAXX- XXAE-AXEX- XXEXXEXXXXXX}
C:\PROGRA~X\ZIPGEN~X\ZGDRAG~X.DLL Cephitt: Карантін, Удалить, через ВС	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 Серинт: Карантин. Удалить. через ВС	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-XXXXXXXXXX dll Cxpurr: Kaparrini, Yaaniris, Yaaniris sepes 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-XXXXXXXXXX dll Cxpun:: Карантин, Удалить, Удалить через ВС	&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 Cxpunr: Kapantun, Yaanuta, Yaanuta seper 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 файла Имя задания		Описание Производитель
C:\Documents and Settings\Чистюля\Рабочий стол\X.bat Скрипт: Карантин, Удалить, Удалить через ВС	X.job	The task has not yet run.	
C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe Скрипт: Карантин. Удалить. Через ВС	Spybot - Search & Destroy - Scheduled Task.job	The task is ready to run at its next scheduled time.	

Обнаружено элементов - X, опознано как безопасные - X

Поставщики пространства имен (NSP)

Настройки SPI/LSP

	Поставщик	Статус	Исп. файл	Описание	GUID		
Обнаруже	ено - Х, 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 Т	CP				
XXX	LISTENING	X.X.X.X	X	[XXXX] c:\windows\systemXX\svchost.exe Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	
XXX	LISTENING	X.X.X.X	XXXXX	[X] System Скрипт: <u>Карантин, Улалить, Улалить через ВС</u>	
XXX	LISTENING	X.X.X.X	XXXXX	[X] System Скрипт: <u>Карантин, Улалить, Члалить через ВС</u>	
XXXX	LISTENING	X.X.X.X	X	[XXXX] c:\windows\systemXX\alg.exe Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	
XXXX	CLOSEXWAIT	XXX.XXX.XXX	XX	[XXXX] c:\securitate\avz\avzX\avz.exe Скрипт: <u>Карантин, Улалить, Улалить через ВС</u>	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe Ckpum: Kapantuu, Удадить, Удадить, через ВС	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashwebsv.exe Скрипт: <u>Карантин, Удалить, Удалить через ВС</u>	
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe Скрипт: <u>Карантин, Улалить, через ВС</u>	
XXXXX	LISTENING	X.X.X.X	X	$[XXXX]\ c: \ \ files \ \ software \ \ avastX \ \ ashmaisv.exe$	

				Скрипт: <u>Карантин</u> , <u>Удалить</u> , <u>Удалить через ВС</u>		
XXXXX	LISTENING	X.X.X.X	X	[XXXX] c:\program files\alwil software\avastX\ashmaisv.exe Скрипт: Карантин, Удалить, Удалить через ВС		
Порты UDP						
XXX	LISTENING			[XXXX] c:\windows\systemXX\svchost.exe Скрипт: <u>Карантии. Удалить через ВС</u>		
XXX	LISTENING			[XXXX] c:\windows\systemXX\svchost.exe Скрипт: <u>Карантин, Удалить через ВС</u>		
XXX	LISTENING			[XXXX] c:\windows\systemXX\svchost.exe Скрипт: <u>Карантин, Удалить через ВС</u>		
XXX	LISTENING			[X] System Скрипт: <u>Карантин, Улалить, Удалить через ВС</u>		
XXX	LISTENING			[X] System Скрипт: <u>Карантин, Улалить Улалить через ВС</u>		
XXX	LISTENING	-		[X] System Скритг: <u>Карантин, Улалить, Удалить через ВС</u>		
XXX	LISTENING	-		[XXX] c:\windows\systemXX\lsass.exe CKPUITT: KARDAHTHH, YJARHTHS, YJARHTHS 42PE3 BC		
XXXX	LISTENING			[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Улалить через ВС		
XXXX	LISTENING	-		[XXXX] c:\windows\systemXX\svchost.exe Скрит: <u>Карантин, Удалить через ВС</u>		
XXXX	LISTENING	-		[XXXX] c:\windows\systemXX\svchost.exe Скрипт: Карантин, Улалить через ВС		
XXXX	LISTENING			[XXXX] c:\windows\systemXX\svchost.exe Скрипт: <u>Карантии, Удалить, Удалить через ВС</u>		
XXXX	LISTENING	-		[XXXX] c:\windows\systemXX\svchost.exe Скрит: <u>Карантин, Улалить через ВС</u>		
XXXX	LISTENING			[XXXX] c:\windows\systemXX\svchost.exe Скрипт: <u>Карантин, Удалить через ВС</u>		
XXXX	LISTENING			[XXX] c:\windows\systemXX\lsass.exe Скрипт: <u>Карантин, Удалить</u> , <u>Удалить через ВС</u>		

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
 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: <u>Карантин</u> , <u>Улалить</u> , <u>Улалить</u> через <u>BC</u>	Protocol N	Microsoft .NET Runtime Execution Engine ()	© Microsoft Corporation. All rights reserved.	$ \{ \textbf{XEXXFXXB-XXEE-XXDX-XXXX-} \\ \textbf{XXCXXFXXEDXD} \} $	
mscoree.dll Скрипт: <u>Карантин, Удалить, Удалить</u> через ВС		Microsoft .NET Runtime Execution Engine ()	© Microsoft Corporation. All rights reserved.	$ \{ \textbf{XEXXFXXB-XXEE-XXDX-XXXX-} \\ \textbf{XXCXXFXXEDXD} \} $	
mscoree.dll Скрипт: <u>Карантин</u> , <u>Удалить</u> , <u>Удалить</u> через <u>BC</u>		Microsoft .NET Runtime Execution Engine ()	© Microsoft Corporation. All rights reserved.	$ \{ \textbf{XEXXFXXB-XXEE-XXDX-XXXX-} \\ \textbf{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 ВС

Вставить заготовку для DeleteFile() - удаление файла

Вставить заготовку для DeleteFile() - удаление файла

Список	файлов			