Kaspersky's free support security utilities

In the following article, TipsMake.com will introduce to you the free support tools, researched and developed by Kaspersky Lab

In the following article, TipsMake.com will introduce to you the free support tools, researched and developed by Kaspersky Lab - especially proved useful in almost cases'. cannot be cured "when users encounter .

Kaspersky Virus Removal Tool

Created to remove all infected files from the system. The latest version is currently 9.0.0.722, with a capacity of about 71.5 MB. Kaspersky Virus Removal Tool 2010 applies the most advanced hazard identification technologies of Kaspersky Anti Virus and AVZ. The use of this tool is usually only for emergencies, and this is only a backup security plan. After removing the threats on any one computer, you need to stop using this tool and install another security application on the system.

Advantages :
- Simple interface, easy to use
- Can install on infected computers, at any level. Safe Mode is supported
- Combine scanning and prevention of system spread, detect traces and analyze operation process
- Collect information from the system and actions of malicious code to prevent further infection

Main functions :
- Remove viruses, Trojans, worms, Spyware, adware modules in automatic or normal mode
- Destroy all popular rootkits today

Minimum system requirements :

- Free hard disk space of at least 80 MB, with Internet connection
- Microsoft Windows 2000 Professional (Service Pack 4 or higher)
- Microsoft Windows XP Home Edition (Service Pack 2 or higher)
- Microsoft Windows XP Professional (Service Pack 2 or higher)
- For the above operating systems, the minimum hardware is as follows Intel Pentium 300 MHz CPU, 256 MB RAM
- Microsoft Windows Vista Home Basic (32-bit)
- Microsoft Windows Vista Home Premium (32-bit)
- Microsoft Windows Vista Business (32-bit)
- Microsoft Windows Vista Enterprise (32-bit)
- Microsoft Windows Vista Ultimate (32-bit)
- Hardware applied to the above operating systems is Intel Pentium 800 MHz 32-bit CPU (x86), 512 MB RAM

- Microsoft Windows 7 Home Premium (32/64 bit)
- Microsoft Windows 7 Professional (32/64 bit)
- Microsoft Windows 7 Ultimate (32/64 bit)
- Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) CPU hardware requirements, and 1 GB (32-bit) RAM or 2 GB (64-bit)

RectorDecryptor

Applied with malicious code **Trojan-Ransom.Win32.Rector** , the latest version is 2.3.0.0, small and lightweight, only 188 KB. Hackers mainly use the **Trojan-Ransom.Win32.Rector model** to affect the normal operation of the victim computer, illegally editing the data so that users cannot access it. When these data have been changed (users cannot access it anymore), they will receive messages from hackers asking them to provide personal information or a fee form like 'ransom' - in exchange, they may receive the original data. The RectorDecryptor application is researched and developed by Kaspersky security experts, very easy to use (because the program has a graphical interface), users only need to download from the above link, unzip and a real folder period on the hard drive and run the RectorDecryptor.exe file:

Click the **Start scan** button to start scanning, the application will search all files that have been encrypted and decrypt them. Select **Delete crypted files after decryption** to delete all copies of the encrypted file with the extension like vscrypt, .infected, .bloc, .korrektor . When this process is complete, the program will create a log file. The whole detail works at the system drive (usually drive C) as **UtilityName.Version_Date_Time_log.txt** , for example, *C: RectorDecryptor.2.2.0_12.08.2010_15.31.43_log.txt*

In essence, the Trojan-Ransom.Win32.Rector template usually targets only files with extensions such as .jpg, .doc, .pdf, .rar. The hacker will then contact the victim to decrypt the data via the nickname †† KOPPEKTOP †† or the following information:

ICQ: 557973252 or 481095
EMAIL: v-martjanov@mail.ru

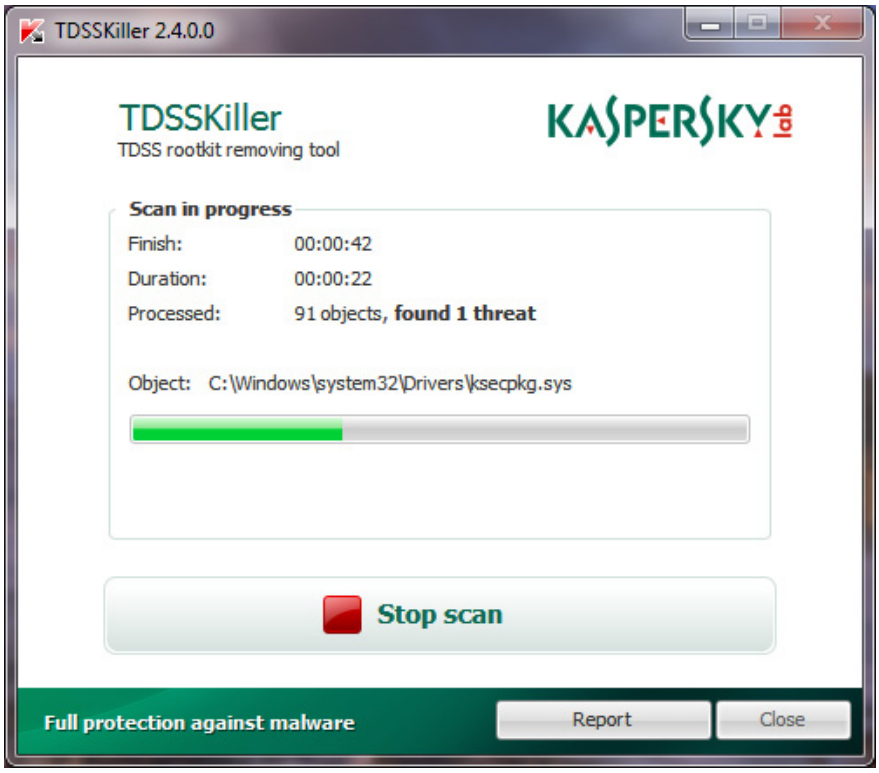
Or the following website address:

http:///trojan.sooot.cn/
http:///malware.66ghz.com/

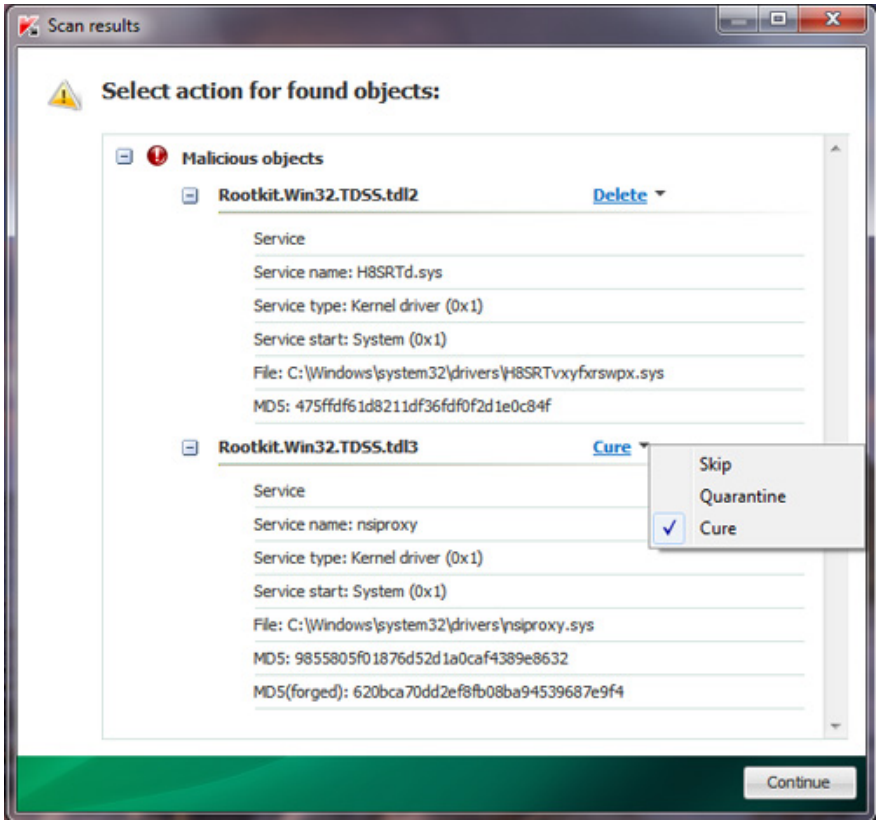
This information is displayed on the victim's desktop computer screen.

TDSSKiller

This is the 'special remedy' of malicious code **Rootkit.Win32.TDSS** , the latest version 2.4.2.1, small capacity - 1.13 MB, you can download directly here. Rootkit.Win32.TDSS line includes various variants such as Tidserv, TDSServ, Alureon . when these Rootkits successfully penetrate the user's computer, the system will be very difficult to remove, even if supported. support of Kaspersky Lab products. As for the basic way, TDSSKiller will replace users who interfere with the Registry to correct the changed keys. For Windows-based computers, the term rootkit is used to refer to a particular type of program that can 'sneak' into all system functions (Windows API). By infiltrating and modifying these low-level functions - other types of malicious code can hide more easily, interfere with the operating system's processes, hide folders and data files, edit registry . TDSSKiller is simple, easy to use because it has a graphical interface, good support for Windows 32 and 64 bit operating systems. To use, download directly from the above path, unzip to any folder on the hard drive and run the file TDSSKiller.exe:



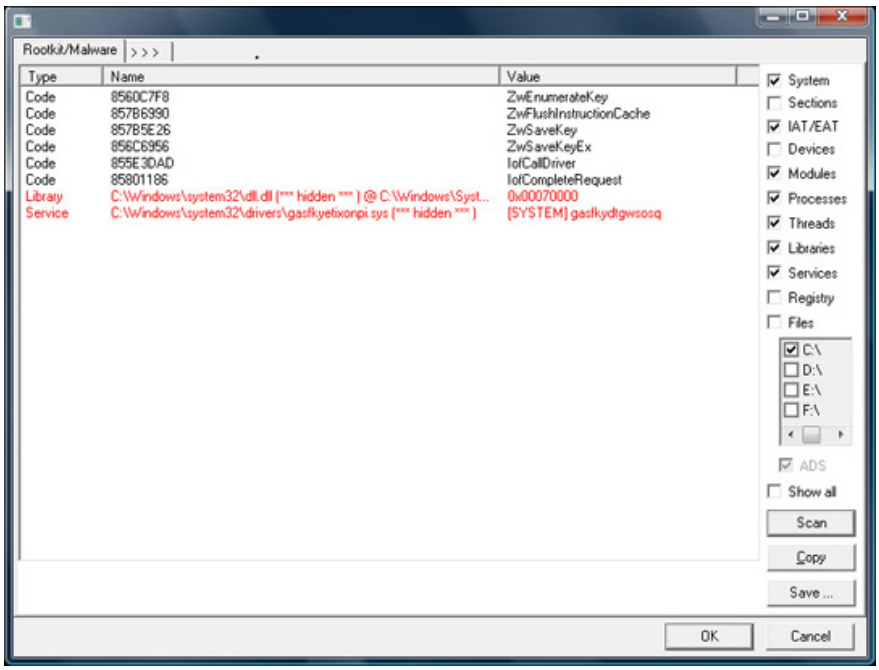
Click the **Start Scan** button to start scanning the entire system, the program will review and detect all infected objects, files . The results are divided into 2 main groups: *malicious* (identified) and *suspicious* (unrecognizable). When the scanning process is finished, the program will display a list of detected objects with specific details. With malicious objects the program automatically applies the Cure or Delete method, to suspicious objects, the user will apply the method themselves (the program's default is Skip). Or you can choose **Quarantine** to completely isolate the infected object, they will be saved to the folder on the system drive, for example *C: TDSSKiller_Quarantine23.07.2010_15.31.43*



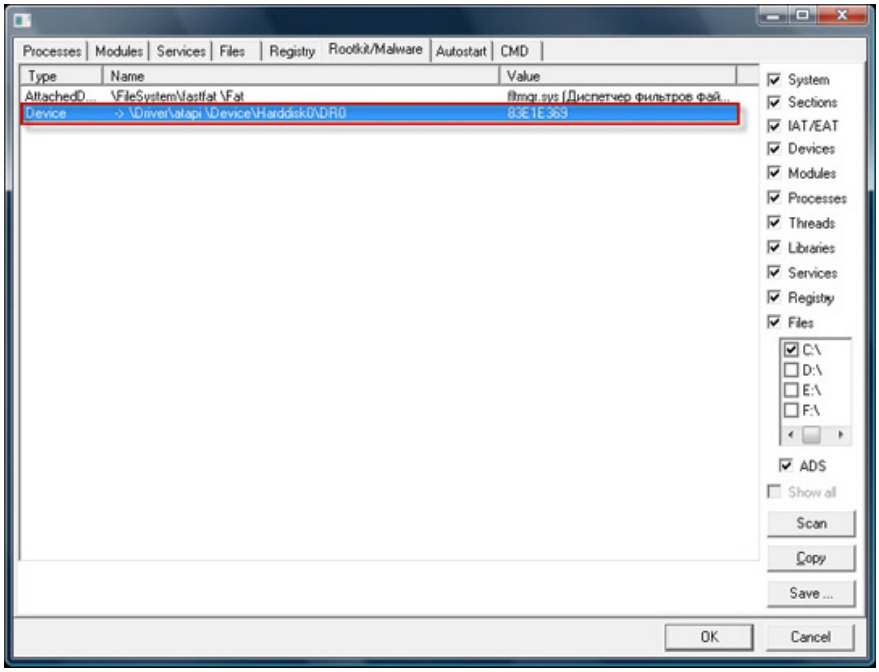
After clicking **Next** , the program will apply the user selected methods and finally display the results. You should restart your computer to complete the process:

This log file is usually saved at the system drive as **UtilityName.Version_Date_Time_log.txt** . The example here is *C: TDSSKiller_Quarantine23.07.2010_15.31.43*

Symptoms of a computer infected with Rootkit.Win32.TDSS (first generation - TDL1 and 2nd - TDL2), for experienced people they will try to track the following functions: IofCallDriver , IofCompleteRequest, NtFlushInstructionCache, NtEnumerateKey, NtSaveKey, NtSaveKeyEx . using Gmer utility:



For those infected by the 3rd generation Rootkit.Win32.TDSS (TDL3), they frequently 'cling' to the system driver file atapi.sys and replace the original device object in which:



KidoKiller

The name Kido is probably not too strange to the computer user community, with the original name **Net-Worm.Win32.Kido** (or also called Conficker, Downadup), they mainly attack computers Use Microsoft Windows operating system based on workstation and server platforms.

The most noticeable features of this Net-Worm.Win32.Kido line are that they create the autorun.inf and *RECYCLED {SID} file_name_nien.vmx files* on removable storage devices, or on storage devices. and sharing data on the local network, on the other hand they themselves store on the system as a DLL file with any name, for example, *c: windowssystem32zorizr.dll* . Self-created system services with random names, for example knqdgsm. At the same time, they try to attack and infiltrate computer systems through port 445 or 139 with MS Windows MS08-067 vulnerability, on the other hand they try to detect the computer's correct IP address by the following address:

- http://www.getmyip.org/
- http://getmyip.co.uk/
- http://www.whatsmyipaddress.com/
- http://www.whatismyip.org/
- http://checkip.dyndns.org/

Next are the signs of the network, with the data traffic increasing dramatically, originating from the infected computer. Security programs will activate the Intrusion Detection System mode to inform the Intrusion.Win.NETAPI.buffer-overflow.exploit vulnerability. And most notably, computers cannot access the websites of security companies such as avira, avast, esafe, drweb, eset, nod32, f-secure, panda, kaspersky . and so you cannot copyright activation of security applications over the Internet, very common is the case of Kaspersky (many customers encounter this situation and assume that the activation key is inappropriate, incorrect or the provider sent the wrong code to they). But for 'ancient' operating systems such as MS Windows 95, MS Windows 98 or MS Windows ME are not affected by Kido. In order to limit the vulnerabilities on the system - through which Kido is easy to exploit and invade, Microsoft security experts require users to apply the

following patches: MS08-067, MS08-068 and MS09-001.

On the other hand, users should be equipped with password protection long enough and difficult to guess (at least 6 characters and contain no information related to themselves such as birthdays, phone numbers, addresses .), turn off Remove the system's autorun feature, download KidoKiller from the above path, unzip to any folder on the drive and run the kk.exe file, block access to ports TCP 445 and 139 in the firewall section. After scanning with kk.exe, you can free access to the two ports as usual.

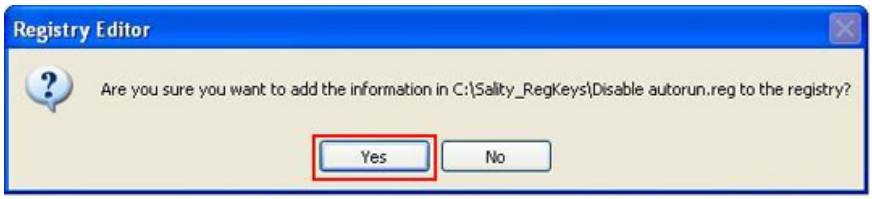
If the computer has the following applications installed:
- Kaspersky Internet Security 2009;
- Kaspersky Anti-Virus 2009;
- Kaspersky Internet Security 7.0;
- Kaspersky Anti-Virus 7.0;
- Kaspersky Internet Security 6.0;
- Kaspersky Anti-Virus 6.0;
- Kaspersky Anti-Virus 6.0 for Windows Workstations;
- Kaspersky Anti-Virus 6.0 SOS;
- Kaspersky Anti-Virus 6.0 for Windows Servers.

Then turn off the File Anti-Virus feature (or Disable temporarily Kaspersky) then activate kk.exe.

SalityKiller

Many people call this 'virus' specializing in 'eating' * .exe files in Windows operating system, the most noticeable symptom is that users cannot use * .exe files as usual, and icons theirs are changed to the Classic template. SalityKiller tool works well for Sality models after **Virus.Win32.Sality.aa** , **Virus.Win32.Sality.ag** and **Virus.Win32.Sality.bh** .

If the infected computer is in the local and domain network model: first, you need to download SalityKiller.zip, unzip to any folder and run the SalityKiller.exe file on each computer on the system (can be applied using Kaspersky Administration Kit or server group policy). Then completely delete the changed registry keys with the following tool Sality_RegKeys.zip, unzip and run the file **Disable_autorun.reg** :

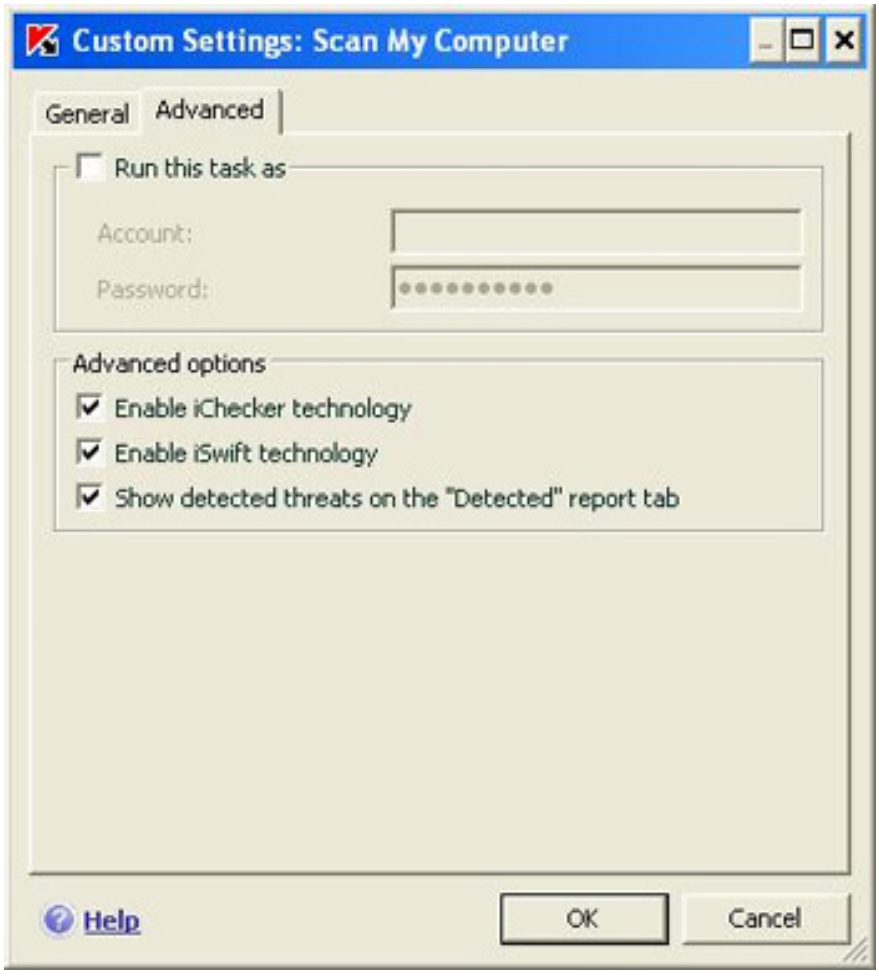


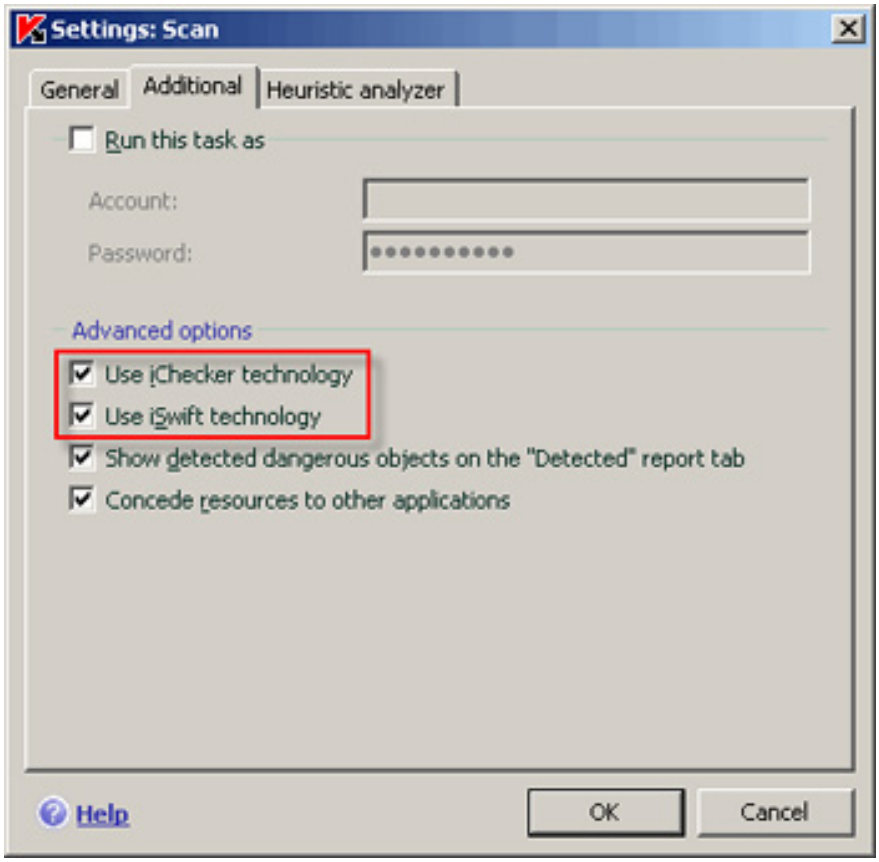
After the scanning process is over, run the reg files corresponding to the operating system from the Sality_RegKeys.zip compressed file on:

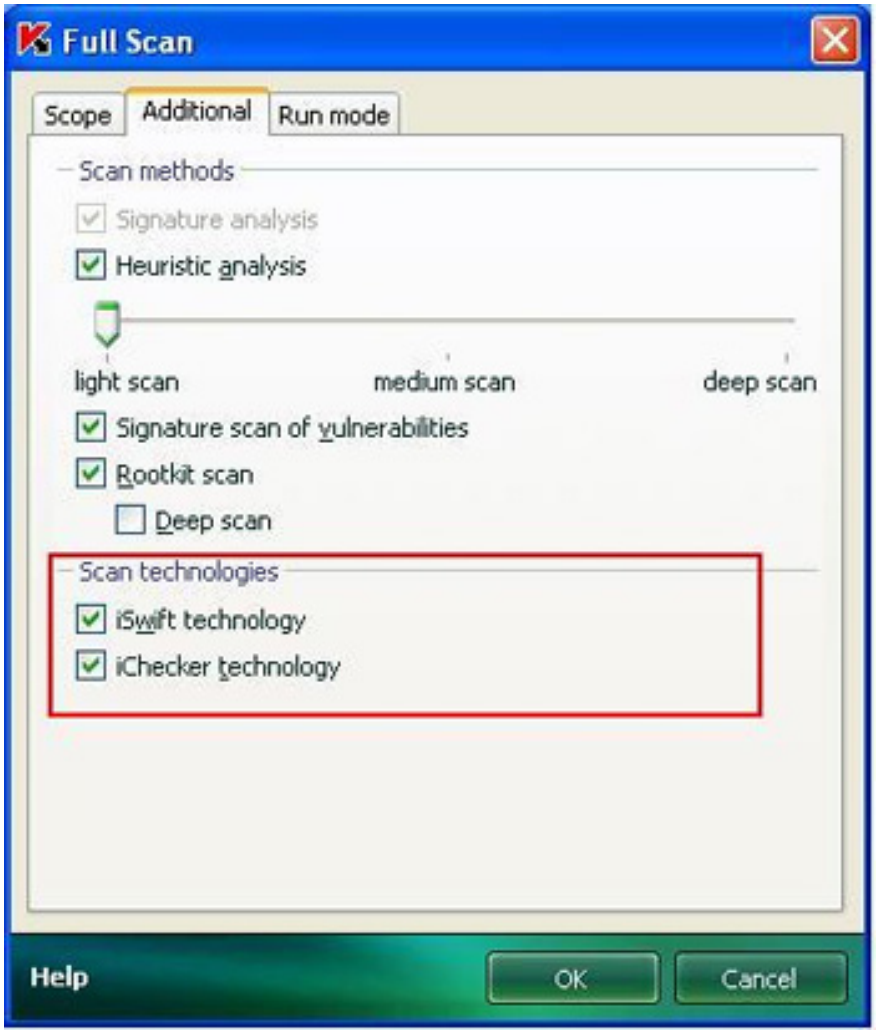
- with Windows 2000 - SafeBootWin200.reg
- with Windows XP - SafeBootWinXP.reg
- with Windows 2003 - SafeBootWinServer2003.reg
- with Windows Vista / 2008 - SafebootVista.reg
- with Windows 7/2008 R2 - SafebootWin7.reg

For standalone computers (not belonging to any local network), you first need to turn off the iSwift and iChecker functions of the following Kaspersky applications:

- Kaspersky Anti-Virus 7.0
- Kaspersky Internet Security 7.0
- Kaspersky Anti-Virus 6.0
- Kaspersky Internet Security 6.0
- Kaspersky Anti-Virus 2009;
- Kaspersky Internet Security 2009;
- Kaspersky Anti-Virus 2010;
- Kaspersky Internet Security 2010;
- Kaspersky Anti-Virus 2011;
- Kaspersky Internet Security 2011;
- Kaspersky PURE;
- Kaspersky Anti-Virus 6.0 for Windows Workstations
- Kaspersky Anti-Virus 6.0 SOS
- Kaspersky Anti-Virus 6.0 for Windows Servers




Settings: Scan
General
Additional
Heuristic analyzer
Run this task as
Account:
Password:
Advanced options
Use iChecker technology
Use iSwift technology
Show detected dangerous objects on the "Detected" report tab
Concede resources to other applications
Help
OK
Cancel



---

klwk.com

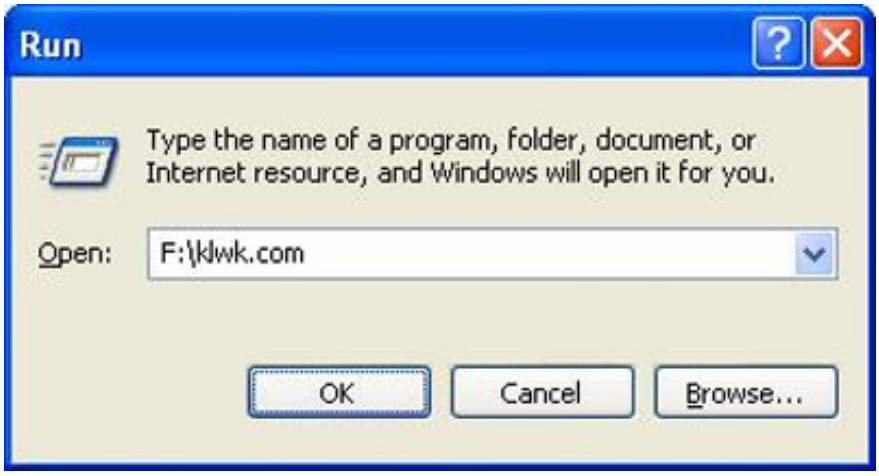
Specially used to "treat" **Trojan-Dropper.Win32.Agent.ztu** and its "allies", including:

I-Worm.Zafi.b
I-Worm.Bagle.at, au, cx-dw
Virus.Win32.Implinker.a
Not-a-virus.AdWare.Visiter
Trojan.Win32.Krotten
Email-Worm.Win32.Brontok.n
Backdoor.Win32.Allaple.a
Trojan-Spy.Win32.Goldun.mg
Email-Worm.Win32.Warezov
Virus.Win32.VB.he
IM-Worm.Win32.Sohanad.as
P2P-Worm.Win32.Malas.b
Virus.Win32.AutoRun.acw
Worm.Win32.VB.jn
Trojan.Win32.KillAV.nj

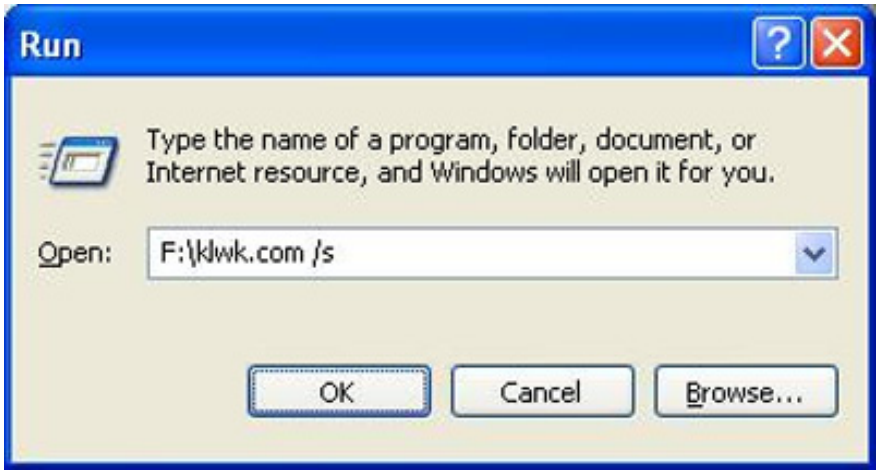
Worm.Win32.AutoRun.cby
Trojan.Win32.Agent.aec
Trojan-Downloader.Win32.Todon.an
Trojan-Downloader.Win32.Losabel.ap
Worm.Win32.AutoRun.czz, daa, dhq, dfx
Net-Worm.Win32.Rovud.ac
Trojan.Win32.ConnectionServices.x-aa
Worm.Win32.AutoRun.dtx
Worm.Win32.AutoRun.hr
Backdoor.Win32.Agent.lad
FraudTool.Win32.UltimateDefender.cm
Trojan-Downloader.Win32.Agent.wbu
Backdoor.Win32.Small.cyb
FraudTool.Win32.XPSecurityCenter.c
Downloader.Win32.VistaAntivirus.a
FraudTool.Win32.UltimateAntivirus.an
FraudTool.Win32.UltimateAntivirus.ap
Trojan-Spy.Win32.Zbot.dlh
Trojan-Downloader.Win32.Small.abpz
Rootkit.Win32.Ressdt.br
Worm.Win32.AutoRun.lsf
Worm.Win32.AutoRun.epo
Worm.Win32.AutoRun.enw
Backdoor.Win32.UltimateDefender.a
Worm.Win32.AutoRun.pwi
Worm.Win32.AutoRun.pfh
Worm.Win32.AutoRun.qhk
Worm.Win32.AutoRun.ouu
Worm.Win32.AutoRun.bnb
Worm.Win32.AutoRun.ll
AdWare.Win32.Cinmus.sxy
Trojan.Win32.Autoit.eo
Worm.Win32.AutoRun.sct Worm.Win32.AutoRun.qkn
AdWare.Win32.Cinmus.wsu
Trojan-Ransom.Win32.Taras.a
Trojan-Dropper.Win32.Agent.ztu
Trojan-Downloader.Win32.Agent.Apnd
Worm.Win32.Autorun.qpa
Net-Worm.Win32.Kido.j
Worm.Win32.Autorun.dcw
Trojan.Win32.Feedel.gen
Trojan.Win32.Pakes.mak
Net-Worm.Win32.Kido.r
Net-Worm.Win32.Kido.t
Worm.VBS.Autorun.cq
Worm.Win32.Pinit.ac
Worm.Win32.Pinit.ae
Worm.Win32.Pinit.af

Worm.Win32.Pinit.gen
Net-Worm.Win32.Kido.bw
Net-Worm.Win32.Kido.db
Net-Worm.Win32.Kido.fk
Net-Worm.Win32.Kido.fx
Net-Worm.Win32.Kido.fo
Net-Worm.Win32.Kido.s
Net-Worm.Win32.Kido.dh
Net-Worm.Win32.Kido.ee
Net-Worm.Win32.Kido.gh
Net-Worm.Win32.Kido.fa
Net-Worm.Win32.Kido.gy
Net-Worm.Win32.Kido.ca
Net-Worm.Win32.Kido.by
Net-Worm.Win32.Kido.if
Net-Worm.Win32.Kido.eo
Net-Worm.Win32.Kido.bx
Net-Worm.Win32.Kido.bh
Net-Worm.Win32.Kido.bg
Net-Worm.Win32.Kido.ha
Net-Worm.Win32.Kido.hr
Net-Worm.Win32.Kido.da
Net-Worm.Win32.Kido.dz
Net-Worm.Win32.Kido.cg
Net-Worm.Win32.Kido.eg
Net-Worm.Win32.Kido.eq
Net-Worm.Win32.Kido.bz
Net-Worm.Win32.Kido.do
Net-Worm.Win32.Kido.fw
Net-Worm.Win32.Kido.du
Net-Worm.Win32.Kido.cv
Net-Worm.Win32.Kido.dv

With extremely small capacity of only about 166 KB, extract any folder or drive (here is drive F), activate the file **klwk.com** :



Run the file **klwk.com** in the above way to review the memory and turn off the operation of the virus.



When using klwk.com/s syntax, the application will scan all hard drives and partitions on the system, remove infected files, lock registry keys containing malicious code.

ZbotKiller

The most recent version is 1.2.0.0, which is about 98.9 KB in size, specialized to remove the malicious program Trojan-Spy.Win32.Zbot - used by hackers to steal personal information related to bank, account number, password .

Some signs of the computer are infected with this type of Trojan in the system directory *(% windir% system32 and% AppData%* - with Windows Vista are: *C: WindowsSystem32* and *C: The UsersAppData is* still with Windows XP Professional, it will be *C: WINDOWSsystem32* and *C: Documents and SettingsApplication Data* will suddenly appear one or more of the following strange files: ntos.exe, twex.exe, twext.exe, oembios.exe, sdra64.exe, lowseclocal.ds or lowsecuser.ds.

The path to the above files is stored here:

- *HKEY_LOCAL_MACHINESoftwareMicrosoftWindows NTCurrentVersionWinlogonUserinit o*
- *HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun*

How to use is very simple, just download the file from the above path, extract and run the file ZbotKiller.exe, wait for the process to finish and restart the system.

KatesKiller

Created to thoroughly remove the **Trojan-PSW.Win32.Kates** line, the latest version is now 1.2.2, which is only about 91.1 KB.

Some signs of Trojan-PSW.Win32.Kates infected computer:

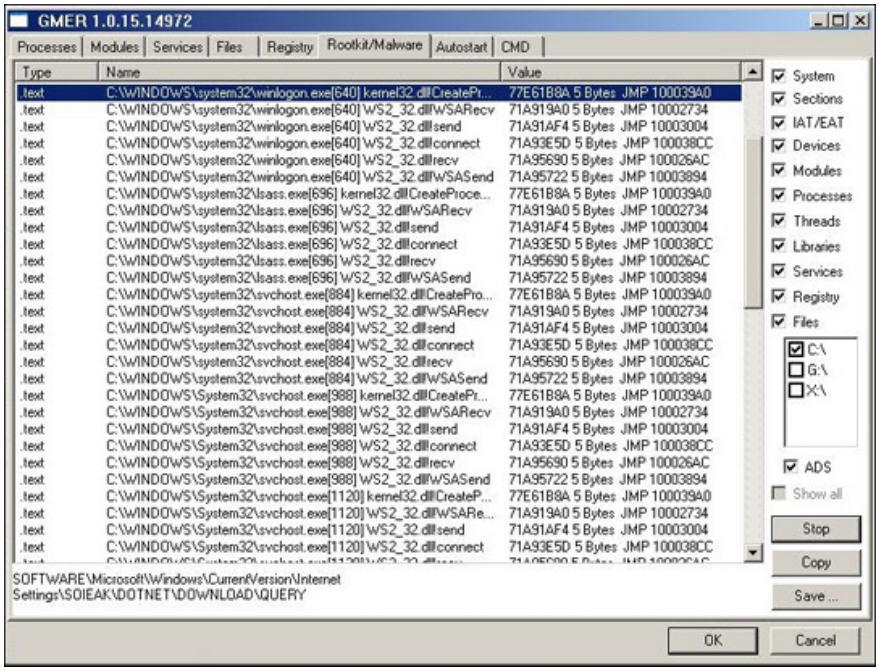
- Security programs detect the presence of trojans on the computer, when deleting these files, they immediately recover under other names (especially for Kaspersky products, this does not happen)

- The explorer.exe application is immediately canceled when the user executes the following command: regedit.exe, cmd.exe and Total Commander

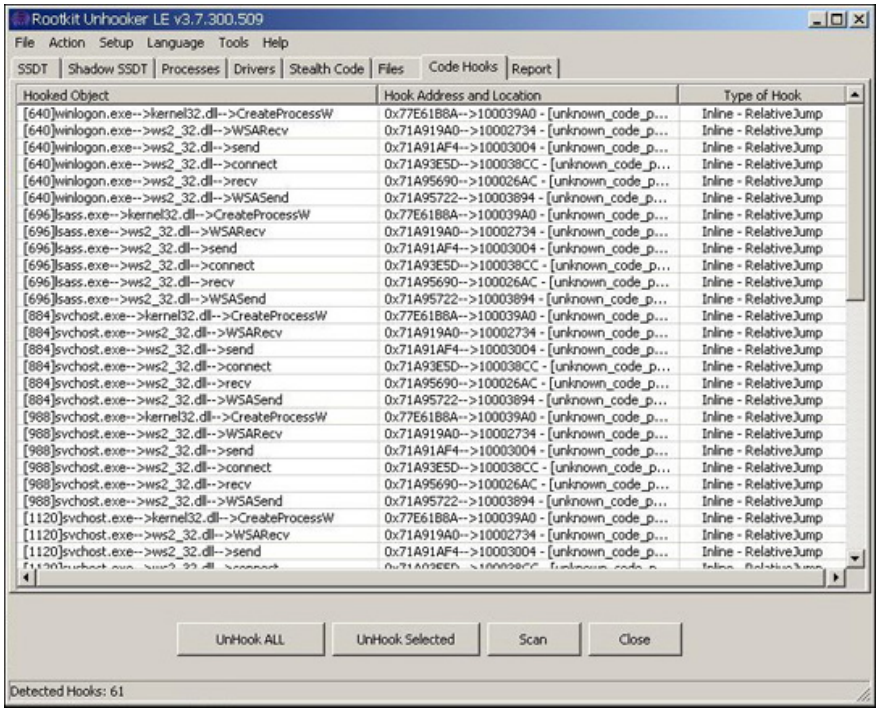
- Files with extension * .bat and * .reg cannot be activated

- The following functions are loaded into most active processes on the system: CreateProcessW, WSARecv, WSASend, send, connect and recv

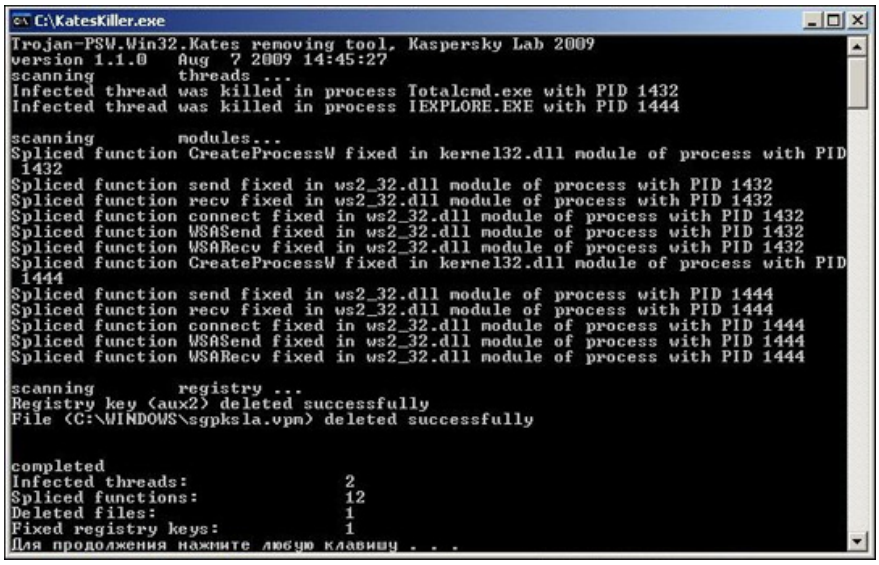
When using Gmer, you can clearly see the operation of the following functions:



Or with Rootkit Unhooker:



Users only need to download KatesKiller here, extract and activate the **KatesKiller.exe** file, the program will search and delete dangerous applications, detect hidden functions and cancel the operation of application functions. This: CreateProcessW, WSASend, WSARecv, send, recv and recv, delete the changed registry keys:



clrav.com

Clrav.com can be applied to the following types of malicious code by Kaspersky experts: *I-Worm.BleBla.b, I-Worm.Navidad, I-Worm.Sircam, I-Worm. Goner, I-Worm.Klez.a, I-Worm.Klez.e, I-Worm.Klez.f, I-Worm.Klez.g, I-Worm.Klez.h, Win32.Elkern.c, I- Worm.Lentin.a, I-Worm.Lentin.b, I-Worm.Lentin.c, I-Worm.Lentin.d, I-Worm.Lentin.e, I-Worm.Lentin.f, I-Worm. Lentin.g, I-Worm.Lentin.h, I-Worm.Lentin.i, I-Worm.Lentin.j, I-Worm.Lentin.k, I-Worm.Lentin.l, I-Worm.Lentin. m, I-Worm.Lentin.n, I-Worm.Lentin.o, I-Worm.Lentin.p, I-Worm.Tanatos.a, I-Worm.Tanatos.b, I-Worm.Win32.Opasoft. a, I-Worm.Win32.Opasoft.b, I-*

Worm.Win32.Opasoft.c, I-Worm.Win32.Opasoft.d, I-Worm.Win32.Opasoft.e, I-Worm.Win32.Opasoft. f, I-Worm.Win32.Opasoft.g, I-Worm.Win32.Opasoft.h, I-Worm.Win32.Opasoft.i, I-Worm.Win32.Opasoft.j, I-Worm.Win32.Opasoft. k, I-Worm.Win32.Opasoft.l, I-Worm.Win32.Opasoft.m, I-Worm.Win32.Opasoft.n, I-Worm.Win32.Opasoft.o, I-Worm.Win32.Opasoft. p, I-Worm.Avron.a , I-Worm.Avron.b, I-Worm.Avron.c, I-Worm.Avron.d, I-Worm.Avron.e, I-Worm.LovGate.a, I-Worm.LovGate.b, I -Worm.LovGate.c, I-Worm.LovGate.d, I-Worm.LovGate.e, I-Worm.LovGate.f, I-Worm.LovGate.g, I-Worm.LovGate.h, I-Worm .LovGate.i, I-Worm.LovGate.j, I-Worm.LovGate.k, I-Worm.LovGate.l, I-Worm.Fizzer, I-Worm.Magold.a, I-Worm.Magold.b , I-Worm.Magold.c, I-Worm.Magold.d, I-Worm.Magold.e, Worm.Win32.Lovesan, Worm.Win32.Welchia, I-Worm.Sobig.f, I-Worm.Dumaru .a - I-Worm.Dumaru.m, Trojan.Win32.SilentLog.a, Trojan.Win32.SilentLog.b, Backdoor.Small.d, I-Worm.Swen, Backdoor.Afcore.l - Backdoor.Afcore.ad , I-Worm.Sober.a, I-Worm.Sober.c, I-Worm.Mydoom.a, I-Worm.Mydoom.b, I-Worm.Mydoom.e, I-Worm.Torvil.d, I -Worm.NetSky.b - I-Worm.NetSky.d, TrojanDownloader.Win32.Agent.a - TrojanDownloader.Win32.Agent.j, I-Worm.Bagle.a - I-Worm.Bagle.j, I-Worm .Bagle.n- I-Worm.Bagle.r, I-Worm.Bagle.z, Worm.Win32.Sasser.a - Worm.Win32.Sasser.d, Worm.Win32.Sasser.f, Backdoor.Agent.ac , Trojan.Win32.StartPage.fw

The latest version is currently 11.0.0.2, small and light ~ 139 Kb, like other Kaspersky support tools, users just need to download, unzip and run the file clrav.com.

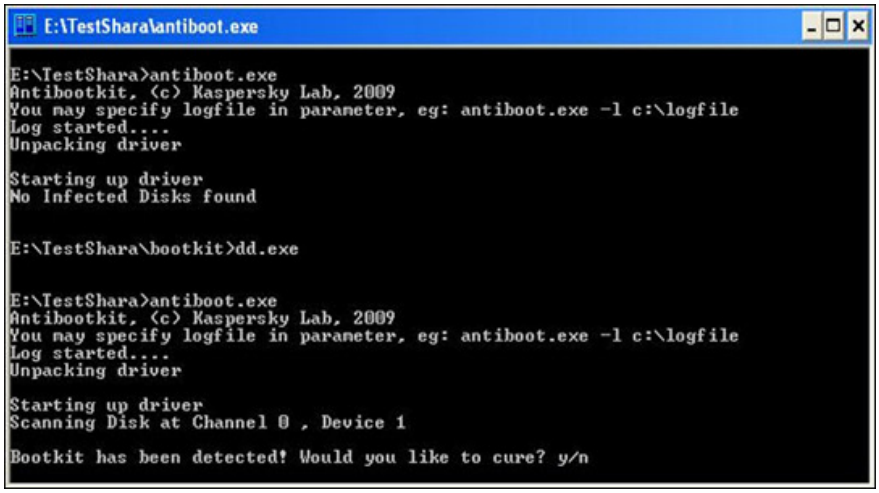
VirutKiller

The main function of this tool is to detect and remove traces of the virus bot. **Virus.Win32.Virut.ce** , q - they are used to steal and 'transport' data from infected computers. To ensure the successful processing of this virus, you should first turn off System Restore of Windows first, download VirutKiller, extract it to any folder on your hard drive and run the VirutKiller.exe file, and the You just need to wait for the scan to finish and restart once. At the beginning of the review, the application will search and disable malicious processes, combined with the search for the following functions: NtCreateFile, NtCreateProcess, NtCreateProcessEx, NtOpenFile and NtQueryInformationProcess. Next, the program will take over the task of reviewing, terminating the spread process and isolating the affected files on the entire hard drive.

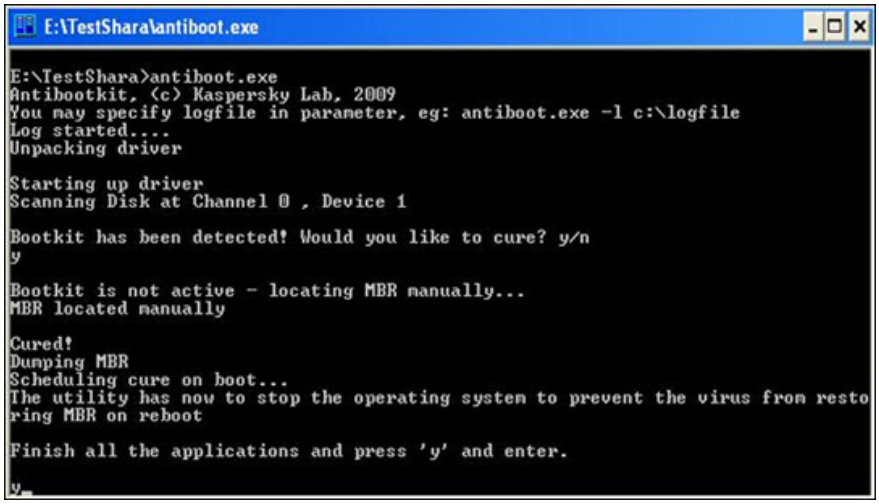
Antiboot

Specially used to kill malicious code **Backdoor.Win32.Sinowal.deg** - they have a very sophisticated mechanism of hiding and hiding themselves, so they are almost impossible to detect on any computer that has been infected. infected. They hide the infected objects behind their original file. Besides, the main body of this malicious program (kernel level driver) is not in the file system. They often hide in unused areas at the last partition of the hard drive. These Backdoor malicious programs do not need an operating system to launch their 'working' process, so they are especially dangerous because users cannot know how many hackers are 'sniffing'. 'in their own computer.

To use Antiboot, download the archive here, extract any folder or hard drive and run antiboot.exe:



Press **Y** to start the system recovery process:

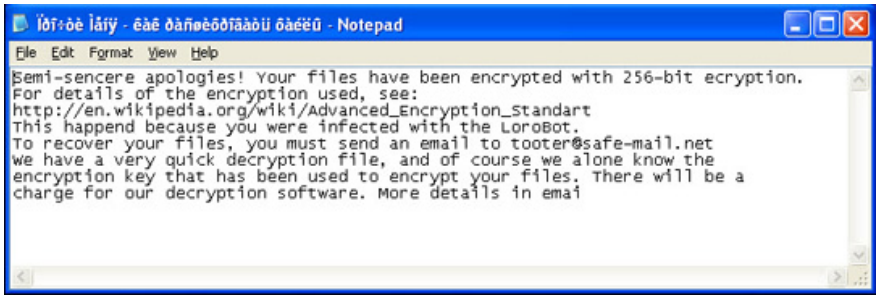


Select Y, then exit the program and restart the system.

XoristDecryptor

Trojan-Ransom.Win32.Xorist - a type of Trojan created to steal user's personal information on an infected computer, and makes the computer's operation become unstable and unstable. After capturing the data, hackers will return it to users who require them to pay for the data back.

Some symptoms of Trojan-Ransom.Win32.Xorist computers are that they receive a request to send any message to decrypt those files, the text font used is Cyrillic - so almost Everyone just saw the squares and strange characters. Another sign is the appearance of a file named in Russian - *?????? ???? - ??? ???????????? ?????* :



Accompany it is the file CryptLogFile.txt in the Windows folder. They can encrypt files with the following extensions: *doc, xls, docx, xlsx, db, mp3, waw, jpg, jpeg, txt, rtf, pdf, rar, zip, psd, msi, tif, wma, lnk, gif, bmp, ppt, pptx, docm, xlsm, pps, ppsx, ppd, tiff, eps, png, ace, djvu, xml, cdr, max, wmv, avi, wav, mp4, pdd, html, css, php, aac, ac3, amf, amr, mid, midi, mmf, mod, mp1, mpa, mpga, mpu, nrt, oga, ogg, pbf, ra, ram, raw, saf, val, wave, wow, wpk, 3g2, 3gp, 3gp2, 3mm, amx, avs, bik, bin, dir, divx, dvx, evo, flv, qtq, tch, rts, rum, rv, scn, srt, stx, svi, swf, trp, vdo, wm, wmd, wmmp, wmx, wvx, xvid, 3d, 3d4, 3df8, pbs, adi, ais, amu, arr, bmc, bmf, cag, orange, dng, ink, jif, jiff, jpc, jpf, jpw, mag, mic, mip, msp, nav, ncd, odc, odi, opf, qif, qtiq, srf, xwd, abw, act, adt, aim, ans, asc, ase, bdp, bdr, bib, boc, crd, diz, dot, dotm, dotx, dvi, dxe, mlx, err, euc, faq, fdr, fds, gthr, idx, kwd, lp2, ltr, man, mbox, msg, nfo, now, odm, oft, pwi, rng, rtx, run, ssa, text, unx, wbk, wsh, 7z, arc, ari, arj, car, cb r, cbz, gz, gzig, jgz, pak, pcv, puz, r00, r01, r02, r03, rev, sdn, sen, sfs, sfx, sh, shar, shr, sqx, tbz2, tg, tlz, vsi, wad, war, xpi, z02, z04, zap, zipx, zoo, ipa, isu, jar, js, udf, adr, ap, aro, asa, ascx, ashx, asmx, asp, aspx, asr, atom, bml, cer, cms, crt, dap, htm, moz, svr, url, wdgt, abk, bic, big, blp, bsp, cgf, chk, col, company, dem, elf, ff, gam, grf, h3m, h4r, iwd, ldb, lgp, lvl, map, md3, mdl, mm6, mm7, mm8, nds, pbp, ppf, pwf, pxp, sad, sav, scm, scx, sdt, spr, sud, uax, umx, unr, uop, usa, usx, ut2, ut3, utc, utx, uvx, uxx, vmf, vtf, w3g, w3x, wtd, wtf, ccd, cd, cso, disk, dmg, dvd, fcd, flp, img, iso, isz, md0, md1, md2, mdf, mds, nrg, nri, vcd, vpb, dic, cch, ctt, dal, ddc, ddcx, dex, dif, dii, itdb, itl, kmz, lcd, lcf, mbx, mdn, odf, odp, ods, pab, pkb, pkh, qdf, qel, rgn, rrt, rsw, rte, sdb, sdc, sds, sql, stt, t01, t03, t05, tcx, thmx, txd, txf, upoi, vmt, wks, wmdb, xlc, xlc, xlr, xlsb, xltx, ltm, xlwx, mcd, cap, cc, cod, cp, cpp, cs, csi, dcp, dcu, dev, dob, dox, dpk, dpl, dpr, dsk, dsp, eql, ex, f90, fla, for, fpp, jav, java, lbi, owl, pl, plc, pli, pm, res, rnc, rsrc, so, swd, tpu, tpx, tu, tur, vc, yab, 8ba, 8bc, 8be, 8bf, 8bi8, bi8, 8bl, 8bs, 8bx, 8by, 8li, aip, amxx, ape, api, mxp, oxt, qpx, qtr, xla, xlam, xll, xlv, xpt, cfg, cwf, dbb, slt, bp2, bp3, bpl, clr, dbx, jc, potm, ppsm, prc, prt, shw, std, ver, wpl, xlm, yps, md3.*

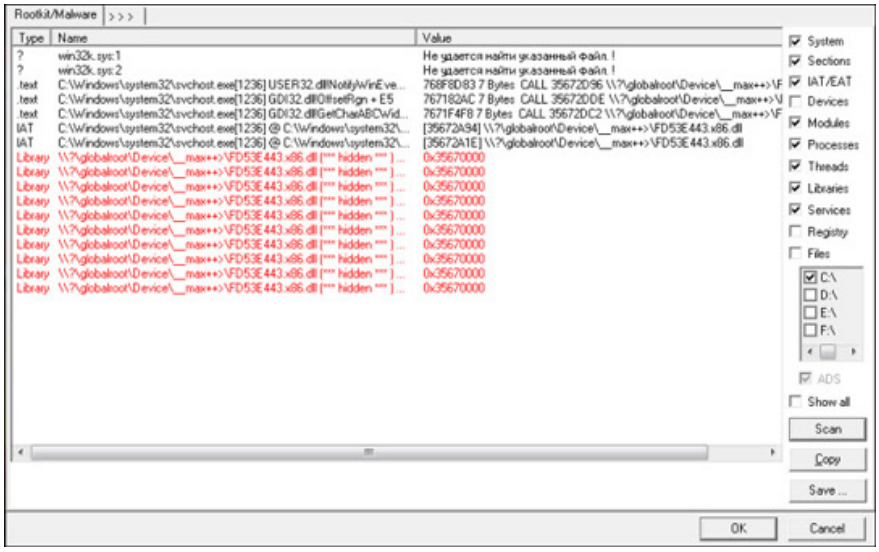
To use XoristDecryptor, download the compressed file here, extract any folder or any hard drive and run the XoristDecryptor.exe file. Wait for the scan to finish, you should restart the computer.

PmaxKiller

This is a utility tool used to remove **Rootkit.Win32.PMax** lines - they infect Microsoft Windows 2000, XP, 2003, Vista, 2008 and 7 32 bit versions. As for 64-bit systems, it is not affected by this malicious code.

Some typical signs of the computer when infected with this Rootkit type, security programs are interrupted in the middle of a scan or operation. In addition, the DACL (Discretionary Access Control List) feature set for executable files is prevented from starting, so when you try to activate a program, the system will display a message. Unauthorized error due to no rights.

If you use Gmer to track processes, you will see hidden modules with links containing strange characters **__max** ++> :



Like other Kaspersky tools, you only need to download the compressed file of PMaxKiller here to your computer, unzip and activate the file PMaxKiller.exe. Wait for the scan to finish and restart the computer.

KL Anti-FunLove

This is a specialized support tool to completely remove the presence of **Win32.FunLove** worm from your computer. The installation and usage process is very simple, since this is a graphical user interface, download KL Anti-FunLove's compressed file here, extract and run KL Anti-FunLove.exe file:

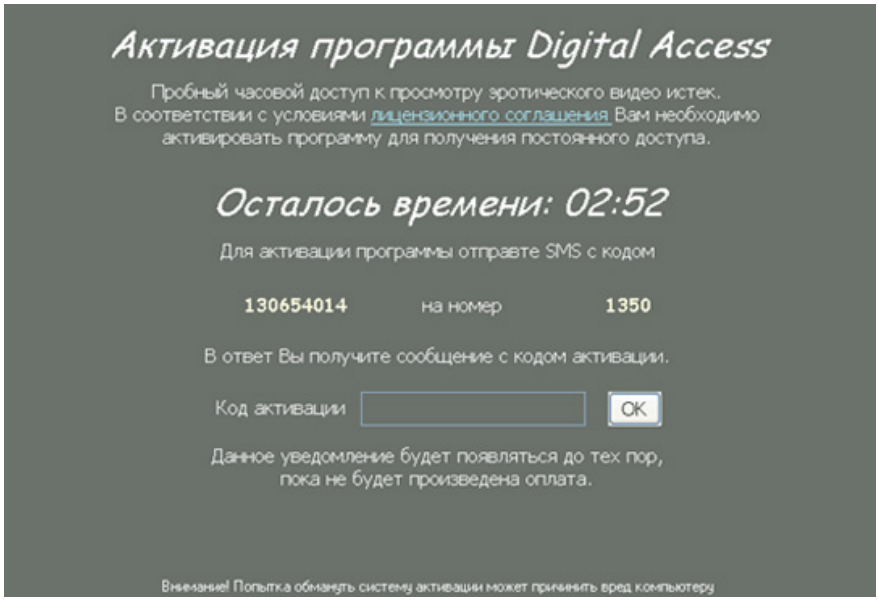
Click **Install** to install, then restart the computer. When the operating system boots up, the program will scan in the memory, hard drive . the whole process is fully displayed. Sau khi quá trình quét và xóa b? mã ??c k?t thúc, b?n nên kh?i ??ng l?i h? th?ng 1 l?n n?a. N?u h? th?ng ho?t ??ng không ?n ??nh, hãy g? b? các ch??ng trình b?o m?t và cài l?i.

Digita_Cure

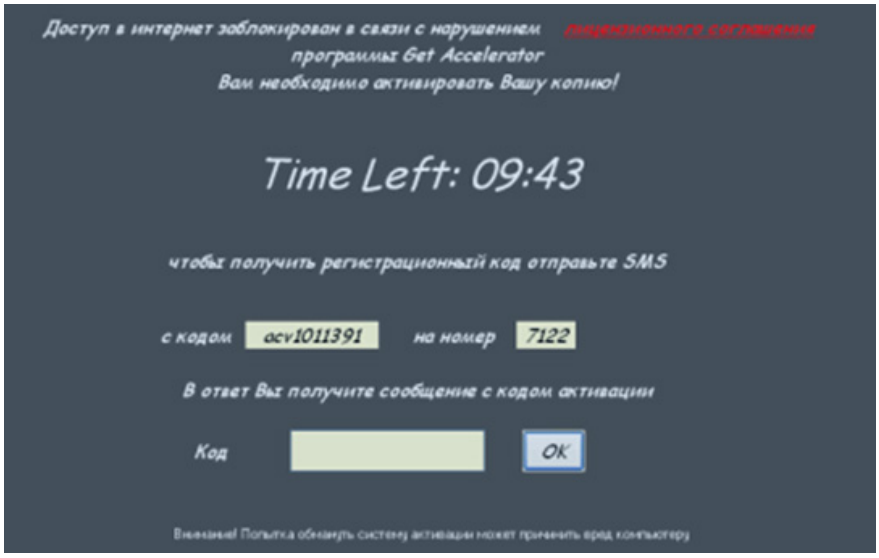
Khi máy tính c?a b?n không th? k?t n?i Internet, ??ng th?i nh?n ???c nh?ng thông báo b?ng ngôn ng? l? thì có th

? máy tính ?ã b? nhi?m **Trojan-Ransom.Win32.Digitala** – bao g?m các bi?n th? sau Get Accelerator, Digital Access, Get Access, Download Manager v1.34. Chúng có kh? n?ng ng?n ch?n các k?t n?i t? h? th?ng t?i Internet, ??ng th?i thông báo v?i ng??i s? d?ng ph?i ch?p nh?n th?a thu?n t? phía tin t?c b?ng cách cung c?p thông tin cá nhân cho chúng, sau ?ó s? ???c 'm? khóa' và truy c?p Internet nh? bình th??ng.

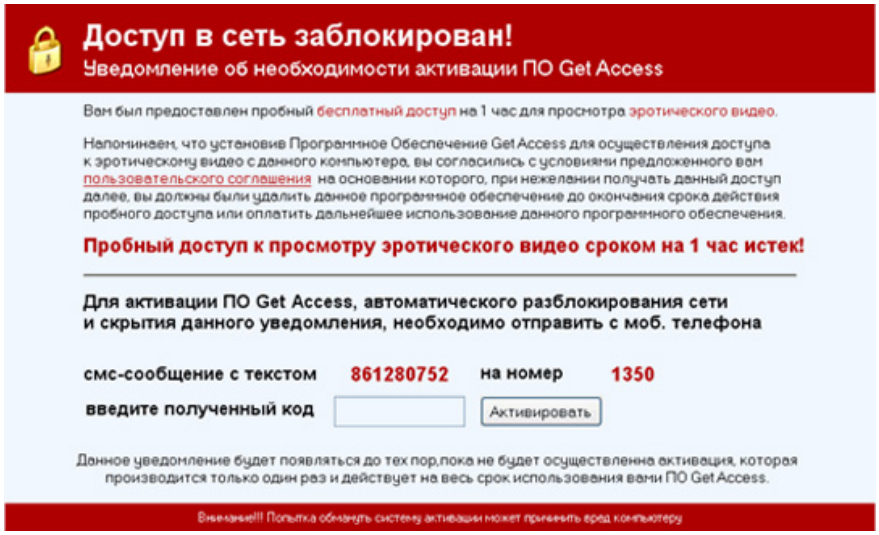
D??i ?ây là 1 s? m?u, v?i dòng Digital Access:



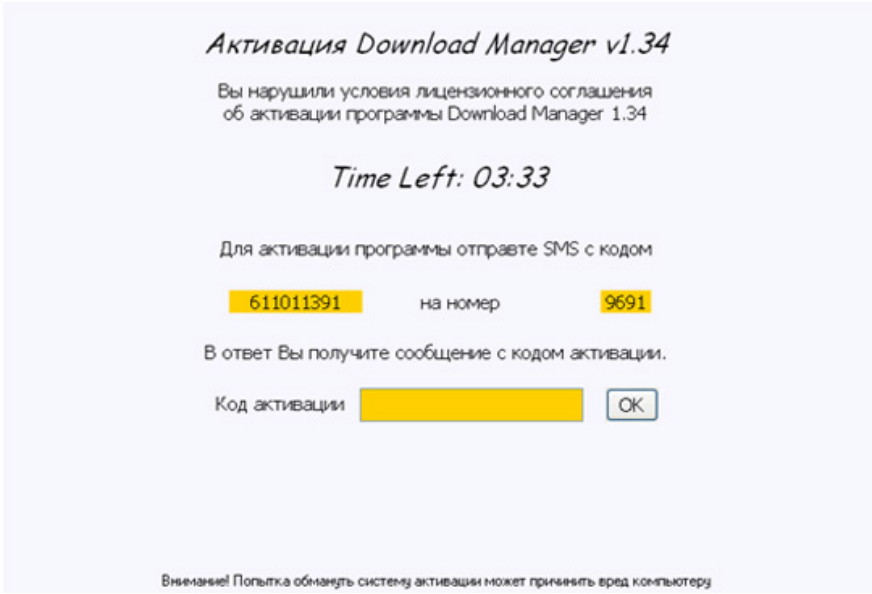
Get Accelerator:



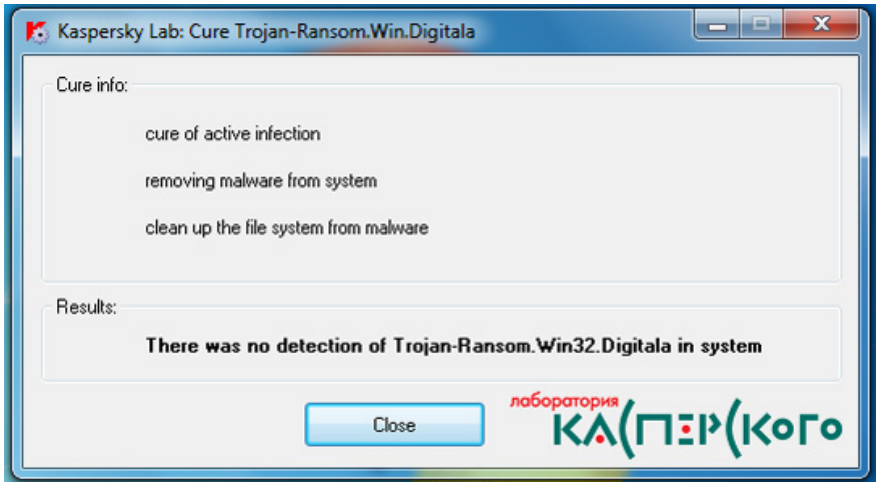
Get Access:



và Download Manager v1.34:



?? s? d?ng Digita_Cure, các b?n t?i file này v? máy tính, gi?i nén và ch?y file Digita_Cure.exe:



L?u ý r?ng ti?n ích này ch? ho?t ??ng v?i b?n 32 bit c?a h? ?i?u hành Microsoft Windows 2000, XP, 2003, Vista, 2008 và 7, vì b?n 64 bit không b? ?nh h??ng b?i Trojan-Ransom.Win32.Digitala.

Anti-Nimda

?ây là công c? cu?i cùng trong danh sách h? tr? c?a Kaspersky, chuyên dùng ?? '?i?u tr?' lo?i virus **I-Worm.Nimda** , v?n lây lan m?nh m? qua Internet b?ng trình duy?t Internet Explorer. T?i file antinimd, gi?i nén và ch?y file antinimd.exe. Ch? quá trình quét này k?t thúc và kh?i ??ng l?i máy tính. Ki?m tra l?i s? t?n t?i c?a các th? vi?n h? th?ng b?ng ch?c n?ng Search v?i tên: MMC.EXE, RICHED20.DLL, LOAD.EXE RICHED20.DLL, MMC.EXE (Microsoft Management Console). N?u b?t k? file DLL nào b? phát hi?n có d?u hi ?u b? lây nhi?m, các b?n nên xóa b? chúng ?i và thay th? b?ng DLL 's?ch' trên máy tính khác có cùng h? ?i?u hành.

M?t l?n n?a, chúng tôi khuyên các b?n nên s? d?ng các ch??ng trình an ninh c?a nh?ng hãng danh ti?ng, có uy tín nh? Kaspersky, BitDefender, Avira, Norton, Panda … t?t c? ??u có s?n trên gian hàng c?a công ty c? ph?n m ?ng tr?c tuy?n Meta. Các b?n có th? tham kh?o thêm chi ti?t t?i ?ây ho?c ?ây. Good luck!

You finished reading the article "**Kaspersky's free support security utilities**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com