

Computer Security

Chodzi lisek koło drogi,
Nie ma ręki ani nogi,
Kogo lisek przyodzieje,
Ten się nawet nie spodzieje

From the news

- ▶ Canada, U.S. issue joint alert on 'ransomware' after hospital attacks
 - ▶ San Diego-based Alvarado Hospital Medical Center was hit by a "malware disruption" on March 31, the San Diego Union-Tribune reports. A spokesperson for the 306-bed hospital confirmed the cyber attack, but would not say which systems had been affected.
 - ▶ The most well-documented ransomware incidents have hit the medical industry. Hollywood Presbyterian Medical Center in Los Angeles paid 40 bitcoins -- about \$17,000 -- to decrypt its files.
 - ▶ Four weeks later, Methodist Hospital of Henderson, Kentucky, said a piece of ransomware known as Locky infected its systems, according to computer security writer Brian Krebs. The hospital did not pay a ransom but was able to restore its systems, according to a local news report.
 - ▶ Adobe Systems Inc issued an emergency update on Thursday to its widely used Flash software for Internet browsers after researchers discovered a security flaw that was being exploited to deliver ransomware to Windows PCs.
- 

Computer Security

Glossary

Computer Malware

Viruses

Trojan Horses

Spyware

Ransomware

Phishing

Spoofing

Drive-by download (drive by installation)

Virus and Spyware definition file

Zero Day Attack

▶ Backups, Backups , Backups.

The only 100% protection from ransomware .
Disconnect the backup media

▶ Updates, Patching

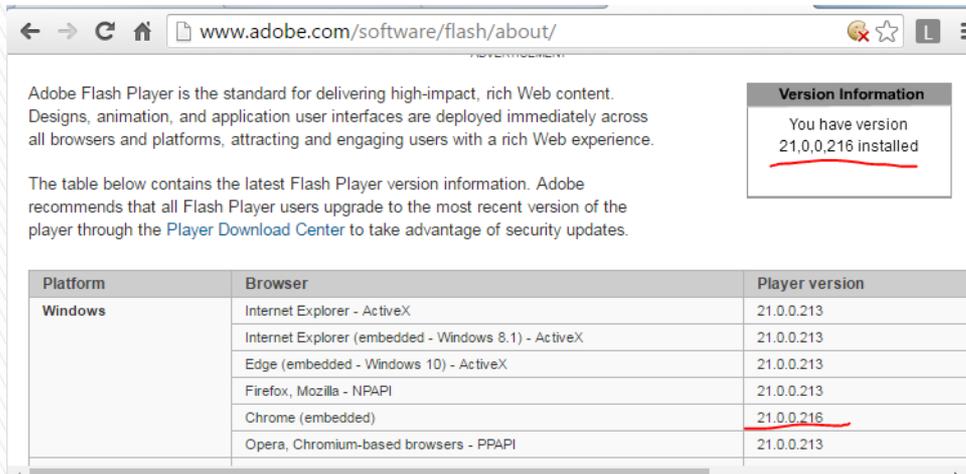
Windows updates – set to automatic.

Adobe flash – always from Adobe site

this week emergency update to Flash version 21_0_0_213

check here :C:\windows\System32\Macromed\Flash – for IE

or on the Web Site: <http://www.adobe.com/software/flash/about/>



The screenshot shows the Adobe Flash Player website. The browser address bar displays www.adobe.com/software/flash/about/. The page content includes a description of Adobe Flash Player, a "Version Information" box, and a table of supported browsers.

Version Information

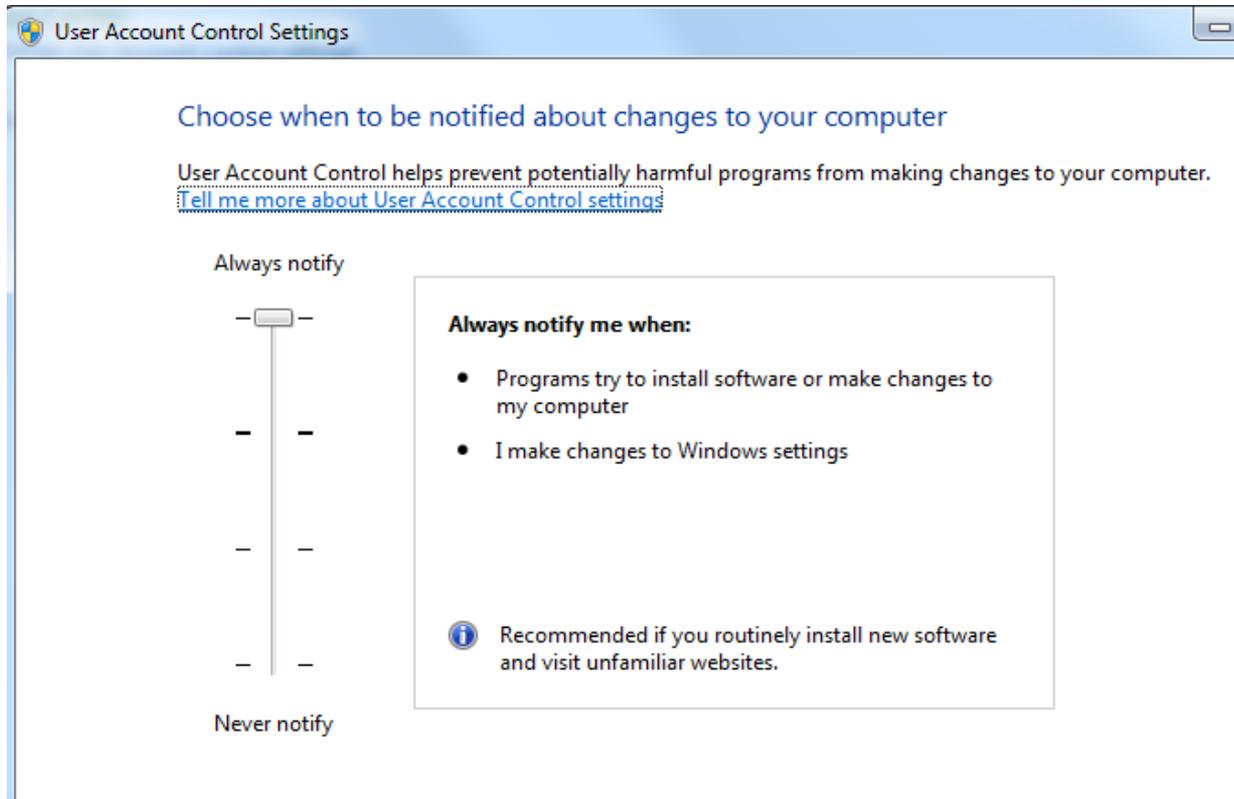
You have version 21,0,0,216 installed

Platform	Browser	Player version
Windows	Internet Explorer - ActiveX	21.0.0.213
	Internet Explorer (embedded - Windows 8.1) - ActiveX	21.0.0.213
	Edge (embedded - Windows 10) - ActiveX	21.0.0.213
	Firefox, Mozilla - NPAPI	21.0.0.213
	Chrome (embedded)	<u>21.0.0.216</u>
	Opera, Chromium-based browsers - PPAPI	21.0.0.213

Protection

UAC User Access Control

It is annoying, but put it on
In Control Panel select “User Accounts” and “Change User Account Control settings”
Move the point to “Always notify”

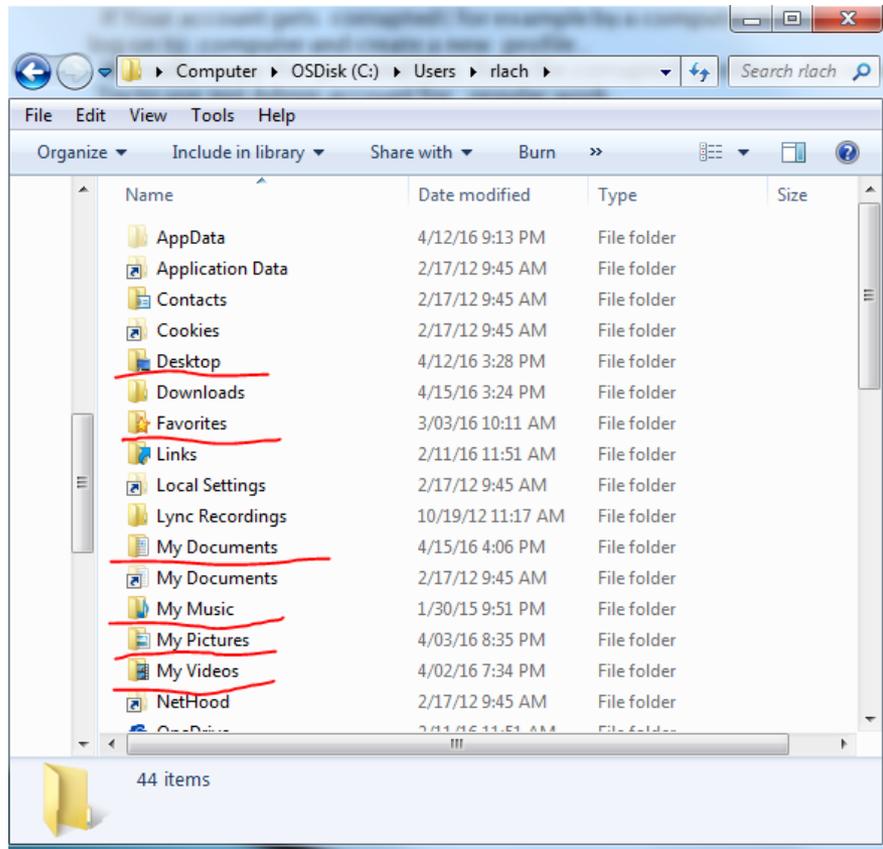


User Accounts

Create a spare user account and put in Administrators group.

If Your account gets corrupted (for example by a computer malware) use the spare admin account to log on to computer and create a new profile .

Manually copy the personal files from the corrupted profile to the new one.



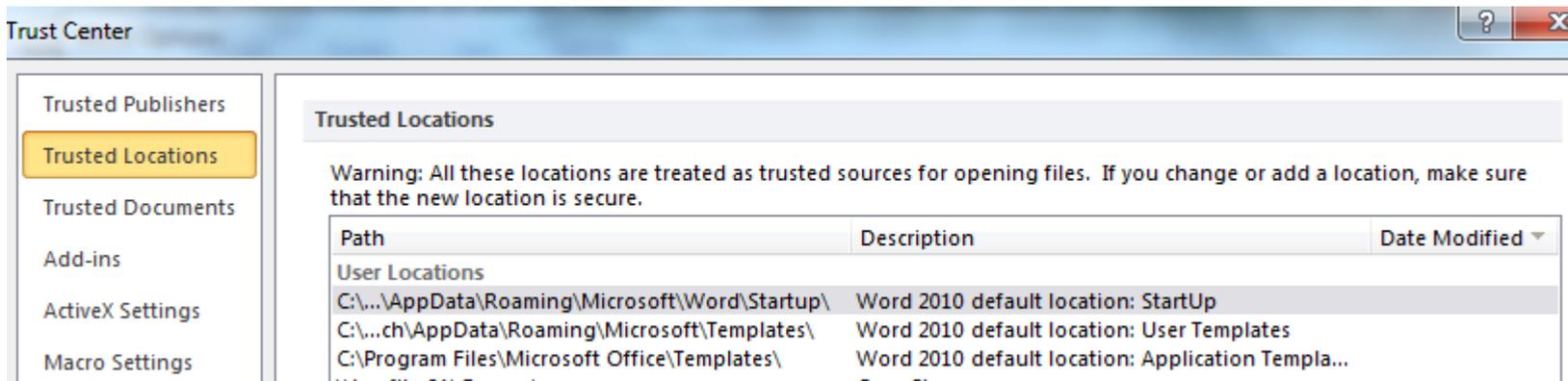
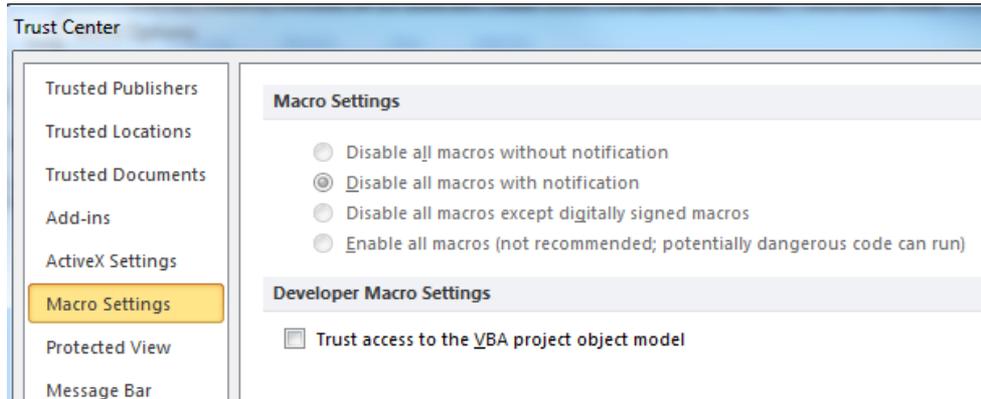
MS Office configuration

Disable Macros.

Create\Add Trusted Locations

In MS Word select : File \ Options \ Trust Center \ Trust Center Settings .

Select “ Disable all macros with notification “

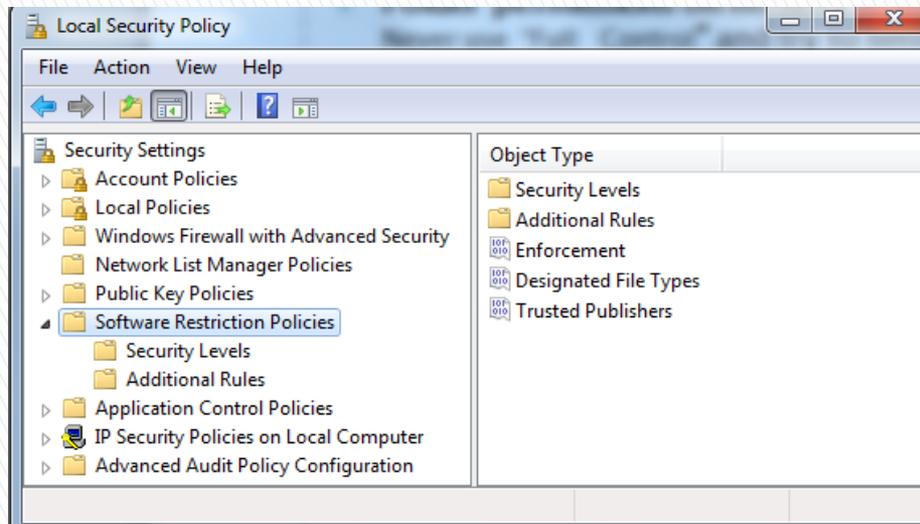


Add some “trusted Locations” .

- ▶ Log on as regular user , not the administrator
- ▶ Folder permissions on network drives
Never use “Full Control” and try to limit “modify “ permission
- ▶ Software Restriction Policy

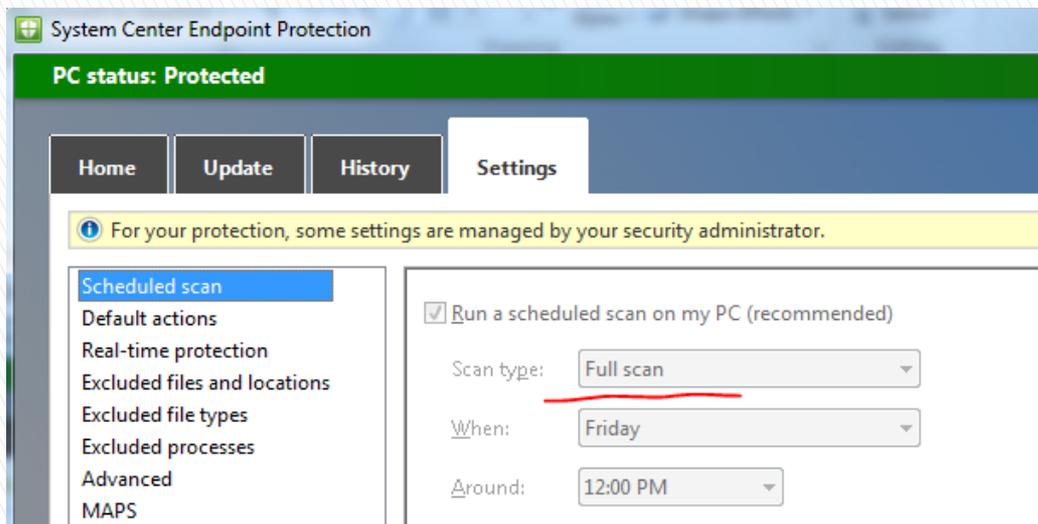
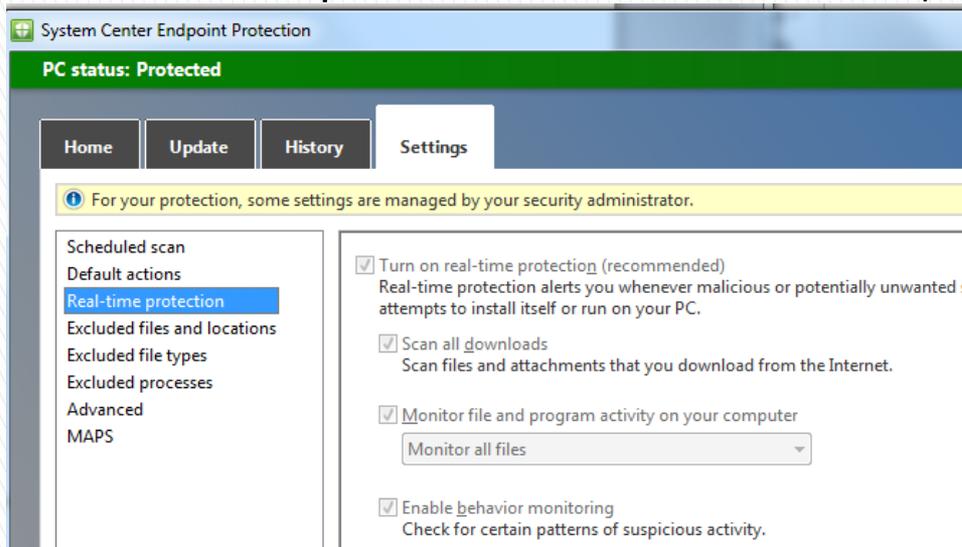
Disable PowerShell !!

Location : C:\Windows\System32\WindowsPowerShell\v1.0



Protection

- ▶ Anti-virus software – configuration
DEMO – Endpoint Protection . Turn on real-time protection. Schedule full scan

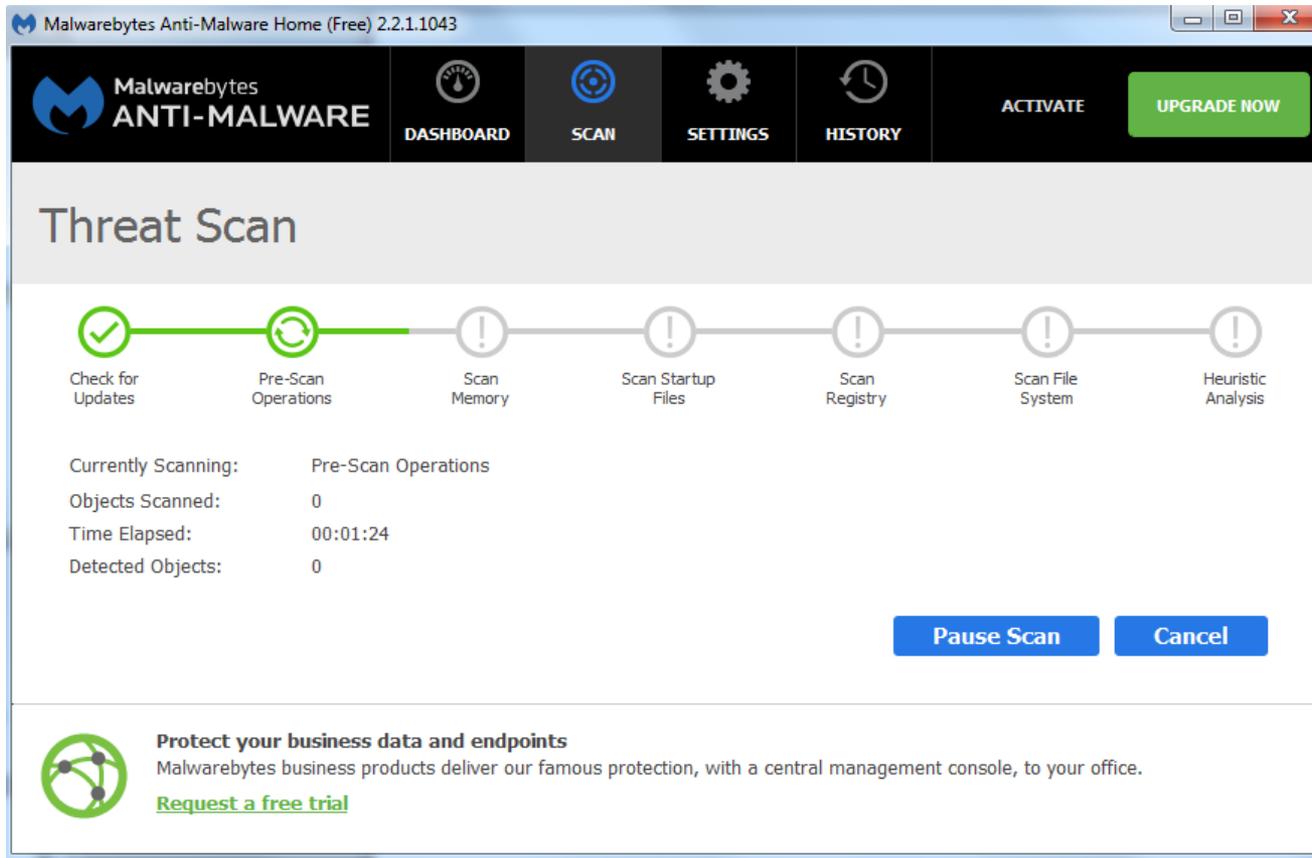


Anti-virus Software

Malwarebytes . Great tool for one time scanning, it does not replace anti-virus software.

<https://www.malwarebytes.org>

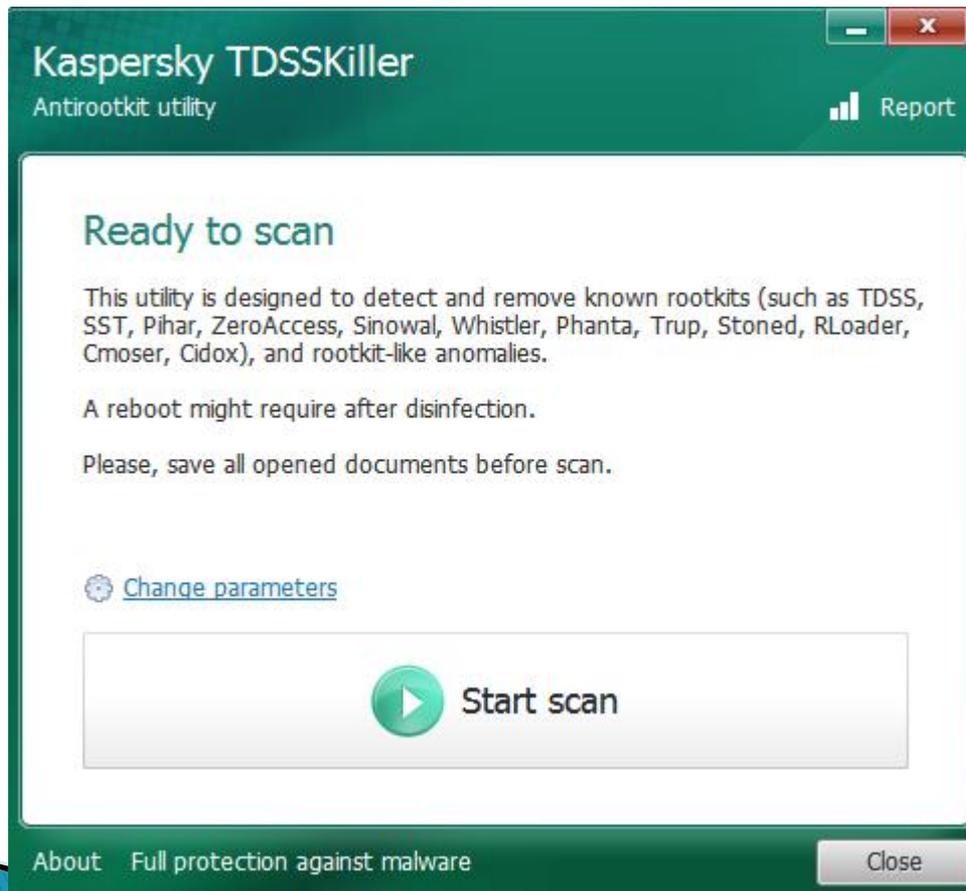
<https://www.malwarebytes.org/mwb-download/thankyou/> download the free version .



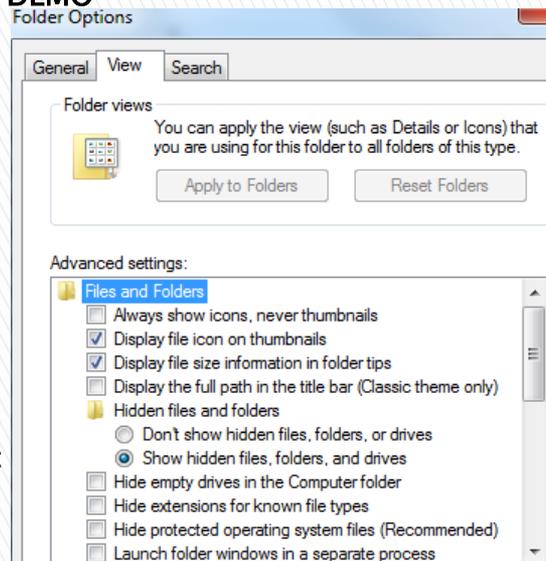
TDSKiller from Kaspersky Lab

Kaspersky TDSSKiller from Kaspersky Lab is a free utility that detects and removes rootkits and rootkit-like anomalies.

<http://usa.kaspersky.com/downloads/TDSSKiller>



Folder Option “ Show hidden files, folders and drives . DEMO



Manually detect and remove malware:

Check the locations for any strange *.exe or *.dll files :

- C:\ProgramData\..
- C:\Users****\AppDat...
- C:\Users****\Downloads

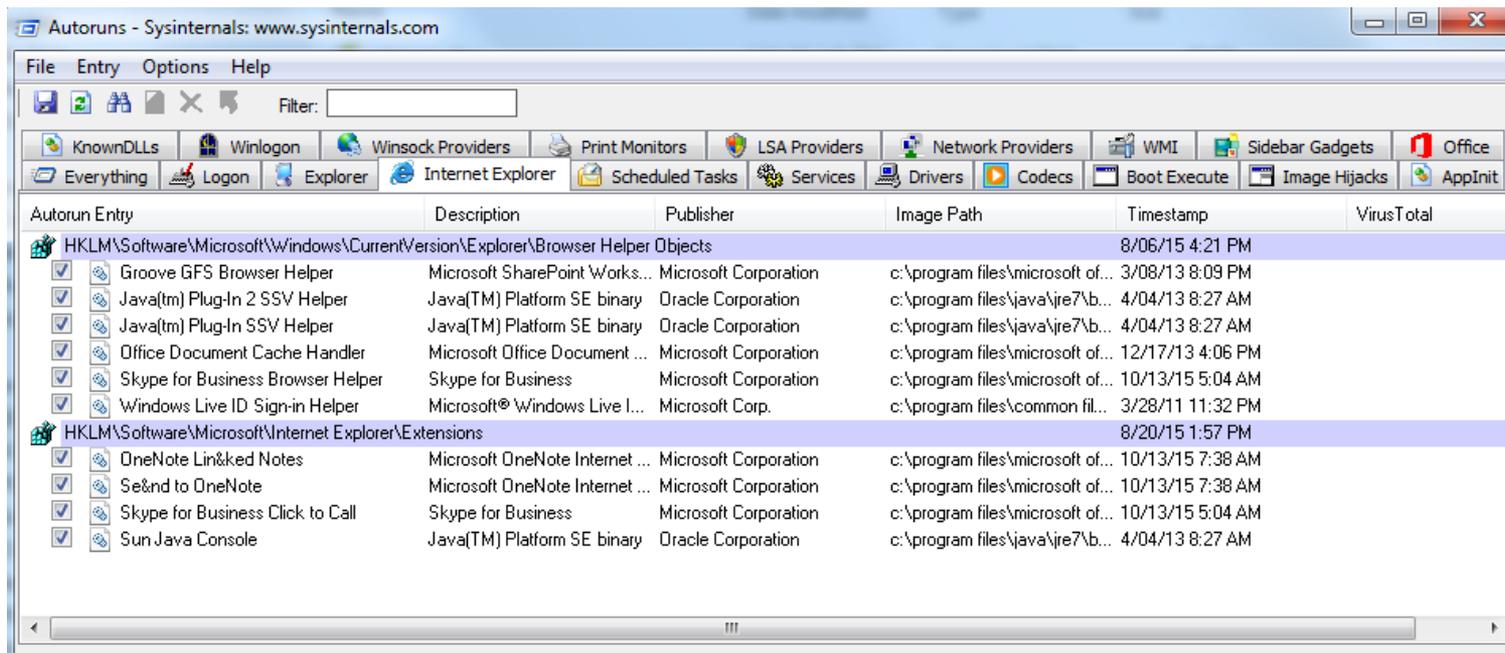
Delete temp and cached files.

- C:\Users****\AppData\Local\Temp\.....
- C:\Users****\AppData\LocalLow\Sun\Java\Deployment\cache
- C:\Users****\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
- C:\Users****\AppData\Local\Google\Chrome\User Data\Default\Cache

Malware Removal

What Is running on Computer ????

- ▶ Task Manager
- ▶ Sysinternals tools downloaded from <https://technet.microsoft.com/en-us/sysinternals/bb842062>
- ▶ Autoruns



Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [APOTEX\rlach]

File Options View Process Find DLL Users Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
WINWORD.EXE	1280	0.37	78,008 K	64,384 K	Microsoft Word	Microsoft Corporation
Snipping Tool.exe	6344	1.86	3,904 K	8,240 K	Snipping Tool	Microsoft Corporation
notepad.exe	4332		1,708 K	728 K	Notepad	Microsoft Corporation
notepad.exe	6860		1,396 K	720 K	Notepad	Microsoft Corporation
POWERPNT.EXE	4720	2.23	74,132 K	71,900 K	Microsoft PowerPoint	Microsoft Corporation
sync.exe	8616	0.37	239,536 K	116,752 K	Skype for Business	Microsoft Corporation
OUTLOOK.EXE	6284	1.12	141,500 K	92,796 K	Microsoft Outlook	Microsoft Corporation
explore.exe	5944	0.74	126,896 K	33,264 K	Internet Explorer	Microsoft Corporation
EXCEL.EXE	4788		15,212 K	11,012 K	Microsoft Excel	Microsoft Corporation
RDCMan.exe	4272	0.37	172,824 K	117,444 K	RDCMan	Microsoft Corporation
mstsc.exe	4548	0.37	32,084 K	34,600 K	Remote Desktop Connection	Microsoft Corporation
notepad.exe	3384		1,712 K	2,996 K	Notepad	Microsoft Corporation
mstsc.exe	7868		19,012 K	11,788 K	Remote Desktop Connection	Microsoft Corporation
notepad.exe	4220		1,392 K	3,672 K	Notepad	Microsoft Corporation
chrome.exe	9056		85,924 K	100,112 K	Google Chrome	Google Inc.
chrome.exe	10056		1,768 K	3,804 K	Google Chrome	Google Inc.
chrome.exe	8764		1,904 K	4,460 K	Google Chrome	Google Inc.

Name	Description	Company Name	Version
ssv.dll	Java(TM) Platform SE binary	Oracle Corporation	10.21.2.11
jp2ssv.dll	Java(TM) Platform SE binary	Oracle Corporation	10.21.2.11
ieexplore.exe	Internet Explorer	Microsoft Corporation	8.0.7600.16968
ntdll.dll	NT Layer DLL	Microsoft Corporation	6.1.7600.16385
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.1.7600.16850
KERNELBASE.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.1.7600.16850
ADVAPI32.dll	Advanced Windows 32 Base API	Microsoft Corporation	6.1.7600.16385
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	7.0.7600.16930
sechost.dll	Host for SCM/SDDL/LSA Lookup APIs	Microsoft Corporation	6.1.7600.16385
RPCRT4.dll	Remote Procedure Call Runtime	Microsoft Corporation	6.1.7600.16385
USER32.dll	Multi-User Windows USER API Client DLL	Microsoft Corporation	6.1.7600.16385
GDI32.dll	GDI Client DLL	Microsoft Corporation	6.1.7600.16385
LPK.dll	Language Pack	Microsoft Corporation	6.1.7600.16385
USP10.dll	Uniscribe Unicode script processor	Microsoft Corporation	1.626.7600.16385
SHLWAPI.dll	Shell Light-weight Utility Library	Microsoft Corporation	6.1.7600.16385
SHELL32.dll	Windows Shell Common Dll	Microsoft Corporation	6.1.7600.16385
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	6.1.7600.16385
iertutil.dll	Run time utility for Internet Explorer	Microsoft Corporation	8.0.7600.16968
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	8.0.7600.16968
WININET.dll	Internet Extensions for Win32	Microsoft Corporation	8.0.7600.16968
OLEAUT32.dll		Microsoft Corporation	6.1.7600.16722

CPU Usage: 10.43% Commit Charge: 66.17% Processes: 92 Physical Usage: 72.93%

How to manually remove malware

- ▶ Simply remove the *.exe or *.dll file .Usually does not work.
- ▶ Kill the process and try to remove it again, still does not work .
- ▶ Remove the process from start -up (Autoruns utility)
- ▶ Rename the malware files, change the extensions.
Often the malware files are re-created . If the file are re-created with the same name create folder with the same name . Use DOS script.
Del malware.exe
MD malware.exe.
- ▶ Restart the PC