Malware Security!

Kaspersky Internet Security 2014 **(Updated and Default Settings)**

User Interface:

Kaspersky Internet Security
Update
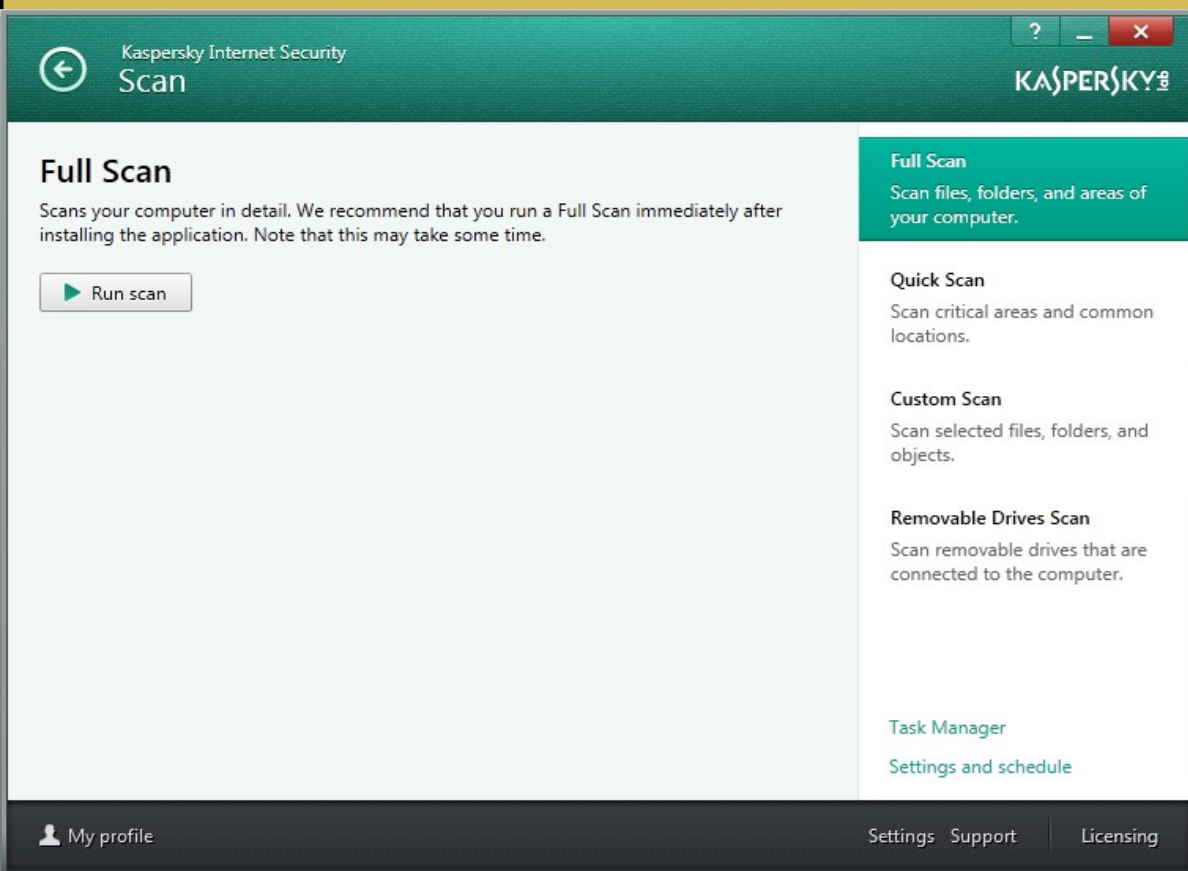
Databases and the application are up to date

By default, Kaspersky Internet Security regularly checks for updates, and automatically downloads and installs the updates in the background. You can also run an update manually at any time.

▶ Run update

Last update:	Run mode:	Signatures:
Today	automatically	5647799

🜨 Virus activity review

👤 My profile   Settings   Support   Licensing

Kaspersky Internet Security
Tools

Vulnerability Scan
Scan the operating system and third-party applications for vulnerabilities.
[Run] [Detected vulnerabilities]

Kaspersky Rescue Disk
Create a bootable CD or USB flash drive containing a set of tools for efficiently detecting and eliminating computer infections.
[Create]

Microsoft Windows Troubleshooting
Scan the system and fix problems caused by malware activity or system failures.
[Run]

Privacy Cleaner
Clear your computer history of recent commands and accessed files, cookies, caches, logs and other data, keeping your user activity private.
[Run]

Browser Configuration
Analyze Microsoft Internet Explorer settings for security strength.
[Run]

👤 My profile   Settings   Support   Licensing

Applications

57 managed applications

Trusted:	57
Restricted:	0
Untrusted:	0

Manage applications

🔒 **Trusted Applications mode is disabled**

Enable   Learn more

Current activity

Running
27 applications, 42 processes

CPU
0%

Memory
33% (1.01 / 3 GB)

Disk
↑0 B   ↓0 B

Network traffic
↑0 B   ↓0 B

Show all activity

👤 My profile   Settings Support   Licensing

- General
- Protection Center
- Performance
- Computer scan
- Additional

Protection

By default, the application launches at the startup of the operating system and protects your computer during the entire session.

Interactive protection

☑ Perform recommended actions automatically
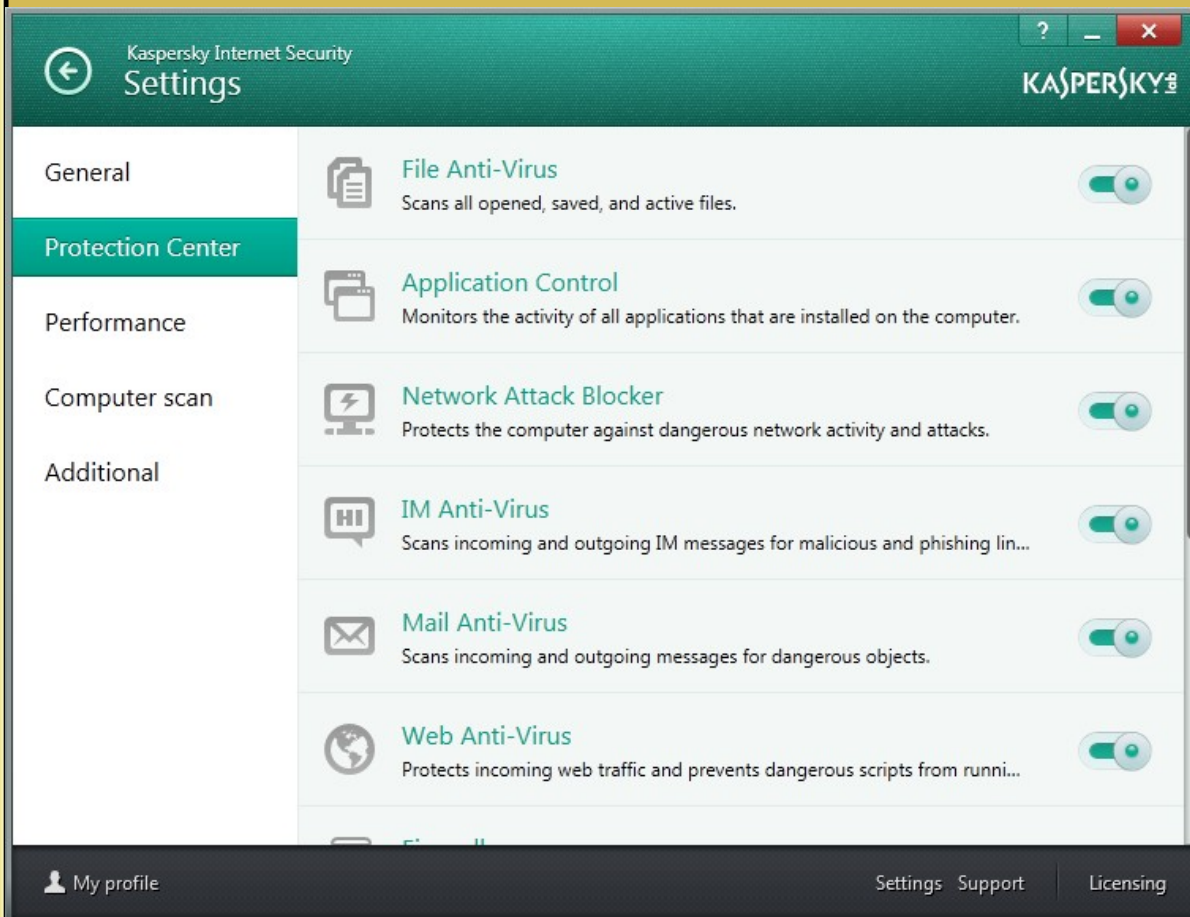 ☑ Do not delete probably infected objects

Autorun

☑ Launch Kaspersky Internet Security at computer startup (recommended)

Set up password protection

A password allows you to prevent settings modification, application termination or removal.

Restore settings   Default Settings ⌄

👤 My profile   Settings Support   Licensing

General

Protection Center

Performance

Computer scan

Additional

File Anti-Virus
Scans all opened, saved, and active files.

Application Control
Monitors the activity of all applications that are installed on the computer.

Network Attack Blocker
Protects the computer against dangerous network activity and attacks.

IM Anti-Virus
Scans incoming and outgoing IM messages for malicious and phishing lin...

Mail Anti-Virus
Scans incoming and outgoing messages for dangerous objects.

Web Anti-Virus
Protects incoming web traffic and prevents dangerous scripts from runni...

My profile

Settings   Support   Licensing

Kaspersky Internet Security

14.0.0.4651(b)

Close

System Memory:
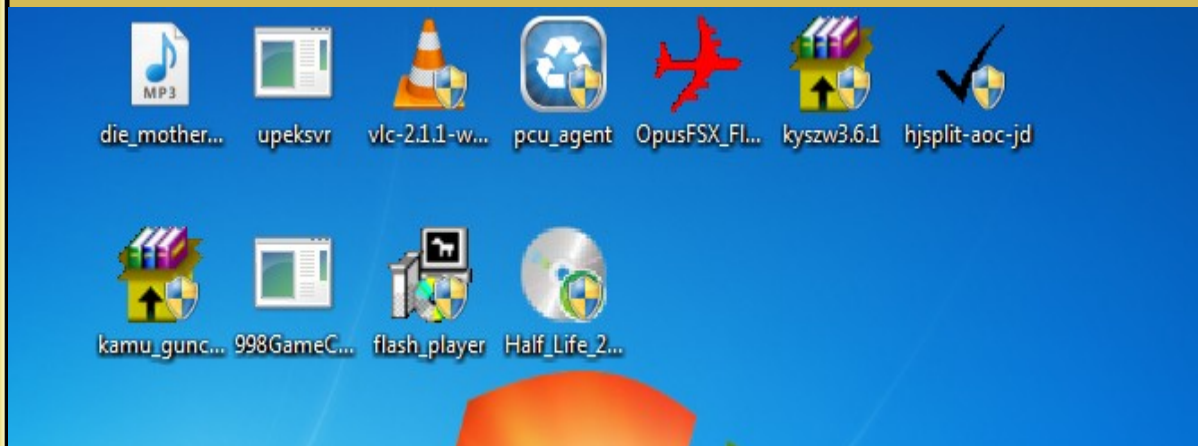
- 3 Running Process

- 78 Megabytes of Ram

- Not to slow on system

avp.exe *32	SYSTEM	00	73,272 K	Kaspersky Anti-Virus
avpui.exe *32	Malwar...	00	2,824 K	Kaspersky Anti-Virus
klwtblfs.exe *32	Malwar...	00	1,372 K	WebToolBar component

System Memory:

- 3 Running Process

- 78 Megabytes of Ram

- Not to slow on system

19/30 Links Blocked

Missed Links:

```
1.  myscaffolding.co.uk/components/com_rsform/controller
    /Demonstrativo-3010_2013.zip---------------------------------------3/51 Virus Total Blocked
2.  i1.stylezip.info/addons/alnaddy_india.exe------------------------------11/51 Virus Total Blocked
3.  draivanaeequipe.com.br/sitev2/antigo/Comprovante_21-11-2013.zip-------------6/51 Virus Total Blocked
4.  downloadspot7.sunbestsky.info/sctmp.exe-----------------------------------10/51 Virus Total Blocked
5.  198.98.113.2/~gbebnvxp/Adobex32x.exe--------------------------------------6/51 Virus Total Blocked
6.  playartepictures.com.br/filmes/images/stories/filmes/frank_hot.jpg----------7/51 Virus Total Blocked
7.  draivanaeequipe.com.br/sitev2/antigo/Comprovante_20-11-2013.zip------------11/51 Virus Total Blocked
8.  103.25.202.156/Js/calc.exe-----------------------------------------------6/47 Virus Total Blocked
9.  200.98.171.98/mtro8/yr1.html---------------------------------------------13/51 Virus Total Blocked
10. 49mp3.com/getfile.php?n=die+mother+fucker+die&u=siri.urz-------------------3/51 Virus Total  Missed
11. 5.248.76.197/upeksvr.exe-------------------------------------------------10/51 Virus Total  Missed
12. 80.241.223.183/~ivan/download.exe-----------------------------------------9/51 Virus Total Blocked
13. applicationscreditforally.asia/v1688?&&&&&&&&&&&&&&&&&&&&&&&&&&
    &&&&&&&&am;&installer;_file_name=snowpiercer(2013%-----------------------10/50 Virus Total Blocked
14. 200.98.171.98/mtro8/yr1.html---------------------------------------------13/51 Virus Total Blocked
15. adlock.in/download/44986/igi-1-free-download-project-igi-im.exe------------7/51 Virus Total Blocked
16. http://www.vlc.de/download/vlc/vlc-2.1.1-win32.exe------------------------3/51 Virus Total  Missed
17. http://www.pangpangclean.com/app/pcu/download/pcu_agent.exe---------------4/51 Virus Total  Missed
18. http://www.opussoftware.co.uk/opusfsi/OpusFSX_Flight1_Purchase.exe--------3/51 Virus Total  Missed
19. http://www.mo111mo.com/up/uploads/files/domain-db7ecb04c1.exe-------------10/51 Virus Total Blocked
20. http://www.ky-soft.com.img.800cdn.com/file/kyszw3.6.1.exe-----------------3/51 Virus Total  Missed
21. http://www.joydownload.com/d/60/hjsplit-aoc-jd.exe-----------------------5/51 Virus Total  Missed
22. http://www.ilon.com.tr/download/kamu_guncelleme.exe-----------------------4/51 Virus Total  Missed
23. http://www.gams998.net/download/998GameCenter_full.exe--------------------3/51 Virus Total  Missed
24. http://www.free-downloadss.com/download/r/flash_player.exe----------------4/51 Virus Total  Missed
25. moonmaderats.pw/nuc/look.php---------------------------------------------9/51 Virus Total Blocked
26. silurian.cn/modules/mod_cmsfix/fix.php-----------------------------------13/51 Virus Total Blocked
27. myhappytree.com/wp-content/plugins/wp-pagenavi/blog.php--------------------6/51 Virus Total Blocked
28. www.micnc.co.kr/pds/ReMoteCNC.exe-----------------------------------------7/47 Virus Total Blocked
29. www.moraldownload.com/download.php?version=1.1.6.20&prefix=H
    alf Life 2 Free Download Full Version For
    Pc&campid=3225&instid[appname---------------------------------------------18/47 Virus Total  Missed
30. www.twonext.com/download/res/DProtect.exe---------------------------------8/51 Virus Total Blocked
```
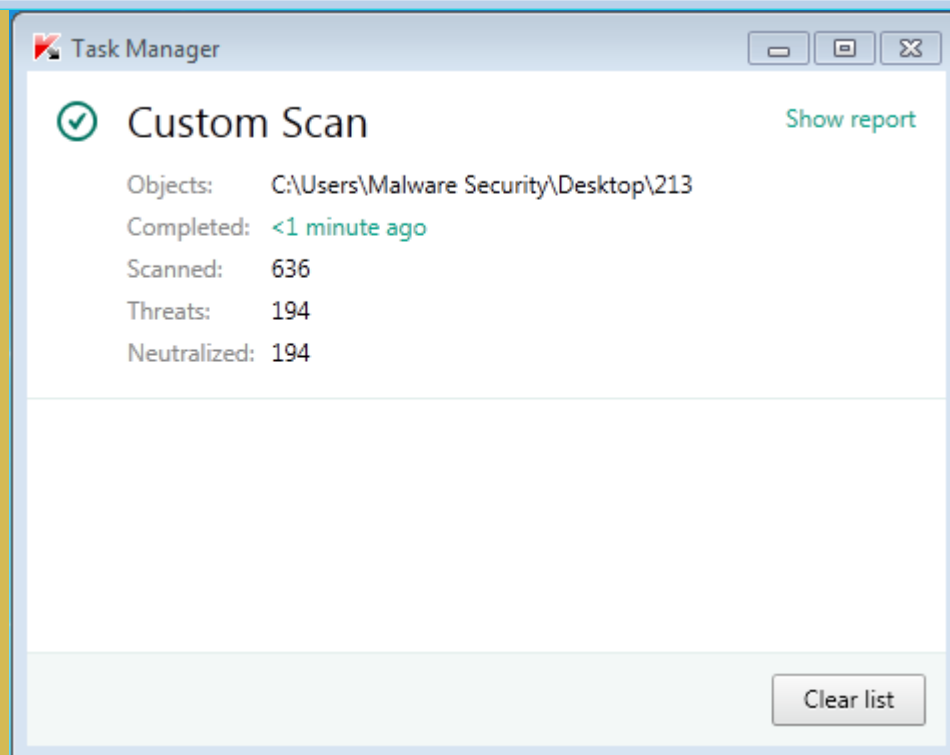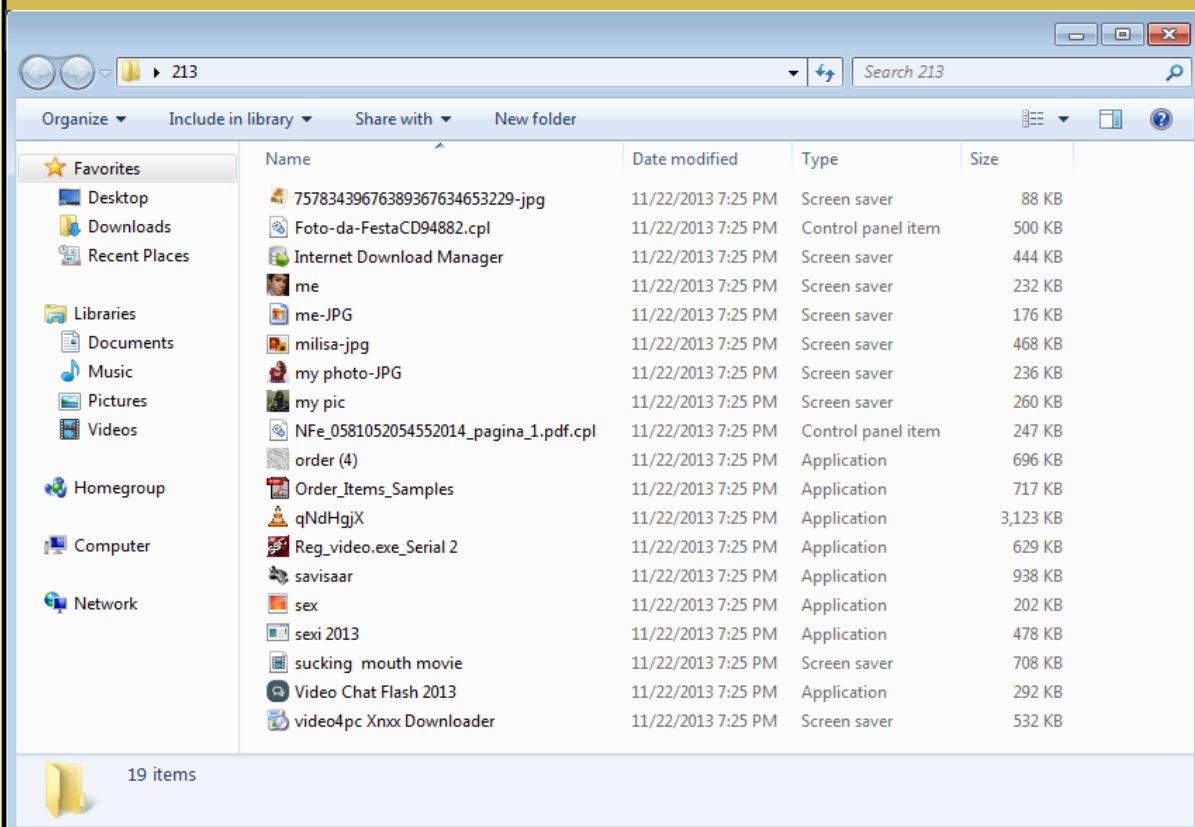

- 11 web links were missed, the 11 web links are files that you see above!

Malware Pack Containing 213 Files (0 Day Old Files):

194/213 Files detected = 91.08%

Caught Later By Behavioral Blocking, Firewall, Etc.:

- I executed 6 missed files from the malware pack and it detected 3 of 6!

Hitmanpro and Malwarebytes results after behavioral blocking test:

HitmanPro 3.7.8 - Build 208 (64-bit)

Scan results

1m 19s

Malicious software was detected. Close all applications and click Next to remove the malicious software. During removal, certain programs may terminate unexpectedly.

Foto-da-FestaCD94882.cpl	⊗ Trojan	Delete ▼
B Trojan.GenericKD.1412171		
data.exe `2936`	⊗ Trojan	Delete ▼
C:\Users\Malware Security\AppData\Local\Temp\		
LocaldACLKGgZvT.exe	⊗ Malware	Delete ▼
C:\Users\Malware Security\AppData\		
Localaj_RayYQpF.exe	⊗ Malware	Delete ▼
C:\Users\Malware Security\AppData\		
a506c4a53dd1d25bdb64df6fdfdcc4f2.exe `Run`	⊗ Malware	Delete ▼
C:\Users\Malware Security\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\		
9e88cb9e74409940b2ec343eebb69946.exe `Run`	⊗ Trojan	Delete ▼
C:\Users\Malware Security\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\		
cack.exe `Run`	⊗ Malware	Delete ▼
C:\Users\Malware Security\AppData\Roaming\		

Identified Threats: 7   (Traces: 15)   7 Items

ⓘ Trial license is activated. 30 days left. Buy Now

[Buy Now]   Save Log   [Next]   [Close]

Malwarebytes Anti-Malware

Malwarebytes
ANTI-MALWARE

| Scanner | Protection | Update | Quarantine | Logs | Ignore List | Settings | More Tools | About |

Scanner
Below is a list of malicious software found on your system. Close all unnecessary applications to ensure successful threat removal.

Vendor	Category	Item	Other
☑ Trojan.Banker....	File	C:\Users\Malware Security\Desktop\213\Fot...	
☑ Trojan.Banker....	Memory Module	C:\Users\Malware Security\Desktop\213\Fot...	
☑ Stolen.data	File	C:\Users\Malware Security\AppData\Local\T...	

[**Remove Selected**]   [Ignore]   [Save Log]   [Main Menu]

[Buy Now]   [Activate]   [Exit]

5 Star Rating:

- **1 Star: User-friendly:** 1/1
- **1 Star: Low Ram Usage, 60mb or less:** 0/1
- **1 Star: 24/30 Web Links, 80%:** 0/1
- **1 Star: Detection 85%+:** 1/1
- **1 Star: Behavioral Blocking, 50%+:** 1/1

3/5

Advantages and Disadvantages:

Advantages:

- Nice Interface
- Good detection rate for 0 day files
- Behavioral blocking seemed to work pretty good
- Good custom scan speeds

Disadvantages:

- Pretty high ram usage
- Web blocking was not the best!
- Updating takes awhile
- Every time I restart computer and I click Kaspersky icon to open it's interface, it says, "Loading the application." Even though the computer finished booting up, Kaspersky is still booting up. (I was just informed by one of the users of Kaspersky today the 23rd that you can "enable concede system resources option in KAV settings," to make it much faster. I am still going to leave it as a disadvantage because an average user would not know about that.)

Summary:

- According to my testings, Kaspersky did manage to do the hard work. I wish they did good on web blocking though to make it easier for me to recommend it, but I will still recommend it because its detection rate was high and the behavioral blocking seemed to work, so if you have a web link that goes through, then at least Kaspersky still has a chance.

Thanks for reading and my signatures are on next page!

My Signature!

I am a Linux User!

Recommended paid Windows Antivirus!

Recommended Free! Windows Antivirus!