Protections

Anti Virus Software

Windows Defender

Microsoft's own antivirus software suite

Pros: Easy setup; low performance impact

Cons: Very poor malware detection; no extra security features

Microsoft Security Essentials

What is Microsoft Security Essentials?

There are a host of nasty intruders on the Internet including viruses, trojans, worms and spyware. Microsoft Security Essentials offers award-winning protection against these intruders without getting in your way. Comprehensive malware protection, Simple, free* download , with Automatic updates

Microsoft Security Essentials is built for individuals and small businesses, but it's based on the same technology that Microsoft uses to protect giant businesses (security products like Microsoft Forefront, the Malicious Software Removal Tool, and Windows Defender). We have a whole team watching for new threats and coming up with ways to squash them.

Microsoft Security Essentials runs quietly in the background. You'll only be alerted when there are specific actions to take. When you're away or busy, Microsoft Security Essentials can take the default action on your behalf and you can open the program later to review and undo those actions if you wish.

Microsoft Security Essentials is efficient and compact. Scans and updates are scheduled to run when the PC is idle and the software works in a way that your PC is still snappy when you're using it. All this makes Microsoft Security Essentials friendly for all sorts of computers—your old PC, your new PC, your laptop, as well as your little netbook.

Kaspersky Lab anti viral

https://www.av-test.org/en/antivirus/home-windows/

Avast - Free, Pro

	Free	Pro
Intelligent antivirus & anti-malware Detects threats no one has even heard of yet.	**yes**	**yes**
Home Network Security Scan your home network for weak spots.	**yes**	**yes**
Browser Cleanup Get rid of annoying browser add-ons.	**yes**	**yes**
Pay & bank online. Safely. Prevent your logins and passwords from theft.		**yes**
Anti-hijack protection Log in to your real banking site, not a fake one.		**yes**
Silent Firewall Shield your computer from hackers.		**yes**
Anti-spam		

Firewalls ZoneAlarm has a Firewall &/or an Antiviral option

Free:

Advanced Firewall
Monitors programs for suspicious behaviour spotting and stopping new attacks that bypass traditional anti-virus protection.

Pro & Antiviral

- Advanced Firewall
- Antivirus & Anti-spyware Engine
- Advanced Real-Time Antivirus
- Enhanced Browser Protection
- Identity Protection

Pro Firewall:

Advanced Firewall
Two-way Firewall
Private Browsing
Identity Protection
Online Backup
Do Not Track
Facebook Privacy Scan
Privacy & Security Toolbar

Extreme has the following additions to the above:

- Enhanced Browser Protection
- Anti-Keylogging
- Anti-Spam
- Parental Controls
- PC Tune-up
- Find My Laptop
- Threat Emulation

Detail explanation of the terms above, for more info go to the web site.

Antivirus/Anti-Spyware Engine
Detects and remove viruses, spyware, Trojan horses, worms, bots and rootkits.
Advanced Real-Time Antivirus
Enhances protection by checking against an always up-to-date cloud database of antivirus signatures.
Advanced Firewall
Monitors programs for suspicious behaviour spotting and stopping new attacks that bypass traditional anti-virus protection.
Two-way Firewall
Makes your PC invisible to hackers and stops spyware from sending your data out to the Internet.
Anti-Spam
Filters out annoying and potentially dangerous emails.
PC Tune-up
Cleans, organizes and streamlines your computer – improving its performance.
Online Backup
Backs up files and restores your data in the event of hardware malfunction.
Identity Protection
Helps to prevent identity theft by guarding your personal data.
Parental Controls
Filters and blocks inappropriate websites and chat rooms and limits time spent online.
Threat Emulation
Opens email attachments and web downloads in a virtual cloud environment to see if they are safe.
Enhanced Browser Protection
Protects your computer from web threats before they reach your browser.
Find My Laptop
Locates your lost or stolen laptop on a map, locks it down and allows remote recovery of important files.
Anti-Keylogger
Prevents identity thieves from stealing your passwords and keystrokes.
Privacy & Security Toolbar
Provides Site Check, Do Not Track, Facebook Privacy Scan, private browsing and more.
Do Not Track
Stops data collecting companies from tracking you online.
Facebook Privacy Scan
Scans your recent Facebook activity and alerts you to privacy concerns. Control what others can see.
Private Browsing
Erases your tracks – allowing you to surf the Web in complete privacy.

Malware

How to easily clean an infected computer

Malware, short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses.

It's not always easy to tell if your computer was compromised or not, because these days cybercriminals are going to great lengths to hide their code and conceal what their programs are doing on an infected computer.
It's very difficult to provide a list of characteristic symptoms of a infected computer because the same symptoms can also be caused by hardware incompatibilities or system instability, however here are just a few examples that may suggest that your PC has been compromised :

- You may receive the error "Internet Explorer could not display the page" when attempting to access certain websites
- Your web browser (e.g., Microsoft Internet Explorer, Mozilla Firefox, Google Chrome) freezes, hangs or is unresponsive
- Your web browser's default homepage is changed
- Access to security related websites is blocked
- You get redirected to web pages other than the one you intended to go to
- You receive numerous web-browser popup messages
- Strange or unexpected toolbars appear at the top of your web browser
- Your computer runs slower than usual
- Your computer freezes, hangs or is unresponsive
- There are new icons on your desktop that you do not recognize
- Your computer restarts by itself (but not a restart caused by Windows Updates)
- You see unusual error messages (e.g., messages saying there are missing or corrupt files folders)
- You are unable to access the Control Panel, Task Manager, Registry Editor or Command Prompt.

MalwareBytes

Today's cyber criminals build software designed to slip past antivirus programs undetected. Malwarebytes Anti-Malware Premium crushes these threats with innovative technologies designed to defend you while keeping your online experience fast and hassle free.

Remove PUP.Software.Updater (Removal Guide)

“PUP,” or potentially unwanted program

PUP.Software.Updater is a specific detection used by Malwarebytes Anti-Malware and other antivirus products to indicate and detect a Potentially Unwanted Program.
A potentially unwanted application is a program that contains adware, installs toolbars or has other unclear objectives.
[Image: PUP.Software.Updater]

Malwarebytes Anti-Malware Premium

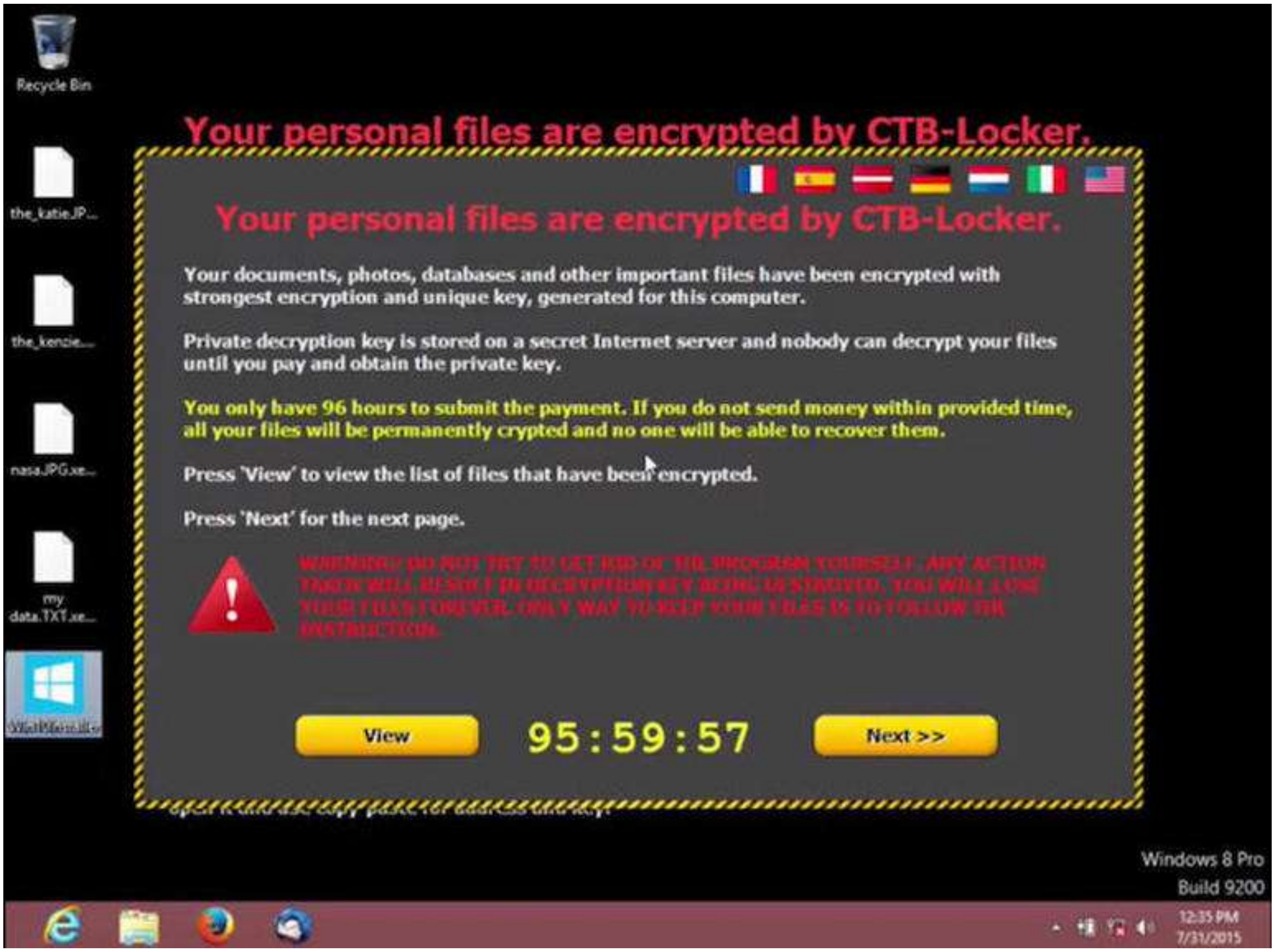
Malwarebytes' flagship application Anti-Malware is a shareware malware-removal tool. The principle difference between the free and premium version of the application is real-time monitoring. If you don't need active scanning against threats, the free version uses the same database and does an admirable job ferreting out infections.

Further info is towards the end of this document.

New Malware Ransoms Data Disguised as Microsoft E-mail

Your data is very valuable and the criminals know this. They want to find ways to “kidnap” your data and hold it for ransom. I’ve warned you about this in Beware of Cryptolocker Malware and Cryptolocker Strikes, The Price Has Gone Up.

The latest threat has the bad guys impersonating Microsoft in an email about Windows 10. Attached to that e-mail is the malware and launching it will give you a screen similar to the one shown below.



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 95:59:57 Next >>

Your files will be encrypted and the only way to get them back is to pay a ransom in Bitcoin. So if you get an e-mail claiming to be from Microsoft, take great caution before you click on anything attached! For more details on this scam, read New Windows 10 scam will encrypt your files for ransom on ZDNet.

For those wanting to upgrade to Windows 10, I've covered the process in the Claim Your Free Upgrade to Windows 10 post. Before you upgrade, read Is Your Computer Ready for Windows 10? As I say in that post, I'm going to wait a month or two before installing just to make sure the bugs are worked out.

If any of you have already updated, make sure to read Activate God Mode in Windows 7, 8 and 10. Of course those of you still on Windows 7 and 8 can read it to get a powerful feature enabled.

ZoneAlarm Pro Firewall more detailed explanation

- **Two-way Firewall**
  Stops Internet attacks at the front door and even catches thieves on their way out. Our two-way firewall proactively protects against inbound and outbound attacks while making you invisible to hackers.
  - Threat Traffic is monitored and blocked – inbound and outbound.
  - Full Stealth Mode makes you invisible to hackers.
  - Kill Controls instantly disable malicious programs.
- **Advanced Firewall**
  No product is 100% effective against viruses or spyware. ZoneAlarm’s advanced firewall monitors behaviours within your computer to spot and stop even the most sophisticated new attacks that bypass traditional antivirus and security suites.
  - OSFirewall™ Monitors programs for suspicious behaviour – spotting and stopping new attacks that bypass traditional anti-virus protection.
  - Advanced-access Protection targets and defeats new, advanced attacks that other firewalls miss, such as raw data access, timing, and SCM and COM attacks.
  - Zero-hour Protection prevents silent outbreaks from gaining system access – before other security programs can even detect the threat.
  - Application Control uniquely shields your operating system during start-up, before most security products have even loaded.
  - Early Boot Protection uniquely shields your operating system during start-up, before most security products have even loaded.
- **Additional Layers**
  Multiple layers of advanced protection provide unsurpassed security.
  - Anti-Spam filters out annoying and potentially dangerous emails.
  - Wireless PC Protection shields you from hackers, identity thieves and other online threats when you connect to an unsecured network.
  - Automatic Wireless Network Security detects wireless networks and automatically applies the most secure firewall protection setting.
  - DefenseNet™ provides real-time security updates, responds quickly to breaking threats and leverages threat data from millions of users – protecting your PC from the latest attacks.

Further Malware info :-

Remove PUP.Software.Updater (Removal Guide)

“PUP,” or potentially unwanted program

PUP.Software.Updater is a specific detection used by Malwarebytes Anti-Malware and other antivirus products to indicate and detect a Potentially Unwanted Program.
A potentially unwanted application is a program that contains adware, installs toolbars or has other unclear objectives.
[Image: PUP.Software.Updater]

PUP.Software.Updater it’s technically not a virus, but it does exhibit plenty of malicious traits, such as rootkit capabilities to hook deep into the operating system, browser hijacking, and in general just interfering with the user experience. The industry generally refers to it as a **“PUP,” or potentially unwanted program**.
The PUP.Software.Updater infection is used to boost advertising revenue, as in the use of blackhat SEO, to inflate a site’s page ranking in search results.

PUP.Software.Updater got on your computer after you have installed a freeware software (video recording/streaming, download-managers or PDF creators) that had bundled into their installation this browser hijacker. This Potentially Unwanted Programs is also bundled within the custom installer on many download sites (examples: CNET, Brothersoft or Softonic), so if you have downloaded a software from these websites, chances are that PUP.Software.Updater was installed during the software setup process.

You should always pay attention when installing software because often, a software installer includes optional installs, such as this PUP.Software.Updater browser hijacker. Be very careful what you agree to install.
Always opt for the custom installation and deselect anything that is not familiar, especially optional software that you never wanted to download and install in the first place. It goes without saying that you should not install software that you don’t trust.

WHEN all else fails go to for a complete answer

http://malwaretips.com/blogs/malware-removal-guide-for-windows/