

Malware

Malware

➤ **Malware, short for malicious software, is any software used 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 (including worms, trojan horses), ransomware, spyware, adware, scareware, and other malicious programs.**

The majority of active malware threats are usually worms or trojans rather than viruses.

Computer Virus

- **A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. The defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.**

Worms and Trojans

- **Worms -- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program**

Worms and Trojans

- **Trojans -- A Trojan horse, or Trojan, in computing is a generally non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.**

Scareware

- **Scareware -- Scareware, included into the class of malware known as Rogueware, comprises several classes of ransomware or scam software with malicious payloads, usually of limited or no benefit, that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.**

Ransomware

- **Ransomware -- Ransomware is a class of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion), while some may simply lock the system and display messages intended to coax the user into paying.**

Spyware

- **Spyware -- Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. "Spyware" is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Spyware is mostly used for the purposes such as; tracking and storing internet users' movements on the web; serving up pop-up ads to internet users.**

Spyware

- **While the term *spyware* suggests software that monitors a user's computing, the functions of spyware can extend beyond simple monitoring. Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, unauthorized changes in browser settings, or changes to software settings.**

Adware

- **Adware -- Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.**

Antivirus Programs

- **Program used to protect and/or remove viruses from your computer**
- **Never install more than one antivirus program on your computer**
- **Free programs**
 - **AntiVir Personal - www.filehippo.com**
 - **Avast! Free Antivirus - www.filehippo.com**
 - **AVG Free Edition - www.filehippo.com**
 - **32 & 64 bit version**
 - **Bitdefender Antivirus Free - www.download.cnet.com**
 - **Microsoft Security Essentials - Windows XP, Vista, and 7**
 - **Panda Cloud Antivirus - www.cloudantivirus.com**
 - **Windows Defender - included in Windows 8.1**

Antivirus Programs

- **You need to**
 - **Check the program settings**
 - **Make sure the data files are being updated every time you start your computer**
 - **Make sure you have the latest version of the program**
 - **Periodically do a thorough scan of the hard drive**
 - **Recognize the name and logo of the program you are using**
 - **Know what to expect if the program detects a virus or other form of malicious software**

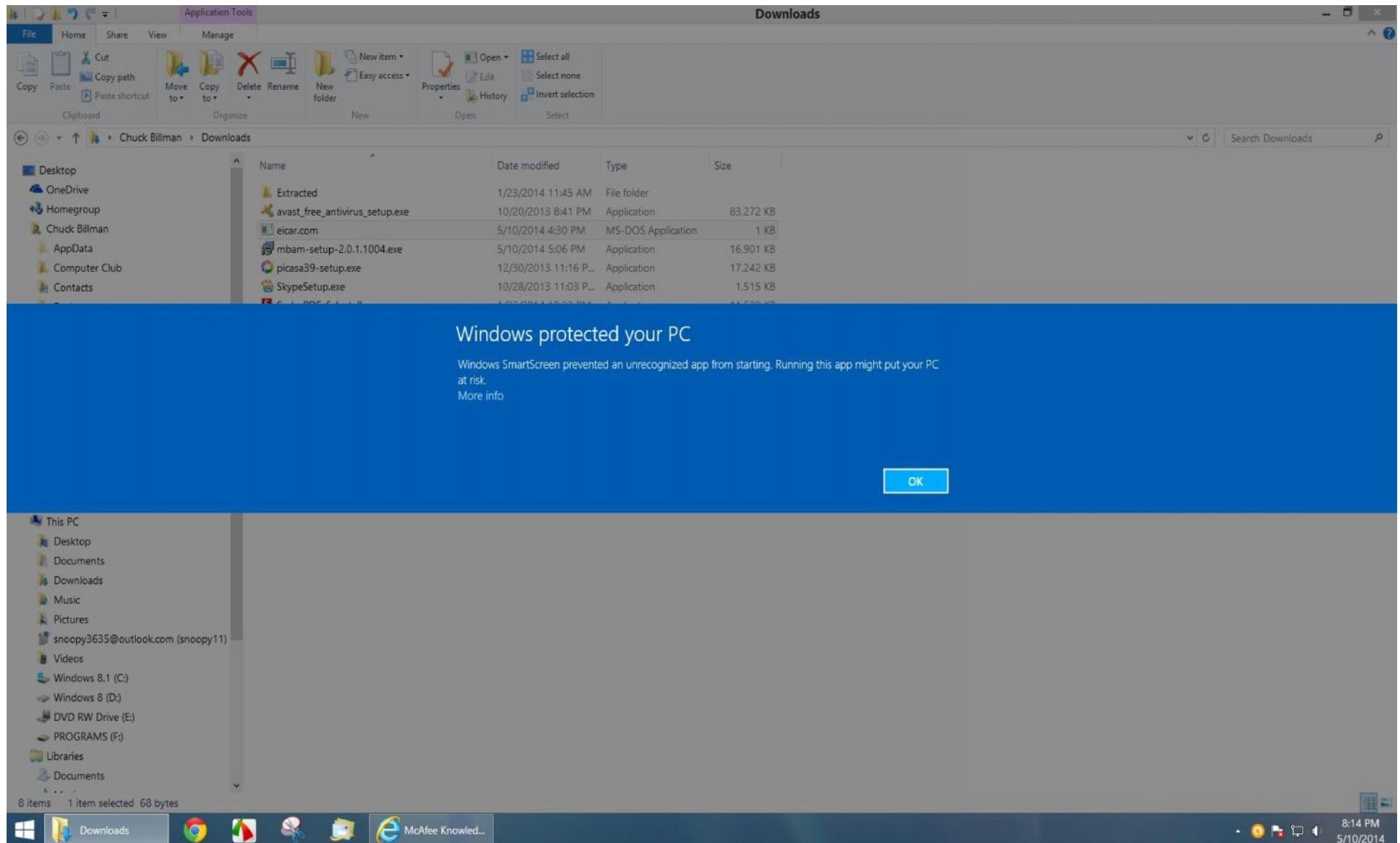
Antivirus Programs

➤ Threat detected by Avast



Windows 8.1 SmartScreen

➤ Threat blocked by the Windows 8.1 SmartScreen



The screenshot shows a Windows 8.1 File Explorer window titled "Downloads" with a blue SmartScreen warning overlay. The warning text reads: "Windows protected your PC. Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk. More info". An "OK" button is visible at the bottom right of the warning. The background shows a list of files in the Downloads folder, including "Extracted", "avast_free_antivirus_setup.exe", "eicar.com", "mbam-setup-2.0.1.1004.exe", "picasa39-setup.exe", and "SkypeSetup.exe".

Name	Date modified	Type	Size
Extracted	1/23/2014 11:45 AM	File folder	
avast_free_antivirus_setup.exe	10/20/2013 8:41 PM	Application	83,272 KB
eicar.com	5/10/2014 4:30 PM	MS-DOS Application	1 KB
mbam-setup-2.0.1.1004.exe	5/10/2014 5:06 PM	Application	16,901 KB
picasa39-setup.exe	12/30/2013 11:16 P...	Application	17,242 KB
SkypeSetup.exe	10/28/2013 11:03 P...	Application	1,515 KB

Malware Detection and Removal Programs

➤ Free programs

- Malwarebytes Anti-Malware - www.filehippo.com
 - Microsoft Security Essentials - Windows XP, Vista, and 7
 - SUPERAntiSpyware - www.filehippo.com
 - Windows Defender - included in Windows 8.1
- ## ➤ Used to detect and remove non-virus malware
- Can have multiple programs installed
 - Check the program settings
 - Must be updated before running
 - Scan the hard drive about every two weeks
 - Remove all that is detected

Registry Cleaners

- **Database that contains information and instructions for practically everything the computer does**
- **Over time invalid entries build up**
 - **The operating system doesn't remove entries that are no longer valid**
 - **Updates to the operating system and programs can generate invalid entries**
 - **Programs that are uninstalled fail to remove entries**
- **A large number of invalid entries in the registry can slow down your computer**

Registry Cleaners

- **Registry cleaners remove or correct invalid entries**
- **The danger -- one incorrect change to the registry could kill your computer**
- **Recommendations**
 - **Have a current backup of your personal data**
 - **Have a Windows boot disc**
 - **Have a Windows recovery or restore disc**
 - **Make a backup copy of the registry**
 - **Close all programs**
 - **Consider exiting programs or applications that are running in the background**

Registry Cleaners

- **Use a safe, reliable registry cleaner**
 - **Free - CCleaner - www.filehippo.com**
 - **Paid - Registry Commander - www.softarama.com**
\$39.95 for 1 or \$54.95 for 2

For those who like to live on the edge -

Registry Recycler - www.registryrecycler.com

Power Tools Lite 2013 - www.macecraft.com

Registry Recycler

- Free - www.registryrecycler.com
- Developer Tribe (Pvt) Ltd., Islamabad, Pakistan



Registry Recycler

➤ Results



The screenshot displays the Registry Recycler application window. The title bar reads "Registry Recycler" with the subtitle "Recycle & Optimize The Registry". The interface includes a sidebar with navigation buttons: Scanner, Defrag, Backup, Startup, and Summary (highlighted in blue). The main area shows a "Summary" section with the date and time of the last scan: "11 May 2014, 01:12PM". Below this is a table with four columns: "Registry Item", "Errors", "Cleaned", and "Ignored". The table lists various registry items and their corresponding error counts, cleaned counts, and ignored counts. At the bottom of the table, it states "Errors Found: 1245" and "Errors Cleaned: 1245".

Registry Recycler
Recycle & Optimize The Registry

REGISTER SETTINGS ? HELP UPDATE

Summary Date & Time of last scan: 11 May 2014, 01:12PM

Registry Item	Errors	Cleaned	Ignored
COM/ActiveX Entries	20	20	0
Uninstalled Entries	0	0	0
Font Entries	0	0	0
Shared DLLs	26	26	0
Application Paths	0	0	0
Help File Information	0	0	0
Windows Startup Items	1	1	0
File/Path References	123	123	0
Program Shortcuts	52	52	0
Empty Registry Keys	1023	1023	0
File Associations	0	0	0
Windows Services	0	0	0

Errors Found: **1245** Errors Cleaned: **1245**