Malware

Malware

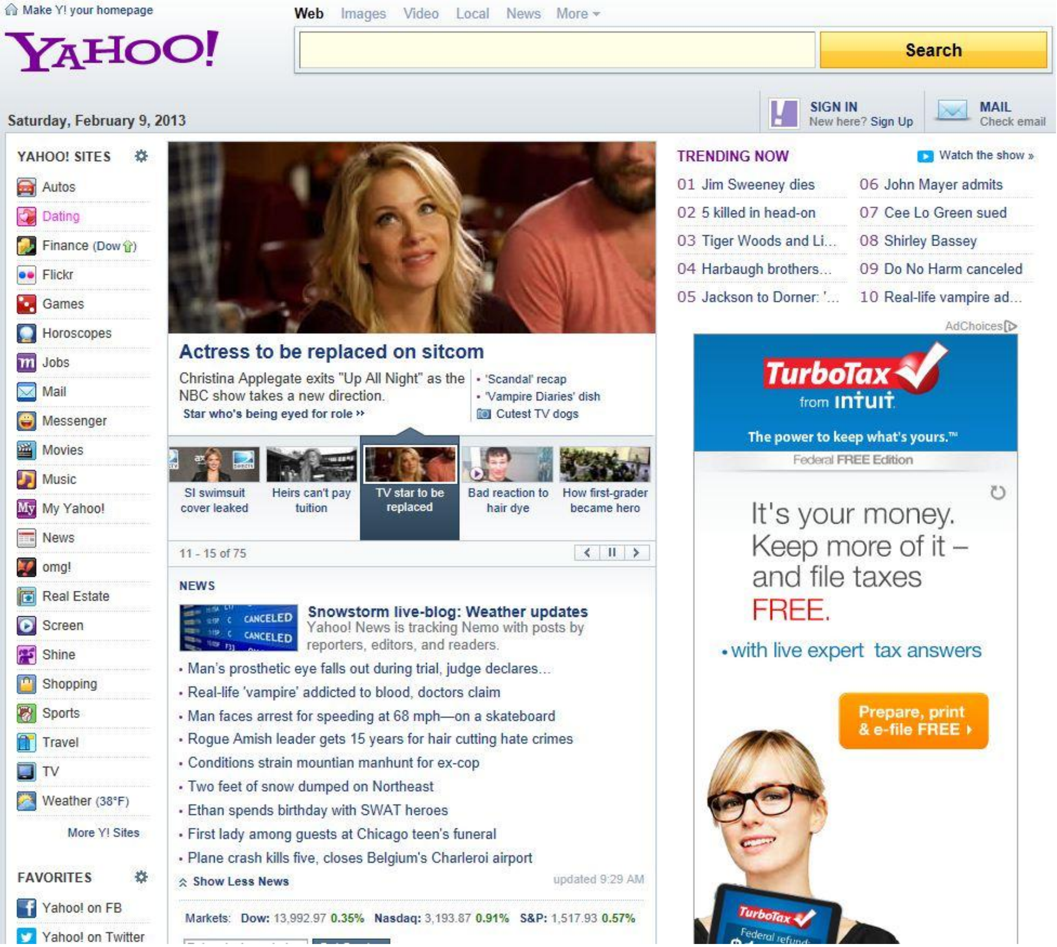
- Malware - short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems
- Why should you be concerned
  - The software can be installed on your computer in a number of different ways
  - Installed without your permission or knowledge
  - Runs unnoticed in the background
  - Allows the installer to control your computer
  - Can allow your computer to be added to a botnet

MALWARE

- **Botnet**
  - **The word botnet stems from the two words robot and network.**
  - **A botnet is a collection of malware infected internet-connected computers that are directed to communicating with other computers in order to perform tasks**
    - **Send SPAM**
    - **Gather user names and passwords**
    - **Capture keystrokes**
    - **Initiate Denial-of-Service (DOS) attacks**
    - **Identity theft**
    - **Click-fraud**

CLICK-FRAUD

- **Click-fraud - A person or botnet computer clicking on a web site advertisement for the sole purpose of generating revenue**



Make Y! your homepage

Web Images Video Local News More

YAHOO!

Search

Saturday, February 9, 2013

SIGN IN
New here? Sign Up

MAIL
Check email

YAHOO! SITES

- Autos
- Dating
- Finance (Dow)
- Flickr
- Games
- Horoscopes
- Jobs
- Mail
- Messenger
- Movies
- Music
- My Yahoo!
- News
- omg!
- Real Estate
- Screen
- Shine
- Shopping
- Sports
- Travel
- TV
- Weather (38°F)

More Y! Sites

FAVORITES

- Yahoo! on FB
- Yahoo! on Twitter

Actress to be replaced on sitcom

Christina Applegate exits "Up All Night" as the NBC show takes a new direction.

Star who's being eyed for role »

- 'Scandal' recap
- 'Vampire Diaries' dish
- Cutest TV dogs

SI swimsuit cover leaked | Heirs can't pay tuition | TV star to be replaced | Bad reaction to hair dye | How first-grader became hero

11 - 15 of 75

NEWS

Snowstorm live-blog: Weather updates
Yahoo! News is tracking Nemo with posts by reporters, editors, and readers.

- Man's prosthetic eye falls out during trial, judge declares...
- Real-life 'vampire' addicted to blood, doctors claim
- Man faces arrest for speeding at 68 mph—on a skateboard
- Rogue Amish leader gets 15 years for hair cutting hate crimes
- Conditions strain mountian manhunt for ex-cop
- Two feet of snow dumped on Northeast
- Ethan spends birthday with SWAT heroes
- First lady among guests at Chicago teen's funeral
- Plane crash kills five, closes Belgium's Charleroi airport

Show Less News

updated 9:29 AM

Markets: Dow: 13,992.97 0.35% Nasdaq: 3,193.87 0.91% S&P: 1,517.93 0.57%

TRENDING NOW

Watch the show »

01 Jim Sweeney dies	06 John Mayer admits
02 5 killed in head-on	07 Cee Lo Green sued
03 Tiger Woods and Li...	08 Shirley Bassey
04 Harbaugh brothers...	09 Do No Harm canceled
05 Jackson to Dorner: '...	10 Real-life vampire ad...

AdChoices

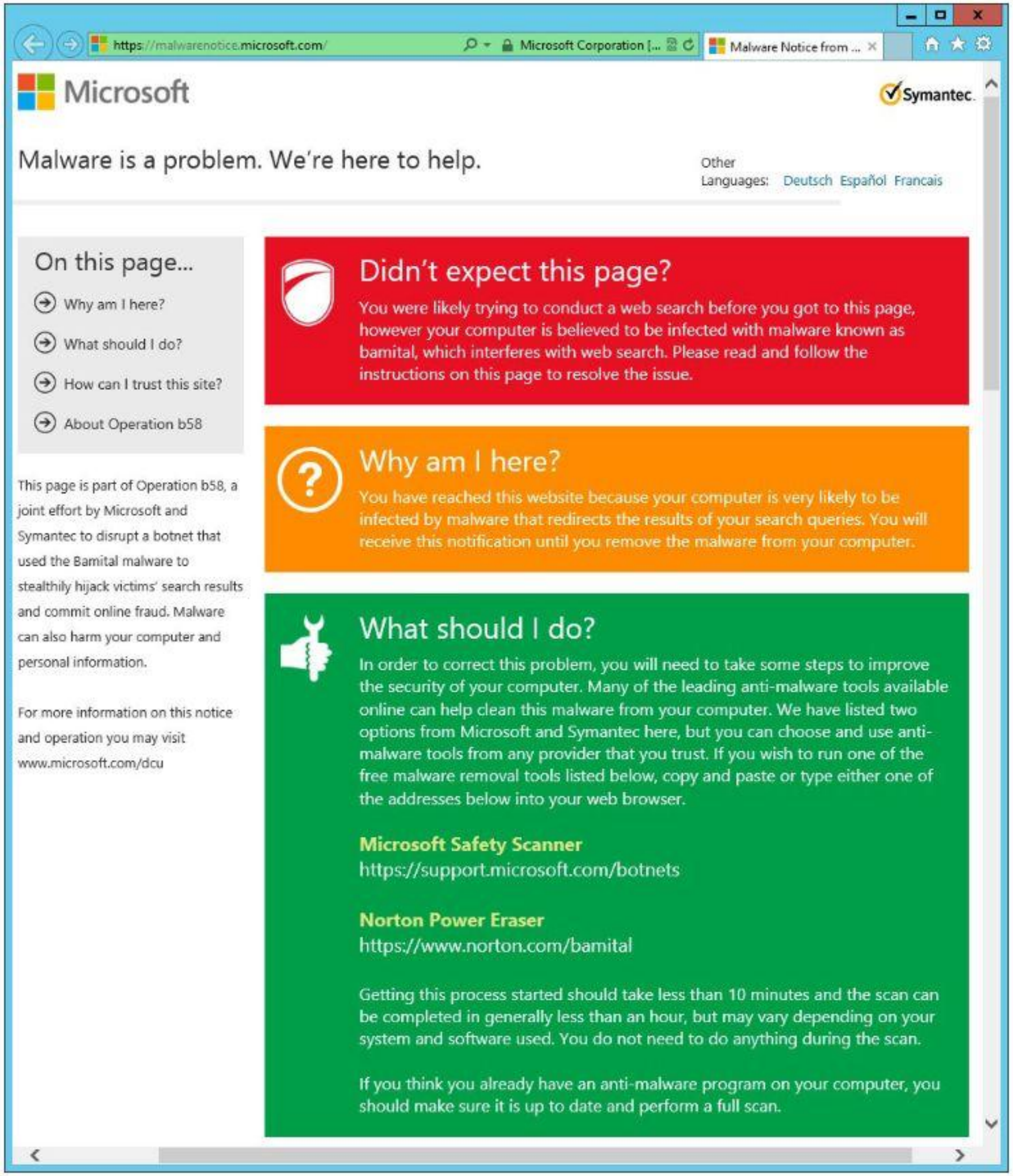
BAMITAL CLICK-FRAUD BOTNET

- When clicking on a search result from Bing, Yahoo, or Google the Bamital software redirected the infected computers to malicious websites
- That resulted in clicks on advertisements that were of no benefit to the advertiser but generated revenue for the botnet owners
- The botnet could also steal personal information and conduct DOS attacks
- At the end of January Microsoft and Symantec partnered to shut down this botnet

BAMITAL CLICK-FRAUD BOTNET

- **Microsoft and Symantec are now in the process of attempting to clean up infected computers**
- **When an infected computer initiates a search query it's directed to a Web page from Microsoft or Symantec that explains how to remove the malicious software**
- **This Web page is legitimate but remember, Microsoft will not send you email or call you on the phone**

Bamital Removal Web Page


https://malwarenotice.microsoft.com/
Microsoft Corporation [...
Malware Notice from ...
Microsoft
Symantec.

Malware is a problem. We're here to help.

Other Languages: Deutsch Español Francais

On this page...

- Why am I here?
- What should I do?
- How can I trust this site?
- About Operation b58

This page is part of Operation b58, a joint effort by Microsoft and Symantec to disrupt a botnet that used the Bamital malware to stealthily hijack victims' search results and commit online fraud. Malware can also harm your computer and personal information.

For more information on this notice and operation you may visit www.microsoft.com/dcu

Didn't expect this page?

You were likely trying to conduct a web search before you got to this page, however your computer is believed to be infected with malware known as bamital, which interferes with web search. Please read and follow the instructions on this page to resolve the issue.

Why am I here?

You have reached this website because your computer is very likely to be infected by malware that redirects the results of your search queries. You will receive this notification until you remove the malware from your computer.

What should I do?

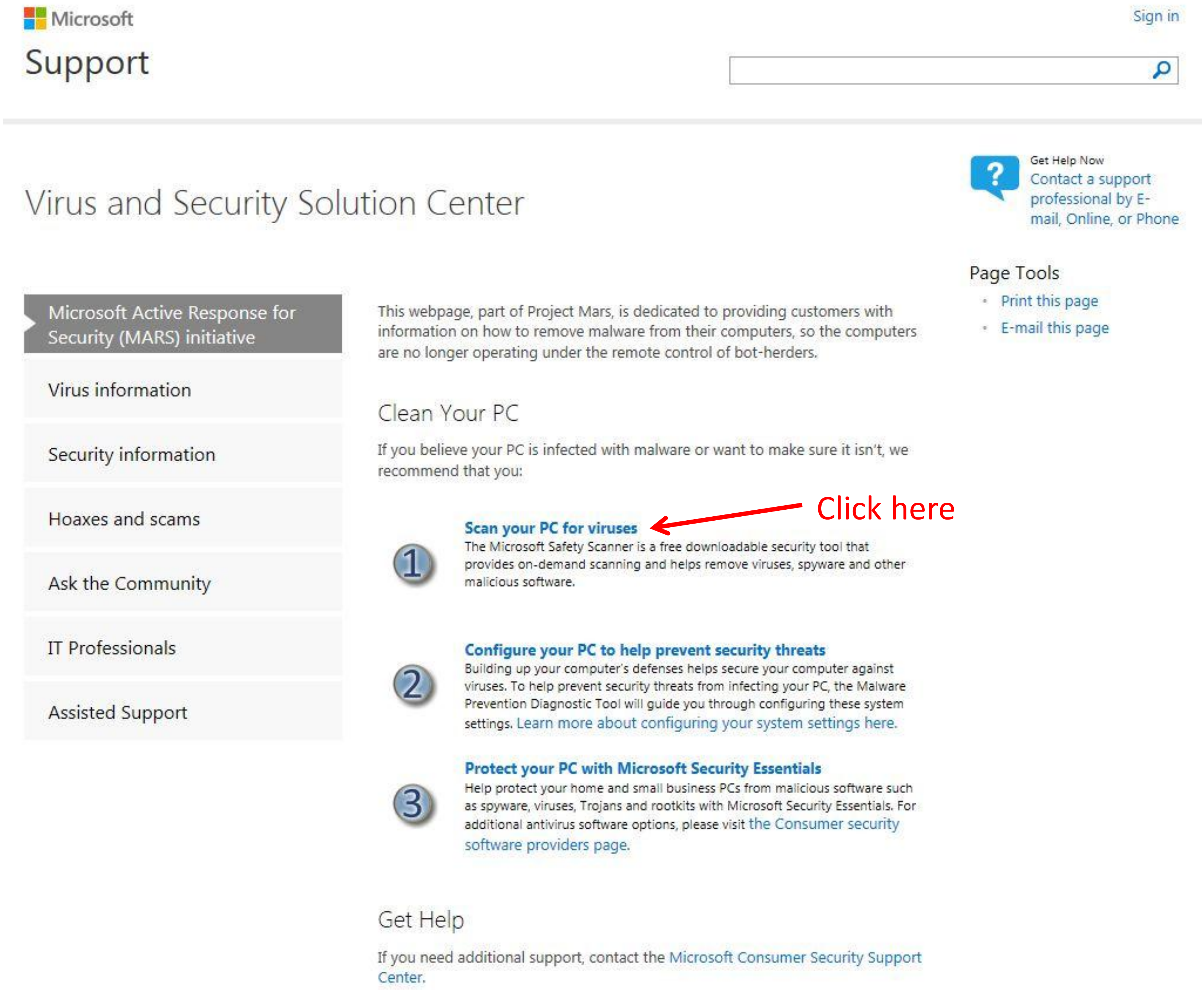
In order to correct this problem, you will need to take some steps to improve the security of your computer. Many of the leading anti-malware tools available online can help clean this malware from your computer. We have listed two options from Microsoft and Symantec here, but you can choose and use anti-malware tools from any provider that you trust. If you wish to run one of the free malware removal tools listed below, copy and paste or type either one of the addresses below into your web browser.

Microsoft Safety Scanner
https://support.microsoft.com/botnets

Norton Power Eraser
https://www.norton.com/bamital

Getting this process started should take less than 10 minutes and the scan can be completed in generally less than an hour, but may vary depending on your system and software used. You do not need to do anything during the scan.

If you think you already have an anti-malware program on your computer, you should make sure it is up to date and perform a full scan.



Virus and Security Solution Center

This webpage, part of Project Mars, is dedicated to providing customers with information on how to remove malware from their computers, so the computers are no longer operating under the remote control of bot-herders.

Clean Your PC

If you believe your PC is infected with malware or want to make sure it isn't, we recommend that you:

1. **Scan your PC for viruses** ← Click here

   The Microsoft Safety Scanner is a free downloadable security tool that provides on-demand scanning and helps remove viruses, spyware and other malicious software.

2. **Configure your PC to help prevent security threats**

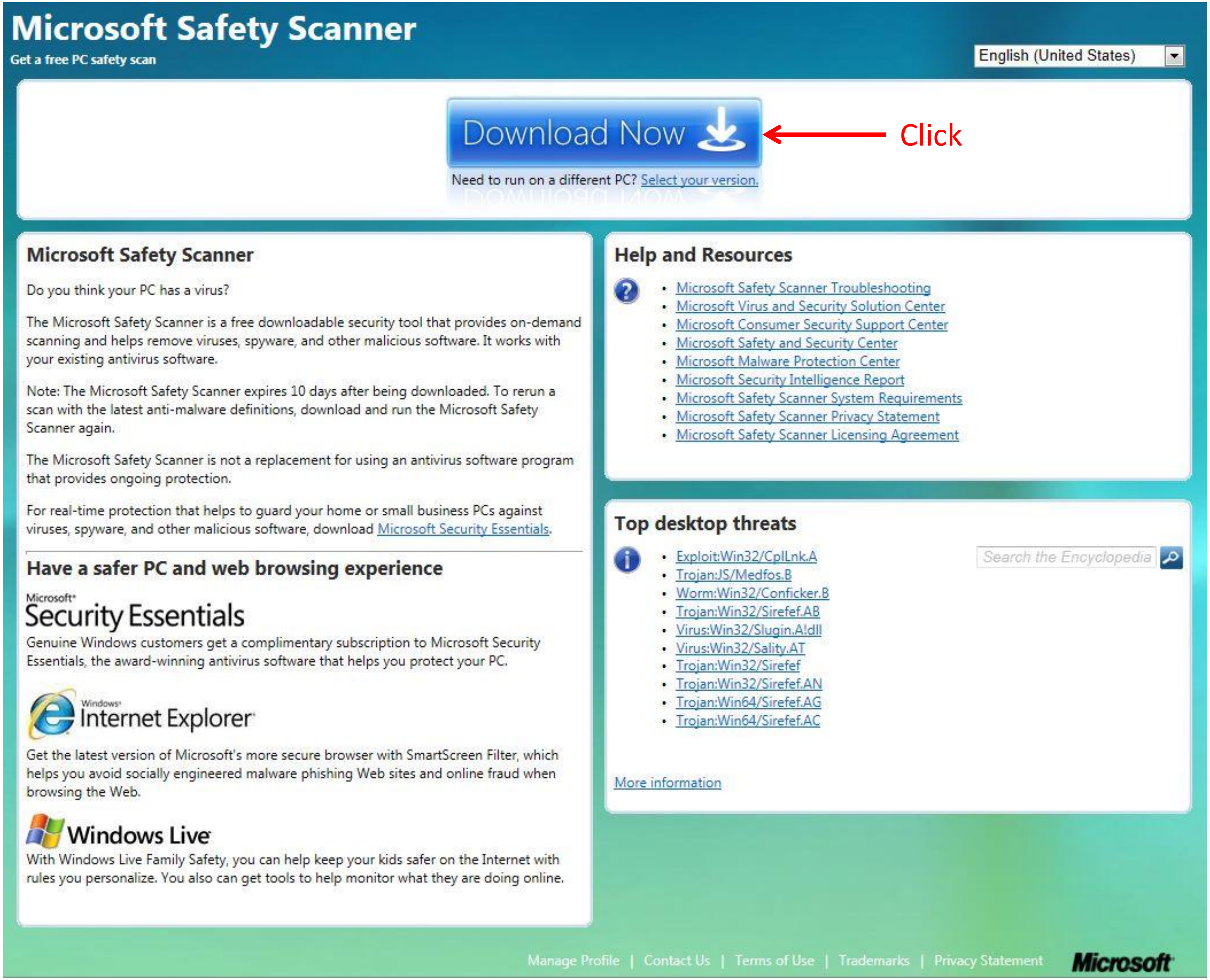
   Building up your computer's defenses helps secure your computer against viruses. To help prevent security threats from infecting your PC, the Malware Prevention Diagnostic Tool will guide you through configuring these system settings. Learn more about configuring your system settings here.

3. **Protect your PC with Microsoft Security Essentials**

   Help protect your home and small business PCs from malicious software such as spyware, viruses, Trojans and rootkits with Microsoft Security Essentials. For additional antivirus software options, please visit the Consumer security software providers page.

Get Help

If you need additional support, contact the Microsoft Consumer Security Support Center.



Microsoft Safety Scanner

Get a free PC safety scan

Click

Need to run on a different PC? Select your version.

Microsoft Safety Scanner

Do you think your PC has a virus?

The Microsoft Safety Scanner is a free downloadable security tool that provides on-demand scanning and helps remove viruses, spyware, and other malicious software. It works with your existing antivirus software.

Note: The Microsoft Safety Scanner expires 10 days after being downloaded. To rerun a scan with the latest anti-malware definitions, download and run the Microsoft Safety Scanner again.

The Microsoft Safety Scanner is not a replacement for using an antivirus software program that provides ongoing protection.

For real-time protection that helps to guard your home or small business PCs against viruses, spyware, and other malicious software, download Microsoft Security Essentials.

Have a safer PC and web browsing experience

Microsoft® Security Essentials

Genuine Windows customers get a complimentary subscription to Microsoft Security Essentials, the award-winning antivirus software that helps you protect your PC.

Windows® Internet Explorer®

Get the latest version of Microsoft's more secure browser with SmartScreen Filter, which helps you avoid socially engineered malware phishing Web sites and online fraud when browsing the Web.

Windows Live

With Windows Live Family Safety, you can help keep your kids safer on the Internet with rules you personalize. You also can get tools to help monitor what they are doing online.

Help and Resources

- Microsoft Safety Scanner Troubleshooting
- Microsoft Virus and Security Solution Center
- Microsoft Consumer Security Support Center
- Microsoft Safety and Security Center
- Microsoft Malware Protection Center
- Microsoft Security Intelligence Report
- Microsoft Safety Scanner System Requirements
- Microsoft Safety Scanner Privacy Statement
- Microsoft Safety Scanner Licensing Agreement

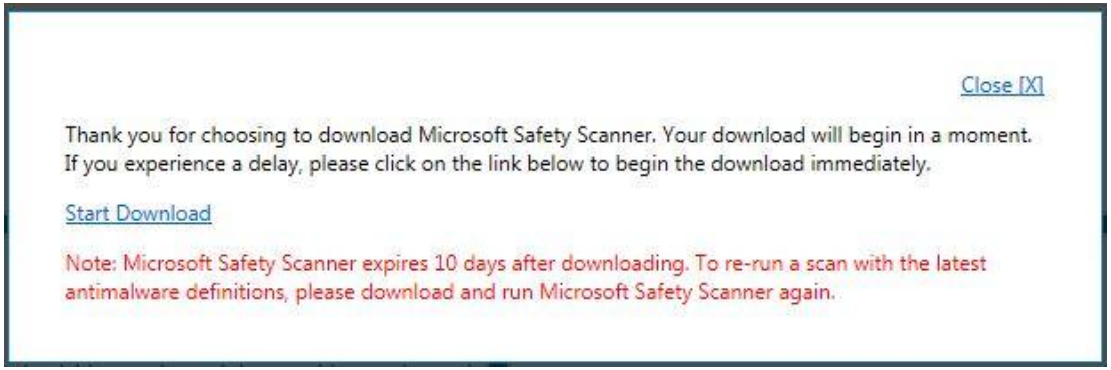
Top desktop threats

- Exploit:Win32/CplLnk.A
- Trojan:JS/Medfos.B
- Worm:Win32/Conficker.B
- Trojan:Win32/Sirefef.AB
- Virus:Win32/Slugin.A!dll
- Virus:Win32/Sality.AT
- Trojan:Win32/Sirefef
- Trojan:Win32/Sirefef.AN
- Trojan:Win64/Sirefef.AG
- Trojan:Win64/Sirefef.AC

More information

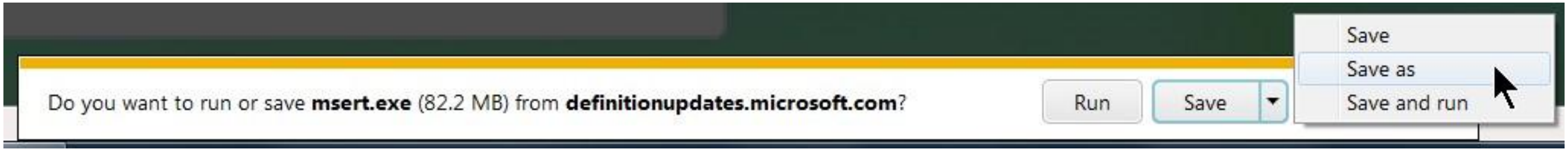
Manage Profile | Contact Us | Terms of Use | Trademarks | Privacy Statement

Microsoft



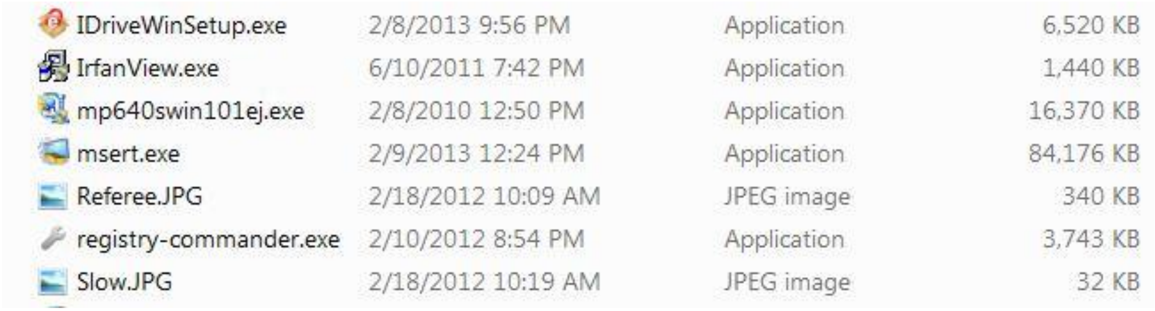
Thank you for choosing to download Microsoft Safety Scanner. Your download will begin in a moment. If you experience a delay, please click on the link below to begin the download immediately.

Note: Microsoft Safety Scanner expires 10 days after downloading. To re-run a scan with the latest antimalware definitions, please download and run Microsoft Safety Scanner again.


Do you want to run or save **msert.exe** (82.2 MB) from **definitionupdates.microsoft.com**?

Save it to the Downloads folder

Go to the Downloads folder and double-click msert.exe



IDriveWinSetup.exe	2/8/2013 9:56 PM	Application	6,520 KB
IrfanView.exe	6/10/2011 7:42 PM	Application	1,440 KB
mp640swin101ej.exe	2/8/2010 12:50 PM	Application	16,370 KB
msert.exe	2/9/2013 12:24 PM	Application	84,176 KB
Referee.JPG	2/18/2012 10:09 AM	JPEG image	340 KB
registry-commander.exe	2/10/2012 8:54 PM	Application	3,743 KB
Slow.JPG	2/18/2012 10:19 AM	JPEG image	32 KB