More on Malware

Malware = Virus, Trojan, Worm, Spyware, Adware, Key-logger, Browser-hijacker, Botnet-Zombie etc, etc, etc

Reminder

To protect yourself and your computer from malware:

- Firewall (Windows XP, Vista and Windows 7 - built in)
- Anti-virus with program AND definition updates
- Anti-spyware program
  (or combined Internet security suit)
- Keep all programs up-to-date
  - Windows operating system
  - Browser - IE, Firefox, Chrome
  - Adobi Reader
  - Adobi Flash
  - JavaScript - (and all browser plugins)

Check - Firewall/Update/Anti-vir & Spy

Windows Firewall - see Control Panel

Windows Update - see Control Panel

Microsoft Anti-virus-spyware - see M'soft Security Essentials
All programs or System tray

Browser - update - Chrome is automatically updated (wrench)

Tools to Help Keep Apps Up To Date

Secunia Personal Software Inspector
http://secunia.com/vulnerability_scanning/personal/

Qualys Browser and Plugin Inspector
https://browsercheck.qualys.com/

Here's the site that will test your java installation to see if you are up-to-date:
http://java.com/en/download/installed.jsp

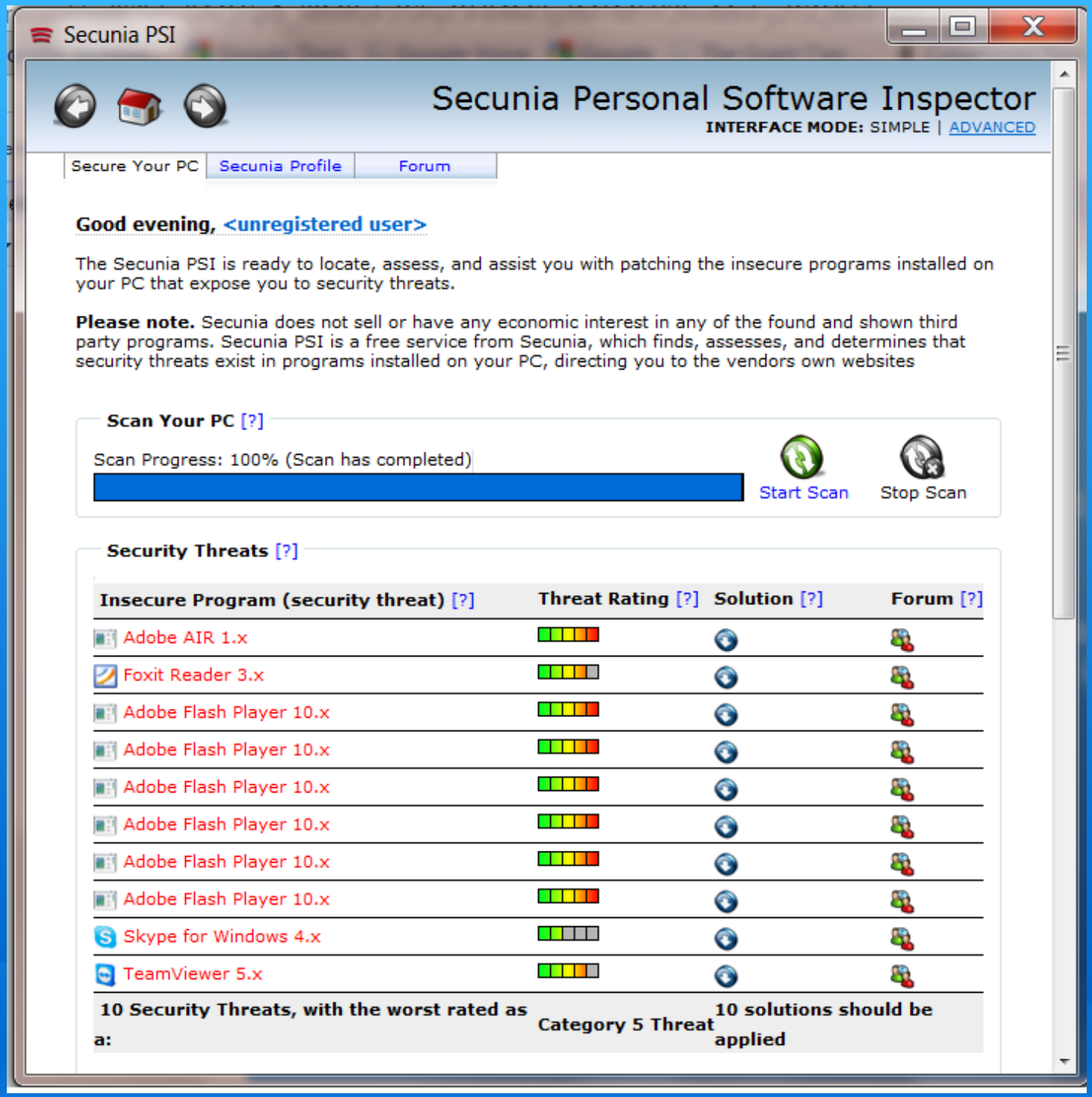
Secunia Personal Software Inspector - Free

Used by millions of home users around the world.

A tool designed to detect vulnerable and out-dated programs and plug-ins which expose your PC to attacks.

Attacks exploiting vulnerable programs and plug-ins are rarely blocked by traditional anti-virus and are therefore increasingly "popular" among criminals.

Scunia Screen Capture



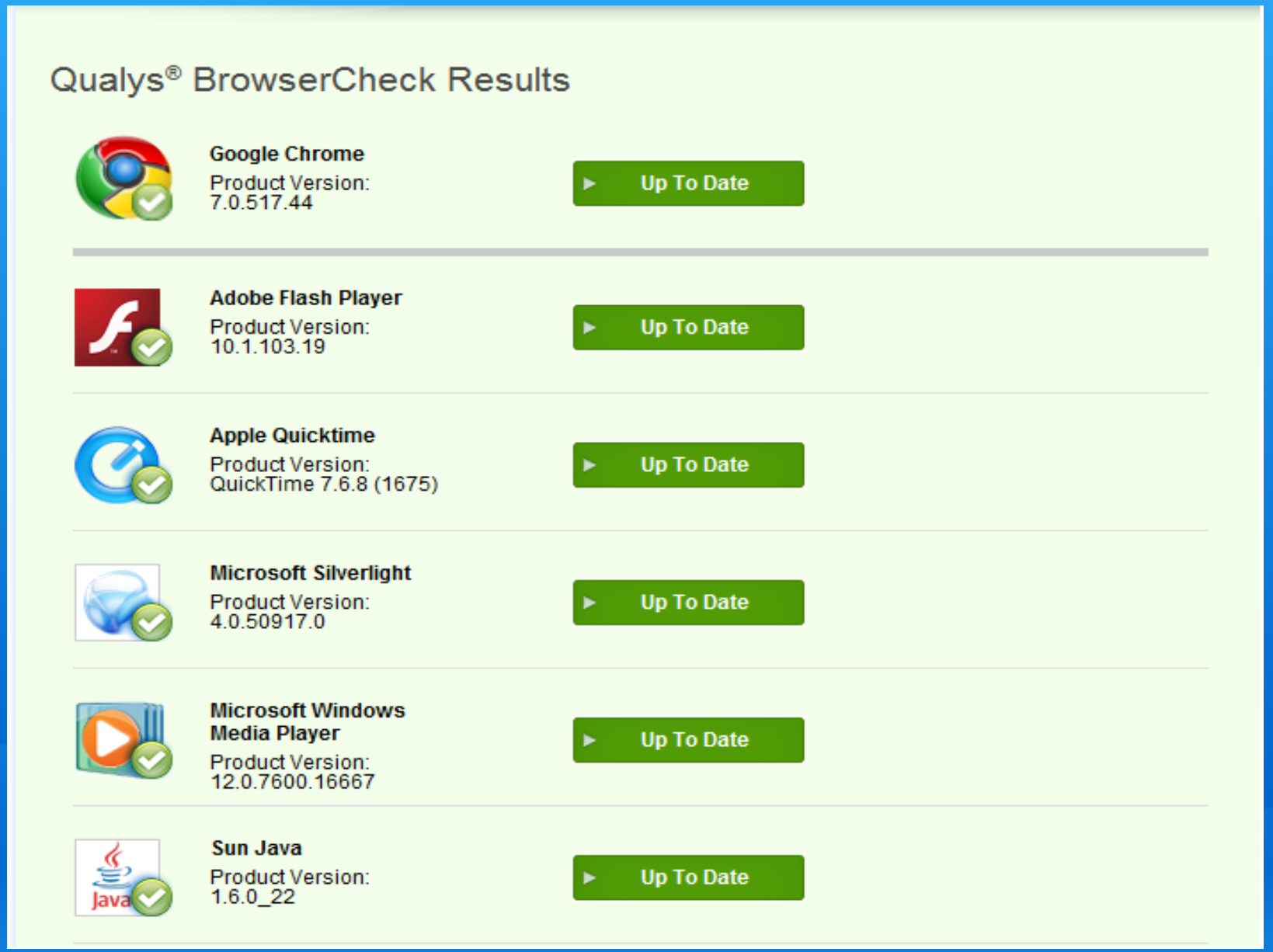
Qualys BrowserCheck (Free)

Qualys BrowserCheck is a tool that scans your browser looking for potential vulnerabilities and security holes in your browser and its plugins. This tool will also help you fix the security issues discovered by the scan.

The threat of browser-based data breaches is growing. The number of vulnerabilities in browser plugins is on the rise. Now is the time to be proactive about the security of your web browser.

https://browsercheck.qualys.com/support.php

Qualys BrowserCheck Results



The Inevitable

A disk crash or other event that renders: (mentioned recently)

- Your computer unusable
- Your data innacessible
- Your computer beyond economic repair

A malware infection that renders: (today's topic)

- Your computer unusable
- Your data innacessible
- Your computer beyond economic repa

THE INEVITABLE :-(

Prepare for the Inevitable

Postpone the Inevitable

Recover from the Inevitable

Have a nice Day :-)

The Inevitable GAP - 1

- The bad guys develop and propagate many new "attack vectors" every day
  (ways to get access to, and "infect" your computer)
- The good guys have "honey-pots" in an attempt to catch infections
  (computers deliberately set to become infected)
- When those computers catch infections they must be analysed to:
  - determine their potency / danger
  - determine how they work
  - design an antidote
  - distribute the antidote to users around the world
    (Antivirus "Definition Updates")
- So.....

The Inevitable GAP - 2

- There is always a GAP or time-lag between release and propagation of the "infection" and distribution of the "antidote"
  - during this time computers are vulnerable
  - so, many computer become infected
  - frequently these computers seek-out other computers and attempt to infect them
  - these computers frequently become part of a Botnet

AV Suites Don't Work !

As a result of this delay, most antivirus programs don't provide complete protection.

http://www.computerworld.com/s/article/9180823/NSS_Labs_Testing_shows_most_AV_suites_fail_against_exploits?taxonomyId=17&pageNumber=2

NSS Labs: Testing shows most AV suites fail against exploits

Finally -Precautions

Prepare for the inevitable:

- Make sure System Restore is ON and working
  - XP
  - Vista
  - Windows 7
- Make sure you have at least one backup copy of your data - preferably more, and TEST that the backup works (Also refer to Hank's Backup Presentation)
- Postpone the Inevitable
  - Keep EVERYTHING up-to-date:
    - Windows, Antivirus, Browser, Browser Plugins, Java, Adobe Flash, Email program, yada..yada
- Recover from the Inevitable
  - To be continued...

If There's Time

C:\Users\paul\Documents\CHH-Presentations\More NewStuff

Recovery Note:

Unless you are prepared, it is likely that you will need to download special tools from the web to remove the infection.

To do this you need a machine that will allow you to connect and download.

Many infections have a "feature" that frustrates your attempts to do that.

Therefore it's advantageous to have a working computer available to download the tools

Windows 7 Recovery Options

Coming to a theater near you in the New Year ;-)

THE END

Stuxnet Worm

Why did Stuxnet worm spread?

http://www.computerworld.com/s/article/9189140/Why_did_Stuxnet_worm_spread_?taxonomyId=17&pageNumber=2

Odds'n Ends or Links

How to prevent click-jacking
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1342882_mem1,00.html

Symantec internet Security threat report 1
Volume XV, published April 2010

Symantec internet Security threat report
Typically, this type of attack begins with some reconnaissance on the part of attackers. this can include researching publicly available information about the company and its employees, such as from social networking sites. this information is then used to create specifically crafted phishing email messages, often referred to as spear phishing, that target the company or even specific staff members. these email messages often contain attachments that exploit vulnerabilities in client-side applications, or links to websites that exploit vulnerabilities in Web browsers or browser plug-ins. A successful attack could give the attacker access to the enterprise's network.
In the case of the Hydraq attack, a previously unknown vulnerability in Microsoft® internet Explorer® and a patched

Bot-nets

http://www.malwarehelp.org/is-your-pc-part-of-a-zombie-botnet-check-now-2009.html
See recommended free anti malware progs

Symantec internet Security threat report 2

A successful attack could give the attacker access to the enterprise's network.
In the case of the Hydraq attack, a previously unknown vulnerability in Microsoft® internet Explorer® and a patched vulnerability in Adobe® reader® and Adobe Flash® player are exploited to install the trojan.
Once the trojan is installed, it lets attackers perform various actions on the compromised computer, including giving them full remote access. typically, once they have established access within the enterprise, attackers will use the foothold that they have established to attempt to connect to other computers and servers and compromise them as well. they can do this by stealing credentials on the local computer or capturing data by installing a keystroke logger.

Is Your Java up-to-date?

Here's the site that will test your java installation to see if you are up-to-date:
http://java.com/en/download/installed.jsp

Go to the site and click on "Verify Java Version"

Note:
Use the "Verify Java Version" site to check whether you have the recommended release. If you're still running Java 6.10 or earlier, you're vulnerable to attack and will need to remove the old versions first (see below). Once that's done, update to the newest Java (currently 6.22).

Watch out: by default, Java updates may offer some unwanted ***freebies*** such as the Yahoo toolbar. Be sure to click these off (unless, of course, you want an extra toolbar.)

Excellent reference on malware with 208 references

http://en.wikipedia.org/wiki/Rogue_security_software