



BY MIKE HALEY

Squiggout Web Designs, LLC

The New Internet

The Internet is a great place for businesses to market their products and services but the ever increasing fraud, malware, viruses and spam is ruining the reputation of the Internet. It all started about twenty-three years ago when a graduate student brought the Internet to its knees with a virus called "Kilroy Was Here." The virus jumped from computer to computer like the plague.

Last month the world's computers were attacked by viruses that make "Kilroy Was Here" look like a joke. At any given time, millions of computers are infected and you may be one of them. The new Internet is one big infection which needs more than a Band-Aid; it needs an inoculation. Here is a list of the top ten computer infections or malware and what they do to your computer. This list is always changing because smart people with too much idol time are always making new viruses. Do not ask me why.

1. Trojan-Spy.Win32.Zbot.gen is currently referred to as the most privacy-infringing nasty parasite you may 'catch' while surfing the web. Trojan-Spy.Win32.Zbot.gen exploits system vulnerabilities to penetrate into victims' machines to subsequently compromise users' privacy. Trojan-Spy.Win32.Zbot.gen is known to be capable of getting on board absolutely undetected. Once in your system, this hazardous Trojan will collect your confidential data including your passwords and banking information and transmit it to remote criminals. Trojan-Spy.Win32.Zbot.gen is also able to discover backdoors in your system's authentication utilities to promote more malware inside your PC for the purpose of its further disruption. While staying resident in your cyber environment, Trojan-Spy.Win32.Zbot.gen will track your keystrokes, which may turn out your logins, password, credit card details, etc. Despite its primitive nature, Trojan-Spy.Win32.Zbot.gen is an extremely dangerous parasite that can indirectly lead to theft of your savings, as well as system performance deterioration. Since the presence of Trojans is often hard to detect, if you notice the slightest unwanted activity on your credit card, you are strongly advised to perform a sys-

tem scan with a trusted tool to check if your privacy is safe.

2. Trojan.DNSChanger.Gen is a generic class of Trojans that reconfigure Domain Name Server settings on compromised machines. The reconfiguration ensures that network requests from those PCs are directed to servers and networks controlled by malicious parties, who can then inject malicious content into otherwise legitimate web pages or redirect requests for standard web sites to bogus, malicious web sites.

3. Trojan-Downloader.Zlob.Media-Codec disguises itself as required upgrade software for Windows Media Player to be able to view adult videos online. It contains a malicious code that downloads a variant of Trojan.Zlob which is the culprit for Rogue Antispyware Programs such as SpywareQuake, SpyFalcon, Winfixer, and others.

4. Trojan.1 is a family of Trojans that causes damage to computer systems by disabling their security systems and compromising their operations so the Spyware may get installed.

5. BehavesLike.Win32.Malware (v) is a heuristic detection for software that exhibits behaviors that are typically associated with malicious threats. It tries to disguise itself as a legitimate application.

6. Exploit.PDF-JS.Gen (v) is detection for threats that exploit a security flaw in PDF files with embedded JavaScript that often installs downloaders that retrieve further malware from remote websites.

7. PersonalAntivirus is a rogue anti-Spyware application that claims to scan for and remove Spyware from users' computers. Personal-Antivirus may be downloaded and installed through exploits or under dubious circumstances without user consent. It hijacks the user's desktop and typically displays exaggerated or false claims of Spyware found to frighten the user into paying for the program. This program looks just

like AVG Virus program and pops up in the bottom left hand corner, just like your virus program. Do not click it... you will be sorry.

8. INF.Autorun (v) is a generic family of threats that use Autorun.inf files to automatically launch backdoors, Trojans, and Trojan downloaders when certain files or folders are accessed by the user. After execution, these malicious files will usually download additional malware to the compromised box.

9. Trojan-Spy.Win32.Pophot.gen is a Trojan that attempts to steal passwords, login credentials, and other confidential or sensitive information from victims' computers and transfer it back to the attacker.

10. Win32.Cekar.E is a hybrid worm/virus that hijacks user's desktops and home pages, tracks users' online activity, and spawns pop-up advertising on the desktop based on that activity. Typically delivered to PCs through so-called "fake codes" on malicious web sites, this threat also infects PE executable files, spreads via removable media, and downloads additional malicious software.

And this is just the top ten from last month according to Sunbelt Software.

What can you do to protect your network or computer? Get a great Anti-Virus /Spyware program, a firewall, and most of all keep it updated. Have the program scan every night for viruses or malware. Use a service provider that scans everything and removes the viruses before it gets to you. Keep your operational system or OS up to date, this is very important because most Trojans exploit your OS to gain access to your computer.

The new Internet requires everyone to be "updated." If we all keep our computer inoculations up to date, making these programs will be a waste of time and the "Golden Age" of the Internet can happen.

Keep safe. Check your computer regularly.

Now Anyone Can Be An I.T. Professional

Renting software and server space is the fastest, most reliable way to set up your company's network. Get it customized, access it anywhere in the world, and pay a fraction of the cost.



Squiggout®

It's called software as a service ▶ 888.883.2754 | sales@squiggout.com | squiggout.com