"Safe Surfing"

"Safe Surfing"

Security Threats Defined

Hackers and Crackers

A **Hacker** is someone who writes **malicious computer programs** designed to infect computers, spread to other computers, gain illegal entry into private computer systems, and to perform **Denial of Service** attacks on corporate web sites for a variety of reasons, mostly **financially motivated**. They are believed to have more than a million '**drone**' computers world wide that they can remotely control to attack us at will.

The term "**cracker**" is not to be confused with "hacker". Hackers generally deplore cracking. However, as Eric Raymond, compiler of *The New Hacker's Dictionary* notes, some journalists credit most break-ins to "**hackers**."

A **Cracker** is someone who breaks into someone else's computer system, via the Internet or dialup modem; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security.

A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or just because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. Financial information is usually the motive, be it a financial institution with account numbers or personal information that can be used for identity theft, or corporate trade secrets or national security information that can be sold or used for extortion.

A classic story of the tracking down of a cracker on the Internet who was breaking into U.S. military and other computers is told in Clifford Stoll's ***The Cuckoo's Egg***.

Viruses, Trojans, Worms, "Diallers", and other Malware

Malware (MALicious softWARE) is a new name for any bad software that was designed to destroy, aggravate, wreak havoc, hide incriminating information, and/or disrupt and damage a computer system or network. This includes any hardware, software, or firmware that is intentionally installed or inserted into a system for a potentially harmful purpose without the knowledge or permission of the system owner. (i.e.: Trojan horse, virus, worm, Spyware, Backdoors, etc.)

Viruses – Any malicious or destructive program that can get loaded onto your computer without your knowledge or permission. The term virus was used because the programs are designed to spread from one computer to another via floppy disk, directly through Internet by exploiting security flaws in operating systems (Windows, Mac OS, and Linux) and Web browsers (Internet Explorer, Netscape, and Mozilla Firefox).

- **Malware** Malicious software designed to damage/disrupt a computer/network
- **Viruses** Malicious program that attaches or targets a specific System
- **Worms** Spread by Network (email attachment or embedded code)
- **"Trojan Horse" Viruses** Small, download with web pages**,** then get "payload"
- **General Unwanted Programs** legitimate tools to kill processes, delete files, etc.

Trends – Antivirus vendors claim that there is an emerging trend to **increasingly target Home Computers** since they are the **weakest link in the security chain**, and the likelihood of financial rewards are increasing

with the rapidly increasing number of home users that store passwords and credit card number son their computers for access to Internet Banking. Corporate and Government systems have learned to use the latest security tools and keep their systems up to date with **security patches** for their operating systems and web browser.

Worms – a computer worm is a **self-replicating** computer program. It uses a network to send copies of itself to other systems usually without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas a **Viruses** always infect or corrupt files on a "targeted computer system" (i.e. Windows, Mac OS, Linux).

The Morris worm was written by Robert Tappan Morris, at the time a computer science graduate student at Cornell University, and released on November 2, 1988 using a friend's account on a Harvard University computer. It quickly infected large numbers of computers attached to the Internet and caused massive disruption. That it didn't spread even farther and cause more trouble is largely due to some errors in its implementation. It propagated via several bugs in BSD Unix and related systems, and its component programs (including several versions of 'sendmail'). Morris was identified, confessed, and was later convicted under the US Computer Crime and Abuse Act. He received three years probation, 400 hours community service and a fine in excess of $10,000.

Many worms have been created which are only designed to spread, and don't attempt to alter the systems they pass through. However, as the Morris worm, and Mydoom showed, the network traffic and other unintended effects can often cause major disruption. A "payload" is code designed to do more than spread the worm - it might delete files on a host system, encrypt files in a cryptoviral extortion attack, or send documents via e-mail.

A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" under control of the worm's author – like the much publicised zombie worms Sobig and Mydoom. A huge network of zombie machines are often referred to as "botnets" and are commonly used by SPAM senders for sending junk email or to cloak their website's address. Spammers are therefore thought to be a source of funding for the creation of such worms, and worm writers have been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threatened DoS attacks.]

Backdoor programs, however they were installed, are often exploited by other malware, including worms. Examples include Doomjuice, which spreads using the backdoor opened by Mydoom, and at least one instance of malware taking advantage of the "rootkit" backdoor installed by the Sony/BMG DRM software they put on millions of music CDs ending in late 2005.

Virus Sources – Viruses are sophisticated computer programs that are "hand crafted" by programmers all over the world. Most are designed to work quietly in the background with few symptoms so that they can spread themselves as far and wide as possible before being detected and removed. The source code for the virus programs and "tool kits" with building blocks and instructions on how to use them are widely available from "**Hacker**" web sites all over the world, mostly in countries that do not strictly pursue such criminals.

Virus Symptoms – Most viruses are designed to work quietly in the background so that they can spread to as many other systems as possible, and do as much damage as possible before they are discovered and removed. The most common symptoms of a viral infection include:

- Significant system slow down;
- Programs crashing more than usual,;

- Windows "blue screen of death" errors that cause the PC to shutdown and reboot;
- Errors about missing files (especially .DLL files) during startup;
- Documents of various types, some or all, disappearing unexpectedly;
- Internet disabled by ISP for sending too many emails, or emails with infected attachments;
- Pop-up Ads in unusually high numbers with similar content;
- Lots of new book mark entries for porn and gambling sites in you web browser;
- Home Page changing without your knowledge, keeps going back to same page;
- Browser Search Hi-Jacking – misspelled URLs go to index page with porn and gambling references
- Dialling your ISP or elsewhere as soon as you start the computer.

Email Threats

Phishing – the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

Worms - many have their own email engine to send out reinforcements via email attachment to every email address that they can find on your computer, be it in an address book or document. Others will harvest email address from web sites for their targets.

Spyware and Adware

Spyware refers to a broad category of malware designed to intercept or take partial control of a computer without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

In simple terms, **spyware** is a type of program that watches what users do with their computer and then sends that information over the Internet. Spyware can collect many different types of personal information about a user. The more harmless programs attempt to track the websites that a user visits and send this information to an advertisement agency for statistical analysis. A more malicious code may log keystrokes to intercept passwords or credit card numbers. Yet other versions simply launch targeted popup ads.

Adware refers to any software which displays advertisements, such as the much maligned **popup ads**; **with or without the user's consent**. Some legitimate uses of adware include useful programs such as the Eudora mail client which can be used freely with full features, with display ads as an alternative to shareware registration fees. This is known as advertising-supported software, but not as spyware. Other examples include Kaaza file sharing, and a popular ad-on for MSN Messenger called Messenger Plus. This sort of Adware is quite different from the malware type which often operates surreptitiously or misleads the user, causing unwanted system behavior.

Tracking Cookies – Anti-spyware programs often report Web advertisers' HTTP cookies as spyware. Web sites (including advertisers) set cookies — small pieces of text data rather than software — to track Web-browsing activity: for instance to maintain a "shopping cart" for an online store or to maintain consistent user settings on a search engine.

Only the Web site that sets a cookie can access it. In the case of cookies associated with advertisements, the user generally does not intend to visit the Web site which sets the cookies, but gets redirected to a cookie-setting third-party site referenced by a **"banner ad"** image. Some Web browsers and privacy tools offer to reject cookies from sites other than the one that the user requested.

Advertisers use cookies to track people's browsing among various sites carrying ads from the same firm and thus to build up a marketing profile of the person or family using the computer. For this reason many users object to such cookies, and anti-spyware programs offer to remove them.

Typical Spyware Examples

A few examples of common spyware programs may illustrate their wide range of behaviors. ***Caveat:*** As with computer viruses, researchers give names to spyware programs which often don't relate to any names that the spyware-writers use. Researchers tend to group programs into "families" based on common behaviors, or by "**following the money**" of apparent financial or business connections. For instance, a number of the spyware programs distributed by Claria Corporation are collectively known as "**Gator**".

CoolWebSearch, a group of programs, installs by exploiting Internet Explorer vulnerabilities. These programs direct traffic to ads on Web sites including ***coolwebsearch.com***. To this end, they display pop-up ads, rewrite search engine results, and alter the infected computer's hosts file to direct DNS lookups to these sites.

Internet Optimizer, also known as **DyFuCa**, redirects Internet Explorer error pages to advertising. When users follow a broken link or enter an erroneous URL, they see a page of advertisements. However, because password-protected Web sites (HTTP Basic authentication) use the same mechanism as HTTP errors, Internet Optimizer makes it impossible for the user to access password-protected sites.

180 Solutions transmits extensive information to advertisers about the Web sites which users visit. It also alters HTTP requests for affiliate advertisements linked from a Web site, so that the advertisements make unearned profit for the 180 Solutions Company. It opens pop-up ads that cover-up the Web sites of competing companies.

HuntBar, aka **WinTools** or **Adware.Websearch**, is a family of spyware programs distributed by Traffic Syndicate. It installs an **ActiveX** controls by **drive-by download** at affiliated Web sites, or by ads displayed by other spyware programs — an example of how spyware can install more spyware, compounding the problem. These programs add toolbars to Internet Explorer, track Web browsing behavior, redirect affiliate references, and display unwanted pop-up advertisements.

SPAM and Junk Mail Senders

Spamming is the abuse of electronic messaging systems to send **unsolicited, undesired bulk messages**. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, and mobile phone messaging spam.

Spamming is economically viable because advertisers have **no operating costs** beyond the cost of their Internet connection rental, and the manpower to maintain their huge mailing lists, and because it is difficult to hold them accountable for their mass mailings. Because the barrier to entry is so low, there are numerous spammers, and the volume of unsolicited mail has become extremely high. The costs, of lost productivity and fraudulent sales, are borne by the public and by Internet Service Providers, which generally just add extra capacity to cope with

the deluge. Spamming is widely despised, and has recently been the subject of new legislation in many jurisdictions.

Prevention is the only real cure for SPAM emails. Don't give out your email needlessly to manufactures or web sites unless you really need to communicate with them. Reputable firms will allow you to control the type and frequency of Junk Mail on their we sites, but once they have your email address, gets onto public space, or listed on a web site then you will start to get your share of SPAM. The Spammer all use webbot computers to scan the World Wide Web every night looking for new email address to add to their mailing lists. Why? Just because it is so profitable. It is estimated that most of the larger spammers make several thousand dollars per day from people who are dumb enough to make on-line purchase for anything from prescription drugs, Viagra, Cialis, Penis Enlargement Pills, fake Rolexes, and Gucci bags.

Most ISP's have implemented SPAM blocking software on their mail systems, but once you are on the list you can be sure that a lot of the mail will get through. The bad news is that the send Non-Delivery Notices to the return address in the SPAM message which are nearly all forged and misdirect the NDN's to some unsuspecting user or ISP. Last year, AccessComm was the target of a malicious attack by a SPAM sender that reported all the originating sender as fictitious AccessComm mail users. The resulting storm of NDN's took down their mail server for several days, and they had to upgrade from two to about 22 mail servers to cope with the traffic.

Most popular desktop email software such as Microsoft Outlook and QualComm's Eudora have Junk Mail filtering built in. This software attempts to learn what is SPAM with your input, and files it away to a separate folder the you can review later to retrieve any good stuff that got there by mistake.

Tools and Solutions

Install Security Updates

The companies that develop and market computer operating systems and networking software components often release software updates that fix or close security vulnerabilities in their products. When new software buts are discovered, they are published by a number of agencies such as CERT.org, a part of the Software Engineering Institute at Carnegie Mellon University, publish all know software bugs and the related security risks for all major operating systems, including Windows, Mac OS, Linux, etc. and network tools such as web browsers, file transfer programs, and instant messaging.

The result of publishing all know program flaws, is that the vendors have about a week to come up with a solution to fix it before it is exploited en mass by hackers and virus writers. These public security reports provide the hackers with nearly all the information necessary to break into any computer that has not been updated by installing all available security patches.

So set your computer to run Windows Update (or if you like Microsoft Update,) and check from time to time by running the Windows Update program from the Start Menu to see if all available critical security updates have been installed.

Use Good Anti-Virus Updated Weekly

Choose a good brand named Anti-Virus product and make sure to update the program at least every two years, and ensure that the Virus templates or DAT files get updated automatically on a regular basis, at least weekly. You have basically no protection is either of the above rules is not obeyed. When AVG or McAfee anti-virus data files are older than a week, the icon loses its color and goes black and white to alert you that there is a problem. Open the Security console and check for the problem. Often it just means that your system has been turned off, or had no Internet access for the past few days. Click on the button to manually update the data and it will probably be fine.

Always set your anti-virus program to do a full system scan at least once per week. Some viruses, usually small Trojans will always sneak through, with Web pages and they can download more dangerous reinforcements.

Don't get sucked into buying the **Full Meal Deal** or "**Internet Security Suite**" from your anti-virus vendor when you renew your annual license to download updates. They generally include a Anti-Virus, Firewall, SPAM filter, and Parental Controls for Web Surfing. This is especially true for older computers with Windows ME or 98. They won't be able to handle the workload, and will slow to a crawl.

Home Users, use **AVG Free Edition**. It's completely free, automatically downloads data file updates, has a scheduled scan capability, and all the reporting that you need.

Firewall Protection

If you are running any version of Windows **prior** to XP SP2, and you do not have a Firewall Router with Network Address Translation (NAT) between you and the Internet, then you need to install a software Firewall. They can be purchased separately from your favorite anti-virus vendor, such as McAfee or Symantec, and are also included in their security suites. Another good alternative is ZoneAlarm from www.zonelabs.com. They have a very good freeware program that will provide adequate protection, and has the flexibility to allow local file and print sharing behind a **firewall router**.

The firewall will block any incoming traffic such as hackers scanning for open ports with services such as web servers, ftp servers, or email waiting and listening for connections. ZoneAlarm will even tell you with a pop-up message every time someone tries to "touch" your computer from the Internet. That is interesting at first but will soon become annoying. Try it – you will likely see more than half a dozen hits in the first 15 minutes.

Firewall Routers only provide one-way firewall protection, keeping the bad guys out. A software firewall can also provide controlled access to the Internet from only known programs, subject to your permission. This can stop **Trojan horse viruses** and **Backdoor programs** from opening up the Internet and allowing the author or another virus to freely enter your computer. However, don't be too complacent, because most serious viruses know how to shutdown the most popular firewall and antivirus programs.

Anti-spyware programs

Lavasoft's Ad-Aware, one of a few reliable freeware anti-spyware programs, after scanning the hard drive of an infected Windows XP system. Many programmers and some commercial firms have released products designed to remove or block spyware. Steve Gibson's *OptOut*, (www.grc.com) mentioned above, pioneered a growing category. Programs such as Lavasoft's *Ad-Aware SE* and Patrick Kolla's *Spybot - Search & Destroy* rapidly gained popularity as effective tools to remove, and in some cases intercept, spyware programs.

More recently Microsoft acquired the *GIANT AntiSpyware* software, and soon release it as ***Windows AntiSpyware beta*** as a free download for Windows XP, Windows 2000, and Windows 2003 users. In early spring, 2006, Microsoft renamed this beta software to Windows Defender, "beta 2." Microsoft has announced that the product will ship (for free) with Windows Vista.

Other well-known anti-spyware products include Webroot's Spy Sweeper, Trend Micro's Anti-Spyware, PC Tools' Spyware Doctor, and Sunbelt's CounterSpy (from the same GIANT Anti-Spyware codebase, that became Microsoft's Windows Defender).

Most major anti-virus vendors such as Symantec, McAfee and Computer Associates have added anti-spyware features to their anti-virus products; however they have proven to be incomplete, but better than nothing. They were reluctant to add anti-spyware functions, citing lawsuits brought by spyware authors. To get around the law suits, McAfee has classified these threats as "**potentially unwanted programs**". Symantec Anti-Virus, categorizes spyware programs as "**extended threats**" and now offers real-time protection from them.

Anti-spyware programs can combat spyware in two ways:

- ***real-time protection***, which prevents the installation of spyware
- ***detection and removal*** of spyware.

Writers of anti-spyware programs usually find detection and removal simpler, and many more programs have become available which do so. Such programs inspect the contents of the Windows registry, the operating system files, and installed programs, and remove files and entries which match a list of known spyware components. Real-time protection from spyware works identically to real-time anti-virus protection: the software scans incoming network data and disk files at download time, and blocks the activity of components known to represent spyware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Because many spyware and adware are installed as a result of browser exploits or user error, using security software to sandbox browsers can also be effective to help restrict any damage done.

Fake anti-spyware programs

Malicious programmers have released a large number of **fake anti-spyware programs**, and widely distributed Web banner ads now spuriously warn users that their computers have been infected with spyware, directing them to purchase programs which do not actually remove spyware — or worse, may add more spyware of their own. The recent proliferation of fake or spoofed antivirus products has occasioned some concern. Such products often bill themselves as "antispyware", antivirus, or registry cleaners, and often feature popups prompting users to install them. This is called rogue software. Known offenders include:

Privacy Defender ✓
Malware Wipe
Pest Trap ✓
SpyAxe ✓
AntiVirus Gold
SpywareStrike
SpyFalcon
WorldAntiSpy
WinFixer ✓
SpyTrooper ✓
Spy Sheriff ✓
SpyBan

"Safe Surfing"

SpyWiper
PAL Spyware Remover
Spyware Stormer
PSGuard ✓
AlfaCleaner
Spyware Quake
BraveSentry
VirusBurst
Trustcleaner Pro
AntispywareSoldier