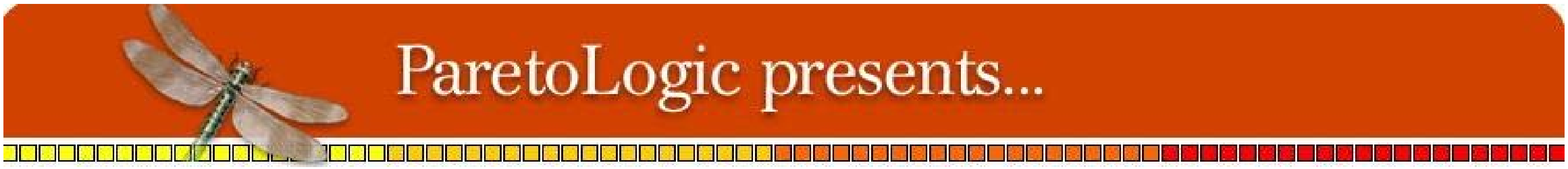


A CyberCrime Report

Information White Paper
March, 2008

This paper uncovers the covert and often unnoticed dealings related to cybercrime. It offers steps to the common user on how to reclaim control of their computer and to restore system performance. Suitable applications for these tasks are identified and recommended throughout this report and in conclusion.

ParetoLogic – The Company

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. We are a member of SIIA (Software Information Industry Association) and we specialize in providing advanced security applications and performance tools for business and personal computer users.

ParetoLogic creates solutions that combine sophisticated technology with a truly user-friendly interface. Our products empower people to secure and optimize their computers and are currently available in eight languages in 186 countries around the world. ParetoLogic has established partnerships on a global scale to make our products available to all computer users regardless of location, language, or computing experience.

We provide attention to the customer needs based on a commitment to delivering exceptional software applications using resource-rich websites. Our solutions exceed expectations.

Addressed in this Product White Paper

This paper includes the following:

CyberCrime – Spyware, Adware, and Malware

Our reliance on computer technology has progressed exponentially. Day-to-day transactions and correspondences are being performed online for business and pleasure. No one can argue the convenience of these new systems and way of life. Unfortunately, keeping pace with our newly established cyber comforts is the evolution of cybercrime. This article defines and describes malicious software, “malware”, known to plague computer systems worldwide.

With the onset of online business and exchange of data and monies, we have experienced the very real, although covert, threat of malware. The Center for Democracy and Technology stated the following in October 27, 2005:

> Spyware has quickly evolved from an online nuisance to one of the most dire threats facing the Internet. As users struggle to maintain control over their computers, many find themselves trapped in a cyclical battle against programs that install themselves without warning, open dangerous security holes and reinstall themselves after they've been deleted.[1]

The “Definitions”

Trying to nail down specific terminology for types of malware and cybercrime is a daunting endeavor. The reason for this is that there is general confusion and inability to attribute common names and identifiers to malware and to classify them accordingly. Many computer users when first encountering malware on their system may think they have a computer virus or a bug. Even for professionals, terminology keeps popping up to describe malicious software that has been around for years but has now been modified or used in new ways.

With this in mind, the names and the descriptions presented here are those that are more commonly known. What is more important is that we list a comprehensive inventory of items and include a brief synopsis. To begin, the word “malware” is a general term that describes software files introduced to a computer system and are damaging to system performance or can disrupt one’s day-to-day computing activities. Malware can also breach system security and be the means of criminal activities including fraud and theft. Typically these items are downloaded without the user’s knowledge or consent and can run and stay resident on a computer despite attempts to uninstall them. Malware is created by software authors with a particular intent and purpose and new malware threats are created and released for public consumption every day.

[1] Anti-Spyware Coalition Definitions and Supporting Documents: http://www.antispywarecoalition.org

Note

Malware items are NOT naturally occurring computer errors. While computer errors, otherwise known as “software bugs”, can result in performance loss or system crashes, they are not a desired outcome for the software creator.

The term “malware” has come to include all types of malicious software. The following list covers some of the varying types of well known malware.

Malware Type	Description
Virus	Results in damage or degradation to the computer system; a virus spreads like an infection from computer to computer and can replicate itself.
Spyware	A general term used to describe malware. Typically it involves partial or full loss of control of computer functioning. Historically thought of as a surveillance tool, thus the name, these items can capture confidential information and transmit the data to a third party for marketing, advertising, or for breach of security and unlawful means. Spyware can steal banking information, passwords, login details, credit card information and more.
Worm	Worms are viruses that utilize system resources and are harmful to network operations. Unlike other viruses they do not and cannot attach to a host program as they proliferate independently.
Trojan	Trojans are a severe security threat and are often used in conjunction with other malicious software. Like the story of the Trojan horse, these items appear harmless, until they are downloaded. Once resident on the system they automatically open in the background, install other items, and can open a backdoor for remote access and other security breaches.
Adware	Typically involves the display of unwanted advertisements in Internet browsers or commercial websites. These items can also collect data for market research purposes.
Keylogger	Keyloggers are programs or devices that secretly monitor and record key strokes and can take screenshots. While some are legitimate, there are those that steal financial data to be retrieved by the virus writer which can result in a security breach and potential loss of funds via online access.
Rootkit	These items represent a severe risk to computer system security. From a technical perspective, rootkits are considered the most sophisticated and most difficult to remove. They are covered in greater detail on page 21.
Downloader	A security breach; when these items infect a system they are capable of downloading countless malware including adware, pornware, and the like.

Malware Type	Description
Browser Hijacker	A marketing related Internet browser alteration. These items alter browser settings including the homepage, search page, favorites, and other controls. Often these alterations can direct user traffic for the purpose of buying something online. These are one of the most common types of malware and have been known to infect millions of computer systems.
Dialer	Automatic unauthorized calls via a dial-up modem. Dialers incur phone charges by accessing the phone line and making calls to pay-per-minute phone services.
Flooder / Distributed Denial of Service (DDoS)	Disables network connections; these items send massive amounts of data to disrupt or bring down a network or Internet connection. They can be targeted at websites and can be used by competitors or those seeking a ransom.
Data Miner / Trackware	Result in a loss of privacy; Data Miners track the user's web usage, searches performed, and general use. This information is then reported to a third party for marketing purposes. Cookies are one example. While most web cookies are harmless some collect private information.
Remote Administrator Tool (RAT)	A security breach and loss of control of computer functioning; a RAT can access a computer remotely and perform unwanted actions including erasure of files, uploading other applications, and more.

Table 1: Types of Malware Security Threats

Other Examples – Ransomware and Stealware

There are other types of malware that have made every-day computer users victims of cybercrime. One such example is "ransomware". This type of malware infiltrates the system and is designed to encrypt personal or business files so that a decryption key is required. The data is held hostage until a ransom is paid. Since 2005, ransomware has been more frequently used.

Another similar "hostage" scheme involves a malware item called Movieland. In a complaint filed against the makers of Movieland (also known as Moviepass.tv and Popcorn.net), the creators are accused of displaying oversized windows and playing music in such a way that the window cannot be minimized or closed. The dispute is based on the user having to pay $29.95 for the program. The software creators state the consumer member did not pay after a 3-day trial period and users state their systems were being held hostage.

Yet another type of malware is "stealware". This type of cybercrime involves the spyware creator diverting payments during an online transaction. The funds are intended for e-commerce affiliate channels and/or third-party distributors. The creators of the spyware are the only ones that profit from this as customers, affiliate operators, and vendors all lose with respect to revenue or unfulfilled sales.

By Location

Certain types of malware are prevalent in various countries. For example, in France and Italy the primary malware threats are pornography Dialers. In these situations, the system is infected with a Dialer program that contacts a phone number associated with pornographic services and remains connected. In Brazil there is a Trojan that directs online traffic from an email to an online bank that has been forged. In this case, the online bank appears to be the Banco de Brazil and users find it difficult to detect the forgery. In North America the majority of malware is centered on advertisement such as adware. This usually comes in the form of pop-ups, tracking browsing habits, spam attacks, and more.

Combinations and Online CyberCrime

One last point of interest speaks to the overlap of malware attacks. There are times, such as the Trojan bank scheme in Brazil, where more than one malware item is employed. It starts with a mass emailing, or “spam attack”. The email includes an attachment or a link and the recipient mistakenly clicks the link or opens the file and is directed to an online site that is in fact a type of Trojan. The user is presented with a message asking to enter in confidential or private information which is recorded and used to access funds. While this is happening malicious items are also covertly downloaded to the computer. In some instances these malware items are part of a botnet herding operation as is described in more detail in the Botnets section on page 22.

The Examples

Attempting to identify and list malware items can be very challenging. One reason for this has to do with the fact that there are many malware variants circulating network systems around the globe. Secondly, these items get named by those researchers discovering them and there is no real standard system in place for naming or sharing this information. As a result, one malware item could be called by two or more different names. Also, new malware is introduced to the general public every day.

Here are some examples of malware:

Malware Type	Examples
Viruses and Worms	In the early 1970's, a virus was released on to ARPANET, the predecessor to the Internet used by the DoD and many universities. It was called the Creeper virus. This virus would infect machines and display the message: "I'M THE CREEPER : CATCH ME IF YOU CAN". Since then there has been many viruses released. A small sampling of these include: Rabbit (1974), Prevading Animal (1975), Elk Cloner for Apple II (1982), the Brain boot sector virus (1986), The Jerusalem virus (1987), the Morris worm (1988), Michelangelo (1992), the Concept virus (1995), the Melissa worm (1999), the Code Red worm (2001), the Blaster worm (2003), MyDoom mass mailer (2004), the Nyxem worm (2006), and Peacomm (2007). This last one came from Russia and was disguised as a news email asking the recipient to download the attachment.
Spyware	Although spyware is a general term we can provide some examples. An example of dueling spyware is the case of Avenue Media filing a legal suit against Direct Revenue. Avenue Media's "Internet Optimizer" is a spyware application that tracks browsing habits before displaying related advertisements to the user. It is installed without consent and is difficult to remove. Direct Revenue also engages in monitoring web activity and it delivers target ads and modifies the user's browser. Direct Revenue allegedly created the ability for its program to disable or remove the Avenue Media's product. The reason for this was to reduce the visibility and occurrence of malware annoyances and thereby prevent the chance of the user taking action.
Adware	A small set of examples of adware programs includes: 123 Messenger, 180 Solutions (180SearchAssistant, Zango), Bonzi Buddy, BlockChecker, ClipGenie, Comet Cursor, Crazy Girls, Cursor Mania, Cydoor, Daemon Tools, Direct Revenue, DollarRevenue, Xango Toolbar, PornDigger!, Smiley Central, TopMoxie, WeatherBug, Weathercast, WhenU, and WinFixer. As an example, Weathercast displays weather information but may also display pop-up or pop-under windows (those windows that appear on the desktop screen or are hidden underneath other windows). Adware can also direct the browser to unsolicited websites.
Trojans	Trojan horse malware are too numerous to mention. As stated these items can be packages of malware that bombard a system. Examples are wide ranging from A to Z: everything from the ABC Trojan (which includes adware, spyware, data miners and remote access) to the Zotob W32 Trojan (which creates a back door entry, exploits the system, and compromises security and confidential information). Another example of a Trojan is one called "waterfalls.scr". It claims to offer a free screensaver but would instead open up access to the computer so that the malware authors could gain control of the system remotely.

Malware Type	Examples
Others	While there is an never-ending list of examples, we can include a few more in other remaining categories: Keylogger: PAL PC Spy and Ultimate Spy Personnal Edition Browser Hijacker: 2020 Search Dialer: Parisvoyeur Data Miner / Trackware: Maxserving cookie Remote Administrator Tool: SpyAnywhere Rootkit: Rootkit AA Trojan and Rootkit.Win32.Agent.dq Ransomeware: Gpcode (including Gpcode.ag, Gpcode.ac and more), Archiveus, Krotten, Troj/Ransom-A, MayArchive, and Cryzip.

Table 2: Examples of Malware Security Threats

Cookies

Those who surf the Internet are likely to receive one or more cookies with each session. While this sounds like a positive experience, web cookies are in fact small files that are downloaded to the system without user knowledge or consent. Many of these files track information about the user's browsing sessions or store information related to login credentials and some provide a service with respect to authentication. For example, a user does not have to re-enter the same login information when accessing their online bank. It becomes troublesome to find and type in a bank card number with every online bank visit. The cookie is used so that the number is automatically displayed and the user has only to enter their password. Other cookies track information related to site preferences and online browsing habits. This information can be used to direct specific advertisements to the user. Cookies are not inherently dangerous but they can be a threat to security and privacy. Some programs written by hackers are designed to steal cookies and the information they contain.

Rogue Software

One final example of malware has to do with a wolf in sheep's clothing. There are fake programs that claim they can remove malicious files and restore computer performance. In many of these situations, the user is browsing to a site and they get some notification that they are infected with some form of malware. While there may be malware on the system, rogue programs do not detect actual instances of malware. Instead they make false claims and in some cases they run a fake scan that takes only one or two seconds and then a message is displayed stating hundreds of malicious items have been found infecting the system. The user is then directed to download and purchase a program. While there are programs that are inefficient or very mediocre at removing malware, rogue programs do not even attempt to remove malware or improve system performance. In some cases they display more annoying advertisements or download more malware on to the system. Rogue software programs are very difficult to remove from the system. Some examples include:

> AntiVirus Pro, AntiSpyware Soldier, AntiVermins, ContraVirus, MalwareAlarm, MalwareBurn, MalwareStopper, MalwareWipe, WinAntiVirus Pro 2006, WinFixer, WinAntiVirus, WinAntiSpyware, SpyDefence, SpyCrush, SpyMarshal, SpyOfficer, SpySheriff, Spy Cleaner, SpywareStrike, SpywareSoftStop, SpywareNo, Spyware Vanisher, Spyware Quake, SpyAxe, Spylocked, SysProtect, ErrorSafe, ErrorProtector, Pest Trap, UltimateCleaner, Ultimate Defender, and Ultimate Fixer.

Getting Infected

In 1986, the first computer virus was released that altered the startup sequence. It was called “Brain” and it resulted in the infection of 360,000 floppy disks. The end of the 80’s was witness to the onset of the polymorphic virus – a virus able to change its binary pattern when replicating itself in order to escape detection. This kind of behavior resembles that of a thief changing fingerprints with each crime. Malware evolution continued with viruses that were using encryption and other stealth technologies designed to avoid detection and to cover up their location in system memory.

In these early days of computing there were only a few ways of getting hit by a virus. The most commonly used methods involved getting an email with a virus attachment or downloading one from a floppy disk. In 1989 the Internet Worm was released on to what was a vulnerable and immature Internet and resulted in bringing down 6,000 computers. Current malware schemes are numerous, elaborate, and are deployed on a worldwide scale. What began as random attacks with questionable motives became increasingly more sophisticated and targeted attacks.

In general, the infection of malware on a computer system can be narrowed down to two basic methodologies:

1. Deception: opening a malicious item without foreknowledge.
2. Exploitation: taking advantage of vulnerabilities in a computer system.

Getting Infected: Deception

Creators of malware are using clever tricks to lure users to download malicious software. Whether from an email, an instant message attachment, a newsgroup, or a website, there are many instances where a user downloads an item that could be harmful to the functioning of their computer. The bottom line – this is a trust issue. There are situations that require downloading files such as a driver for a hardware device, a codec for coding and decoding media files, or trialware so that a user can try or sample a program or game before purchasing it. When things are not as they appear, it could mean the difference between getting what is expected and having just installed a Trojan or a rootkit.

Pop-ups

One of the most common and annoying schemes involves having a window pop-up on the screen. Pop-ups can be advertisements or they can be part of a deceptive ploy. Unethical advertisers often create pop-ups with content relating to gambling or pornography. The content is adult-oriented and, in many cases, the ability to turn these off using conventional means is uncontrollable. When the user attempts to close the window, additional windows appear until dozens of windows are propagating themselves on the display screen. Even more troublesome is the occurrence of pop-up advertisements in the absence of any Internet browser. A more deceptive scheme involves trying to lure the user to click on the window by presenting some message such as: “Click here to have all media content displayed on this page”. By clicking the window the user has inadvertently begun an installation of malicious software. See the Solutions section on page 28 to find out how to deal with these.

The Email Attack

Of the methods of malware deception the most well used remains the email attack. In the past the email scam was very simple – there was very little wording and an attachment was included. In the early days of emailing there was no actual occurrence of spamming. Users felt that an email was from someone they had some familiarity with. Spam messages, those repetitive, unsolicited, and annoying emails from marketing sources, are a common occurrence. In recent days spamming has spread to blogs, instant messaging, web searches, forums, and even mobile phone messages.

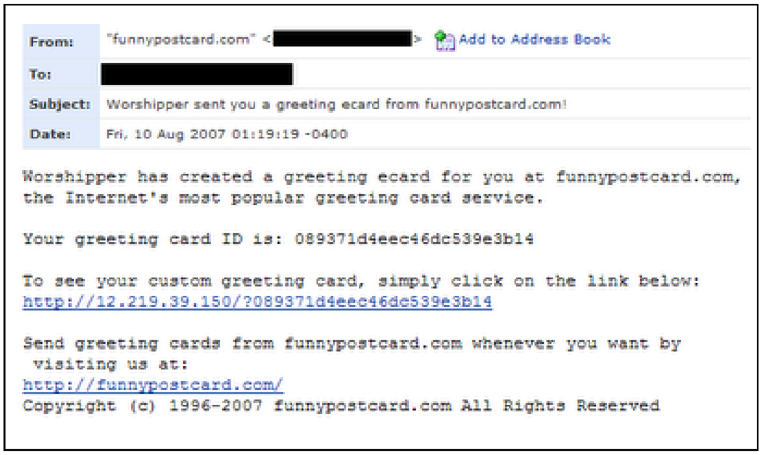
For malware creators, the effectiveness of spam, in and of itself, is likely not enough to achieve the desired outcome. For one thing there are filters that are designed to block out these intruders before they get to the recipient. Secondly, users are better trained to not open attachments – especially executables, files with an .exe extension. As a result, the deception has evolved.

Spam attachments have more recently been in a compressed format. These are known as “packed” files as they are compressed, or packed, with one or more files to compress the data so as to make it easier and faster to transfer and to upload and download. Unfortunately, packed files require specific programs to read them and, until the file is opened, the user cannot tell what it is. It is a jack-in-the-box situation. While using compressed file attachments is not as widely relied on as in previous days, it is still used and there are new techniques arising. For example, .rar files have been employed to bypass email filtering. These files can include very large files such as video or audio files.

Although email is handled more cautiously by users, spamming is still deployed in vast amounts. In one study[2], it was found that 66% of unsolicited commercial emails contain at least one form of deception. eWEEK reported[3] on some attacks use .rar attachments accompanied by “slick invitations to view pornographic content” to add to the success of the recipient opening the attachment.

> "Most of these are appealing to lustful young men. It's a game of percentages. This is just another way to get control of machines. It may hit fewer machines, but they're probably more technical users, so their machines would be of higher value. It's a good example of the fact that virus writers are probing every nook and cranny."

There are spam messages that can appear with MSN instant messaging. Some of these are cleverly disguised to be like that of a known contact and include a compressed attachment such as a zip file. Other deceptions such as fake e-cards are less blatant. In this one shown below[4], a link is included so that the curious reader will click something in order to view an online greeting card.



From:	"funnypostcard.com" <[redacted]> Add to Address Book
To:	[redacted]
Subject:	Worshipper sent you a greeting ecard from funnypostcard.com!
Date:	Fri, 10 Aug 2007 01:19:19 -0400

```
Worshipper has created a greeting ecard for you at funnypostcard.com,
the Internet's most popular greeting card service.

Your greeting card ID is: 089371d4eec46dc539e3b14

To see your custom greeting card, simply click on the link below:
http://12.219.39.150/?089371d4eec46dc539e3b14

Send greeting cards from funnypostcard.com whenever you want by
 visiting us at:
http://funnypostcard.com/
Copyright (c) 1996-2007 funnypostcard.com All Rights Reserved
```

[2] Federal Trade Commission; April 2003

[3] http://www.eweek.com/article2/0,1895,1756636,00.asp

[4] http://spywarebox.blogspot.com

This method of deception preys on new users who have likely taken up computer related activities for purposes of staying in touch with families and friends using email and greeting cards. In these instances a legitimate ecard site is often used along with some sender with a pseudo-name such as “worshipper”, “partner”, “a family member”, or “classmate”. Once the user clicks on the link they are directed to a site where malicious items are installed such as a Trojan remote access program.

Phishing

Another scheme that is even more elaborate in its method of entrapment involves using fake emails also known as “spoof” or “hoax” emails. The email appears to be sent by a legitimate source such as a trusted website from a business, bank, or e-retailer. In some situations the user is asked to enter login credentials including username and password. In other instances a link is presented and the user is taken to a “spoofed” or counterfeit website that appears very legitimate. These schemes are attempting to gain password or PIN information, debit or credit card numbers, social security numbers or bank account information so as to extort finances.

We recommend the following website for further information on email spoofing: http://www.cert.org/tech_tips/email_spoofing.html

While Phishing attacks do not typically involve installing malware on the computer system they are becoming a more prevalent form of cybercrime and installing malware while browsing to a spoofed website is also an outcome of the hoax.

Trojans

One of the most well utilized methods today for breaching computer systems involves Trojan malware. While emailing is the most common method of deception, Trojan horse schemes are the most invasive and harmful to the computer system. With Trojans the culprit malware items are smuggled on to the system by masquerading as a harmless application or program component. The most deceitful of these is a subcategory referred to as rogue software programs as described on page 9. Users download these programs based on promises to remove malware when in fact they actually download their own set of adware, spyware, or malicious code.

There are numerous classifications of Trojans. Some of these are categorized based on how they perform as seen with the following table.

Trojan	Description
Logic Bomb Trojan	This is activated based on certain conditions being met.
Time Bomb Trojan	This Trojan is activated based on a date or time.
Dropper Trojan	This type performs a legitimate task but also drops viruses, worms, or other malware on the computer.

Table 3: Classifications of Trojans

Trojans can further be classified based on the target and mode of attack. These include the following (their mode of attack is in brackets):

Trojan	Description
Security Disabler Trojan (Disables)	This Trojan disables security programs so as to render the system vulnerable. It is typically used in conjunction with another Trojan that delivers a payload.
Data Sending Trojan (Downloads)	After gaining access to the system, these items are designed to download sensitive data back to the malware creator including passwords, PIN numbers, credit card information, and more. Alternatively they can install a Keylogger and record the keystrokes that are entered.
Remote Access Trojan (Gains Control)	These are typically hidden in games or small programs and result in getting total control of the victim's computer.
FTP Trojan (Uploads)	This Trojan gains access to the computer and creates an access point by opening port 21. Once this occurs the system is breached and the attacker can connect using FTP (File Transfer Protocol) and then upload more malicious software.
Proxy Trojan (Spreads)	Proxy Trojans gain control of a user's machine and can involve fraud. The host computer is used as a proxy so that more attacks can be launched from the host.
Distributed Denial of Service (DDoS) Trojan (Floods)	As mentioned earlier, a DDoS attack floods networks with useless data and traffic so as to bring down the network. DDoS is covered in more detail on page 23.

Trojan	Description
Destructive Trojan (Deletes)	These are designed to locate and delete files from the system. They can erase, overwrite, or corrupt files.

Table 4: Major Types of Trojan Threats

Trojans can be dangerous and harmful in many ways. In the Solutions section on page 28 we will look at methods of combating these high security risks.

Getting Infected: Exploitation

The second general method of malware infection is through means of exploitation. For hackers, also known as “blackhats” or “crackers”, getting malicious code on the computer using exploitation requires knowledge of security measures and the means to effectively bypass them. Users are often uncertain how or when unwanted items and malicious software infects the system. We will look at two methods: “drive-by” attacks and embedded malware.

Drive-By Downloads

One of the most common means of contracting malware is by simply viewing Internet sites. A drive-by download occurs when an Internet surfer browses a web page and one or more malware items are downloaded without the consent or knowledge of the user. While there are many who feel this is likely exasperated or blown out of proportion, there have been studies done recently that depict the reality of this offense. First off, we can assume that the majority of web creators have no intention of downloading harmful or unwanted items to a visitor’s computer. However, no website or computer server is invulnerable to attack. Web pages can be sabotaged without the knowledge of the web master.

What are the facts related to malware hacks? In April 2007, BBC news reported that malicious software has doubled in the last year and that there is a rise in the spread of malicious code via the web. In the first quarter of 2007, there were 5,000 web pages being infected per day. The report goes on to say that 70% of the infected websites were actually legitimate sites but were infected by malware hackers. In a study performed by Google, 4.5 million web pages were analyzed and of these 450,000 were capable of drive-by download attacks and a further 700,000 were thought to contain code that could compromise a computer system. This means that one in ten web pages had some form of malicious code.

According to the University of Washington study mentioned above, out of 20 million Internet addresses examined, an average of one out of 62 Internet domains results in a drive-by download. One of the researchers, Hank Levy, stated: “If our numbers are even close to representative for Web areas frequented by users, then the spyware threat is extensive." He also said that: “For unsuspecting users, spyware has become the most 'popular' download on the Internet.”

JavaScript, a programming language, is required to view many of the rich-media items displayed on websites. Despite its popularity, JavaScript can be used by hackers to seek out vulnerabilities or to control computers. Hackers can use JavaScript and HTML commands to take down websites or to exploit vulnerabilities of the servers so as to leave them open to attacks. If you were to look at the website text code it may seem “garbled” but it could actually be the means of harboring malicious JavaScript commands. The reason is that certain characters, such as left tag “<” and right tag symbols “>”, are converted by the website or blog reader in such a way that all the text in between are treated as executable code. Seemingly garbled text can hide malicious JavaScript commands that can do damage without having to install or run an outside file.

An article by Computerworld (August, 2006), revealed that reading online blog articles can lead to picking up malware:

> “…users who employ Web-based services such as Bloglines or Web browsers such as Firefox to read Web site feeds and blogs are vulnerable to embedded malicious code that can install spyware, log users' passwords, scan PCs and corporate networks for open ports and more…”

Embedded Malware

Malware authors are seeking out and taking advantage of attack vectors. Attack vectors are entry points or a means of establishing access to a computer system. Exploitation of security vulnerabilities can occur in many ways. One example took place in New York where confidential information was stolen using public computer terminals. For a period that spanned over a year, a hacker named Juju Jiang sabotaged Internet terminals at Kinko stores in New York. He installed a Keylogger and successfully stole more than 450 usernames and passwords as the malware was designed to record all the keystrokes entered from the public terminals he had sabotaged. Once acquiring the necessary credentials he then hacked user’s home computers remotely and attempted to transfer funds. One potential victim watched as their computer began to operate seemingly on its own. Once the authorities were notified, Jiang’s activities were traced and he was arrested. Along with his known offences he also admitted to selling the stolen data online.

A study performed by the University of Washington, emphasizes the malware risk incurred from visiting and downloading files from popular websites including news, game, and sites focusing on celebrities. From their sample of 20 million web addresses, they found more than one in 20 executables included malware. While most of these were adware items, 14% of the malware files contained more malicious functionality. This technique, referred to as “piggybacking”, involves a malicious item being installed along with the intended legitimate program. This is particularly dangerous in that security programs such as anti-virus programs and firewalls are configured to trust the file being downloaded as valid thereby opening the door for malicious items to go undetected.

Recently adware creators have begun to embed advertisements within programs, also known as Adware bundlers. Once adware is executed on the system, it is difficult to trace how it got there as the ad appears unexpectedly some time after the installation. Spam emailing uses embedding techniques to escape detection from email filters. Instead of typed email messages, the spam message body is comprised of an image or wallpaper. Spam emails can also contain attachments with embedded malware in what are typically benign file formats such as .doc and .txt files (Microsoft Word document and Rich Text formats). When opening these files the user is shown some text asking them to click an item like an icon or graphic. This action results in having a Trojan or Keylogger installed on the computer.

There was a time that images were considered completely safe to download and this has proven to be false. Microsoft Windows has had issues with buffer overflow vulnerabilities (see Vulnerabilities on page 19). By rendering certain image formats such as Windows Metafile (WMF) and Enhanced Metafile (EMF), a remote hacker could have code execute on the system. In response, Microsoft made security patches available for the operating system and for Windows Picture and Fax Viewer.

The vulnerability of image files has nasty implications considering the many ways that these images could be rendered including within Internet Explorer or Microsoft Office programs such as Word, Outlook, and PowerPoint. Along with this there are numerous ways in which these files could be distributed such as web pages, email, or file transfers. Microsoft released a public bulletin[5] regarding the vulnerabilities associated with WMF. In this bulletin they stated:

> A remote code execution vulnerability exists in the Graphics Rendering Engine because of the way that it handles Windows Metafile (WMF) images. An attacker could exploit the vulnerability by constructing a specially crafted WMF image that could potentially allow remote code execution if a user visited a malicious Web site or opened a specially crafted attachment in e-mail. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Microsoft was not alone in needing to patch vulnerabilities related to buffer overflow exploits. In the beginning of 2006, a technical cyber security alert[6] was issued for QuickTime. In this report it is stated that the exploitation of the QuickTime "…vulnerabilities could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition." Users were recommended to upgrade to version 7.0.4.

Websites can be hacked for the purpose of controlling the website components. The Google study on page 15 speaks to the fact that hackers inject malicious code to web pages to control banner adverts and widgets. Widgets are small programs such as a calendar or web counters. In one instance the researchers discovered 50 different malware items downloaded after browsing to one site that was hosted by a hijacked server. When considering what can happen with a single point of infection and when factoring in the fact that a large number of websites are hacked daily so as to release a payload to would-be drive-by surfers, it is evident that a very real and growing threat is at hand. A report by the BBC (August 2007) reports that one organization had detected 5,000 web pages infected per day.

Tools of the Trade

There are numerous tools available that make it easy for hackers to combine and embed their code into other legitimate code. One could easily acquire Keyloggers, data stealing Trojans, or customized malware packages with update services (see E-Crime: Profit and Profile on page 24 for a cost breakdown of these items). There are also tools referred to as binders and linkers, or link editors. With binders and linkers, modules from an executable program can be combined with malware items.

[5] http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx

[6] http://www.us-cert.gov/cas/techalerts/TA06-011A.html

Binders are commonly known to hide malicious modules, such as a Trojan, by binding the modular code to a legitimate file such as a text file like Notepad. The Trojan runs at the same time without alerting the user or the system. There are also questionable tools such as Silk Rope and Back Orifice ("BO" for short). Silk Rope was described by its author as: "a down-and-dirty little wrapper for Back Orifice. It very nicely trojan-ized BO into a small collection of files that looked more-or-less harmless."

Back Orifice was designed for remote administration – a legitimate functionality for technicians who are servicing or assisting other users from a remote location. However, in the wrong hands it can be an open door that allows complete remote access to a user's system. It is known as a RAT client (Remote Administrator Tool) and when emailed to a user and installed, the remote hacker can manipulate programs, alter files, capture keystrokes, take screenshots, and even alter the user's settings. It was created by a programming group called "Cult of the Dead Cow" known for producing other hacking applications including SMB Relay, RasEnum, and PE Crunch. It has been designated as malware by the anti-malware community.

Vulnerabilities

Malware creators hone their skills in an effort to take advantage of security holes and vulnerabilities. By some estimates there are thousands of distinct malware variants being released per day. As stated by the SANS Institute (SysAdmin, Audit, Network, and Security): "Attackers are opportunistic." They set out to exploit the best known flaws with effective and widely distributed attacks tools like those mentioned previously. They are indiscriminate and rely on a portion of users not taking sufficient precautions.

Buffer Overflows or Buffer Overrun

This condition occurs when a program exceeds the amount of memory it is allotted and it overflows to adjacent locations. When this happens, malware authors can take advantage of a system flaw. In other words, a malicious act can take place to trigger a buffer overflow which then releases other malicious instructions. The data that flows over is going where it was not intended and the result can be corruption of data, program termination, or even a security breach. While buffer overflows were originally a concern when first appearing on the scene, this method has not, at present, been widely adopted by hackers. Time will tell if this becomes a more attractive venue of attack.

The SANS Institute released a report in 2005 on the most serious security threats. In the report they turn to the top experts on hacking techniques and security technology. According to the article, there was a 10% rise in the number of vulnerabilities. Despite the release of security patches and efforts to close potential attack vectors, there is still a rise in system and application vulnerabilities.

One of the experts, Ed Skoudis, is the author of Counter Hack and Malware and is considered the top instructor in the US on hacker techniques. When Skoudis was asked about the significance of a 10% increase he responded:

> “Quite simply, we are deploying flaws faster than we are deploying fixes. We think we're making progress, but we are barely scratching the surface of a mountain of underlying flaws, and a 10% increase, while not dramatic, is a sign that we are moving in the wrong direction.”

Skoudis was also asked to point out the greatest changes in the cybercrime and security field. He responded that hackers are adapting by altering their paths of infiltration. “In particular, they are finding and exploiting flaws in client tools, because a victim user inadvertently pulls malicious code into the system via items like web browsers, mail readers, newsgroup readers, and media players.”

SANS gathered a panel of malware and security experts and posed several questions related to system vulnerabilities. There are many salient points and cautions listed from this discussion:

- Attackers have the ability to modify or create audio files that can take control of a user’s computer after an audio file is downloaded and played.
- A shift has taken place from attacks on Windows systems to attacks on applications running on Windows. The targeted programs include management programs, backup applications, and licensing systems.
- There are vulnerabilities to media applications including iTunes and RealPlayer.
- IE continues to be vulnerable and exploited for its security flaws while other web browsers, including Mozilla and Firefox, are also revealing promising attack vectors. Browsers that have been less popular are getting the attention of attackers as their popularity increases.
- The number of machines turned into botnets is increasing and are being used to install spyware and adware.

How do attackers take advantage of system vulnerabilities? One key target is the one tool that connects us to the web – the Internet browser. Microsoft’s Internet Explorer (IE) continues to be the most used browser. In July of 2007, the percentage breakdown was as follows IE7: 20.1%, IE6: 36.9%, IE5: 1.5%, Firefox: 34.5%, Safari: 1.5%, and Opera: 1.9%. Not only is Internet Explorer popular with users, it is also a popular attack vector and a prime target of malware security breaches. One of the reasons for this is that it offers the ability for third-party programs to include their functionality. This is done with Browser Helper Object (BHO) technology. On the plus side, ActiveX content offers the ability for websites to use rich media content. However, malware attackers can take advantage of this open functionality. The trade-off for getting rich media content on the Internet is that a potential portal is made available.

Another prime target area involves account and user privileges. “Administrator” is the default account for Windows operating systems. As a result, hackers that gain access can make alterations to a system without needing any further authorization. Other user accounts have fewer assigned privileges and this lessens the ability for malware to make changes to a system. The Vista operating system, the latest operating system from Microsoft, addresses this issue by introducing User Account Control (UAC). There were early reviews and criticisms of this functionality pointing to the excessive prompts for administrator credentials even when performing routine file operations.

Rootkits

Those who have heard of rootkits are likely well aware of malware technologies, or Unix systems, or may have heard of the Sony BMG Music Entertainment news story. In 2005, Sony BMG was found to have used rootkit technology. Their intent was to use sophisticated technology with their music CD’s as part of a Digital Rights Management (DRM) system. In other words, rootkit technology was used as a means of copy-protection. The issue with this is that rootkits use cloaking technology and can be utilized by blackhats to hide malicious software. After legal suits were filed, Sony BGM provided a workaround for users made available from their website.

The term “rootkit” comes from the words “root access” or administrative access, and “kit” a Unix term for tool. Rootkits were first created on Unix systems. Originally they were a programmatic tool designed to replace standard tools with a version that gave specialized privileges to a particular user group and allowed their activities to remain hidden from other users. Rootkit technology can hide items including any associated resources such as files, system objects, registry keys, ports, drivers, processes, and more. By masking the activities of these items, malware activities can escape the detection of standard and less capable security and diagnostic tools. One example of this is the ability of a rootkit to cloak its processes from the operating system.

There is a relationship between rootkits and other types of malware programs. Some malware can be used to first install a rootkit to the computer system and then the rootkit can be used to mask other malware items. While rootkit technology has been around for more than a decade now, many feel that it is new because of recent attention given to it. Rootkits can infiltrate any platform including Unix, Linux, Macintosh OS X, and of course Microsoft which typically gets more focus from malware as it has a majority of the market share.

Microsoft and eWEEK have published reports about the prevalence of rootkit threats. Based on their studies, anywhere from 14% to 20% of all malware is rootkit related. There is positive news about rootkits – they are on the decline according to Microsoft and data from security software tools. This could be a result of the anti-rootkit technology that has been introduced of late. However, Microsoft states this trend “bears watching” and that “high-value entities” could be the target of attacks.

Botnets

There has been a recent trend related to infecting and controlling computer systems. Sabotaged computers become part of a collective known as a “botnet” and can be used to accept commands from the “botnet herder”. An article by eWEEK in the fall of 2006 described this phenomenon in some detail. The infected computer, also known as a “bot”, is seeded with malware code using similar techniques as previously stated in this report. They can be covertly controlled from a remote location. There were over four million computers during the first six months of 2006 that were infected and utilized as part of a botnet army of sabotaged computers. It was discovered by Microsoft, in this same period, that these millions of computers were controlled with variations of malware designed as backdoor Trojans and other bot code. There were more than 43,000 variants of bot coding.

A botnet can include a wide array of computers that use multiple operating systems including Linux and Macintosh OSX machines. The reason that botnets can be indiscriminate of the operating system is that the attack vector is typically a flawed third-party application. With a botnet infrastructure the hacker controlling the botnet can access the infected systems simultaneously through an Internet Relay Chat or some other Internet chat technology. Instructions are given to propagate malware upgrades to maintain resistance or diversion from anti-malware systems. The remote attack can lead to the installation of malware such as Keyloggers to attain credentials.

A bot can be instructed to perform spam attacks. In this way the hacker creates a buffer that serves to maintain stealthy and covert activities. In effect, computers in the bot army are turned into spam servers. The owner of the computer may not even be aware that their machine is sending out thousands of email messages.

Spamming is not the only service rendered. Once a computer is turned into a bot it is a zombie and can be utilized in any way the hacker chooses. For example, the bot could be used as a host to store data that is contraband such as child pornography. Another well known use is to have the bot take part in a Denial of Service attack or Distributed Denial of Service attack (DDoS).

In a small scale DDoS attack, proxy computers can run code referred to as an exploit. Typically it is a single point of attack which can be a means of disrupting a competitor's online service resulting in denial of operations. With other situations, it can be more criminal in nature. For example, botnets can be used so that the 'zombafied' computers commit the crime. There is a known report of one DDoS attack by Russian hackers where hundreds of thousands of computers were infected so as to be part of a botnet collective. The hackers then utilized the combined bandwidth of these machines by having them browse to a single website which would overload it. The hackers targeted businesses in the US and the UK that relied heavily on online sales and they demanded a ransom be paid or denial of services would continue. In the end, these criminals were able to gain over four million dollars.

There is an ongoing competition for bot computers and herders actively protect their flock. There are instances where hackers will remove other malware items that are simply annoying. The reason for this is that they do not want the user to install anti-malware applications which would put their malware in danger of being detected. This was the case with the dueling spyware creators, Direct Revenue and Avenue Media. Direct Revenue, an adware company, created the ability to delete instances of competing malware on a user's computer so that the system would not slow down too noticeably and cause the user to take action. Avenue Media, one of the competing spyware creators, filed a lawsuit and in the end the two companies agreed to not disable each other's products. One has to wonder about the justice system working to resolve the unethical practices of companies such as these.

What is of more importance than the fight for control of sabotaged computers is how the systems are manipulated as the botnet herder sees fit. To recap, it could be to lower security settings so as to exploit the system further, to host child pornography, or to take part in click fraud. With click fraud the bot is instructed to click advertisement links so as to generate a “charge per click” where advertisers pay money each time a user clicks on the advertisement.

Another well known example of a DDoS attack involved a credit card processing company called Authorize.net. Prior to the attack the company was given mail notice that they were to be attacked. When it was carried out as promised customers were unable to perform transactions for up to a week. Considering a large corporation could be brought down using cybercrime techniques such as this, malware hackers have gained a greater sense of confidence when setting their sites on an even less secure victim – the individual user.

E-Crime: Profit and Profile

In days gone past, the motivation behind malicious computer activities, such as virus infections, was obscure and commonly thought to be vandalism or mischief. It was a way for savvy computer technologists to show their technical prowess by gaining entry or affecting some system control. Today’s hackers and blackhats are motivated by monetary gain. A computer crime and security survey[7] found that of 530 firms surveyed, 75% reported a loss from cyber attacks that totaled losses of over 200 million dollars. Theft of proprietary information was the greatest of these and next was loss due to denial of service attacks which increased substantially from the previous year. The majority of those surveyed (78%) stated that the Internet was the most frequent point of attack.

According to a consumer report by the Washington Post (August of 2006), consumers paid more than 7.8 billion over a two year period for repairs or replacing computers as a result of virus and malware infections. While this number could be inflated, the report went on to cite a finding made public by the Federal Trade Commission in 2005: “Internet-related complaints made up nearly half of all fraud complaints received by the Federal Trade Commission in 2005, with people claiming losses of $335 million.” Phishing scams, as described previously on page 13, increased five-fold and totaled $630 million in 2004 and 2005. This comes out to an average loss of $850 for each incident.

[7] Computer Security Institute (CSI) and the FBI; 2003

Malware attacks today are profit motivated. Malware authors target the general public, governments, businesses, and even the stock market in order to derive some financial gain. Stock market cybercrime is referred to as a “pump and dump” scam where stock prices are artificially inflated so that unethical speculators can sell off stock when the price is pumped up. In recent years, pump and dump spammers have increased their efforts to the point that one third of all spam is related to hot stock tips. Most often the penalties and sentences are lighter for Internet offences.

Cybercrime can be thought of as an electronic black market. Less criminal activities form a type of “gray market” and include utilization of adware and other forms of malware to promote advertising. Malware authors involved in this gray market use unethical and deceptive means such as unfair and convoluted EULA’s (End User License Agreements), piggy-back installations, rogue applications, and the like. The risks are low and the rewards high; a prime condition for crime. Email spamming is an excellent example. If a single spammer can send out millions of spam emails in a day, it can result in some percent of the population responding. Even when a small percent of the population responds, the spam attacker can make thousands of dollars a day (see page 27). If using a botnet, they can also avoid detection.

These activities are being normalized in the cyberworld. A report by Maksym Schipka[8] states that the malware world of today is not fuelled by organized crime. Instead it resembles the retail industry.

> It is clear that there are individuals who can produce exploits/trojans/RATs and other malware and sell them to those who need them, there are also people who hunt for or can produce good quality (often very well verified and well structured) lists of virtual and real identities, and there are those who buy the products and services from the above two and either benefit from them directly or resell the ‘service’ to third parties, such as dubious marketing agencies who, in turn, use those ‘services’ to ‘help’ their clients.

So this is not organized crime and there is not an underlying hierarchy that characterizes organized criminal activities. Malware authors create their wares for a variety of purposes and for varying fees. Creating a Keylogger could incur a fee of $300 and a high-end Trojan that steals confidential information could come at a cost of up to $3,500. There are occurrences of customized malware for targeted attacks with a price tag of tens of thousands of dollars. The Schipka report also refers to update services offered by the blackhats where fees range from 5 to 60 dollars per update and even include a service agreement so as to ensure speed and quality of the service.

[8] A Road To Big Money: Evolution Of Automation Methods in Malware Development

Known Deceptions

In most cases, it doesn’t take a superior knowledge of computer programming to create these attacks. An ordinary hacker can obtain malware tools from freely available sources and can then exploit vulnerable systems both at the individual user and enterprise levels. The attacks are carried out using increasingly covert means and are targeted at individuals and small groups so as to escape detection and to prey on the weakest links of the security chain. In many cases these attacks prey on those that are trusting or can be seduced into the possibility of receiving money.

One of the most well-known examples is the Nigerian fraud letters which originally began with mail and then evolved to faxes and emails. There are over 2,000 variations of fraudulent emails that promise lucrative rewards or declare a sense of urgency so as to gain banking information or donations. Victims include individuals, businesses, and charities, as well as government and learning institutions. Another example involves “advance fee fraud” and can impact those who participate on Craigslist and eBay. Scammers use a fake cashier’s check to pay for the goods. Stolen or forged credit cards are also used. Other instances of eBay scams include phishing attempts where PayPal customers are informed that their accounts are about to expire and they need to update their confidential information immediately.

Hackers also take advantage of high profile and world events. When there were severe storms in Europe blackhats sent out emails with a subject line of: “230 dead as storm batters Europe.” This was referred to as the Storm Trojan and hundreds of thousands of the spam messages were delivered. The users who opened the email became the victims of this storm when a backdoor Trojan installed to their computers and stole data or sabotaged the computer to turn it into a spam server bot. Another high-profile event, the Super Bowl, lead to three websites associated with the venue, being hacked. In these attacks a JavaScript file was hidden in the front page header of the websites.

One of the largest spam attacks occurred in April 2007 and hit email recipients with a subject heading of: “Worm Alert!, Worm Detected, Spyware Detected!, Virus Activity Detected!” With the email came a compressed zip attachment that was the software patch. To make the scam even more convincing, the zip file is password protected and the required password is given in the email. When the file is opened a rootkit is installed to cloak the malicious activities and then system security is disarmed, confidential information collected, and the computer is turned into a bot. Almost 5 million copies of what is known as the Storm spam were launched within a 24 hour period.

Web browser vulnerabilities exist and malware creators are continually probing for vulnerabilities. Frequently, websites that have been poorly coded or have not been protected with the latest patches fall prey. The defacement of the site involves attacking the host server and replacing or altering the index page with a hacked one. The user visits what they think is a legitimate website with a sense of security due to an established sense of familiarity associated with the site only to be infected with malware. This is an easy method for hackers as they do not have to create a fake website. As a result, the rate of sabotaging popular websites is increasing.

To this list of examples we add one final hacking scheme to provide a clear cost/benefit breakdown. This instance is also noteworthy in that the hack involved gaining write permission to the index page of many sites with one hit. In June of 2007 there was an MPack attack that compromised more than 8,000 Italian websites. Of the sites affected, 90% were hosted by the same company. The invisible malicious code redirected visitors browsing on the pages to an MPack server. MPack, also known as “Webattacker II”, is a malicious software package that sells for about $700. If browser security is insufficient and the exploit is successful, a customizable Trojan is installed on the victim’s computer. As stated in a report[9] by Guillaume Lovet, “the attackers crafted a botnet of 10K in a blink” and utilized a strategy that involved a minimal amount of human resistance. The cost breakdown from Lovet assumes 10,000 computers used for spam relay purposes each sending 100,000 emails and receiving .03 cents from advertisers per email. For attaining the software and contracting the hacking services the costs would be close to $10,750. From these figures we can determine what the spammer stands to gain:

10K (infected computers) x 100K (emails) x .0003 = $300,000

Undetected Malware

The focal point of this paper has been one of security. However, from an individual user perspective, next to financial loss and security breaches there is a secondary concern, the loss of performance brought about on the computer system. Malware items not only bog down system functioning but in some instances can leave the user helpless or susceptible to system errors and crashes. Quite often this can be the only clue of malware items taking up residence on the system. While some performance degradation may be from

[9] Menace 2 The Wires: Advances in the business models of Cyber Criminals

installing and uninstalling applications, there is an increasing frequency of degradation due to excessive files downloaded to the host computer.

Aside from the build up of day-to-day clutter accumulated from online activities and from the disorganization of large quantities of stored files, one has to take note of other associated risks that could be the cause of slow down and crashes. While any operating system can be a target for malware, it has been estimated that Microsoft Windows systems face five times the number of malware threats. These systems have suffered countless security exploits from hackers. There have been studies[10] that reveal how quickly these systems can fall prey to security compromises. Studies also point out that there are numerous malware items on computers that go undetected by the user. In the 2004 America Online and National Cyber-Security Alliance study, 93 malicious components on average were found on 80% of the computers in the study group. Of the participants in the study group, 89% were not aware of the condition of their computers.

Solutions

To avoid being a victim of cybercrime, it is essential to take the right precautions. There are general and specific measures presented here. We will begin with specific solutions and then turn our attention to best practices.

Phishing Attacks

Phishing attacks are a worldwide phenomenon. There has been a great deal of sophistication and diversity with these attacks. A wide-array of customers from financial institutions and online service are targeted. For example, there have been MSN phishing scams where the user is directed to what looks like a Microsoft site and asked to enter credit card information for verification purposes. In order for these attacks to work, confidential information has to be entered.

[10] For example, the study: “Automated “Bots” Overtake PCs Without Firewalls Within 4 Minutes”

There are bank institutions that have security information and warnings in place to inform their clientele.

Note

Never disclose your password(s) to anyone, especially online, not even to the police, your financial institution or your Internet Service Provider. Check your bank's security policies and public warnings and take action when you do come across dubious emails by contacting your financial institute.[11]

If you are directed to a site that looks suspicious you can look for a number of tell-tale signs of fraudulence. Begin by taking a close look at the web URL that is listed in the top address bar of the Browser. You can ask yourself: "Does this web address appear forged in some way? Are there misspellings?" Some spoofed sites will use two letter v's in place of a "w" as can be seen here: www.bankofhavvaii.com. Second, can you change the address and go to the home page? Try to truncate the end of the address by deleting the last part. For example, if the address is: "http://www.MyBank.org/ExpireWarning.html" you can change it to "http://www.MyBank.org/" and it should take you to the home page with active links and buttons.

Drive-by Downloads

It is essential to maintain caution when browsing the Internet. Adult-oriented websites often have pop-up windows and become an easy avenue for unauthorized installation of malicious items. Having the necessary web browser security, firewall protection, and anti-malware security software is essential. The following sections speak to this in more detail.

Note

Another way to avoid installation of malware is to not interact with any pop-up windows that appear. Safe computing includes disabling pop-ups from appearing by adjusting the browser settings.

With Internet Explorer version 7, you can do the following:

1. Click **Tools | Pop-up Blocker**.
2. Select **Turn On Pop-up Blocker**.

Even with these settings, there may be instances when a pop-up advertisement gets through. Do not click on it. Even clicking the X in the top right corner can cause it to self-replicate. Instead, do one of the following:

- Press the key combination **Ctrl** + **W** to close the window, or

[11] This warning notice is one provided by TDCanadaTrust.

- Press the **Ctrl** + **Shift** + **Esc** key combo. Windows Task Manager appears and you can select the pop-up window in the Applications list and click the **End Task** button.

Rootkit and Botnet: Prevention

As rootkits and botnets are difficult to detect, your first course of action is to assess if something is wrong with the computer. Is it behaving strangely? For example, it could be generating a lot of online traffic communications without any user intervention or it could be significantly slower than when it was first purchased. It could be displaying advertisements or pop-up windows. We suggest that you examine if there are any running processes on the system that look suspicious.

While there is an onboard Microsoft utility for this (Windows Task Manager), we recommend using a more advanced and free application called Process Explorer.[12]

If suspicious items are running in the background and are utilizing system resources, an anti-malware application can be used to remove the items. An effective anti-malware package has the ability to both detect and remove items residing on your system and will also include the ability to detect if an item is downloading to your system in real-time. ParetoLogic Anti-Virus PLUS is a tool that does all of this and continues to update its database so as to stay current with the latest variants of malware that are created and released. The ability to identify and analyze computer system activity carried out by malware offenders is pivotal in bringing about system security.

Be Secure

Even when rootkits are detected, it can be very difficult to remove them completely. They are like a weed that gets pulled out but the roots are still deeply embedded and parts remain. Rootkits can infect a system at the kernel level – the lowest level abstraction layer that is the central component of the operating system. While some Trojan malware items can be removed, the rootkit portion may stay resident. Your best option is to use proper security measures from the start.

[12] Download at: http://www.microsoft.com/technet/sysinternals/utilities/processexplorer.mspx.

Firewall: Use a firewall to protect against invaders and hackers that attempt to gain access. The best protection is a firewall that is a combination of software and hardware technologies.

Security Updates: Perform regular checks for any security updates offered for your operating system. You can get security updates from Microsoft from their Download Center or through their updates utility. Microsoft releases security patches on the second Tuesday of each month or whenever critical updates are required.

With the introduction of Windows 98 came the Windows Update service. If your computer has not had many of the security updates that are available, you will need to set aside some time to complete this process. Once you have caught up with all the security updates that are available, any new updates will only take a few minutes to install. To do this you can go to the Start button and select the Help and Support option. In the “Pick a Task” section, choose the Windows Update option.

Browser Settings

Check your Internet Browser settings to see that they are sufficiently secure. For example, with recent versions of Internet Explorer you can do the following:

1. Click **Tools** and select **Internet Options**.
2. Click the **Security** tab.
3. Adjust the Security level slider so that it is set to **Medium-high** or **High**.
4. Click **Apply** and then **OK**.

By altering your settings you can accept only as much web content as you want downloaded to your computer. Check your browser settings to find out what options are available. Another option is to use third-party applications to filter out unwanted material.

Be Smart

Now that you have a more secure system you want to avoid testing the limits by using sound practices based on common sense.

Safe surfing

While any websites is vulnerable to being hacked, it remains common knowledge that sites containing adult-oriented content have a high likelihood of malware infestation. Studies reveal that the sites posing the greatest risks for piggybacking malware are those providing pirated software such as warez sites where items are offered in violation of copyright restrictions, followed by game and celebrity-focused sites, and pornographic websites. Not browsing to these web pages is the first step. You can also use a browser that is less likely to have security risks. Internet Explorer is the most popular web browser (as described on page 20) and is highly targeted by hackers.

Another good computing practice involves the regular removal of temporary files and unwanted clutter from your system. Resident files such as web cookies can be a concern as depicted on page 9. You can turn off cookies in your browser but this disables the ability to view some websites. ParetoLogic Anti-Virus PLUS detects cookies that are suspect or needing to be removed. Scan results display a list of cookies and other detected malware items as well as a corresponding threat level – low, moderate, or high. Another valuable application we highly recommend is ParetoLogic Privacy Controls. This tool detects temporary files stored on your system, enables you to permanently deletes files using overwrite technology, and even removes traces of history for the purpose of privacy and confidentiality.

Cautious Computing

Having a safe and secure computing environment does not necessarily ensure computer safety. Safe online practices include being skeptical. Users on a MacIntosh system can be tricked by a Phishing attack. Be cautious and do not feel pressured to enter information or click on anything that you do not feel is required. Download and open only the files that are from trusted sources. This might mean doing some research about the program or the manufacturer. Keep in mind that Rogue software can be very misleading and well disguised.

When you decide to download an item choose only the software you want on your system. During installation, if you do not want all the extras that are bundled with the software program, pay attention during the installation steps. Good programs will include the ability to install only what you want. In other words, there should be options to disable the program from installing to the Startup folder, to not include any Internet browser objects for the toolbar, and to not have any third party items added during the installation. Take the time to install applications and to even read the license agreement if you feel suspicion is warranted.

When it comes to emails, do not open email attachments that are from a non-trusted source and open only emails that are safe and from a known sender. Delete emails that are spam or, better yet, use a product that handles spam attacks. ParetoLogic Spam Controls integrates with the anti-malware application or can be used separately. By cutting down on the success of spam, dubious marketing ploys lose their effectiveness.

Be Able

Once your system is well armed and you are practicing cautious computing, you can take the next step of being prepared and able to recover from the worst situations.

Perform Regular Backups

The more recent Microsoft operating systems offer automated backup functionality. You can go to the Microsoft site to find out more about it for XP Home edition.[13] This utility is not included by default when you first start on an XP Home computer. When you set up the backup you need to choose what to backup and where to store it. We recommend using an external drive. These hard drives are very affordable and can store large amounts of data which is especially useful when dealing with vast quantities of media files. Frequent backups to previously backed-up files can be tedious. We suggest using a very handy tool offered for free by Microsoft. The tool is called SyncToy[14] and provides the ability to compare and then synchronize your back-up files with the more recent ones.

Security Tools

A good security application creates back up files every time items are detected and removed. In the case where an item is falsely identified or a required file is missing, you should be able to easily restore from back-up files. Ensure that the software programs you are running can reinstate backups. You can also determine if your operating system supports System Restore functionality. For example, XP has a Help and Support section which includes a System Restore service.[15]

[13] http://support.microsoft.com/kb/320820

[14] Do a search for SyncToy at: http://www.microsoft.com/downloads/

[15] See: http://www.microsoft.com/technet/community/newsgroups/faqsrwxp.mspx.

Cyber Reality

Our reality is that we are “living in exponential times”.[16] There are over 200 million Internet searches performed each day – 6.4 billion per month.[17] There are more text messages sent and received each day than there are people on the planet. Fiber Optics technology has exceeded the ability to transmit 10 trillion bits of data per second. This is the equivalent to about 150 million simultaneous telephone conversations.[18]

These facts are collected from online sources. We look to the Internet for facts, for current and quick information, for shopping and online transactions, and for pastime pleasures and interests. Web 2.0 is the next generation of online computing offering integrated applications and services. With all this exponential growth in technology what can we expect from cybercrime activity?

> Today, the profits generated by cybercrime worldwide are somewhere between $50 billion and $100 billion per annum, flirting with the revenues yielded by the ‘historic’ business of trading illegal drugs.[19]

Given the ongoing sophistication and evolving nature of malware technology, these new online tools are subject to exploitation and the fight between blackhats and anti-virus creators, also known as “whitehats”, is becoming more heated. There are hordes of malware threats at the disposal of malcontents and shrewd, unethical software programmers. These malware instruments range from those that are fairly benign (web cookies), to ones that are annoyances (Adware and Browser Hijackers), to those that are security risks (Data Miners, Keyloggers, and Trackware). The most dangerous of these are those that lead to financial loss and are criminal in intent including DDoS attacks, pornography Dialers, Remote Administrators, Ransomware, and Trojans.

Ironically, the sophistication of these malware programs has advanced as a result of attempts to avoid detection and to remain stealthy from anti-malware tools. In some cases this may not mean using new malware technology but recycled technology in new ways or creating diversion tactics and swift deployment of infestation. As technology improves to detect and remove these items, malware authors modify and create new variants and find new attack vectors.

[16] Shift Happens, Karl Fisch; February 2007
[17] http://www.nwgusa.com/markenwg.cfm; November 8, 2007
[18] Fiber Crosses the 10-Trillion-Bit Barrier; Technology Review; March 2001
[19] Menace 2 The Wires: Advances in the business models of Cyber Criminals; Guillaume Lovet

Cyber-criminals continue their assault. Effective means of protection has to include "live" security practices. That is, anti-malware and security software must actively respond to current threats and leave system control in the hands of the user rather than involuntarily being recruited in the ranks of a botnet. In other words the computer performs and behaves as it did when it was first started. Our reliance of computer technology necessitates investing in ongoing measures to maintain secure and safe computing. One could derive the following equation to summarize:

> A new cyber reality + an ongoing malware pandemic = an unprecedented need for technological security.

ParetoLogic is dedicated to the creation of solution software that provides peace of mind. The clearest course of action is to use an informed choice and to take advantage of effective and reliable safeguards.

See the following page for a list of ParetoLogic products. Included in this list are links that will take you directly to a site for more information about each application and a download button so that you can try out the product.

ParetoLogic – The Products

ParetoLogic Anti-Malware Products; these tools provide easy and efficient methods of finding and removing unwanted and malicious computer items. To download and try out a free scan of the products follow these links:

ParetoLogic Anti-Virus PLUS
http://www.paretologic.com/download/antivirusplus/

ParetoLogic Anti-Spyware
http://www.paretologic.com/products/paretologicas/

ParetoLogic Anti-Spyware with Spam Controls
http://www.paretologic.com/products/paretologicas/plus_spamcontrols/

XoftSpySE Anti-Spyware
http://www.paretologic.com/products/xoftspyse/

XOFTspy Portable Anti-Spyware (for U3 platform USB drives)
http://www.paretologic.com/products/xoftspypa/

ParetoLogic Security and Performance; products in this category are for security and for recapturing power and performance for your computer system.

ParetoLogic PGsurfer (Free)
http://www.paretologic.com/products/pgsurfer/

ParetoLogic Spam Controls
http://www.paretologic.com/products/spamcontrols/

ParetoLogic Privacy Controls
http://www.paretologic.com/products/paretologicpc/

RegCure Registry Cleaner
http://www.paretologic.com/products/regcure/