Global Information Assurance Certification Paper

Alas for Adware – We Know It Too Well

A Thesis Of The Nature of Adware In Practice

By

Arthur W. Stephens

Respectfully submitted Friday, April 15, 2005, as Practicum
in partial fulfillment of requirements for:

The GIAC Security Essentials Certification

The SANS Organization

(http://www.sans.org)

© SANS Institute 2000 - 2005 Author retains full rights.

– Contents –

– Prologue –

In doing a favor for a friend, I booted up his pc. He'd complained that not only was he was having trouble "navigating" any of his programs, but that I could just forget any Internet access; Internet Explorer refused load his default web page in any event. It took 10 minutes from login to complete desktop resolution as all of the "ware" added to his computer rose like so much backed up electronic bile into RAM, as well as all over his screen in the form of pop-up windows, many of them blank.

My initial thought was that his computer was badly virused; he insisted, however, that his anti-virus software was up to date. When I was able to look in "Add/Remove Programs", I counted over 68 items, the existence of which my friend was at a complete loss to explain. After asking some probative questions, it came out that he had been doing some shopping online, along with downloading .wav files to play on the pc, and had also been inspired to install a program from a website that purported to be both an effective "pop-up blocker" and "internet browsing speed enhancer".

The above described scenario occurred roughly two years ago, and no adware removal tool that I could readily find at that time would even load, let alone remove any of this cyber-garbage. (His virus definitions were less than up-to-date, I might add, and refused to function, even when I tried to put the new definition files in the appropriate folders by hand, reboot, and initialize the software.) His computer had been indeed reduced to a simple stone.[1]

From that time to present, essential distinctions between both definition and behavior of "malware", "spyware" and "adware" have been rendered effectively immaterial. What with bundled (or P2P software,) e.g. Kaazaa, "Browser Experience Enhancing" software, e.g. Gator/Claria, Trojans that act as relay stations, worms that propagate via Trojans, remote code by which people hack computer systems from a tertiary computer, (e.g. via RATs,) what results are seemingly only two general classifications of threat as far as the end-user/IT industry are concerned; "active" and "passive".

Active threats are hereby defined as deliberate hack attempts that are thrown against the firewall/antivirus, IDS (Intruder Detection System) perimeter protection, (or in the corporate environment, through users covertly, deliberately circumventing these defenses from within, i.e. an "inside job",) and the "passive" threat of users who unwittingly download all manner of preprogrammed sewage onto their computers via web-driven email, web surfing, file sharing, and online shopping.

Following, we will review the threats themselves, and then proceed to analyze the environmental conditions surrounding them and contributing to them, including the legitimization of some types of these threats by corporate litigation and governmental legislation. Once accomplished, based on the evidential material obtained from these analyses, this paper will consider methods to at least mitigate, if not outright solve the inundation by these pests of the internet computing environment in which we exist.

[1] From "Computer Haiku", http://www.funny2.com/haiku.htm

– Pathogenesis –

Defining our terms from the outset; "Adware is [at its most benign] any software that is supported by advertising revenue."[2] It is designed to advertise products and services to people "located" on the internet via an electronic proxy; specifically their computer. It is designed to do this only on computers and nowhere else, e.g. not on the television, radio, or any other medium. (I promise that this excruciatingly obvious statement is worth reinforcing. I'll get to the point eventually.) Spyware is specifically designed to gather information and report on it to someone other than the person being reported on. It "snoops" around for information stored in any number of programs loaded on to a given computer. The importance of this information, from the most insignificant to the most confidential is, for purposes of the general definition, immaterial - though absolutely critical when gauging severity of repercussions to the user resulting from the behavior of said spyware.

Malware programs are so called due to their propensity for not merely information gathering, (malware clearly can be spyware, as will be demonstrated,) but also because the presence of it by definition corrupts or degrades in some form the computing environment in which they are loaded. This corruption can take the form of any of the following general aspects; the computer can be used as a relay node for distribution of harmful software or illicit activity, it can allow egress to the computer from someone that has no right to access of said machine for any reason, or it can outright destroy the software, degrade the integrity of the information stored in the computer, or ultimately cause the computer to cease to function at all. Thus, malware are usually categorized by how they spread, and where they "live" in the host OS.[3] One of the best definitions of the noun "malware" is that it codifies:

> "...a blanket industry term used to describe the variety of "malicious software" that is in circulation around the world. The definition includes viruses, worms, Trojans, computer "bombs", and other forms of intentionally destructive software, as well as annoying but generally non destructive software pranks."[4]

Even now, the above described can be differentiated from the classic computer "virus", in that, at it's most basic, a computer virus: "is simply a self replicating computer program that can "infect" other computer programs."[5] What is more:

> "Note that the definition doesn't actually require a virus to cause any

[2] "Spyware, Adware, and Peer-to Peer Networks – The Hidden Threat to Corporate Security" Kevin Townsend, April 2, 2003 http://research.pestpatrol.com/Whitepapers/CorporateSecurity.asp.
[3] www.pcmag.com/article2/0,4149,34058,00.asp "Know your enemy", Brett Glass, ExtremeTech
[4] LabMice.net "Computer Virus Primer for Network Administrators" 11/13/2003 http://labmice.techtarget.com/antivirus/articles/avprimer.htm
[5] Ibid

> damage, and many don't. In fact, a virus's ability to replicate itself and spread to other computers often relies on its ability to stay undetected. The more malicious and destructive it is, the more attention it draws to itself, and the more likely it is to be discovered and eradicated. Successful viruses try to stay undetected and replicate themselves as much as possible before actually delivering their final payload."[6]

"Proof of Concept" viruses definitely fall under this distinction, as they are typically written as academic exercises merely to exist, as opposed to cause harm. It is reasonably obvious, however, that even a comparatively non-destructive virus, (remember "Wazu"?,) clearly falls under the definition of a "prank", and that the ultimate "[delivery of the] final payload" of a non-humor oriented virus can be devastating; therefore all viruses are "malware" for purposes of this discussion.

A comparatively new and insidious cousin to the above is that of Phishing; i.e. social engineering designed and executed with the sole purpose of gathering confidential information on the level of the most insidious spyware without requiring spyware to be loaded on a target computer. It is also apropos to include other social-engineered fakery - which has been around for quite a while - that targets unsuspecting users to trick them into actively damage their computer, without any malware or the like having had to have been installed. Both of these conditions can be generally termed computer scams, or hoaxes. Entire sub-sites are devoted to hoaxes, and can be found on any and all anti-virus or computer security websites worth the name. Phishing and hoaxes will be discussed presently.

Following is a brief discussion of the of cyber-pest taxonomy, starting with an oldie but a baddie, the virus; (if you wish to skip what is basically a definition of terms, the next section starts on page 8. Some observations about the behavior of viruses and other malware are made in this section as evidential material toward discussion of adware, and cited later in the paper, however.)

Before things were all so complicated, one usually "got" a virus from booting one's computer from an infected floppy disk, or from the old-style BBSs. These days it seems all that you need is an active, unprotected internet connection, or as is equally likely, some close, trusted friends with active and unprotected internet connections. Or their friends and family...

There are five very basic classifications, (past the subphylum of internet malware,) of viruses per se; boot sector, file infector, macro, retro and multi-partite.[7]

Viruses must be introduced into the environment of computer software in some way. The definitive aspect of a virus of any sort is that it is a program introduced covertly, and certainly therefore against the intention of the targeted user's computer. Further, it is designed to replicate itself by insinuation into existing code and thereby "infect" other

[6] Ibid
[7] Ibid

files in the computer. The virus can be programmed to be triggered by some condition or event. It can be linked to a certain time, date, key stroke, opening a particular file, etc., and the "payload" results of the virus when activated. Not all viruses contain a payload per se; in some cases, again, and example is that of the "Proof of Concept" virus. They are an exercise in coding.

Their more malicious siblings, beginning with Boot Sector, and Latent viruses, usually do something, either for fun or toward some other purpose; often to compromise the computer and software environment into which they have been loaded. (Boot sector viruses were more frequent earlier in computing history when floppy disks were a principal source of information exchange, as cited above. Even though floppy disks are practically defunct, it would be rash to assume that therefore boot sector viruses are becoming less of a threat, particularly with the advent of the disk on key.) Further, boot sector viruses were not necessarily file infectors. Latent viruses simply "hide out" until an event awakens them to action. The "Sparse infector" is a subset of this form of virus, in that it only intermittently infects files or programs, based on any given criterion chosen by the creator of the virus. [8]

Multi-Partite, Polymorphic, Companion (known also as "spawning") and Parasitic viruses are where the traditional lines of viruses and other malware begin to significantly blur. Let us look more closely, albeit quickly, at these subclasses.

> "Also called dual infectors, these [multi-partite] viruses use more than one mechanism to spread themselves and infect other systems. Earlier versions infected both the data on a disk as well as the Master Boot Record. Modern versions (such as MTX) spread as a Trojan, a file virus, and a non parasitic worm."[9]

The Trojan, which is itself considered its own class of malware, is a dual infector in this case because it contains a virus which attacks the host computer. It is the delivery system for the virus and payload, though obviously not a virus per se. A Polymorphic virus "alters its code and produces a functional variation of itself in the hope of escaping detection." The virus is designed to do this in order to hopefully evade detection, in that the "signature" would change often enough to keep ahead of the antivirus definitions.[10]

Companion viruses appeared early on, when DOS was not so abstracted from the OS, as is the case today. The .com file is an "image replica" of what is to be loaded into RAM, and loads right away due to the fact that no processing is needed. It is the code for basic commands that are to run on the computer, and "can be limited to 64k". The .exe, however, contains instructions for DOS that must be carried out in DOS before it loads to RAM, and has no comparable size limit; thus making it a more complicated

[8] "Know your enemy", Brett Glass, ExtremeTech www.pcmag.com/article2/0,4149,34058,00.asp
[9] LabMice.net "Computer Virus Primer for Network Administrators" 11/13/2003 http://labmice.techtarget.com/antivirus/articles/avprimer.htm
[10] Ibid

file with which to contend.[11] This suggests why the .com file was initially so attractive for an exploit; no processing, potentially reduced chance of interception:

> "Companion viruses take advantage of a quirk in MS DOS based operating systems, and use malicious files with .COM extension, instead of actually infecting .EXE or executable files. When you type in a command by referencing its filename without specifying the extension, the operating system "fills in" the extension for you and executes any .COM file before using it's equivalent .EXE file. A companion viruses creates copies of itself using the names of real .EXE files found on the PC (for example PROGRAM.EXE), and renames the infected file PROGRAM.COM. This tactic has also been used to create other forms of non-viral (non replicating) malware."[12]

Parasitic viruses are a further permutation on this concept; they activate whenever the .exe, .sys, .bat, etc., file in which they are hiding is itself activated. They try to escape detection by either overwriting or hiding in existing code, thus ultimately destroying the host file.

Another close relative of theirs is the Macro virus, which exists in the programming of files such as .xls or .doc in Windows, and upon opening of the infected files, they proceed to infect the host software, (Excel, Word, etc.) thereby infecting any other file opened by that software. And they are also capable, at their worst, of ultimately infecting the entire Windows OS.[13]

Coming full circle; the Retro Virus infects anti-virus software per se, thereby compromising the security of the infected computer. This is well presumably to clear the way for more malware.[14]

"And now for something – not necessarily – completely different..."[15]

Worms are very much related to viruses, more so than Trojans; but originally were considered to be in their own classification.

> "Worms are computer programs that replicate themselves across network connections, without modifying or attaching themselves to a host program. Some experts consider worms as a special type of virus instead of giving them their own category, however the classifications that traditionally separate worms and viruses are beginning to blur. Many of the more modern variants that are commonly described as worms, can also be classified as viruses or worm/virus hybrids."

---

[11] "Computer Systems" http://myweb.tiscali.co.uk/whitefiles/b1_s/1_free_guides/fg1mt/pgs/h01.htm
[12] Opcit
[13] Ibid
[14] Ibid
[15] "Monte Python" quotation permutation – an example of a polymorphic viral effect.

This excellent definition highlights perhaps the most clearly observable distinction between a virus and a classic worm; the worm does not modify or attach itself to a host program, and it replicates itself, by itself. However, it is very true that this distinction has been eroded with the advent of hybrid worm/viruses. Further, Trojans now deliver worms, or worm/virus hybrids, and can include programming designed to replicate themselves by sending out copies of their original code from infected computers. As would ultimately be expected, worms that create variations of their own code and accomplish this in the wild have been observed, making them by definition "polymorphic" as well; W32.Mimail.Q@mm is such a worm.[16] (There are open source toolkits that facilitate this behavior; three of which are known as ADMmutate, CLET, andJempiScodes [Ktw01,DUMU03,Sed03][17] In fact RATs (more clearly defined below) are very effectively delivered via Trojans.

As stated previously, Trojans are delivery vehicles for whole species of these cyber-pests, and were considered non-replicating. This is in all practically no longer absolutely the case. For example, when a Trojans is acting as a shield behind which a hacker is hiding and executing commands on another completely different computer, the Trojan is itself can sometimes behave similarly to a latent virus, in that it is not actually effecting other software in the host environment...yet. Summarily, some of the most seriously damaging malware:

> "...can be classified as Trojan Worms – a hybrid between Trojan horses and worms. A Trojan worm requires a user to activate it, as does a Trojan horse, before it can infect a computer. But once this is done, it takes control of the machine and sends itself – via e-mail, Internet Relay Chat or other means – to other systems without further intervention."[18]

The type of behavior above described is absolutely crucial to the discussion of whether adware can be classified as spyware or outright malware. Worms can propagate themselves, they can transmit information gleaned from the infected computer, and very often they do either or both using email addresses taken from the contact list of said computer. Examples of such worms are, Win32.Mydoom.AU (which also opens a back door, thereby qualifying it as a RAT as well,) W32.Mytob.AM@mm [this is a fun one in that not only is it a RAT, it also blocks access to security websites from which one could download and execute the appropriate solution) W32.Envid.O@mm, (which contains a link to the Website that contains a copy of the worm. It then terminates processes related to antivirus and security programs, as would a retrovirus...) and the list of these and related evil code goes on and on.[19]

Having now been mentioned sufficiently often, RATs[20] are:

---

[16] Symantec http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.q@mm.html
[17] Advanced Polymorphic Worms: Evading IDS..."Oleg Kolesnikov, andWenke Lee, College of Computing, Georgia Inst. of Technology http://www.cc.gatech.edu/~ok/w/ok_pw.pdf
[18] "Know your enemy", Brett Glass, ExtremeTech www.pcmag.com/article2/0,4149,34058,00.asp
[19] Symantec Security Response, http://securityresponse.symantec.com/avcenter/vinfodb.html

> "...programs that are activated whenever a computer is turned on and run silently in the background without the owner's knowledge. In addition, these programs often notify the controlling computer when they're active, provide information on what processes are running, and allow the intruder to install other malware such as password stealers."[21]

Along with DDoS agents, these are typically delivered by Trojans, or Trojan/worm hybrids, although a custom logic bomb set by a disgruntled employee can certainly cause identical results. Bottom line; they allow non-authorized users, most often outside the IDS/firewall perimeter to do effectively as they wish.

At this point, it is well to consider other forms of malware that are not classified as viruses, but are most certainly unwelcome cyber-pests.

Logic Bombs and Mines are similar in concept, and yet also vary often in execution and psychology. They both are code that is written to deliberately cause damage should certain conditions occur. However, they are typically custom designed to their environment and are not intended to spread and "infect" other systems. They will often trigger off of certain conditions, as in the case of the following:

> "In one famous case, an administrator buried a [logic bomb] program on his company's server that checked for the existence of his user account. If his account was deleted or disabled, the program would launch and begin deleting files on servers across the network. Unfortunately, this type of logic bomb is usually a custom program or script that is difficult to detect and would not be identified by anti-virus software. Mines too are either written into their environment, or they are left for unsuspecting employees to find, masked as an innocuous document, spreadsheet or the like."[22]

Software that has been written to assist IT administrators in recovering passwords is a gift to the would-be hacker. "John the Ripper" and "Brutus" are a couple of the "applications" available.

Key-stroke logging software is software that – you guessed it – records key strokes made by the user on his or her computer, typically without their knowledge or consent. Some "packaged" examples, intended for corporate monitoring of their employees, are. "007 Spy", Spy Anytime", "Realtime Spy PC"; but all that is needed is a well written executable file with appropriate programming, lodged in a Trojan, and every word, including passwords, background information and the like will be recorded and retrieved by an unauthorized third part. This is of particular interest when we consider

[20] With due respect to Charlie Brown, industry slang for "Remote Access Trojan" + "s"
[21] LabMice.net "Computer Virus Primer for Network Administrators" 11/13/2003 http://labmice.techtarget.com/antivirus/articles/avprimer.htm
[22] Ibid

the ever graying area between outright malware, and “legitimate” advertising internet software.[23]

This has been the general overview of the ever expanding bestiary of cyber monsters. But what of the “internet browsing experience enhancing” software, that are legitimate business applications created for the purposes of pursuing life, liberty and happiness in the free-enterprise marketplace?

If you thought the forgoing was bad, “... fasten your seatbelts, it’s going to be a bumpy internet.”[24]

[23] Ibid
[24] “Permuted” (with respect,) from Bette Davis

– A Cyber-Social Disease –

(Our Litigious Society Re Adware, Pt. I)

Both this section and the next specifically deal with adware; how it operates, and whether or not adware has been deliberately written with the intention of a) covertly harvesting personal information, b) invasion or hijack of existing programs and operating systems, or c) denial of computer resources and functionality. Further, what about its operation would cause the IT industry to label it as "malware" despite efforts to the contrary on the part of the authors of the adware itself, will be addressed

To recapitulate briefly, viral malware replicates, and it does so more or less indiscriminately.

> "Worms like 'Code Red' are able to spread worldwide in a matter or hours. You usually recognize a viral infection from the odd system behavior it causes, but if, by some chance you don't, the recipients of your unwitting mass emails or a system administrator will notify you soon enough. Viruses and worms, if they work, always have malicious intent. The result of a viral infection is essentially a denial of service, since it denies you the use of your computing resources until the problem is fixed"[25]

The last observation is also critical to this discussion along with the definition of the Trojan Worm, found on page 6.. Theoretically, advertising software is not intended maliciously, nor is it absolutely designed to deny you your own computer resources, steal your private information, and certainly not report on how you use your own property...or is it?

> "Adware and spyware are most certainly a real – and growing – threat. One of the problems is that employees are increasingly using the Internet at work, but one in three companies have no way of managing employee use of the Internet in the workplace. At the same time, one in three companies have already detected spyware on their network and 70% of IT professionals believe peer to peer (P2P) file sharing creates and open door for hackers. Without any question, employees are installing adware and spyware on corporate systems – usually without the knowledge of the IT Department."[26]

By definition; if Claria/Gator, etc. software reports back to a home server with information gathered from a private home/corporate computer, it is engaging in behavior exhibited by and recognized as spyware; or to be more specific, any one of or a combination of a few of the duly defined species of malware listed in the previous

[25] "The Challenge of Non-Viral Malware", Pete Cafarchio, TISC Insight Newsletter, Vol. 4 Issue 12. http://research.pestpatrol.com/Whitepapers/NonViralMalware.asp

[26] "Spyware, Adware, and Peer-to-Peer Networks: the Hidden Thread to Corporate Security" Kevin Townsend, April 2, 2003, http://research.pestpatrol.com/Whitepapers/CorporateSecurity.asp

section. How it is so doing contributes further to any similarities to spyware per se:

> "While not necessarily malware, Adware is considered to go beyond the reasonable advertising that one might expect from freeware or shareware. Typically a separate program that is installed at the same time as a shareware or similar program, Adware will usually continue to generate advertising even when the user is not running the originally desired program."[27]

The only thing at all possibly differentiating adware from spyware by this definition is either the degree to which the information transmitted (in either direction) is harmful in anyway to the end-user computer environment, or to the personal data of the user stored on the computer. If enough adware "continues to generate advertising" in concert with or separately from disparate adware distributors, bandwidth critical mass will at some point be reached, thus rendering the computer operationally useless. Obviously, personal contact info, website purchase tracking, not to mention credit identification and the like, can ultimately completely destroying the individual financial privacy, or even identity of the average home user.

However, it is by virtue of the nomenclatural, and thereby perceived behavioral distinction of "adware" to "malware" at which the ability to combat adware is at best merely hampered (or at worst, outright defeated,) both on the practical technical level as well as in the rarified and idealized, but most certainly cutthroat and coeval realms of legislation and litigation; on which the efforts of the anti-adware IT industry are in danger of being predicated. (There is much more on the specific legalities with respect to adware in the next section.)

Firstly, to the technical.

> "Parasite Software - Some shareware, freeware, and adware programs are being packaged with additional software that can monitor your browsing habits, and even sell your unused CPU time and unused disk space to other vendors which in the process also consumes your network resources. Of course the legal tools that allow these vendors to do this are buried in the end user license agreement that no one actually reads. "[28] [This advertising "condition" can't exist on your TV or radio – yet! Ed.]

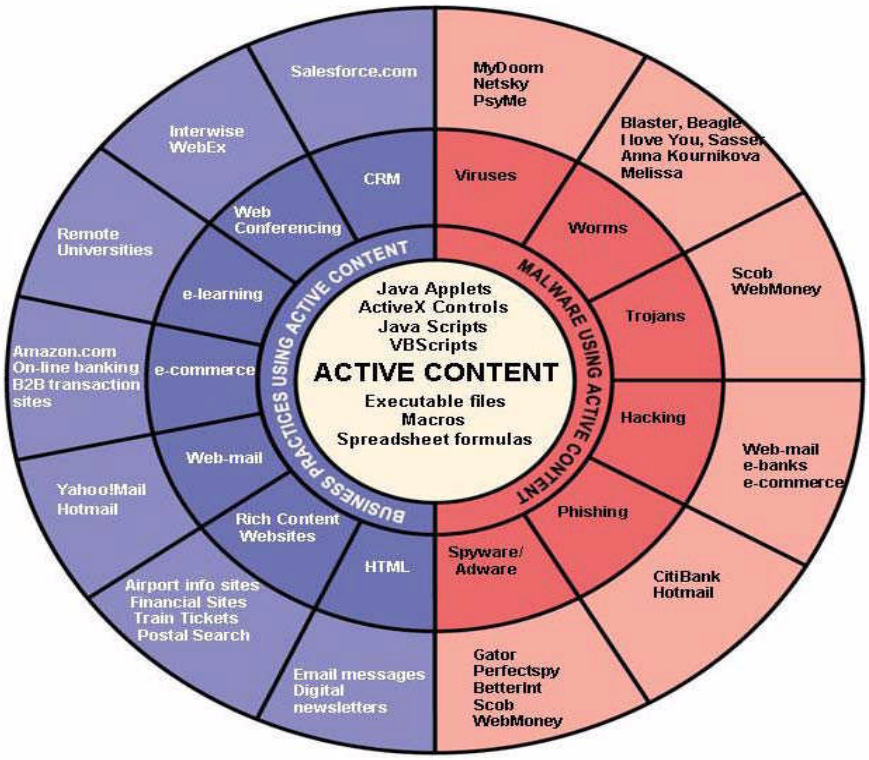
The preceding definition is very good; it covers just about everything. Recalling our initial definition that Adware is "any software that is supported by advertising revenue," how is it that this stuff invades the computing environment in the first place? Part of the answer is provided at the end of the previous definition; they contain "license agreements", to which users respond in the affirmative, knowingly or not. Even better is when pre-existing, otherwise useful programming designed to ease computing for

[27] Security Glossary - Vision Technology Management, LLC www.visiontm.com/Spy/Glossary.htm
[28] LabMice.net "Computer Virus Primer for Network Administrators" 11/13/2003 http://labmice.techtarget.com/antivirus/articles/avprimer.htm

the user is turned against the user by the authors of adware. Enter Active Content, and cookies.

"Active Content", i.e. embedded components in any given website can now be utilized as effective as Trojans for delivering any combination of nasty malware. Recently, concerns over ActiveX controls, Java applets and scripts, Visual Basic scripts, etc., have prompted IT industry analyst and anti-spyware company advisories to have these functions disabled in Windows IE and Firefox until more effective protections can be created. Having a computer that is not up-to-date with security patches is the cyber equivalent to throwing an open house for Al Qiada operatives. Further, macros that are found in spreadsheet and word processing programs using Visual Basic are de facto active content as well.

> "Active content has become part of common business practices, and is used in business applications such as web conferencing, e-learning, e-commerce and others. However, at the same time, active content technology may be exploited to carry malicious mobile code, which is downloaded and executed on a local system without the explicit knowledge or consent of the user. This dichotomy creates a difficult security challenge for enterprises and businesses. The figure below illustrates how active content can be used for both business (left side) and malware (right side) purposes."[29]



[29] "Combating the New Generation of Malware" Finjan Software, 2004, www.finjan.com

This example graph compiled by Finjan gives a very concise general visual reference both for what has been discussed in the first part of this paper, and what is shortly to come. Active content is not malware; active content can permit malware, spyware, and those so-called "legitimate" adware devices to become resident on a given computer operating system.

Indeed, the nature of ActiveX has given rise to a phenomenon known as the "drive-by download.

> "A drive-by download is a program that is automatically downloaded to your computer, often without your consent or even your knowledge. Unlike a pop-up download, which asks for assent (albeit in a calculated manner likely to lead to a "yes"), a drive-by download is carried out invisibly to the user: it can be initiated by simply visiting a Web site or viewing an HTML e-mail message. Frequently, a drive-by download is installed along with another application. For example, a file sharing program might include downloads for a spyware program that tracks and reports user information for targeted marketing purposes, and an adware program that generates pop-up advertisements using that information. If your computer's security settings are lax, it may be possible for drive-by downloads to occur without any action on your part."[30]

Anyone who has ever had their browser homepage reset to something else without their knowledge or consent knows at least one of the effects of a drive-by download; some of the others can be both invisible and very nasty. Xupiter is an IE toolbar program that has a rep for changing ones home page, downloading spyware, and redirecting all searches to its own site. As if that were not enough, it makes itself very difficult to remove.[31] Because ActiveX functions as it does, end user acceptance is in fact not necessary to have unwanted code come draining down into your OS.

> "Most spyware installs through an ActiveX plug-in when a browser window is opened. Disabling ActiveX controls entirely can cripple IE to the point where many legitimate sites don't work at all, and using the Trusted and Restricted Sites feature in IE isn't always helpful either. One way to stop spyware from installing itself is to attack it in the Registry, by preemptively blocking specific ActiveX controls from being installed."[32]

Another form of code that heretofore has been rather calmly accepted on the part of average users is that of the cookie. Cookies are not just for breakfast anymore; with respect to their purpose on the internet, they were originally intended to assist with the

[30] "Drive-by Downloads" http://whatis.techtarget.com/definition/0,,sid9_gci887624,00.html
[31] Ibid.
[32] "Blocking spyware via the ActiveX kill bit" Serdar Yegulalp, 09 Jun 2004
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1059905,00.html

task of browsing between either similar or completely disparate sites.

> "Are cookies spyware or adware? Some people go ape over cookies and have no perspective on them at all. First, without cookies, browsing becomes a much less convenient experience. You'd have a lot more typing and memorizing to do without cookies. What people don't like about cookies is how they get tracked as they move from site to site, and how a picture of their habits is taken and sold, and so on. This sounds sinister, but for the most part I consider it part of the price for free content. Also, some of the better-known "threats," such as Avenue A (which you'll probably find on this page), conform to P3P (Platform for Privacy Preferences), so you have some control generally in Internet Explorer over whether you'll accept their cookies on their terms."[33]

There exists a four-part, absolutely brilliant technical treatise on the progression of the effects of malware on an unprotected computer system, that was compiled by a SANS Organization Handler named Tom Liston, which is entitled "Follow the Bouncing Malware".[34] I want to include this crystal clear description of the functionality of how spyware in general can hijack one's computer, using tracking cookies as signposts.

> "hp2.exe is what is known as a "dropper" program. That is, it is actually a small "stub" program with another (sometimes more than one) program attached to it as "data". When the program executes, it writes out the "data" to a file and then executes the resulting program. hp2.exe drops a UPX packed executable that, when executed, will contact www.totalvelocity.com/Bundling/tvmupdater4bp5.exe, which installs/updates the "TV Media Display" spyware.
>
> At this point, I followed one link on the site, that required I have Flash installed. Since I didn't have Flash installed, I went "back". But because I now had cookies placed on my computer from my original visit to the site, one of yahoogamez' files, popup.js, does something differently:"[35]

Mr. Liston includes the actual code of the malware, which does clearly reference cookies that had been placed on the XP OS, un-service packed and unprotected computer, constructed for his experiment. And it is therefore also here that that the facilitation of malware via the existence of browser cookies is undeniably shown to be the case. His treatise is a must-read for any would-be security specialist.

A digression of sorts must now occur. The next two examples are not viral malware, they are not the result of invasive code on a computer, but they are related by actual effect on the user. Technically, what we are about to look at are two variant forms of

[33] "What's Spyware? Let's Ask Congress!" By Larry Seltzer April 5, 2004 http://www.eweek.com/article2/0,1759,1561797,00.asp
[34] "Follow the Bouncing Malware, I-VI" Tom Liston http://isc.sans.org/diary.php?date=2004-07-23
[35] Ibid

social engineering exploits. The first is best described as an attempt at tricking the computer user to take action that will effectively cause harm, loss of resources, disgorgement of information or at least as egregious a waste of time as if there were a virus or worm present. It is called an "Hoax."

One of my favorites is the jbdgmgr.exe or "Teddy Bear" hoax. It has been around forever, and the focus of it is the legitimate file "jbdgmgr.exe," which is part of the Java Script function. Clearly, some enterprising, bored wise-apple one day thought to him/herself, "Oh, a teddy bear icon in code-geek territory; I bet I can make regular people believe that this is the result of a virus, since they'd never believe Microsoft would do something that nauseatingly precious and cutesy...." 'Turns out that this was a reasonable assumption. It comes in the form of an email and insists that every friend once removed from reality and their half-maiden aunt that you have, has had this and they are SURE that it is true. The email advises that you delete this file.

Congratulations, you just nuked a not-unimportant part of Java Scripting on your PC. It's a bother, but granted, not on the same order as zapping WIN32K.SYS. Still, you were tricked into doing it all on your own, without even benefit a Trojan disguised as Anna Kournikova as an excuse to initiate the action.

Which phinally (sic) leads us to discuss Phishing. Technically, Phishing is by itself not a type of software, or executable code. It is cited herein due to its working proximity to legitimate software, utilized for malicious means, and therefore effectively employing said legitimate software as if it were malware in practice. The working definition provided by the "Anti-Phishing Working Group" is as follows:

> "Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, data suggests that phishers are able to convince recipients to respond to them. As a result of these scams, an increasing number of consumers are suffering credit card fraud, identity theft, and financial loss."[36]

I have a first-hand account of this phenomenon. My mother was contacted via email by her ISP, or so she thought, with a request to update her account information as a *protection* against fraud – and to do so on pain of her account being terminated if she did not send the information requested(!) This was sent from ('gotta love it!) "Suspend Notification [processing@majorISP.com]"; (the ISP name has been intentionally left out.)

> "Dearest majorISP services user,

[36] "Phishing Activity Trends Report", http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf, the Anti-Phishing Working Group

> This is an automated email notification sent to your registered email-address. Please don't reply to it as it will not reach the just department.
>
> Recently there have been many reports of fraud activity regarding stolen account information and stolen identities.
>
> This requires a full update on your records matching our database information to suit the future prolongation of account billing. You will be prompted to provide full and complete information regarding your account with us just so you can identify your online personality.
>
> Please take five minutes to fill out the forms. Failure to update your online records will result in a halt of your account and a possible reactivation fee.
>
> Please Click Here to update your billing account data.
>
> Thank you for using majorISP,
> majorISPCards Center.. "

Isn't that slick? I had dropped by for a casual visit; and when I walked in the room, she had in fact clicked on the link, and gone to a web page with the proper logos, color scheme – everything just right, except for the actual internet address. It was similar in concept, (if not actual content,) to the following:

> "212.77.50.14:5180/majorisp/?Nb=TteXJNUBKNt...." etc.

I had recently returned from the SANS Boot Camp, and noted at once that a) it was a direct email asking for confidential financial material, and b) the .url had an IP address, NOT the name of the organization, next to the http://. Two dead give-aways first up that all was not well. (There is a tertiary one in a grammatical error found in the first paragraph: "Please don't reply to it as it will not reach the 'just' department." Most either native English speakers, or well trained corporate, non-native speakers would have used "correct" or "right", as usage of the word "just" in this context is clearly, well... not right, to use a word. It's just another piece of evidence for which to be observant.) She was horrified when I gave her the background; and sure enough, when we called the ISP, prior to any other preamble on the pre-recorded greeting was a warning about an email scam trying to solicit credit card information from majorISP customers.

How 'bout that, I'd learned something. What is troubling, though, is that in the news recently, there have been reported both very successful scams where the name of the faked organization was seemingly properly placed in the .url, as well as an attack where the email when opened actually downloads a Trojan – piece by piece, named "Sepuc" – which then harvests personal data and reports it back to whomever sent it. The nastiest part is that the email is completely empty, with no subject line. Someone

who did not know would think it were just a misfire and never realize hat they have just been Trojaned.[37] Further:

> The increasing sophistication of the new attacks is not just the result of criminals getting better at their craft; they're also starting to cooperate with crackers and virus writers to swap ideas and methods.
>
> "These worlds are starting to collide. The code behind these newer attacks is very polished and, in some cases, even has comments in it," said Dan Maier, a member of the Anti-Phishing Working Group, in Redwood City, Calif. "They're sharing code with crackers, using spamming techniques. It's a scary combination."
>
> Maier said he has also seen attacks recently in which users who click on a link to a fraudulent Web site are redirected through several sites, some of which attempt to load Trojans or back doors onto the users' machines. So, even if the user is smart enough not to enter any personal information into the Web form, his or her data still could be at risk, said Maier, who also serves as director of product marketing at Tumbleweed Communications Corp., a secure e-mail provider also in Redwood City.[38]

They really are getting better at their work.

There was no subversive code involved in my personal example; merely subversive usage of email, and certainly an IIS server, (or possibly UNIX, as indicated by some of the composition of the url,) and a brilliant facsimile of majorISP's web interface design. The escalation illustrated in the latter example is terrifying.

So how is it that this "behavior" on the part of people contriving all of this garbage has gone unchecked, and how does this impact the war on Adware?

[37] http://www.eweek.com/article2/0,1759,1582698,00.asp
[38] http://www.eweek.com/article2/0,1759,1582698,00.asp

– Prophylactic Computing Vs. Politics and the Law –

(Our Litigious Society Re Adware, Pt. II)

It is now time to consider not so much what adware is but what it really accomplishes, either by design or actual effect. What is more, the question of to what degree any actions that IT professionals and internet consumers are permitted to take in our own defense, must be answered. Because the Internet is not a passive medium as is television - wherein the observer/user is even so remotely held "captive" by what images are selected by the network station for broadcast – but a dynamic medium where the end user actually has control over the process by which the information is disseminated, (how dare we!) advertisers had to adapt to that critical environmental difference. Like any comparatively successful biological vermin, the creators of adware have indeed adapted, and they have done so to their own advantage, (surprised?) with no thought for any collateral damage that their actions might cause.

Internet Adware is a new form of advertising; it has no legal or legislative precedence in existence, and as such the legal and legislative processes are playing "catch-up". In an environment not merely freed from restriction, but where definitive criteria by which acceptable behavior has never heretofore existed, authors of adware have had entire parsecs[39] of rope with which to run; and run they have. Their software has insinuated itself into the private computer environment because it is directly deemed necessary by the authors to do so; not because the user has had any native desire to have it there. What is more, they also have you asking their permission to invade your computer. It has come full circle

It quickly became apparent that if the user could move away from the advertisement, its effect would be lost in that instant. Further, if the location of the advertising were uniform with other material on the webpage sought by the user, the advertisement might be ignored while in plain site, pun intended, and not register with the user even then. Hence, the banner add, and the dreaded "pop-up".

> First, the Internet pop-up ads cover your computer screen. Then, your browser takes you to strange Web sites on its own. And then your whole computer slows to a crawl.
>
> Odds are, you've been hit by "spyware," the equally dangerous but lesser known cousin of the computer virus.
>
> "It felt like someone else took over my computer," said Wendy Brabon, president of Rochester's eBusiness Association, who found her home office computer jammed with spyware. "My browser was constantly going out and doing things I didn't want. It just took over so I could not do my work at all."[40]

[39] 1 Parsec = 30,856,747,300,083 km or 19,173,493,858,367 miles

[40] "Spyware lurks online" Richard Mullins,

To be fair; pop-ups, banner ads, toolbars and the like, were probably originally intended only to attract the eye. Where the problems started is when they hijacked someone's pc, and suddenly the user found that they no longer controlled, or even in a sense owned their own machine; someone else outside of their sphere of influence was calling the shots.[41] In a thoroughly unchecked, unsupervised, and uncalled for overabundance of zeal and desire to "win" customers, adware companies starting indulging in behavior professionally that had only previously been utilized by hackers and pranksters. The point behind that statement is that the invasive technology exists, coupled with the intention to sell product. The focus of any corporate Sales Rep is to assess the potential customer with the intent of getting said customer to buy whatever product is for sale. This is done in the field by individuals reading body language, countering perceived cons with pros, and in a real sense, psychological manipulation. In an interactively static environment such as the television, color, sound, endless repetition of carefully researched phrases of language are all designed to imprint themselves on the potential consumer. What is the focus of all advertising?

> Persuasion is the changing of attitudes by presenting information about another attitude. This information is then processed one of two ways: centrally or peripherally. If it is processed centrally the attitude change is more likely to have permanence. If the information is processed peripherally it will be more susceptible to later change... First and foremost an advertisement has to catch your attention. One way in which it does this is by appealing to your emotions.[42]

So, would it at this point be safe to say that the behavior of a computer choked with adware catches one's attention? Therefore, it has by definition been successful advertising. The argument currently at full boil is: has it also been successful invasion by advertisers of personal privacy and property?

As an highly appropriate aside, "there is no honor amongst peddlers of adware."[43] They even attack each other using the same tactics. I don't know why I'm in the least surprised, they have done it in the non-cyber market place for years:

> "The lawsuits against advertisers come amidst a lengthy legal battle between L.L. Bean and Claria itself. Claria, formerly known as Gator, has repeatedly come under fire for its method of targeting and delivering advertising -- which often results in advertisers' pop-up ads appearing over competitors' sites. When Claria, which is planning an initial public offering of stock, filed papers with the Securities and Exchange Commission (SEC), it cited pending suits with Hertz Corporation, L.L.

---

http://www.democratandchronicle.com/biznews/0801AC53C5I_business.shtml
[41] "Follow the Bouncing Malware, I-VI" Tom Liston http://isc.sans.org/diary.php?date=2004-07-23
[42] "Social Psychological Factors Underlying the Impact of Advertising", Jon Gresko, Lynn Kennedy, & James Lesniak http://www.users.muohio.edu/shermarc/p324ads.shtml
[43] Permutation on the time-honored saying by your humble author.

> Bean, Six Continent Hotels Inc. and Inter-Continental Hotels Corporation, TigerDirect, True Communication, Wells Fargo & Company, WFC Holdings Corporation and Quicken Loans. [44]

But that is only the half of it:

> "Adware maker Claria has sued L.L.Bean, charging the retailer with filing a frivolous lawsuit against its advertisers. Claria, formerly known as Gator, filed the complaint last week in the U.S. District Court for the Eastern District of Texas. The Redwood City, Calif.-based company is firing back at L.L.Bean after it logged four complaints in Portland, Maine, district court in recent weeks against Atkins Nutritionals, J.C. Penny, Nordstrom and Gevalia Kaffee."[45]

To continue on; without question there is also a need to consider a ready-made Petri dish of suspect download-ready – and to date well utilized – software, a cyber-breading ground for adware, and malware of all kinds; Peer to Peer networking, or P2P.

> A pure peer-to-peer file transfer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server. A typical example for a non peer-to-peer file transfer is an FTP server. One user uploads a file to the FTP server, then many others download it, with no need for the uploader and downloader to be connected at the same time.
>
> Some networks and channels, such as Napster, OpenNap, or IRC @find, use a client-server structure for some tasks (e.g. searching) and a peer-to-peer structure for others. Networks such as Gnutella or Freenet, use a peer-to-peer structure for all purposes and are sometimes referred to as true peer-to-peer networks, though Gnutella at least is greatly facilitated by directory servers which inform peers of the network addresses of other peers. [46]

The forgoing is not all that is facilitated; it was reported on the SANS Storm Center on March 2nd, 2005 that someone had downloaded Skype, a peer to peer VOIP (Voice Over Internet Protocol) app, and been back-doored with a RAT in the process.[47] P2P is very popular for obvious reasons; one can "present" material without "publishing" it and thus try to avoid copyright infringement. Laws and interpretation of those laws are

---

[44] "L.L. Bean Sues Other Marketers for Claria Pop-Ups" By Pamela Parker May 18, 2004, www.clickz.com/news/article.php/3355321
[45] http://news.com.com/Claria+sues+L.L.Bean/2110-1038_3-5229760.html, Claria sues L.L.Bean, By Stefanie Olsen, 2004
[46] "Wikipedia, the free Encyclopedia", http://en.wikipedia.org/wiki/Peer-to-peer
[47] SANS Handler's Diary March 2nd 2005 Handler on Duty: Johannes Ullrich http://isc.sans.org/

being retooled for this new environment; and it is indeed from under this guise that some legislation is taking aim at curbing internet copyright abuse, (more on that in a moment.)

> Besides invading your privacy (some programs record keystrokes and capture information such as Social Security and credit card numbers), an accumulation of spyware can crash your computer system. [Wendy] Brabon tried to erase the spyware programs from her computer, but they seemed to resurrect themselves.
>
> A similar disaster happened to Rhonda Penders, an administrative assistant in Adams Basin. "All of a sudden there were bookmarks for casinos and adult Web sites all over my computer that we would delete but would come back on their own," Penders said. "… I have teenage boys and at first I yelled at them. But then we were able to find out they weren't even on the computer."[48]

The above, however, is simply another note in what is perceived by advertisers as merely the eternal whine of the effected consumer in revolt; perceived only as an inconvenience to their overriding, seemingly divinely granted right to conduct business as they see fit.

> But spyware likely won't go away soon because major advertisers crave Internet exposure and pay millions to companies that design spyware software. "There are some very large advertisers doing this," said Nate Elliott, an analyst with Jupiter Research in New York City."
>
> Part of the problem is defining "spyware." Internet security firms say its any program that surreptitiously watches Internet behavior for advertising or other reasons — malicious or not — or that can transmit that information back to the Internet. Companies that make such software prefer to call it "adware," to emphasize the advertising component.[49]

Even worse, in order to legitimize what they do, advertisers who either design or have this software designed try to ensure that it is your fault if you allow them to advertise on your computer. No, that was not a misprint. Before downloading freeware from a given website, part of the non-monetary price you pay is to allow advertising software to be placed on your computer. You are presented with a legalistic set of verbiage called an End User License Agreement, or EULA. This is again the information that "... nobody reads," that was cited under the definition of Parasitic Software in the previous section. And it is presented to you, as ostensibly you seeking the permission of Gator to use their product GAIN gratis, for example. No monetary outlay required, just accept whatever advertising that is presented. To put it another way; adwareing insult to

[48] "Spyware lurks online" Richard Mullins, http://www.democratandchronicle.com/biznews/0801AC53C5I_business.shtml
[49] Ibid

injury, Gator claims that not only is their software not spyware solely due to the fact that the populace are "clearly notified before downloading it", but it is their right to download it as a form of payment for using their “product”. And you are not allowed to return it after having found it defective, either.

> According to a report prepared by Harvard Law student Benjamin Edelman, if you use Gator, now owned by Claria, you may be in a bit of a bind if you want to remove the GAIN (Gator Advertising Information Network) adware which has been installed on your computer by the Gator software.
>
> According to Claria itself, more than 35 million users have the GAIN adware installed on their systems, although PC Pitstop says that only a very small minority of those 35 million actually knowingly agreed to the adware being installed.
>
> However, the End User Licensing Agreement (EULA) which you would have signed when downloading and installing Gator says, buried way towards the bottom, that you agree that “you will not use, or encourage others to use, any unauthorized means for the removal of the GAIN Adserver, or any GAIN-supported software from a computer.”[50]

According to Edelman, the only “authorized” method for remove was Windows Control Panel, Add/Remove Programs. But instructions for doing so were by no means clear.[51] To put a fine point on it, there is not nearly incentive enough on the part of advertisers to really change their tactics. If they can, by exploitation of functionality, or by tricking people into accepting their software, such that the responsibility is on the user because, “They said yes” to the EULA, these behaviors on the part of internet advertisers will not change, don’t even mention the word “stop”.

> “One of the first things Gator's software does is to generate a tracking number that is unique to the computer. Privacy rights advocate Richard Smith discovered that part of this unique number seemed to include the address of his Ethernet adapter.
>
> Gator collects information about which web pages are loaded into Internet Explorer. The software records how the user interacts with the ads popped up by Gator. Gator's software rifles through the user's computer to record the names of all the software installed on that computer. The software will gather the user's first name and zip code. The software collects information that is entered into the forms on a web page, including part of the user's credit card number!

[50] “Claria defends right to live” http: //channels.lockergnome.com/net/ Archives 12/01/2004
[51] http://www.benedelman.org/ Highly recommended site; he is a legal “consumer advocate” contra adware.

> All of this information is cross referenced with that unique tracking number generated when the software is installed, then it is uploaded to Gator-owned servers over the internet."[52]

Does any part of the forgoing sound at all similar to what has previously in this paper been defined as a Trojan Worm and how operates? (Please reference back to page 5 if you wish. Frankly, I think something along the lines of a "MyDoom" variant is reasonably comparable given the operation of Gator's software as described above.) And yet, the claim made by Gator/Claria, whomever, is that by clicking "Yes" to the EULA, the user has given the advertiser permission to have their programming function – in ways that directly emulate clearly defined malware.[53]

> "The behavior of this software apparently fits PC Pitstop's definition of spyware. It also fits the definition used by every single company which makes an antispyware program. However, it does not fit Gator's own definition of spyware. And that is the whole problem.
>
> There is no "official" definition of the word "spyware" as it relates to adware. However, there are several unofficial definitions published by various web sites. Because of this, people tend to point to whichever definition best fits their own needs.
>
> It seems that Gator did just that, finding a definition for spyware that does not include their software's behavior and then suing to make that definition stick. I am very glad that PC Pitstop settled that lawsuit and avoided the danger of Gator's definition becoming a "legal" definition."[54]

What scares me is that Gator "won" by attrition; even worse, having PC Pitstop back down due to the possibility of legal precedent in favor of adware being set, by virtue of no codified, legally viable and pre-accepted definition of harmful software.

It only gets better; in some cases what you agreed to does not even occur.

> Several companies often named as spyware makers argue that their practices are not as bad as some claim.
>
> "(Our) software doesn't 'sneak on' to people's computers, as is often alleged," said Anthony Citrano, a spokesman for WhenU.com, an Internet marketing firm in New York City that uses downloaded software to present targeted pop- up ads based on surfing habits. "People choose to download a free, ad-supported version (of software) rather than buying a

[52] "Gator Sues To Lose Spyware Lable" Spyware Weekly Newsletter, 10-28-2003 http://www.spywareinfo.com/newsletter/archives/1003/28.php
[53] "Unwitting Collaborators, Part 3: Spyware", by Frank Fiore & Jean Francois http://www.awprofessional.com/articles/article.asp?p=27568&seqNum=3&rl=1.
[54] Ibid

> paid version, and the license agreement is very clear about that."
>
> WhenU software is included in free programs such as "WeatherCast," which shows current weather conditions, and "ClockSync," which updates a computer's clock.
>
> Once installed, the program watches Internet use. So if a user searches for vacations, a pop-up may appear for Priceline.com, offering discounted travel packages. WhenU lists some of the world's largest advertisers as clients: American Express, Bank of America, British Airways, Ford, Microsoft, Priceline.com and Verizon.[55]

"Once installed, the program watches Internet use." That's a nice way of saying that it is watching where you go, what you do, and how you interact with it. Everything that you do!

> "There is a lot of misunderstanding about this," said Todd Sawicki, director of marketing for 180solutions Inc. in Bellevue, Wash., another company often named as a maker of spyware. "This is better called 'adware' or 'sponsorware,'" he said, because free programs they offer are supported by advertising sponsors.
>
> When users download free programs from 180solutions, the software monitors where users go on the Internet, then presents pop-up ads from sponsors, Sawicki said. For instance, if you're searching for a rental car and type "Avis" into a search engine, you'll likely get a pop-up advertisement for a competing car rental company that has retained 180solutions for advertising. "We really provide a value to users that saves them a lot of time, because when they are searching for something, we present them an offer right then that's a good value," Sawicki said.
>
> That kind of explanation is "patently absurd," said [Nate] Elliott, of Jupiter Research. "What their software does is detect a Google search going on and when the results page pops up, it launches a huge window with its own results. … Everyone wants to paint themselves as the good guys, even if what they are doing is really sketchy."
>
> Intrusive advertisements irked Major League Baseball enough that the organization several weeks ago took a stand on spyware after noticing pop-up ads covering its Web site. "We sent cease-and-desist letters to a significant number of companies who had pop-ups on our site," said MLB spokesman Jim Gallagher. "Many didn't know their ads were being served up on our site. All they had done was provide a spyware marketer

[55] "Spyware lurks online" Richard Mullins, http://www.democratandchronicle.com/biznews/0801AC53C5I_business.shtml

with the demographics they were interested in getting in front of."[56]

At this point it is well to remember that information gathering is only part of the equation. Enough of this clutter can halt – at it's worst, irreparably – computer function, requiring complete reinstall of OS, and very likely loss of personal data. Even if no data mining is occurring, what results is in practice a Denial of Service Attack. I opened this thesis with a personally experienced example of precisely this potential result. And that, coupled with highly questionable information gathering and covertly executed observational tactics, overwhelmingly reduces most adware to the level of malware in practice, if not by intent, or by admission on the part of the "purveyors" of said adware and their alleged services.

The problem has escalated to the level that now the United States Government has at last felt compelled to enter the fray.

> The Senate is considering 2 pieces of legislation that would drastically change the pop-up advertising and file sharing landscape of the Internet.
>
> Perhaps the most controversial legislative proposal is the Inducing Infringement of Copyrights Act (Induce Act), which directly targets peer-to-peer users and technology.
>
> Another piece of legislation floating in the Senate is the Software Principles Yielding Better Levels of Consumer Knowledge Act (Spyblock Act), which targets pop-up advertising and other "spyware"-related activities. In effect, the Act makes it unlawful for a person who is not the user of a protected computer to install software without (1) adequately notifying the user, (2) obtaining the user's express consent, and (3) providing uninstall features.
>
> The Safeguard Against Privacy Invasions Act (SPY Act) seeks to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs. The SPY Act directs the FTC to prohibit installing spyware programs on covered computers without express consent in response to a clear and conspicuous request or through an affirmative request. More specifically, the Act would require the FTC to establish requirements for installing spyware that requires affirmative action on the part of the user of the covered computer to agree to a license, contract, or other agreement, including setting forth on a Web page license or contract terms, mechanisms for agreeing to such terms, and the name and street address of the person or entity transmitting the spyware. The SPY Act further directs the FTC to prohibit the use of any spyware program for collecting any personally identifiable information from the covered computer unless notice of such use is

[56] Ibid

provided. The FTC would also be responsible for enforcing the Act..[57]

It is the second and third pieces of legislation in which everyone should be interested, from the technical solutions stand point at least; particularly when gauging potential effectiveness of such litigation. The tragically obvious problem is that legislation can compel only to a point. For example, when given the benefit of the doubt, and a company creates reporting software that ostensibly only provides product and service browsing information back to the company, but it is found out to do much more than that, what form of legal action can truly repair the damage already done?

> "The KaZaA Media Desktop application had an adware component that displayed advertisements and offers to those playing the game. The adware component reported its use back to the software company for tracking purposes for its advertisers. But the way it was implemented and dropped to users' systems made anti-virus vendors consider it a spyware-Trojan because—unknown to its users—it reported back to the company their personal information and could compromise the integrity of their network. The spyware-Trojan didn't do any damage to the user's system and wasn't deliberately produced to create a backdoor to a user's network. But that was its unexpected consequence.
>
> When the problem was discovered, KaZaA quickly informed the industry and its users and provided a quick downloadable patch to correct the problem, stating that KaZaA took its users' privacy seriously and had strict guidelines in place for the software they bundled. Suffice to say, it was an embarrassment to the company."[58]

Further, who is really going to be in charge of defining what differentiates adware from malware or spyware? Perhaps more critically, who will be defining just where the boundary is and by what criteria it is composed, thereby clearly indicating when it is or is not violated; Congress, the IT industry, the advertisers, or whomever happens to have the sharpest attorney and wins a precedent setting court case?

> In general terms, some of the actions banned by the [Spy Block] act include:
>
> * installing software without notice to and consent from the user
> * installing software without a proper uninstall available
> * misleading the user about who is responsible for the program or about the services provided by it
> * not taking reasonable measures to protect users' privacy.

[57] "The Technology Trade", By Jason Allen Cody, October 2004, Findlaw.com
[58] Unwitting Collaborators, Part 3: Spyware", By Frank Fiore, Jean Francois. http://www.awprofessional.com/articles/article.asp?p=27568&seqNum=3&rl=1

> The act requires that disclosure precede and consent be obtained for each instance of "information collection, advertising, distributed computing and settings modification." The program is required to remind users, more or less constantly, that they can uninstall it and how to do so.
>
> OEM, preinstalled software is exempt as long as users are still informed of any "information collection, advertising, distributed computing and settings modification." All of these notifications and consents are waived if the function is "reasonably needed to … provide capability for general-purpose online browsing, electronic mail or instant messaging, or for any optional function that is directly related to such capability and that the user knowingly chooses to use." It's also waived if the function is related to determining whether the license is valid or to provide technical support.
>
> But some of the language in that first waiver—"for any optional function that is directly related to such capability and that the user knowingly chooses to use"—sounds like wiggle room for companies such as Claria Corp., formerly called Gator Corp., that install misleading ad servers on users' computers. Claria recently used the threat of lawsuits to stop people from referring to its product as "spyware." Fine, we'll call it "adware," as some security programs such as Norton Antivirus 2004 do.[59]

On the purely technical level, adware can be treated along with viruses and other malware very easily. However, when Claria can successfully conclude suit, on any level and by any definition of successful litigation, to distance themselves from comparison to spyware – and do so despite examples of some highly indicative activity such as have been cited herein – how can the legal profession provide any assistance against the technical problem if it is even perilous to name observed behavior with the appropriate language; much less support the designers of technical solutions to take protective action against it?

The anti-virus companion industry of “anti-adware” has arisen as a result of this very issue. Private information, pirated by adware, has demonstrably been broadcast on the internet in a fashion that is ultimately indistinguishable from malware; potentially irreparably damaging the organization or individual user from which/whom it was taken. However, because the adware entities responsible cannot be legitimately treated as the creators and distributors of de facto malware, the hands of those tech agencies devoted to protecting personal and corporate computers are tied, legally. What is more; in such an environment, how does one appropriately gauge reparation to the victim, or punishment of the perpetrators, when harm has been done? More basically, how is “harm” determined? And does the individual user have a ghost of a chance compared to a corporate entity? Will the home user be taken seriously?

Will legislation and law enforcement, (in tandem with technology,) actually help to

[59] “What's Spyware? Let's Ask Congress!” By Larry Seltzer April 5, 2004
http://www.eweek.com/article2/0,1759,1561797,00.asp

solve the problem? Only time will tell on that subject, and according to some, it is not off to an auspicious start, even where clearly criminal activity is the case:

> "Security officials at several banks, who spoke on condition of anonymity, said they have run up against a wall in trying to find new ways to deal with phishing attacks and are getting little or no help from federal law enforcement agencies. The phishing phenomenon exploded last year and caught many in the banking industry unawares. Virtually every major bank has been hit with at least a handful of phishing attempts, but many banks are just now setting up response teams and codified procedures to deal with the problem.
>
> This time lag has given the scammers a tremendous head start on the banks and made it difficult for security teams to get their arms around the problem quickly.
>
> "Phishing isn't a simple thing. It's been around since the '90s. It's really gotten sophisticated and had an impact on these businesses' ability to work," said Dave Cullinane, president of the Information Systems Security Association..."The money-making capability of it is huge. If something like this happens to a bank, it's not a good thing because people think of a bank as a place that will protect your information."
>
> Cullinane added that in his experience, the FBI and other federal agencies are generally unresponsive to requests for help from banks on phishing attacks unless the bank can show substantial financial losses. "If you're running on the assumption that calling the FBI will get you assistance, it won't," he said."[60]

Only time – and enough people with their lives in financial ruin, blaming Government for not protecting them better – will tell. Perhaps.

[60] http://www.eweek.com/article2/0,1759,1737627,00.asp

– From Vulnerability Awareness To Remediation –

Let us for the moment leave the question of legislative effectiveness in its current state of limbo. For the present, addressment of this issue must be accomplished on the technical and behavioral level of the IT industry and the individual users; from private individuals at home through to corporate employees who's job functions depend on clean, functional computer software and hardware.

Firstly, "Know Your Enemy!" Continuing education regarding adware related cyber threats and how they operate is as mandatory as proper implementation, upgrade, maintenance and administration of the technological components. These include IDS's, firewalls, proper architecture of these components, physical security of the actual hardware, and anti-virus solutions. (As an example of how critical architecture can be, a colleague of mine experienced a company which had mandated that kernel level access control monitoring of servers would take place. Therefore, every kernel call was logged as either accepted or denied. Naturally this produced both lots of traffic and immediate complaints about poor performance. There were six hundred (600) servers being so monitored; on a token ring architecture. Bandwidth maxed out at 16mb. Lesson: you MUST be aware of your environment and architecture.)

Secondly, utilization of some form of "anti-adware" solution is as critical as an anti-virus solution; though how and where it is applied varies depending on who is doing it, and for what environment. In a small office for example, it might be more cost effective to have individual anti-adware and anti-virus clients on the few computers present, with a router running a firewall connecting to the internet, as opposed to a full corporate, server based solution.

Thirdly, clearly defined user habits must be tailored to the specific environment and then adhered to. This last consideration is where things get exponentially problematical, particularly in the workplace.

Blocking or filtering of certain websites, file types, disallowing access of personal email via web interface, or at worst outright denial of web access are certainly effective methods of curtailing the effect of web pests in the corporate environment. When it is required of a given employee to access "questionable" websites, as can be the case of a patent attorney researching copyright infringement for example, close monitoring of their computer activity is obviously an absolute requirement. Third party solutions exist to help filter files and .urls; *e*Trust Secure Content Manager from CA, and Policy Patrol Web" by Red Earth Software are two such commercial packages.[61]

Just as an arbitrary example, the cost to a given business might be reasonably calculated with a formula, as follows:

So what might spyware be costing you? We'll start by assuming a fully

[61] http://www3.ca.com/Solutions/Overview.asp?ID=4673&TYPE=S, http://www.redearthsoftware.com/File-filter.htm

> loaded user salary is $72,000 per year and there are 260 working days per year. If a spyware infection involves nothing more than getting rid of it when found, and that process takes the user and the support person she works with, say, two hours to fix, then we're looking at a cost per incident of:
>
> ($72,000/260 days)*((2 people * 2 hours)/(8 hours per day)) = $138.
>
> In a 1,000-person organization with a spyware infection rate of 5% per month we would have some 600 cases per year for a total cost of around $83,000. And if a dialer goes into action that could be a low figure![62]

But is the severity of complete isolation from the internet with regard to the worker always warranted from a merely economic standpoint?

> National Survey Finds 22.9 Million Hours a Week Wasted on Spam
> College Park, Md. – February 3, 2005 – Spam's price tag now reaches $21.58 billion annually in lost productivity according to the results of the 2004 National Technology Readiness Survey (NTRS). Findings from the 2004 NTRS, an annual survey that tracks U.S. consumers' technology opinions and behaviors, indicate that online users in the United States spend an average of three minutes deleting spam each day they check e-mail. Aggregating their usage across the 169.4 million online adults in the United States, this equals 22.9 million hours a week, or $21.58 billion annually when based on the average working wage.

This report did not address users accessing private web mail; this is work related email, inclusive of spam. Just as it is impractical to the point of absurdity to funnel all email of a large corporation through a few "designated" users, it can be equally impractical to do the same where reasonable internet access is required in order for daily business to function.

Access to the internet and various websites is often a fact of corporate computing existence that is shared among many employees for a variety of valid reasons; it is certainly the case with regard to private computing. Therefore, how websites are accessed, what is done on a given site, with what software it is accomplished and with consideration as to the nature of the website, are all factors that must be addressed in addition to what combination of defenses are in place. In the corporate environment, these factors must be addressed with any and all workers accessing the internet by IT and Management in tandem.

Multi-tiered defense strategies are clearly requisite for maintaining computer security in the workplace, by all means; and when possible even at home. A personal router with

[62] The cost of spyware" Network World, 04/26/04
http://www.nwfusion.com/columnists/2004/0426backspin.html

a firewall implemented, behind which the individual pc's are running anti-adware and anti-virus software is a good, if no doubt comparatively rarely implemented example for the average home user. VPN technology allows for added security when communicating with work from home, but can be a security hole if a home computer is compromised, and file transfer necessary for business occurs between the private pc and the office intranet.

Enterprise-wide anti-adware solutions are becoming available; Symantec, and Pest Patrol among others have corporate solutions available. However, these are not complete solutions to the problem. They are currently only partially effective:

> Tech suppliers say they're doing all they can to make it easier for home users to secure their own PCs: guiding consumers to a raft of products and services they can use to lock out cyber-intruders. But critics say that's akin to making car drivers responsible for installing their own seat belts. (One fore Ms. Davis. Ed.)
>
> "As long as we rely on the end user as the primary mechanism to secure their own computer, we will continue to have large quantities of unsecured devices," says Mitchell Ashley, chief technology officer at StillSecure.
>
> In the past eight months, USA TODAY interviewed more than 100 tech industry executives, consultants, analysts, regulators and security experts who say tech suppliers could be doing much more to buttress Internet security. In pointing fingers, critics say that Microsoft could do more to supply basic protection for every Windows PC, that Internet service providers could significantly tighten key Web gateways, and that anti-virus companies could move more quickly to develop and distribute smarter software.
>
> Instead, leading tech suppliers — bedeviled by competitive rivalries and hesitant to bear more product-support expenses — have proved incapable of joining forces to put up a unified defense, which is what it will take to clean up the Web, critics say.
>
> "They're not working together, and because they're not working together, they're putting all of us at risk," says Alan Paller, research director of SANS Institute, a Washington-based Internet-security think tank and training center.
>
> Much is at stake. Worldwide losses from cyber-attacks will swell to an estimated $16.7 billion by the close of the year, up from $3.3 billion in 1997, according to tech consultant Computer Economics. As cyber-attacks become more invasive, businesses across the USA are becoming wary of using e-mail as a tool. Some are pulling back plans to

> open more of their networks to customers, partners and mobile workers.
>
> Meanwhile, consumers remain largely ignorant about the extent of the threat. Cyber-intruders have begun to wrest control of millions of PCs in homes, small businesses, college campuses and government agencies. Compromised PCs are being transformed into obedient zombies slotted into underground networks to broadcast spam, carry out identity theft scams, even conduct cyber-blackmail.
>
> What's needed, security experts agree, is for tech suppliers to collaborate on implementing system-wide measures that protect consumers by default.[63]

In defense of the tech industry, it would no doubt help on said "collaboration" if there were actual legal consensus as to entirely what it is against which they are supposed to defend consumers; not to mention how they may go about it without fear of litigious reprisal. They are certainly not responsible for people who use marginal P2P clients, or who indiscriminately download files from questionable websites. On the flip side, if IT mandated filtering ultimately clashes with legitimate corporate internet business, such filtering would probably be perceived of as a liability to the business in that moment, and would more than likely cease; or at least be curtailed. That said, until those "measures" cited in the article above are realized, both the legal and technical, the end user is by default the "primary mechanism" by which computer security will either succeed or fail; in both the workplace and in the private sector.

Given all of the preceding, included in any corporate policy regarding internet access there must be policy extant reasonably holding users accountable for their actions on the Internet, once policy has been explained and education has been accomplished. It can be as basic as a listing of Computer Commandments:

> Thou shalt not use P2P at work
> Thou shalt not download and activate .wav or .mpg files at work
> Thou shalt not bring and activate .wav or .mpg files from home
> Thou shalt not download private email on corporate equipment
> ... etc.

As a none-cyber example; would speed limits be at all meaningful if there were no tickets issued? Even as it is, people violate the speed limit all of the time. However, properly implemented network security procedures can be made more effective than the somewhat more random highway patrol catch-of-the-day. Review of security logs by IT personnel is as critical as any other facet of defense. Yes, that sounds terribly Internet Fascist User Snooping Squad of me, (or I-FUSS for short,) but without accountability, the likelihood of any sort of general employee compliance with prescribed internet protocol is not great – nor should it be expected.

[63] Tech industry presents less-than-unified defense By Byron Acohido and Jon Swartz, USA TODAY http://www.usatoday.com/tech/news/computersecurity/2004-09-09-zombie-response_x.htm

(Of course, having said all of this, it is worth mentioning that once in place, all of the technological defense systems really should remain uncompromised by the individuals tasked with their maintenance, of all people. KYN – Know Your Network! KYN is KEY, (sic). I recall a friend relating to me an absolute classic; a Senior Systems Administrator in a fit of piqued expediency – to put it far too politely – physically bypassed the interposing IDS and deliberately plugged an internal subnet switch into an internet switch that was, of course, outside of the firewall/DMZ. This striking exercise in Vulnerability Enhancing Architecture was accomplished in order to run "bandwidth tests" with the corporate ISP. My friend, who was in fact Information Systems Security Officer for a company that spanned 4 states and 7 offices at that time, very understandably and rightly had an entire herd of cows over that one.)

I am not going to presume to give recommendations of brands of either hardware or software; that is not the point, and one can find analyses of every conceivable IT security solution very easily from many trustworthy sources. PC Magazine, CNET News.com, eWeek.com, obviously the SANS Organization are all resources in the archives of which excellent technical, practical information can be found from which intelligent choices can be made. What is to the point of this dissertation is that all of the coolest, shiniest state of the art hardware running the most cutting edge software is just so much expensive metal sculpture if the end user is circumventing these protections by poor computing habits. It is at the juncture of technological solution and application of security conscious internet usage that vulnerability awareness – and particularly remediation – is at its most delicately critical state of being.

– Tamen Permissum Mihi Dico Vos Quare –

("But let me tell you why...")

(For some ersatz reason, I am of the opinion that disseminating bad news in Latin – or as this case might be, disseminating news in bad Latin – helps take the sting out of it.)

Based on the evidence presented, the war on cyber pests currently rages on, with absolute containment of said pests as the ultimate goal of technology; provided it is permitted to do so legally. It is certainly beyond the control of legislation or litigation to absolutely contain at the present time, (as has been at least cursorily illustrated,) and it is thereby ultimately and solely under the control of the IT industry working with the end user, to disallow the permission of the offending software to find a home.

I found this listing of the damage done by malware of all kinds interesting, and to the point:

> ID theft shot up 79 percent last year from 2002, affecting 3.4 percent of U.S. consumers, according to Gartner, a business research and consulting firm. One reason it's growing is that such thieves face only a 1-in-700 chance of getting caught. ID thefts directly cost U.S. businesses $1.2 billion in 2003, Gartner estimates. Source: Associated Press, October 7, 2004
>
> Nearly 2 million Americans have had their checking accounts raided by criminals in the past 12 months, according to a soon-to-be released survey by market research group Gartner. Consumers reported an average loss per incident of $1,200, pushing total losses higher than $2 billion for the year. Source: MSNBC, June 14, 2004
>
> The research firm Gartner estimated that 30 million adults experienced a "phishing" attack in the year ending in April 2003, and that 1.78 million of them fell for it. Source: Associated Press, October 7, 2004
>
> Phishing has victimized some 1.8 million consumers and cost banks and credit-card issuers nearly $1.2 billion in the past year. Source: Christian Science Monitor, October 7, 2004
>
> Spyware has surpassed viruses as the number one threat facing the computer today. In fact, most estimates report that 90 percent of computers already have been infiltrated by spyware. Source: TechNewsWorld, March 19, 2004
>
> As it turns out, one-third of Internet users have been similarly afflicted, according to a recent survey by Consumer Reports. "Spyware, without question, is on an exponential rise over the last six months," says Alfred

> Huger, senior director of engineering with Symantec Security Response (SYMC), the maker of Norton security software. Microsoft (MSFT) reports that spyware was the cause of one-third of all computer crashes in the past year. Source: BusinessWeek, September 29, 2004[64]

Happily, it does seem that some companies are getting a clue, at least so they say:

> Some companies that do online advertising have begun to think more carefully about it. Online retailer Overstock.com Inc., which installed spyware on customers' PCs a few years ago, has stopped. "It's an ethical issue. Spyware is evil," says Jonathan Johnson, Overstock's VP of corporate affairs.
>
> Overstock is suing rival SmartBargains.com LP in Utah for using pop-up ads to offer competitive products just as a shopper is about to check out at Overstock. "It's akin to a shopper standing in line with a cart full of merchandise at Target and a Wal-Mart greeter comes up to get the customer to buy the same stuff at the Wal-Mart across the street," Johnson says. SmartBargains didn't return phone calls seeking comment.[65]

The problem is of course, can the adware industry truly be relied upon to police itself:

> In an attempt to cut down on misbehaving adware and spyware, Google has released a set of suggested principles for software makers to follow when writing programs that embed themselves on Internet users' PCs.
>
> The guidelines, released Tuesday evening, say software should follow common-sense rules of politeness: It should admit what it's doing, permit itself to be disabled and not do sneaky things like leak personal information.
>
> Google's software principles come as interest is growing at the state and federal level in regulating and perhaps even banning adware and spyware. Utah has already enacted such a law, and the U.S. House of Representatives and the Federal Trade Commission have convened hearings on the issue in the last few weeks.
>
> In a sense, Google's move is a defensive, self-regulatory measure aimed at encouraging the mainstream software industry to find a way to make spyware and adware acceptable.[66]

---

[64] E-Security, 2004. http://www.bigplanet.com/corp/company/industry_statistics.shtml,
[65] "Fighting Spyware on all Fronts: http://www.smallbizpipeline.com/showArticle.jhtml?articleId=159903579&pgno=2
[66] "Google defines good manners for adware" http://news.com.com/Google+defines+good+manners+for+adware/2100-1029_3-5215941.html

The caveat to that is when one visits Google's site and reads the fine print re the "principles", and realizes that perhaps even Google is hesitant to offend the adware architects, thereby inviting retaliation:

> These guidelines are, by necessity, broad. Software creation and distribution are complex and the technology is continuously evolving. As a result, some useful applications may not comply entirely with these principles and some deceptive practices may not be addressed here. This document is only a start, and focuses on the areas of Internet software and advertising. These guidelines need to be continually updated to keep pace with ever-changing technology.[67]

Summarily; be they at home or at the office, technology can go only so far; the end user 'gotta do it, too. Either by virtue of education or compelled by an externally imposed policy on the usage of computer equipment, those end users granted internet access are going to continue to be the most critical components in keeping a corporate network free of adware pests, and their malicious cousins. And until the Utopia of an internet-wide "solution" against its abusers is realized, it will still be up to the individual home users to fasten their seatbelts.

[67] http://www.google.com/corporate/software_principles.html

– Bibliography –

(In order of citation)

"Computer Haiku", http://www.funny2.com/haiku.htm

"Spyware, Adware, and Peer-to-Peer Networks – The Hidden Threat to Corporate Security" Kevin Townsend, April 2, 2003.
http://research.pestpatrol.com/Whitepapers/CorporateSecurity.asp

"Know your enemy", Brett Glass, www.pcmag.com/article2/0,4149,34058,00.asp

www.LabMice.net "Computer Virus Primer for Network Administrators" 11/13/2003
http://labmice.techtarget.com/antivirus/articles/avprimer.htm

"Computer Systems"
http://myweb.tiscali.co.uk/whitefiles/b1_s/1_free_guides/fg1mt/pgs/h01.htm

Symantec Security Response - http://securityresponse.symantec.com/

Advanced Polymorphic Worms: Evading IDS..."Oleg Kolesnikov, andWenke Lee, College of Computing, Georgia Inst. of Technology
http://www.cc.gatech.edu/~ok/w/ok_pw.pdf

"The Challenge of Non-Viral Malware", Pete Cafarchio, TISC Insight Newsletter, Vol. 4 Issue 12.
http://research.pestpatrol.com/Whitepapers/NonViralMalware.asp

Security Glossary - Vision Technology Management, LLC
www.visiontm.com/Spy/Glossary.htm

Combating the New Generation of Malware" Finjan Software, 2004, www.finjan.com

"Drive-by Downloads" http://whatis.techtarget.com/definition/0,,sid9_gci887624,00.html

"Blocking spyware via the ActiveX kill bit" Serdar Yegulalp, 09 Jun 2004
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1059905,00.html

What's Spyware? Let's Ask Congress!" By Larry Seltzer April 5, 2004
http://www.eweek.com/article2/0,1759,1561797,00.asp

"Follow the Bouncing Malware, I-VI" Tom Liston
http://isc.sans.org/diary.php?date=2004-07-23

"Phishing Activity Trends Report",
http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf, the Anti-Phishing Working Group

– Bibliography –
(Continued)

Filter reference sites: http://www3.ca.com/Solutions/Overview.asp?ID=4673&TYPE=S
http://www.redearthsoftware.com/File-filter.htm

The cost of spyware" Network World, 04/26/04
http://www.nwfusion.com/columnists/2004/0426backspin.html

Tech industry presents less-than-unified defense By Byron Acohido and Jon Swartz, USA TODAY http://www.usatoday.com/tech/news/computersecurity/2004-09-09-zombie-response_x.htm

E-Security, 2004. http://www.bigplanet.com/corp/company/industry_statistics.shtml

"Fighting Spyware on all Fronts:
http://www.smallbizpipeline.com/showArticle.jhtml?articleId=159903579&pgno=2

"Google defines good manners for adware":
http://news.com.com/Google+defines+good+manners+for+adware/2100-1029_3-5215941.html_- and software_principles.html

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event