Some Notes on Malware[1]

M. E. Kabay, PhD, CISSP[2]

1 Rogue software

Science fiction authors have long written about artificial life forms. In the early 1970s, author David Gerrold named a program VIRUS and imagined it spreading from computer to computer through phone linkages.[3] Others imagined life-forms evolving in computer networks and predators seeking them out and destroying them.[4] It was a common joke among science fiction fans that one day the North American telephone grid would develop consciousness.

John Brunner's classic book *Shockwave Rider* described a program called a "tapeworm" that could roam the global network, cleaning up information per the sender's programming.[5] At about the same time, researchers at Xerox Palo Alto Research Center (PARC) experimented with using "worms" to perform basic maintenance functions on their local area network.

This isn't entirely science fiction any more.

Computer organisms are reproducing worldwide. Some are mutating at a furious rate, spawning offspring in the blink of an eye. Aggressive anti-virus programs (AVPs) contend with viruses in memory and on disk. With the help of unethical, immoral, careless, stupid or crazy virus authors, viruses evolve in response to selection pressures, hiding themselves in new niches of the computer universe, or "cyberspace." Virus authors even take ideas from each other's viruses, leading to a form of primitive viral sexuality.

2 What are viruses and worms?

Viruses are little programs that copy themselves into "host" programs, into documents or other files from Microsoft Office products, or into special executable "bootstrap" areas of disks. Once these infected programs are executed, the computer viruses, like biological viruses, subvert the normal functions of the operating system (OS). These parasitic programs commandeer CPU, memory and disk resources to replicate themselves. They insert themselves into other host entities, thus spreading the infection. When victims distribute infected programs, diskettes and documents, the viruses extend their range. Computer viruses even show some parallels to sexual reproduction: they can exchange "genetic" material through the agency of the twisted human beings who enjoy creating harmful programs and who share their knowledge with each other. Some macro viruses have been demonstrated to exchange executable code *without* human intervention when they infect the same documents.

Worms are free-standing programs which replicate, usually in networks. They do not integrate their code into host programs.

---

[1] These review materials were prepared for students in the undergraduate and graduate programs in information assurance at Norwich University. I hope that they will be helpful to other instructors and to the general reader. For free access to additional teaching materials see my Web site at http://www2.norwich.edu/mkabay

[2] Associate Professor, Information Assurance & Program Director, Master of Science in Information Assurance, Division of Business & Management, Norwich University, Northfield, VT 05663-1035 USA. mailto: mkabay "at" norwich "dot" edu

[3] Gerrold, D. (1972). *When HARLIE was One.* Republished 1988 by Spectra Books (ISBN 0-553-26465-6). AMAZON link < http://tinyurl.com/dxztw >.

[4] See "A taste of computer security: Viruses" < http://kernelthread.com/publications/security/viruses.html >

[5] Brunner, J. (1975). *Shockwave Rider*. Republished 1995 by Del Rey (ISBN 0-345-46717-5). AMAZON link < http://tinyurl.com/9s5jv >

The popular press has confused the public about these distinctions and seems to apply the word "virus" to practically any kind of computer problem, whether involving replicating code or not. During the Michelangelo scare of 1992, parents were reported as having threatened to take their children out of school for fear the computer virus would affect their health. Several callers to the NCSA virus hotline asked whether viruses could enter their computer through the power cord.

In a splendid example of faulty fact-checking, an issue of *U.S. News and World Report* in January 1992 published an article about the "Iraqi Virus" that had supposedly been used by the US in the Gulf War against Iraq. This virus was supposed to have been inserted in the printer ROMs of equipment sent to the Iraqis before the war; the report said that the virus crawled up the parallel interface cable and infected the host computers running the printers. This report gained wide publicity through the work of a television news show. Unfortunately, the report was based on an April Fool's joke published in 1991 that had caused computer-savvy readers to chuckle briefly and move on to the next spoof. This story has spread through various documents written in the years since then until many people seriously believe that it was a real event. However, despite irrefutable proof of its origin, the story has never been retracted.[6]

3 What do viruses do?

Computer viruses insert their own executable instructions into the normal code of their hosts. Except for the "overwriting" viruses, no functional virus deliberately damages the program it infects. A virus which causes problems in execution of its host will be discovered too quickly to replicate.

3.1 Never harmless

Some computer viruses may be intended to be harmless. Unfortunately, virus writers often write bad code, so their viruses have flaws. Virus authors fail to take into account changes in OS versions – and you can't order an upgrade to your current virus version from your neighbourhood store. These people are testing their programs on our computers – without our permission.

Other viruses are obviously intended to do harm. Their "payloads" include nasty messages clearly identifying the damage they cause or are designed to cause.

Whether intentionally or not, viruses have been observed to

- destroy a disk directory, making it impossible to retrieve your files without special repair utilities;
- erase or modify specific programs or data files;
- interfere with program functions (e.g., slowing down processing);
- create bad sectors on disk;
- decrease disk free space;
- write unwanted volume labels on disks;
- format all or part of a disk;
- use up portions of RAM;
- hang a system, forcing a reboot;

[6] Smith, G. *Crypt Newsletter*. Review of James Adam's 1998 book *The Next World War*. < http://www.soci.niu.edu/~crypt/other/adams.htm >

- interfere with screen displays.

Even when viruses do not in fact cause any tangible or visible harm, their mere presence casts into doubt the integrity of all the programs and data in the infected system.

As for scary messages such as "Now erasing hard disk," I expect to learn one day that a victim will have been found dead of a heart attack. In front of this unfortunate person will be a screen display announcing some horrifying attack on their computer. I wonder if we will ever see a virus author convicted of manslaughter?

3.2 Wasting time

Even trivial effects can have a noticeable effect on productivity. Fridrick Skulason, creator of FPROT (a well-known anti-virus product, or AVP), reported at an NCSA conference in the early 1990s that he had tried the experiment of allowing the Ping-Pong virus (also known as the Italian or Bouncing Ball virus) to continue sending a blip back and forth all over his screen while he was trying to work on a paper. After half an hour he had a headache and felt very irritated with the creator of this pesky virus.

In a session of the *Information Systems Security* course at the University of Ottawa's Institute for Government Informatics Professionals around 1994, a participant reported a case in which a secretary enquired politely if it was possible to "turn off the screen saver in WordPerfect." The entire 12-PC secretarial pool was under the impression that their word processing software came with an undocumented feature – a bouncing ball that moved all over the screen.

Viruses even affect productivity of people whose PCs weren't infected. This phenomenon is known as the *water-cooler effect*. Observers have seen an entire day lost when even a single microcomputer is affected by a virus. Coworkers spend longer on breaks discussing the virus; they congregate at the water cooler and spend valuable time recounting anecdotes about the virus infections their friends have experienced, the virus infections their spouse's friends experienced, and the virus infections they have read about in the computer magazines they read.

Finally, viruses interfere with technical support. Naive users are all too ready to ascribe any problem to viruses. Help-desk staff have reported cases of the Bad-Version Virus, the I-Purged-the-File-but-Forgot Virus, the I-Was-Saving-a-File-When-the-Power-Failed Virus and the Computer-Plug-Fell-Out-of-the-Wall Virus. Convincing the befuddled user to go through systematic diagnosis under these conditions can be a strain on both parties.

3.3 OK, already: install and maintain your antivirus software!

At this point, practically everyone who has ever touched a computer knows that one should run antivirus software that updates itself every day through an Internet connection. Depending on how one counts them, there are about 100,000 different kinds of viruses and worms in existence, of which some 600 or so have actually been noted in real users' computers.[7] There are many acceptable anti-malware solutions available on the market (and even free).[8]

4 Trojan horses

Some of my younger students have expressed bewilderment over the term Trojan "*horse.*" They associate "Trojan" with condoms and with evil programs. Here's a version of the original story:

> ...But Troy still held out, and the Greeks began to despair of ever subduing it by force, and by advice of Ulysses resolved to resort to stratagem. The Greeks then constructed an immense

[7] The number on the WildList for May 2005 was 569 on the main list and 3255 for all sightings. See < http://www.wildlist.org/ >

[8] For a good list of reputable vendors, see the Anti-Virus Product Developer's Consortium run by ICSA Labs (for which I was Director of Education from 1991 to 2000) at < http://www.icsa.net/html/communities/antivirus/avpdmembers.shtml >.

> wooden horse, which they gave out was intended as a propitiatory offering to Minerva, but in fact was filled with armed men. The remaining Greeks then...sailed away....
>
> [The Horse is then dragged into the walled city of Troy and the people celebrate the end of the long war.]
>
> ...In the night, the armed men who were enclosed in the body of the horse...opened the gates of the city to their friends, who had returned under cover of the night. The city was set on fire; the people, overcome with feasting and sleep, put to the sword, and Troy completely subdued.[9]

Bullfinch's *Mythology* thus describes the original Trojan Horse. See < http://homepage.mac.com/cparada/GML/WOODENHORSE.html > for extensive information about the story. Today's electronic Trojan is a program which conceals dangerous functions behind an outwardly innocuous form.

4.1 Case studies

One of the nastiest tricks played on the shell-shocked world of microcomputer users was the FLU-SHOT-4 incident of March 1988. With the publicity given to damage caused by destructive, self-replicating virus programs distributed through electronic bulletin board systems (BBS), it seemed natural that public-spirited programmers would rise to the challenge and provide protective screening.

- Flu-Shot-3 was a useful program for detecting viruses. Flu-Shot-4 appeared on BBS and looked just like 3; however, it actually destroyed critical areas of hard disks and any floppies present when the program was run. The instructions which caused the damage were not present in the program file until it was running; this self-modifying code technique makes it especially difficult to identify Trojans by simple inspection of the assembler-level code.

- HP itself put a Trojan into the HP3000 operating system with IOCDPN0.PUB.SYS. This program's name implied that it ought to be an I/O driver for a CarD PuNch, just like IOTERM0 and IODISC0. Indeed, IOCDPN0 was tagged as a required driver by SYSDUMP so you couldn't get rid of it. However, rather than being an innocuous old driver, the program was actually a powerful utility for accessing the low-level routine ATTACHIO. Using IOCDPN0, one could read and write to the memory structures controlling terminals, tapes, printers, and other peripherals. There were even macros to permit HP technicians to repeat I/O operations when MPE couldn't help because of bad data or other unacceptable conditions. A typical use would be to read a bad tape and recover valuable data unreadable through normal I/O.

- Another Trojan was a blocking-factor program that one of my colleagues wrote. This vanilla program, derived from the Contributed Software Library (CSL) from INTEREX, the International Association of HP Computer Users, calculated optimum blocking factors admirably – but it posted an invisible timed terminal read at an undocumented but fixed period after initialization. If the user knew exactly what to type at exactly which time, he or she could obtain system manager (SM)status and all other capabilities for their user ID for that session. In a sense, this example also illustrates the concept of a back door.

- An incident that looked like a Trojan Horse occurred in 1983, when HP issued one of its periodic revisions of the MPE/V operating system. My operations team and I were just beginning our acceptance tests at 03:00, after production had completed and the operator had finished a full backup. We shut down the HP3000, switched disk packs to the test configuration, and began booting the system with the fresh Master Installation Tapes from HP. To our horror, we saw the message "WARNING: EXPERIMENTAL SOFTWARE PASS ' 9" appear on our console, followed by the usual "DO NOT INTERRUPT WHILE BOOTING." Even though we knew that the only risk was that we'd trash our test disk packs, the message still shocked us. It turned out to be a only a harmless leftover from the Master Installation Tape quality assurance process.

- One of the participants in my Information Systems Security course reported a case of tampering on a UNISYS mainframe used in a military installation. A user was catching up on his work one evening when

[9] Bullfinch, T. (1855). *The Age of Fable.* Now part of *Bullfinch's Mythology*. Modern Library Edition, Random House (c. 1940, no ISBN). P. 185. Currently available edition as Modern Library Paperback; AMAZON link < http://tinyurl.com/7c46v >.

suddenly his display showed every single file in all of his disk directories being deleted one by one. Nothing he could do would stop the process, which went on for several minutes.

He reported the incident immediately to his superior officers. Panic ensued until midnight, when the it was found that a program called JOKE.RUN had been assigned to the function key. The program merely listed file names with "DELETING..." in front of each. No files had actually been deleted. Investigation found the programmer responsible; the joke had originally been directed at a fellow programmer, but the redefinition of the function key had accidentally found itself into the installation diskettes for a revision of the workstation software. It took additional hours to check every single workstation on the base looking for this joke. The programmer's career was not enhanced by this incident.

Some of the first PC Trojans included

- The Scrambler (also known as the KEYBGR Trojan), which pretends to be a keyboard driver (KEYBGR.COM) but actually makes a smiley face move randomly around the screen
- The 12-Tricks Trojan, which masquerades as CORETEST.COM, a program for testing the speed of a hard disk but actually causes 12 different kinds of damage (e.g., garbling printer output, slowing screen displays, and formatting the hard disk)
- The PC Cyborg Trojan (or "AIDS Trojan"), which claims to be an AIDS information program but actually encrypts all directory entries, fills up the entire C: disk, and simulates COMMAND.COM but produces an error message in response to nearly all commands.

4.2 1993-1994: Internet monitoring attacks

Trojan attacks on the Internet were discovered in late 1993. Full information about all such attacks is available on the World Wide Web site run by CIAC, the Computer Incident Advisory Capability of the U.S. Department of Energy < http://ciac.llnl.gov/ciac/index.html >. On February 3, 1994, CIAC issued Bulletin *E-09: Network Monitoring Attacks*. The Bulletin announced,

CIAC and other response teams have observed many compromised systems surreptitiously monitoring network traffic, obtaining username, password, host-name combinations (and potentially other sensitive information) as users connect to remote systems using telnet, rlogin, and ftp. This is for both local and wide area network connections. The intruders may (and presumably do) use this information to compromise new hosts and expand the scope of the attacks. Once system administrators discover a compromised host, they must presume monitoring of all network transactions from or to any host "visible" on the network for the duration of the compromise, and that intruders potentially possess any of the information so exposed. The attacks proceed as follows. The intruders gain unauthorized, privileged access to a host that supports a network interface capable of monitoring the network in "promiscuous mode," reading every packet on the network whether addressed to the host or not. They accomplish this by exploiting unpatched vulnerabilities or learning a username, password, host-name combination from the monitoring log of another compromised host. The intruders then install a network monitoring tool that captures and records the initial portion of all network traffic for ftp, telnet, and rlogin sessions. They typically also install "Trojan" programs for login, ps, and telnetd to support their unauthorized access and other clandestine activities.

System administrators must begin by determining if intruders have compromised their systems. The CERT Coordination Center has released a tool to detect network interface devices in promiscuous mode. Instructions for obtaining and using the tool appears later in this bulletin – the tool is available via anonymous ftp. If a site discovers that intruders have compromised their systems, the site must determine the extent of the attack and perform recovery as described below. System administrators must also prevent future attacks as described below.

CIAC works closely with CERT-CC, the Computer Emergency Response Team Coordination Center of the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, PA. The instructions from CERT-CC included detailed instructions on verifying the authenticity of affected programs and instructions on removing the key vulnerabilities.

A few weeks later, CIAC issued Bulletin E-12, which warned ominously,

> The number of Internet sites compromised by the ongoing series of network monitoring (sniffing) attacks continues to increase. The number of accounts compromised world-wide is now estimated to exceed 100,000. This series of attacks represents the most serious Internet threat in its history.
>
> IMPORTANT: THESE NETWORK MONITORS DO NOT SPECIFICALLY TARGET INFORMATION FROM UNIX SYSTEMS; ALL SYSTEMS SUPPORTING NETWORK LOGINS ARE POTENTIALLY VULNERABLE. IT IS IMPERATIVE THAT SITES ACT TO SECURE THEIR SYSTEMS.
>
> Attack Description
>
> The attacks are based on network monitoring software, known as a "sniffer", installed surreptitiously by intruders. The sniffer records the initial 128 bytes of each login, telnet, and FTP session seen on the local network segment, compromising ALL traffic to or from any machine on the segment as well as traffic passing through the segment being monitored. The captured data includes the name of the destination host, the username, and the password used. This information is written to a file and is later used by the intruders to gain access to other machines.

Finally, another CIAC alert (E-20, May 6, 1994) warned of "A Trojan-horse program, CD-IT.ZIP, masquerading as an improved driver for Chinon CD-ROM drives, [which] corrupts system files and the hard disk." This program affects any MS-DOS system where it is executed.

4.3 Cases from the INFOSEC Year in Review Database[10]

1997.04.29 The Department of Energy's Computer Incident Advisory Capability (CIAC) warned users not to fall prey to the AOL4FREE.COM Trojan, which tries to erase files on hard drives when it is run. A couple of months later, the NCSA worked with AOL technical staff to issue a press release listing the many names of additional Trojans; these run as TSRs (Terminate - Stay Resident programs) and capture user IDs and passwords, then send them by e-mail to Bad People. Reminder: do NOT open binary attachments at all from people you don't know; scan all attachments from people you do know with anti-virus and anti-Trojan programs before opening. (EDUPAGE)

1997-11-06 Viewers of pornographic pictures on the sexygirls.com site were in for a surprise when they got their next phone bills. Toronto victims who downloaded a "special viewer" were actually installing a Trojan program that silently disconnected their connection to their normal ISP and reconnected them (with the modem speaker turned off) to a number in Moldova in central Europe. The long-distance charges then ratcheted up until the user disconnected the session — sometimes hours later, even when the victims switched to other, perhaps less prurient, sites. The same fraud was reported in Feb in New York City, where a federal judge ordered the scam shut down. An interesting note is that AT&T staff spotted the scam because of unusually high volume of traffic to Moldova, not usually a destination for many US phone calls. In November, the FTC won $2.74M from the bandits to refund to the cheated customers.

1998-01-05 Jared Sandberg, writing in the Wall Street Journal, reported on widespread fraud directed against naïve AOL users using widely-distributed Trojan Horse programs ("proggies") that allow them to steal passwords. Another favorite trick that fools gullible users is the old "We need your password" popup that claims to be from AOL administrators. AOL reminds everyone that no one from AOL will ever ask users for their passwords.

[10] Kabay, M. E. (2005). INFOSEC Year in Review. See < http://www2.norwich.edu/mkabay/iyir > for details and instructions on downloading this free database. PDF reports are also available for download.

1999-01-29 Peter Neumann summarized a serious case of software contamination in RISKS 20.18: At least 52 computer systems downloaded a TCP wrapper program directly from a distribution site after the program had been contaminated with a Trojan horse early in the morning of 21 Jan 1999. The Trojan horse provided trapdoor access to each of the contaminated systems, and also sent e-mail identifying each system that had just been contaminated. The 52 primary sites were notified by the CERT at CMU after the problem had been detected and fixed. Secondary downloads may also have occurred."

1999-05-28 Network Associates Inc. anti-virus labs warned of a new Trojan called BackDoor-G being sent around the Net as spam in May. Users were tricked into installing "screen savers" that were nothing of the sort. The Trojan resembled the previous year's Back Orifice program in providing remote administration — and back doors for criminals to infiltrate a system. A variant called "Armageddon" appeared within days in France.

1999-06-11 The Worm.Explore.Zip (aka "Trojan Explore.Zip) worm appeared in June as an attachment to e-mail masquerading as an innocuous compressed WinZIP file. The executable file used the icon from WinZIP to fool people into double-clicking it, at which time it began destroying files on disk. Within a week of its discovery in Israel on the 6th of June the worm had spread to more than 12 countries. Network Associates reported that ~70% of its largest 500 corporate customers were infected. [Readers should remember that the larger the number of computers in a company, the more likely that at least one will be infected even when infection rates are low. If the probability of infecting one system is "p" and there are "n" targets in a group each of which can be infected independently, the likelihood of at least one infection in the group is $P = \{1 - (1 - p)^n\}$ which rises rapidly as n increases.]

1999-09-20 A couple of new Y2K-related virus/worms packaged as Trojan Horses were discovered in September. One e-mail Trojan called "Y2Kcount.exe" claimed that its attachment was a Y2K-countdown clock; actually it also sent user IDs and passwords out into the Net by e-mail. Microsoft reported finding eight different versions of the e-mail in circulation on the Net. The other, named "W32/Fix2001" came as an attachment ostensibly from the system administrator and urged the victims to install the "fix" to prevent Internet problems around the Y2K transition. Actually, the virus/worm would replicate through attachments to all outbound e-mail messages from the infected system. [These malicious programs are called "virus/worms" because they integrate into the operating system (i.e., they are virus-like) but also replicate through networks via e-mail (i.e., they are worm-like).]

2000-01-03 Finjan Software Blocks Win32.Crypto the First Time: Finjan Software, Inc. announced that its proactive first-strike security solution, SurfinShield Corporate, blocks the new Win32.Crypto malicious code attack. Win32.Crypto, a Trojan executable program released in the wild today, is unique in that infected computers become dependant on the Trojan as a "middle-man" in the operating system. Any attempt to disinfect it will result in the collapse of the operating system itself. It is a new kind of attack with particularly damaging consequences because attempting to remove the infection may render the computer useless and force a user to rebuild their system from scratch.

2000-08-29 Software companies . . . reported that the first . . . [malware] to target the Palm operating system has been discovered. The bug, which uses a "Trojan horse" strategy to infect its victims, comes disguised as pirated software purported to emulate a Nintendo Gameboy on Palm PDAs and then proceeds to delete applications on the device. The . . . [malware] does not pose a significant threat to most users, says Gene Hodges, president of Network Associates' McAfee division, but signals a new era in technological vulnerability: "This is the beginning of yet another phase in the war against hackers and virus writers. In fact, the real significance of this latest Trojan discovery is the proof of concept that it represents." (Agence France Presse/New York Times 29 Aug 2000)

2000-10-27 Microsoft's internal computer network was invaded by the QAZ "Trojan horse" software that caused company passwords to be sent to an e-mail address in St. Petersburg, Russia. Calling the act "a deplorable act of industrial espionage," Microsoft would not say whether or not the hackers may have gotten hold of any Microsoft source code. (AP/New York Times 27 Oct 2000)

However, within a few days, Microsoft . . . [said] that network vandals were able to invade the company's internal network for only 12 days (rather than 5 weeks, as it had originally reported), and that no major corporate secrets were stolen. Microsoft executive Rick Miller said: "We started seeing these new accounts being created, but that could be an anomaly of the system. After a day, we realized it was someone hacking into the system." At that point Microsoft began monitoring the illegal break-in, and reported it to the FBI. Miller said that, because of the immense size of the source code files, it was unlikely that the invaders would have been able to copy them. (AP/Washington Post 30 Oct 2000)

2002-01-19 A patch for a vulnerability in the AOL Instant Messenger (AIM) program was converted into a Trojan horse that initiated unauthorized click-throughs on advertising icons, divulged system information to third parties and browsed to porn sites.

2002-03-11 The "Gibe" worm was circulated in March 2002 as a 160KB EXE file attached to a cover message pretending to be a Microsoft alert explaining that the file was a "cumulative patch" and pointing vaguely to a Microsoft security site. Going to the site showed no sign of any such patch, nor was there a digital signature for the file. However, naive recipients were susceptible to the trick.

[MORAL: keep warning recipients not to open unsolicited attachments in e-mail.]

2002-04-03 Nicholas C. Weaver warned in RISKS that the company Brilliant Digital (BD) formally announced distribution of Trojan software via the Kazaa peer-to-peer network software. The BD software would create a P2P server network to be used for distributed storage, computation and communication – all of which would pose serious security risks to everyone concerned. Weaver pointed out that today's naïve users appear to be ready to agree to anything at all that is included in a license agreement, whether it is in their interests or not.

2003-02-14 E-mail purporting to offer revealing photos of Catherine Zeta-Jones, Britney Spears, and other celebrities is actually offering something quite different: the secret installation of Trojan horse software that can be used by intruders to take over your computer. Users of the Kazaa file-sharing service and IRC instant messaging are at risk. (Reuters/USA Today 14 Feb 2003)

2003-05-22 Data security software developer Kaspersky Labs reports that a new Trojan program, StartPage, is exploiting an Internet Explorer vulnerability for which there is no patch. If a patch is not released soon, other viruses could exploit the vulnerability. StartPage is sent to victim addresses directly from the author and does not have an automatic send function. The program is a Zip-archive that contains an HTML file. Upon opening the HTML file, an embedded Java-script is launched that exploits the "Exploit.SelfExecHtml" vulnerability and clandestinely executes an embedded EXE file carrying the Trojan program.

2003-07-14 Close to 2,000 Windows-based PCs with high-speed Internet connections have been hijacked by a stealth program and are being used to send ads for pornography, computer security experts warned. It is unknown exactly how the trojan (dubbed "Migmaf" for "migrant Mafia") is spreading to victim computers around the world, whose owners most likely have no idea what is happening, said Richard M. Smith, a security consultant in Boston. The trojan turns the victim computer into a proxy server which serves as a middle man between people clicking on porn e-mail spam or Web site links, according to Smith. The victim computer acts as a "front" to the porn Web site, enabling the porn Web servers to hide their location, Smith said. Broadband Internet users should always use firewalls to block such stealth activity, he said. Computers with

updated anti-virus software will also be protected, said Lisa Smith of network security company Network Associate's.

2004-01-08 BackDoor-AWQ.b is a remote access Trojan written in Borland Delphi, according to McAfee, which issued an alert Tuesday, January 6. An email message constructed to download and execute the Trojan is known to have been spammed to users. The spammed message is constructed in HTML format. It is likely to have a random subject line, and its body is likely to bear a head portrait of a lady (loaded from a remote server upon viewing the message). The body contains HTML tags to load a second file from a remote server. This file is MIME, and contains the remote access Trojan (base64 encoded). Upon execution, the Trojan installs itself into the %SysDir% directory as GRAYPIGEON.EXE. A DLL file is extracted and also copied to this directory (where %Sysdir% is the Windows System directory, for example C:\WINNT\SYSTEM32) The following Registry key is added to hook system startup: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion \RunOnce "ScanRegedit" = "%SysDir%\GRAYPIGEON.EXE" The DLL file (which contains the backdoor functionality) is injected into the EXPLORER.EXE process on the victim machine. More information, including removal instructions, can be found at: http://us.mcafee.com/virusInfo/default.asp?id=description &virus_k=100938

2004-01-09 A Trojan horse program that appears to be a Microsoft Corp. security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control. Idefense Inc., a Reston, Va., computer security company, said the malicious code is the latest example of so-called social engineering to fool Windows users. It is similar to the W32Swen worm, which last year passed itself off as a Microsoft patch.

2004-03-17 The U.S. Department of Homeland Security has alerted computer security experts about the Phatbot Trojan, which snoops for passwords on infected computers and tries to disable firewall and antivirus software. Phatbot . . . Has proved difficult for law enforcement authorities and antivirus companies to fight.... Mikko Hypponen, director of the antivirus software company F-Secure in Finland says, "With these P2P Trojan networks, even if you take down half of the affected machines, the rest of the network continues to work just fine"; security expert Russ Cooper of TruSecure warns, "If there are indeed hundreds of thousands of computers infected with Phatbot, U.S. e-commerce is in serious threat of being massively attacked by whoever owns these networks." (Washington Post 17 Mar 2004)

2004-05-12 Intego has identified a Trojan horse −− AS.MW2004.Trojan −− that affects Mac OS X. This Trojan horse, when double−clicked, permanently deletes all the files in the current user's home folder. Intego has notified Apple, Microsoft and the CERT, and has been working in close collaboration with these companies and organizations. The AS.MW2004.Trojan is a compiled AppleScript applet, a 108 KB self−contained application, with an icon resembling an installer for Microsoft Office 2004 for Mac OS X. This AppleScript runs a Unix command that removes files, using AppleScript's ability to run such commands. The AppleScript displays no messages, dialogs or alerts. Once the user double−clicks this file, their home folder and all its contents are deleted permanently. All Macintosh users should only download and run applications from trusted sources.

2004-05-18 Security experts are tracking two new threats that have emerged in the past few days, including a worm that uses seven mechanisms to spread itself. The worm is known as Kibuv, and researchers first noticed its presence Friday, May 14. Kibuv affects all versions of Windows from 98 through Windows Server 2003 and attempts to spread through a variety of methods, including exploiting five Windows vulnerabilities and connecting to the FTP server installed by the Sasser worms. The worm has not spread too widely as of yet, but with its variety of infection methods, experts say the potential exists for it to infect a large number of machines. The second piece of malware that has surfaced is a Trojan that is capable of spreading semi−automatically. Known as Bobax, the Trojan can only infect machines running Windows XP and seems to exist solely for the purpose of

sending out large amounts of spam. When ordered to scan for new machines to infect, Bobax spawns 128 threads and begins scanning for PCs with TCP port 5000 open. If the port is open, it exploits the Windows LSASS vulnerability. Bobax then loads a copy of itself onto the new PC, and the process repeats. Antivirus and antispam providers say they have seen just a few machines infected with Bobax as of Tuesday, May 18.

2004-05-20 A Trojan horse may be responsible for an online banking scam that has cost at least two Winnipeg, Canada, customers thousands of dollars. The Winnipeg Police Service is investigating two cases where money was transferred unknowingly from bank accounts. The investigation is focused around a man who recently emigrated to Canada from an unidentified locale in Eastern Europe. According to computer security experts, online banking scams and identity theft are proliferating in Canada. While Canadian e−banking customers have yet to see a surge in identity theft similar to the U.S., the banks say the onus is on consumers and enterprises to protect themselves. Keystroke loggers are the most frequently used tactic for crooks targeting banking information, said Tom Slodichak, chief security officer of WhiteHat, an IT security provider. "Although a Web session with their financial institution is usually encrypted, the keystroke logger intercepts the keystrokes before any encryption occurs, so they will get all the information−−the account numbers, the names, the passwords or PINs or whatever they need to impersonate that [individual]," he said.

2004-08-10 Malicious code that dials premium rate numbers without a user's consent has been found in a pirated version of Mosquitos 2.0, a popular game for Symbian Series 60 smartphones. The illicit copies of the game are circulating over P2P networks. News of the Symbian Trojan dialler comes days after the arrival of the first Trojan for handheld computers running Windows Pocket PC operating system, Brador−A.

2004-10-25 An e−mail disguised as a Red Hat patch update is a fake designed to trick users into downloading malware designed to compromise the systems they run on, the Linux vendor warned in a message on its Website. While the malicious site was taken down over the weekend, the SANS Internet Storm Center posted a message on its Website saying the hoax "is a good reminder that even though most of these are aimed at Windows users, always be suspect when receiving an e−mail asking you to download something."

2004-11-23 A new attack by Trojan Horse software known as "Skulls" targets Nokia 7610 cell phones, rendering infected handsets almost useless. The program appears to be a "theme manager" for the phone. It replaces most of an infected phone's program icons with images of skulls and crossbones, and disables all of the default programs on the phone (calendar, phonebook, camera, Web browser, SMS applications, etc.) – i.e., essentially everything except normal phone calls. Symbian, the maker of the Nokia 7610 operating system, says that users will only be affected if they knowingly and deliberately install the file and ignore the warnings that the phone displays at the conclusion of the installation process. Experts don't consider the Skulls malware to be a major threat, but note that it's the third mobile phone bug to appear this year – and therefore probably means that this kind of problem is here for the foreseeable future. (ENN Electronic News.net 23 Nov 2004)

2005-01-13 Users are being warned about the Cellery worm – a Windows virus that piggybacks on the hugely popular Tetris game. Rather than spreading itself via e-mail, Cellery installs a playable version of Tetris on the user's machine. When the game starts up, the worm seeks out other computers it can infect on the same network. The virus does no damage, but could result in clogged traffic on heavily infected networks. "If your company has a culture of allowing games to be played in the office, your staff may believe this is simply a new game that has been installed – rather than something that should cause concern," says a spokesman for computer security firm Sophos. (BBC News 13 Jan 2005)

2005-01-24 Two new Trojan horse programs, Gavno.a and Gavno.b, masquerade as patch files designed to trick users into downloading them, says Aaron Davidson, chief executive officer of SimWorks International. Although almost identical with Gavno.a, Gavno.b contains the Cabir worm, which attempts to send a copy of the Trojan horse to other nearby Symbian−based phones via short−range wireless Bluetooth technology. The Gavno Trojans, according to Davidson, are the first to aim at disrupting a core function of mobile phones−−telephony−−in addition to other applications such as text messaging, e−mail, and address books. Gavno.a and Gavno.b are proof−of−concept Trojan horses that "are not yet in the wild," Davidson says. Davidson believes the Trojan programs originated in Russia. To fix infected phones, users will need to restore them to their factory settings.

2005-02-11 Microsoft Corp is investigating a malicious program that attempts to turn off the company's newly released anti-spyware software for Windows computers. Stephen Toulouse, a Microsoft security program manager, said yesterday that the program, known as "Bankash-A Trojan," could attempt to disable or delete the spyware removal tool and suppress warning messages. It also may try to steal online banking passwords or other personal information by tracking a user's keystrokes. To be attacked, Toulouse said a user would have to be fooled into opening an email attachment that would then start the malicious program. (The Age 11 Feb 2005)

SOPHOS anti-malware company summarizes the Trojan's functions as follows:
* Steals credit card details
* Turns off anti-virus applications
* Deletes files off the computer
* Steals information
* Drops more malware
* Downloads code from the internet

2005-04-08 On Thursday, April 7, the same day that Microsoft announced details of its next round of monthly patches, hackers sent out a wave of emails disguised as messages from the software company in a bid to take control of thousands of computers. The emails contain bogus news of a Microsoft update, advising people to open a link to a Web site and download a file that will secure and 'patch' their PCs. The fake Website, which is hosted in Australia, looks almost identical to Microsoft's and the download is actually a Trojan horse — a program that can give hackers remote control of a computer. Microsoft said it is looking into the situation.

4.4 Hardware Trojans

On November 8, 1994, a correspondent reported to the RISKS Forum Digest that he had been victimized by a curious kind of Trojan:

> I recently purchased an Apple Macintosh computer at a "computer superstore," as separate components - the Apple CPU, and Apple monitor, and a third-party keyboard billed as coming from a company called Sicon.
>
> This past weekend, while trying to get some text-editing work done, I had to leave the computer alone for a while. Upon returning, I found to my horror that the text "welcome datacomp" had been *inserted into the text I was editing*. I was certain that I hadn't typed it, and my wife verified that she hadn't, either. A quick survey showed that the "clipboard" (the repository for information being manipulated via cut/paste operations) wasn't the source of the offending text.
>
> As usual, the initial reaction was to suspect a virus. Disinfectant, a leading anti-viral application for Macintoshes, gave the system a clean bill of health; furthermore, its descriptions of the known viruses (as of Disinfectant version 3.5, the latest release) did not mention any symptoms similar to my experiences.
>
> I restarted the system in a fully minimal configuration, launched an editor, and waited. Sure enough, after a (rather long) wait, the text "welcome datacomp" once again appeared, all at once, on its own.

> Further investigation revealed that someone had put unauthorized code in the ROM chip used in several brands of keyboard. The only solution was to replace the keyboard. Readers will understand the possible consequences of a keyboard which inserts unauthorized text into, say, source code. Winn Schwartau has coined the word, "chipping" to refer to such unauthorized modification of firmware.[11]

4.5 Diagnosis and prevention

It is difficult to identify Trojans because, like the ancient Horse built by the Greeks, they don't reveal their nature immediately. The first step in catching a Trojan is to run the program on an isolated system. That is, try the candidate either on a system whose hard disk drives have been disconnected or which is reserved exclusively for testing new programs.

While the program is executing, look for unexpected disk drive activity; if your drives have separate read/write indicators, check for write activity on drives.

Some Trojans running on micro-computers use unusual methods of accessing disks; various products exist which trap such programmatic devices. Such products, aimed mostly at interfering with viruses, usually interrupt execution of unusual or suspect instructions and indicate what's happening but prevent the damage from occurring. Several products can "learn" about legitimate events used by proven programs and thus adapt to your own particular environment.

If the Trojan is a replacement for specific components of the operating system, as in the network monitoring problem described by CIAC above, it is possible to compute check sums and compare them with published checksums for the authentic modules.

The ideal situation for a microcomputer user or a system/network manager is to know, for every executable file (e.g., PROG, .COM, or .EXE) on the system

- Where it comes from
- What it's supposed to do.

Take, for example, shareware programs. In general, each program should come not only with the name and address of the person submitting it for distribution but also with the source code. If the requisite compiler is available, one can even compare the object code available on the tape or diskette with the results of a fresh compilation and linkage to be sure there are no discrepancies. These measures make it easier to hope for Trojan-free utilities.

It makes sense for system managers to forbid the introduction of foreign software into their systems and networks without adequate testing. Users wishing to install apparently useful utilities should contact their system support staff to arrange for acceptance tests. Installing software of unknown quality on a production system is irresponsible.

When organizations develop their own software, the best protection against Trojans is quality assurance and testing (QAT). QAT should be carried out by someone other than the programmer(s) who created the program being tested. QAT procedures often include structured walk-throughs, in which designers are asked to explain every section of their proposed system. In later phases, programmers have to explain their code to the QAT team. During systems tests, QAT specialists have to ensure that every line of source code is actually executed at least once. Under these circumstances, it is difficult to conceal unauthorized functions in a Trojan.

5 Spyware

Spyware sends information about user activities to remote sites without the knowledge or approval of the user. This communication is often referred to as "phoning home" in a reference to Steven Spielberg's famous 1982 movie

[11] Tate, C. (1994). Hardware-borne Trojan Horse programs. RISKS 16.55 < http://catless.newcastle.ac.uk/Risks/16.55.html#subj3 >

"E.T.: The Extra-Terrestrial."[12] Spyware has enraged many privacy advocates because much of the *adware* that touts ree access to software in return for allowing ads to appear on computer screens has misrepresented the degree to which it monitors user activity.

5.1 Problems with spyware

Computer scientist Steve Gibson created the OptOut site and associated programs to help users cooperate in researching the activities of spyware and to stop their depredations.[13] Gibson defines spyware as follows:

> Spyware is ANY SOFTWARE which employs a user's Internet connection in the background (the so-called "backchannel") without their knowledge or explicit permission.
>
> Silent background use of an Internet "backchannel" connection MUST BE PRECEDED by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use.
>
> ANY SOFTWARE communicating across the Internet absent these elements is guilty of information theft and is properly and rightfully termed: Spyware.

In his passionate attack on spyware, Gibson writes, "I believe that what you're doing by "customizing", "targeting", "tailoring" and "identifying" the nameless Internet consumer is FUNDAMENTALLY different from anything that has come before. And I believe that doing this secretly and WITHOUT MY PERMISSION is FUNDAMENTALLY wrong, unethical, and EVIL."[14]

Other commentators have noted that spyware may cause other problems for infected users. For example, one writer succinctly summarizes the situation as follows:

> [15]Spyware threats come in different flavors. The spyware agent can be malware (modifies system settings, and can perform undesirable tasks on your system), hijacker (redirects your browser to web sites), dialer (dials a service, most likely porn sites, for which you are billed!), trojan horse (is attached to a program, and performs undesirable tasks on your system), collectware (collects information about you and your surfing habits).
>
> In addition to doing a detailed check of your browser history, spyware can install DLLs and other executables files, send continuous data to the parent, leave a backdoor open for hackers to intercept your personal data or enter your computer, can install other programs directly on to your computer without your knowledge, can send/receive cookies to other spyware programs and invite them into your computer (even if you have cookies disabled), and they can add Trojan horses to your system. Most spyware and adware programs are independent executable files which take on the authorization abilities of the victim. They include auto install and auto update capabilities and can report on any attempts to remove or modify them.
>
> Spyware programs can reset your auto signature, disable or bypass your uninstall features, monitor your keystrokes, scan files on your drive, access your applications, change homepages in addition to displaying advertising content online or offline. They can read, write and delete files and even reformat your hard drive and they do this while sending a steady stream of information back to the advertising and marketing companies. The majority of these programs once installed can not easily be deleted from your system by

[12] Internet Movie Database entry at < http://www.imdb.com/title/tt0083866/ >

[13] http://grc.com/optout.htm

[14] Gibson, S. (2005). The ethics of anonymous surveillance for profit. < http://grc.com/oo/ethics.htm >

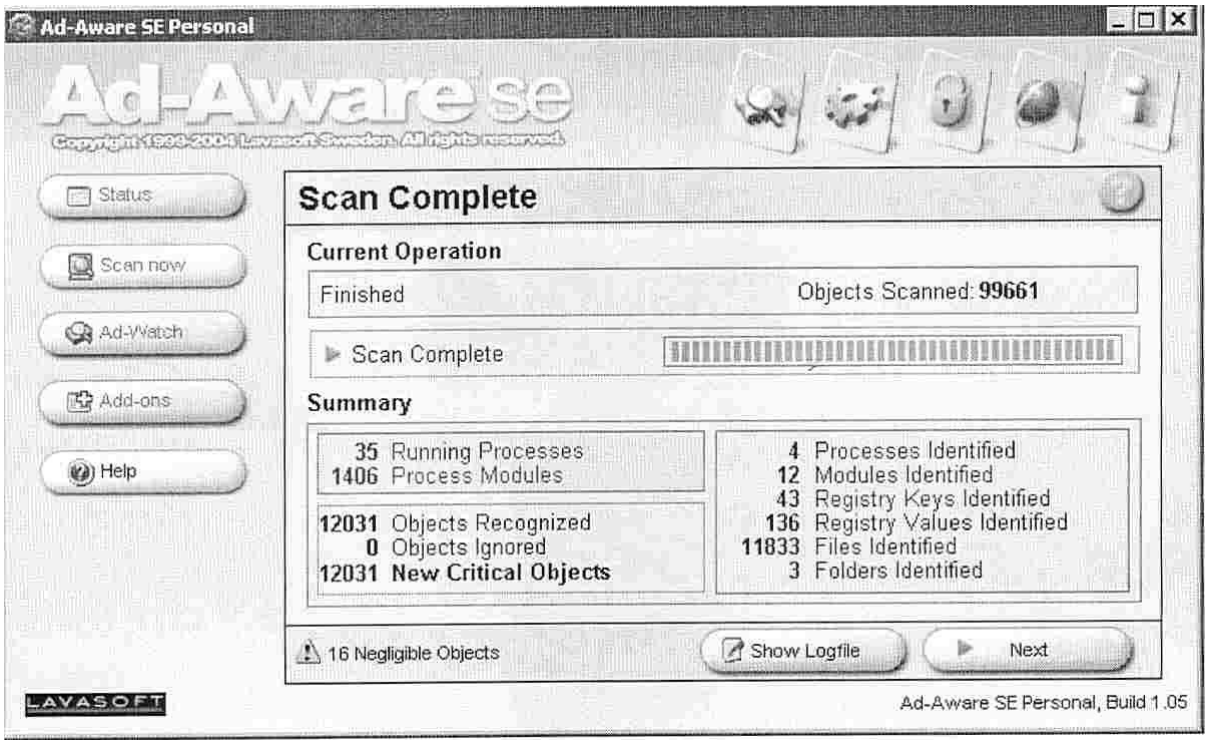
[15] Center for Democracy and Technology: Spyware. < http://www.cdt.org/privacy/spyware/ >

normal methods and often leave components behind to continue to monitor your behavior and reinstall themselves.[16]

5.2 Spyware follies

One of the readers of my *Network World Fusion Security Newsletters*, O. J. Jonasson, CMC, CISSP, SCSE, SCSA, a security consultant, very kindly sent me the following note and has allowed me to quote him:

> In the course of conducting a Technology Planning project for a small local government client, I came across an item that I thought you might amusing.
>
> During interviews, one of their technical support staff was relating their problems with spyware and I politely agreed it's a nuisance these days. But added, that with products like Ad-Aware for home PCs and network appliances like the Fortiguard series for blocking spyware at the network perimeter, its certainly manageable.
>
> He seemed unimpressed and proceeded to tell me of one scan he had performed with Ad-Aware on a desktop in their Aquatic Center that found 12,031 spyware instances. He added that, to him, it was a little more than a nuisance.
>
> Based on my normal skepticism and years of tongue-lashing from my senior consulting partners over supporting documentation and "best evidence," I quite naturally, asked for a copy of the scan – which is attached.



> I imagine it should set the baseline for the *Guinness Book of World Records* – unfortunately, they don't have a category for spyware. Perhaps [*Network World Fusion*] should start their own.

[16] http://www.simplythebest.net/info/spyware.html

Shortly after I received Mr Jonasson's story, reader Ken Ramsey sent me a pointer to a recent article in the 27 January 2005 issue of the excellent "WindowsSecrets" newsletter. Author and editor Brian Livingston reports at length on a recent research study which suggests that even the best anti-spyware products caught barely two-thirds of the test pests implanted on PCs; some of the most popular were down below 50%.[17] It would be important, however, to examine the methodology to find out what pests were used to infest the sample machines and whether they represent the "wild-type" infestations found in real-world machines. Similar issues arose in the early 1990s when the National Computer Security Association (NCSA, later ICSA Labs) started testing antivirus products for certification.

Livingston also mentions an interesting study of real-world infection and infestation rates (high) and security measures (poor) published in October 2004 using 329 "typical dial-up and broadband computer users."[18] The research was carried out by AOL and a new "NCSA:" the National Cyber Security Alliance.[19]

5.3 Web bugs

Web bugs are very small (often only one pixel) images on a Web site; HTML e-mail that includes the URL for these tiny images can record who opened the e-mail message at what time. If there is an instruction requiring automatic refresh of the image as part of the HTML code, is even possible to tell how long the e-mail message was left open on screen.

The service from DidTheyReadIt[20] uses precisely this approach. As described on their Web site and in an article by Mark Glassman in the June 3, 2004 edition of the New York Times, users append ".didtheyreadit.com" to the e-mail address of someone whose reading habits you want to monitor (with respect to your e-mail, that is).[21] The company's servers convert your message to HTML, add a Web bug, and send your converted message to its destination. When a recipient using an HTML-tolerant e-mail reader opens or even previews your spyware-equipped document, the company's servers record when the Web bug was downloaded, the IP address of the reader, and how long the file was kept open. This information is then sent to the sender in an e-mail message.

Similar services are provided by MSGTAG[22] and by ReadNotify.[23]

Evidently, these systems depend on HTML e-mail.[24] In addition to the clumsy method of disconnecting from the 'Net before opening HTML e-mail, there are already simple tools that destroy this functionality at little or no cost.

Wizard Industries makes Email-Tracking Blocker and sells it for $2.99, including a year of updates.[25] This 370 KB utility needs to be run only once. According to the manufacturer, it works with any e-mail service and blocks all tracking services.

Email Sentinel Pro from DSDevelopment is freeware for individuals (non-commercial use) and shareware for corporations ($14.95 per seat).[26] This 815 KB utility runs in the background to convert HTML e-mail messages into

---

[17] Livingston, B. (2005). Anti-adware misses most malware. WindowsSecrets. < http://windowssecrets.com/050127/ >

[18] AOL/NCSA Online Safety Study < http://www.staysafeonline.info/news/safety_study_v04.pdf >

[19] NCSA (Security) < http://www.staysafeonline.info/ >

[20] http://www.didtheyreadit.com

[21] Glassman, M. (2004). Who got the message? There's a way to know. *New York Times*.
< http://www.nytimes.com/2004/06/03/technology/circuits/03spyy.html >

[22] http://www.msgtag.com

[23] http://www.readnotify.com/

[24] Kabay, M. E. (20004). HTML e-mail not worth the risk. *Network World Fusion.* < http://www.nwfusion.com/newsletters/sec/2004/0517sec1.html >

[25] http://www.wizard-industries.com/trackingblocker.html

plain ASCII. It can be configured to handle attachments as well; can keep the original HTML messages in a quarantine buffer in case they are needed; can log its activities; works with any e-mail client; includes whitelist and contact-import; requires no user interaction once it's running. I tested this product and found that it worked fine with one of my e-mail accounts (an IMAP server) but failed with my backup account (a POP3 server). Not only was the message converted to plain text, but an inserted embedded JPG image was converted to an attachment – very convenient and perfectly safe.

For the time being, this suits me fine; I suppose that the inventors will eventually fix bugs that crop up, especially as organizations cough up their $14.95 donations if they are satisfied with the product.

So if you are not keen on having people watch whether you have opened their e-mail messages without telling you that they are doing so, you don't have to stand for it – and it won't cost much or anything to try these defensive tools.

6 Scumware

In recent years, a new way of abusing computer users has spread like a disease through the Web: *scumware*. Scumware is any software that significantly changes the appearance and functions of Web pages without permission of Webmasters or copyright holders. For example, a number of products overlay banner advertisements with other ads, sometimes for competing products. Scumware may add unauthorized hyperlinks to a user's view of a Web page – sometimes using links to possibly objectionable sites. Such programs can interfere with existing hyperlinks by adding other destinations to the intended target. In addition, some products install themselves without warning users of these functions; others bury the details of their Web-page modifications in the extensive legalise of end-user license agreements. Some scumware is difficult or impossible to control; for example, the programs are difficult to uninstall, introduce instability into the operating system, and conflict with other applications.

Scumware is sometimes known as thiefware.

One of the best-known instances of scumware was better documented than most: the Microsoft XP Smart Tags "feature" was announced as an improvement for MS-Office products. Using Smart Tags, specific words in lists could have pop-up menus; these menus could offer options for useful functions such as choosing the style of pasting wanted for text (e.g., formatted, unformatted and so on). Smart Tags were also planned for the MS Internet Explorer (IE) v6 Web browser; however, many critics argued that the way Smart Tags were to be implemented, there would be an opportunity to hijack Web content by showing extra hyperlinks. These extra links would direct users to MS-related sites or to sites which had bought space in the Smart Tag space. There were waves of outrage all over the industry and MS withdrew its proposal for Smart Tags in IE.[27]

6.1 Examples of scumware

Surf+ is an example of a product that adds unauthorized embellishments to Web pages.[28] Using this product, ordinary words become hyperlinks; the scumware adds underlines and highlights keywords in green. It is thought

---

[26] http://www.emailaddressmanager.com/email_sentinel.html

[27] For overviews of the scumware problem, see

- http://www.thiefware.com/
- http://office.microsoft.com/assistance/2002/articles/oQuickSmartTags.aspx
- http://news.cnet.com/news/0-1003-200-6210768.html?tag=mn_hd
- http://www.alistapart.com/stories/smarttags/
- http://scumware.com/press.html

[28] Administrator (2003). How Surf+ works. < http://tinyurl.com/4mf25 >

that about 500,000 users have installed this product. The company makes money by selling links to competing sites; some Webmasters have reported noticeable declines in Web advertising as a result of the modification of user's view of their Web pages. To the horror of some Webmasters, some of the added links send visitors to porn sites who have paid for the, ah, exposure.

TopText (also known as ContextPro) from eZula is bundled with other software (e.g., the KaZaa peer-to-peer file sharing software).[29] Estimates of the installed base run as high as 2 million users. This toolkit is a browser plug-in that gives Internet Explorer the ability to show additional links underlined in yellow lines. The makers defend their product by pointing out that surfers know what they're getting into if they read the end-user license agreements; that their service successfully provides a legal method for increasing business to their clients; and that their system helps to pay for free services for which users would otherwise have to pay.

Greg Searle reported in RISKS on yet another way of annoying Web users.[30] A company called Fastclick provides code that hides pop-up windows (*popunders*) behind the windows already on screen. These pop-ups remain in place and are revealed only after one minimizes or closes the other windows on screen – by which time it is difficult to determine where the pop-ups came from. The solution, such as it is, is to disable JavaScript; alternatively, if one can locate the offending sites, one can put them on a firewall's or brower's exclusion list.

Some products such as Gator used to deliberately *overlay* banner ads; they inserted their own choice of advertisement using exactly the same dimensions as the original banner add and fixed their substitute to the same place on the Web page, thus obliterating the original entirely.[31] Gator, later known as Claria Corporation, enraged anti-scumware activists by its practice of threatening defamation lawsuits against anyone criticizing their products.[32]

Some firewalls also allow the user to reject ads; for example, ZoneAlarm Pro v3.0 has a three settings for ad blocking: HIGH blocks all ads; MEDIUM blocks ads that don't load within a user-stipulated time as well as all pop-up ads; and OFF lets all ads through. Ad-blocking software can perform the same function without firewall capabilities; type "ad blocker" into GOOGLE or another search engine and you'll find dozens of such tools.

So here's the essential problem: a Webmaster creates a Web page and includes links and advertisements. Some other company or person provides software to a user that alters the functions and appearance of the Web page before the user can see the intended Web page. Many vendors and users say that it's the user's own business what they do to the Web page once it reaches the user's own computer; however, many Webmasters and other content providers argue that their work is being modified without their permission. I will return to this issue in section 6.3 below.

6.2 Home-page snatchers, features, ad-mail, data modification

In addition to Web-page modifiers, another variant of scumware makes unauthorized changes in the system registry to alter a user's home page. For example, there was a pornographic Web site (now a dead URL) called "mycpworld.com" that exploited typing errors by people trying to reach "mypcworld.com". As described by Lincoln Spector writing for *PCWorld*, the rogue Web page apparently forwarded browsers to an offshore Web site that included a JavaScript module which inserted an undocumented change in the system registry at every system bootup to alter the browser's home page to the porn site.[33]

In a related problem, some programs from Microsoft make changes to text without notification or control. For example, Microsoft XP versions of FrontPage 2002, Word 2002, Excel 2002, PowerPoint 2002, or Outlook 2002

---

[29] See eZula's description at < http://www.ezula.com/TopText/TopText.asp > and compare the critical analysis at < http://www.doxdesk.com/parasite/TopText.html >

[30] Searle, G. (2001). New technology for sneaky advertising. RISKS 21.47 < http://catless.ncl.ac.uk/Risks/21.47.html#subj8 >

[31] Martin, M. (2003). Gater eWallet. < http://tinyurl.com/5cy3r >

[32] "jcokos" (2003). Scumbag: Gator / Claria < http://tinyurl.com/79vyc >

[33] Spector, L. (2002). Invasion of the browswer snatchers. < http://www.pcworld.com/news/article/0,aid,84464,tk,dnWknd,00.asp >

removes double slashes from all hyperlinks typed in its Office XP suite. There is no way of turning off this "feature."[34]

Some forms of scumware intercepts e-mail. John Gehl and Suzanne Douglas of the estimable *NewsScan* daily news summary[35] wrote,

> Admail, a new technology marketed by Australian online marketing firm Reva Networks, enables advertisers to intercept e-mail messages as they enter the mail server and "wrap" them in advertising content tailored to the recipient's demographic profile. Reva Networks CEO Robert Pickup says the concept has proven more effective than other forms of online advertising. "Because the advertising is embedded within a regular e-mail and not a separate e-mail message from an advertiser, users are more likely to open the message and hence be exposed to the advertising offer." Pickup says he doesn't think consumers will be annoyed by the ads "as long as it's relevant to them." But Australian Consumer Association IT policy officer Charles Britton says he doesn't think that consumers will passively accept advertising with their personal e-mail: "Without some incentive, why would you want advertising in your e-mail?" (ZDNet Australia 22 Jun 2001)

Geoffrey Brent identified yet another weird data modification back in 2002. If you open two MS-Excel files and copy a cell containing a number and paste it into a cell in the other file, everything works fine. For example, 1.2345 gets copied as 1.2345 regardless of how many figures are showing in the cell. However, if you open file A, copy a number, *close file A*, and then paste the number into file B, you get a value that is identical to what was *visible* rather than to what was entered in the original cell. Thus in the example above, if 1.2345 in the source were visible as 1.23, the copy would become 1.23 in the destination worksheet.[36] Although this is an undocumented, unauthorized data modification, this time it presumably results from quality assurance failures, not intention or malice.[37]

I will review some of the ethical and legal issues underlying the trouble over scumware. In particular, the question comes down to who owns the image of a Web page when it's in a browser window?

6.3 Legal and ethical issues with scumware

In an interview with Stephanie Olsen in September 2001, Gator chief Jeff McFadden discussed his view of the ad overlays.[38] First of all, said McFadden, Gator ads can be moved away from the ad they overlay and they are clearly labeled as coming from Gator. They are no different from any other window that might obscure part of another window. Asked about a popup ad for a credit card that overlay an identically-sized ad for a competing credit card, McFadden assured the interviewer that the overlay was popped us because the product deduced that the viewer might be interested in credit cards; the product does not "know" that its ad is overlaying the banner from a competing product.

Why did McFadden launch a lawsuit against the Interactive Advertising Bureau (IAB) in August 2001?[39] McFadden told Olsen that, "Some IAB representatives made some egregious statements about the company – a little bit of name calling, but mainly telling people that they thought that our ad model was illegal. I spoke to the IAB and they said they weren't interested in retracting those statements. And that can have a pretty substantial impact on our business. We have 200 advertisers, many of them Fortune 500 and Fortune 50 companies, and I just can't have them saying that what they're buying from us is illegal. So we filed the action (last) Monday."

---

[34] Arnold, J. (2001). Office XP modified what you type…. < http://catless.ncl.ac.uk/Risks/21.42.html#subj12 >

[35] < http://www.newsscan.com >

[36] Brent, G. (2002). Excel cut-and-pasting behavior. RISKS 21.88 < http://catless.ncl.ac.uk/Risks/21.88#subj10 >

[37] The behavior described was still true for Excel 2002 (Excel "XP") version 10.6501.6735 SP3 running in July 2005.

[38] Olsen, S. (2001). Nobody's going to skin this Gator. C|net < http://news.com.com/2008-1082-272563.html?legacy=cnet >

[39] Featherly, K. (2001). Gator chomps first, sues Internet Advertising Bureau. BizReport < http://www.bizreport.com/news/1990/ >

But how is what scumware does any different from, say, having a user put a Post-It (TM) note on her monitor that obscures part of a Web page? Surely users can do what they want with Web pages that have been copied to their own cache?

Well, no, not really.

A look at the IAB's 28 August 2001 press release shows an uncompromising title (caps are in the original): INTERACTIVE ADVERTISING BUREAU (IAB) ASSERTS GATOR.COM'S BUSINESS PRACTICES VIOLATE THE CONTRACT, TRADEMARK AND COPYRIGHT INTERESTS OF WEB PUBLISHERS AND ADVERTISERS: UNFAIR COMPETITION AND DECEPTIVE PRACTICES IN VIOLATION OF FEDERAL LAWS."[40]

Before we go any further, let me warn readers using the mandatory disclosure that I am not a lawyer and this is not legal advice. For legal advice, consult an attorney experienced in these areas of intellectual property and contract law.[41]

From my point of view as a lay observer, the arguments presented by the IAB and other opponents of scumware boil down to the following (and I am using the generic "scumware" instead of focusing only on Gator's products):

- Scumware makes unauthorized changes in the appearance and content of Web pages that affect more than a single user.
- The changes imposed by scumware interfere with contractual relationships between Web content providers and advertisers.
- The introduced advertisements and links may convey a false impression implying relationships and possibly endorsements that do not exist.
- The modifications may be creating an unauthorized derivative work.

From an international perspective, European laws are more restrictive than US laws in defining what are called the *moral rights* of not only a copyright holder but also the rights of the creators of intellectual property. Scumware, under this doctrine, may violate the content-creator's rights of integrity, disclosure, retraction, and replies to criticism. Unauthorized modification of what users see on a Web page may violate all of these rights.[42]

Those opposing scumware will have to articulate why they don't also go after firewalls and ad-blockers that speed up Web access by reducing the amount of graphical data transmitted to a browser. Perhaps one factor reducing the outrage over *blocking* ads is that no one is going to be offended by *not* seeing an ad; although the advertisers may not like the idea, at least there is no chance of casting the Web site in a false light (an important element of the concept of defamation in US jurisprudence).

From a purely ethical (as opposed to narrowly legal) standpoint, it seems to me that scumware is a bad idea on several grounds:

---

[40] The IAB press release was originally at < http://www.iab.net/news/content/08_28_01.html > but is no longer on the Web at that URL. I checked GOOGLE again in July 2005 but could not locate the original statement.

[41] See also the dated but still useful and interesting course *Cyberspace Law for Non-Lawyers* by law professors Larry Lessig, David Post and Eugene Volokh from the mid-1990s; archived at < http://www.eff.org/legal/CyberLaw_Course/ >

[42] Al Fasoldt has an excellent set of commentaries along these lines:

- Scumware, Part 1: Sneaky software hits a new low. < http://twcny.rr.com/technofile/texts/bit100301.html >
- Scumware, Part 2: Typical scumware programs and what they do. < http://twcny.rr.com/technofile/texts/bit101001.html >
- Scumware, Part 3: How to hunt it down and get rid of it. < http://twcny.rr.com/technofile/texts/bit101701.html >

- The people who benefit from the introduced materials (links and ads) are not the people who invested time and money in creating the underlying content; this situation seems unfair.

- If everyone engaged in such behavior, Web pages could become cluttered with extraneous matter and obscure the underlying content entirely – just imagine running several different scumware programs at once to see what might result.

- Obscuring other people's messages and adding unauthorized linkages seems disrespectful of the human beings who created the original Web page; such behavior seems to me to be disregarding the Web designers' feelings and intentions.

7 Stopping spyware and scumware

First, you must decide if you approve of transmitting information about your Web-surfing habits to advertisers or if you like having advertisements and hyperlinks inserted into the views of Web pages that appear on your screen. If you do, there's no problem for you as a user.

For those who don't like the idea of covert data transfer and extraneous links and ads, the most obvious measure for preventing infestation is not to install spyware and scumware at all. Unfortunately, this is not as easy as one would like. As we have seen in previous articles, spyware and scumware can infest other software and be installed with little or no notice to the user. Nonetheless, before installing freeware, shareware, or adware (products that offer services in return for sending the user targeted ads), everyone would do well to read about the product using an Internet search engine such as Google.

Check the lists of known scumware at http://scumware.com to see if the product you are thinking of installing is a known offender. Without gritting your teeth too hard, read the end-user license agreement (EULA). Look for language, no matter how convoluted or how tiny the point size, that indicates that the product is likely to add to or modify the appearance of Web pages you download. In addition, look for language that threatens to delete or inhibit any of your *other* programs. As I was completing the original version of this article in 2002, Declan McCullagh's admirable PoliTech list published a fascinating glimpse of the mindset of some adware makers. The RadLight adware product comes with a EULA that reads in part, "You are not allowed to use any third party program (e.g Ad-aware) to uninstall application bundled with RadLight. Such programs will be removed."[43]

While you are installing *any* software, from no matter what source, always keep your firewall active if at all possible. Be sure to configure your firewall to alert you to any attempt to contact an external address from inside your system; although such attempts may occasionally be necessary (e.g., for updates to critical components), in many cases they can be blocked safely. You can always study the issue more closely if necessary by examining the TCP address of the target and doing a reverse IP-block lookup to find out where the critter is trying to connect. Once you know the name of the registrant and the Domain Name System entry for the target, block the transmission without hesitation if you don't know why a module on your system is trying to communicate with a site you know nothing about. You can always reverse your decision later if you determine that the connection is in your interest.

To identify undocumented or forgotten adware, spyware and scumware, several real-time scanners can spot trouble for you. The scumware.com site lists several:

- NOD32 - Real time Virus Detection & Removal 01/28/2005)

- CoolWebShredder - CWS variants 01/28/2004)

- Free Virus Information & Tools 01/28/2004)

[43] See < http://www.politechbot.com/p-03439.html > for details.

- AdAware - Scumware Detection & Removal 07/19/2003)

I have been happy with the PestPatrol product that was created under the direction of my old friend Bob Bales, one of the original founders of the old National Computer Security Association (later called ICSA and eventually TruSecure) for which I worked for a decade. Bob gave me a free perpetual license for his product years ago and I have been using and updating it ever since to remove scumware and spyware. It also includes TSR (terminate-stay-resident) tools that scan memory constantly for new pests that try to install themselves and prevents them from infesting a protected machine. PestPatrol was bought by Computer Associates around 2002 and is now a well-respected and regularly-updated product.[44]

[44] See < http://store.ca.com/v2.0-img/operations/safer/site/0605/1.htm > for current information.

