BLACK HAT:

MISFITS, CRIMINALS, AND SCAMMERS IN THE INTERNET AGE

John Biggs

Apress®

Black Hat: Misfits, Criminals, and Scammers in the Internet Age

Lead Editor: Jim Sumser
Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, Jason Gilmore, John Franklin, Chris Mills, Steve Rycroft, Dominic Shakeshaft, Jim Sumser, Karen Watterson, Gavin Wray, John Zukowski
Project Manager: Kylie Johnston
Copy Edit Manager: Nicole LeClerc
Copy Editor: Mark Nigara
Production Manager: Kari Brooks
Production Editor: Ellie Fountain
Proofreader: Linda Seifert
Compositor: Molly Sharp, ContentWorks
Indexer: Valerie Perry
Artist: April Milne
Cover and Interior Designer: Kurt Krames
Manufacturing Manager: Tom Debolski

Library of Congress Cataloging-in-Publication Data
Biggs, John, 1975-
Black hats : misfits, criminals, and scammers in the Internet age / John Biggs.
p. cm.
Includes bibliographical references and index.
ISBN 1-59059-379-0 (alk. paper)
1. Computer security. 2. Computer crimes. I. Title.

QA76.9.A25B539 2004
005.8--dc22

2004010327

Printed and bound in the United States of America 10987654321

Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010 and outside the United States by Springer-Verlag GmbH & Co. KG, Tiergartenstr. 17, 69112 Heidelberg, Germany.

In the United States: phone 1-800-SPRINGER, e-mail orders@springer-ny.com, or visit http://www.springer-ny.com. Outside the United States: fax +49 6221 345229, e-mail orders@springer.de, or visit http://www.springer.de.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail info@apress.com, or visit http://www.apress.com.

CHAPTER 3

Deep Cover: Spyware

Jennifer Pazdan thought she needed an exorcism.

In 2002, Pazdan, then a student at the University of Illinois at Champaign-Urbana, recalled downloading the popular file-sharing programs Morpheus and Kazaa as well as an addictive video game called Snood. Then her computer started acting strangely. Small ads started popping up on her desktop and hiding themselves under her browser windows. Her new computer took on a life of its own, taking ten minutes to perform basic tasks as the hard drive churned like a jet engine. Software that she didn't recognize began causing her Internet browser to crash, forcing her to shut down her computer repeatedly.

"This has all been a really frustrating and time-consuming experience," she said.

Chances are Pazdan's nightmare has happened to you. You're surfing the Internet and a small window pops up, something innocuous or perhaps something racy enough to catch your attention. There are search assistants, XXX toolbars, helpful tools like BonziBUDDY and Claria, formerly Gator. These tools, called adware, or in angrier circles, spyware, are designed to allow companies to target their marketing campaigns toward certain groups of Internet users. But spyware doesn't stop there. Some programs even cede control of your computer to an attacker, allowing them to capture your passwords, credit-card numbers, and personal email.

Whether it's through negligent programming or poor system configuration, faulty adware can be seen as a parasitic program designed to supply its makers with revenue or market share, and it damages the host computer in the process. I've seen spyware that constantly reloads itself under a new name. As you stomp out one copy, another rages in into the fray, hogging resources with each new zombielike process. The software that infested Pazdan's computer probably installed itself silently without notification. Often, however, spyware writers include some basic information that appears in long licensing legalese, known as an End User License Agreement (EULA), which is shown before installation. Many users—myself included—ultimately barrel through this

information (see Figure 3-1) without reading or caring what they click to complete the installation.

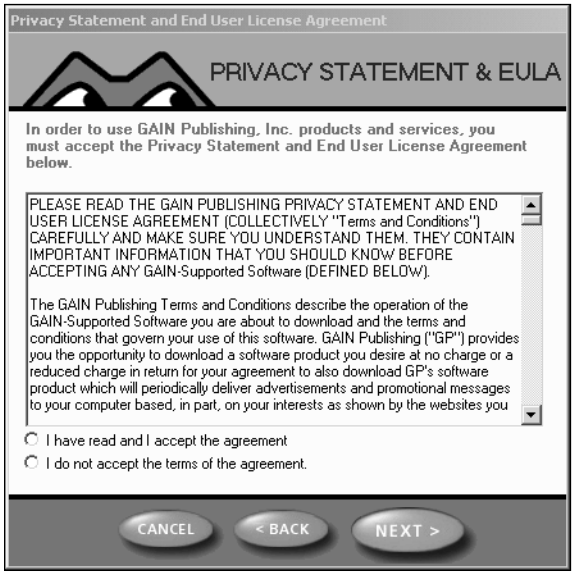

Figure 3-1 Ever read one of these? Neither have I. Many of these EULAs contain clauses that forbid you from writing negative reviews of the software, owning programs and images you create using the software, and a number of other nasty little surprises.

There are many different types of spyware, and like cancer, they can be separated into two categories, malignant and benign. Ask anyone who has battled with spyware, and they may have a few more colorful terms to offer.

Benign Spyware

The term "benign spyware" is almost an oxymoron. Spyware is designed to allow marketers to get a better picture of website visitors and computer users with or without those users' permission. These forms of spyware are relatively innocuous and are based on noninvasive technologies. You can think of these programs and systems as bloodhounds that can follow your tracks online.

Data Miners

These programs capture your browsing habits and send information on the sites you visit, such as how long you stayed at each site, and how many products or services you purchased at online stores. These programs often run in

the background, quietly collecting information and then reporting back to a spyware "mother ship" where this data is processed. Interestingly enough, Microsoft's own activation scheme once included a full data-mining component that reported the programs that were installed on any particular computer as well as a list of hardware components.

Ad Servers

This form of spyware displays ads that may or may not be related to your browsing habits. For example, when you visit an online travel site, ad servers will create small windows that offer access to a competing travel site. This spyware often creates pop-ups and, less frequently, pop-unders that advertise goods and online services.

Rerouters

There are two forms of rerouter spyware: Internet rerouters and hard rerouters. When you're attacked by an Internet rerouter, it's usually because you've mistyped a common URL and you're being rerouted to a competing site. Suppose you wanted to visit `www.google.com`, but you mistyped and ended up at `www.googl.com`. There you would find a competing site that offers to set your start page, which is the page that opens when you start up your Internet browser, to another advertising site.

Hard rerouters, on the other hand, are programs that replace legitimate web content with advertisements that are served up by a competing site. For example, a hard rerouter may be able to recognize banner ads on a web page and replace those ads with its own ads. It may also reroute you completely, ignoring the URLs you type in and choosing to send you elsewhere.

Trackers

These can be as innocuous as the "cookies" that your web browser uses to handle online forms and login functions for web-based email and the like. A tracker assigns a specific number or ID to your computer, allowing various sites to cater advertising to your particular system or track your movements on the Internet. Unlike data miners, trackers usually aren't programs. In this case, you're passively tracked by participating websites.

Malignant Spyware

These programs are the worst of the worst. Black hats use them to collect valuable information about you. Using a simple Trojan horse or keystroke logger, they can collect passwords, personal information, and credit-card numbers.

Keystroke Loggers

Keystroke loggers, or keyloggers, capture and transmit every single keystroke you type on your computer. They may also take screenshots and record your desktop as you work or allow someone to view your desktop while you work.

Backdoors

These allow a black hat to log in to your computer and control it remotely.

Trojan Horses

These are programs that masquerade as other programs and then inject a malignant payload. They're usually used in conjunction with other types of spyware.

Chameleons

Like Trojan horses, these programs mimic the behavior of common, trusted applications. For example, some chameleons appear as AOL login screens, inviting a user to enter a login and password. Instead of connecting to AOL, this program sends the information to a black hat waiting in the wings and reports an error.

As you can see, some spyware watches your browsing habits and reports back to a central server, thereby creating an analytical model of your behavior. Other systems point users toward sponsor sites and force the user's start page to change almost daily, usually to something they would never want to look at in the first place. Other systems are quieter, watching for upgrades and system changes and reporting back with license information for installed software.

In 2002, Microsoft's System Update utility was branded spyware by online activists because it returned a list of all installed software and hardware on host systems. System Update runs regularly on all computers running Windows XP and Windows 2000 and allows Microsoft to add patches, or additions and bug fixes, to systems. Privacy advocates were outraged when they saw that most of their software holdings were being sent back to the giant in Redmond, ostensibly to understand and improve future versions of Windows. This, however, is like your Volkswagen calling Germany and telling a central computer what you like to listen to on the radio, whether you drive over the speed limit, and what kind of tires you installed. It's information that isn't valuable to a tech team but of inestimable value to a marketing cabal.

Many DVD- and CD-playing programs also report the title and IP address of the systems they're running on, although software manufacturers claim that

this information isn't stored in any central database. This information is used to gauge the popularity of downloads and, in the case of the unlimited-music download service eMusic, ban repeat downloaders from the service, accusing them, often erroneously, of giving out their account login information to other nonpaying users. These tactics, though useful in the short term, erode the inherent trust between many online customer-company relationships, as DoubleClick quickly found out during the dot-com boom. The company, which tracked a user's clicks from website to website, faced a drubbing in the press for playing fast and loose with user's private browsing habits.

Browser cookies are another usually innocuous form of spyware. These tiny files can be used to track a user's shopping cart in online stores or email websites and allow users to log in automatically without having to retype passwords. Many online marketers, however, use these files to track a user from page to page without their knowledge, measuring a user's habits down to the second and giving marketing teams a detailed report of the most and least popular pages on the site. In fact, every time you visit a website, your IP address and browser types are sent along with your various clicks and requests. Although the vast majority of websites discard this information, it's always available to eavesdroppers or interested marketers. At this point, many software companies are getting into the act, posting scary-looking messages and banners warning unwitting users that their IP address is being broadcast to the world. In the right hands, this information can allow an intruder to access your computer, although cases of this are extremely rare. Some privacy enthusiasts even go so far as to surf anonymously using systems like Anonymizer, which masks the browser's IP address completely.

The real question is whether these small attacks on your privacy and systems truly add up to a growing epidemic. Like spam, adware and its technologies, when used thoughtfully and tactfully, can be beneficial for marketers, who gain a better understanding of their customers, and users, who can use these feedback methods to pinpoint goods and services on the Internet. However, an overdose of often poorly designed and intrusive spyware is enough to make any computer user think twice about downloading or browsing a seemingly polluted Internet.

Know Your Enemy

The rise of spyware has been aided by the growth of broadband Internet connections. Most spyware requires an uninterrupted connection in order to maintain a connection with a distant server. Before the rise of always-on Internet service, some of these programs would attempt to dial an ISP almost constantly. This process usually brought up a small window and interrupted a

user's work, a tip-off to the true nature of the spyware. Now that many systems no longer use dial-up connections, spyware can remain hidden and send occasional messages out across the network unnoticed.

When spyware was in its infancy, early programs actually changed content on web pages, replacing ad banners on some pages with their own images and creating hyperlinks based on advertisers. Imagine if you visited a site about cellular phones and every mention of the word "phone" was a linked to a cut-rate phone service provider. This spyware not only installed itself without the end-user's knowledge, but also monitored and actually changed web pages on the fly, overriding the real ads on some pages. There was a program released in 2001 called TopText that did this, and the outcry was deafening. Webmasters resented the fact that the browser, an already complex program that was designed to render online content as accurately as possible, would begin subverting the designer's wishes and adding links and advertisements with no one's tacit approval.[1]

The first real spyware fracas occurred in 1999 when Intel announced it would embed a unique serial number in all of their Pentium III processors.[2] These numbers could be read by software and hardware and ostensibly be used to improve encryption schemes and allow system administrators to track inventory. Regular users, however, saw a far more sinister problem. The serial numbers gave companies a chance to pinpoint a user's computer on a network and assign software, media, or services to work or not work on certain machines. This antipiracy measure could easily be expanded to watch mobile devices, using the Pentium III chip, move on a network and allow marketers to pinpoint a user's position and habits. Technology, clearly, has given Orwell's vision of Big Brother a boost.

Intel relented and informed users that they could disable the serial-number function through a startup menu. But the damage was already done. With every new step forward in technology, an army of antispyware advocates and their lawyers follow one step behind, scrutinizing each advancement in terms of privacy and control. Whereas earlier hardware and software systems were often accepted outright as improvements, fears of identity theft and privacy issues have stymied more than one technology often before it even leaves the R&D labs.

Creators of adware and other pieces of invasive software defend their programs, saying that they serve a useful purpose in the software ecosystem, adding special features that users may never have known they were looking for. Unlike viruses and worms, they say, adware is mostly innocuous and

---

[1] *Danny Sullivan, "Forget Smart Tags; TopText is Doing What You Feared," SearchEngineWatch.com.* See `http://searchenginewatch.com/sereport/article.php/2164091`.

[2] *Jack Robertson, "Intel To Embed Serial Numbers On Pentium III Chips," TechWeb, January 20, 1999.* See `www.techweb.com/wire/story/TWB19990120S0017`.

provides a service to users. Spyware gives adware a particularly bad name, says Avi Naider, CEO of WhenU, the company behind SaveNow, a program that Pazdan had to remove before her computer began acting normally. SaveNow is a program that displays advertising when users visit certain websites. A web surfer on a travel site will see an ad for a competing travel site. A sport site visitor will see an offer for a subscription to a competing print magazine.

Mr. Naider defends his product as a tool that serves up advertisements based on a user's personal preferences, and he says it doesn't rely on the usual scattershot methods used by many advertisers. He makes it clear that users seek out his product, accepting it as they download other popular software. Unfortunately, in Pazdan's case, she failed to read the fine print that informed her that SaveNow would be added to her computer. This oversight cost her hours when her computer was out of commission.

Adware advocates are adamant that it's the user's responsibility to read and accept the agreements before installing any software.

"It's a source of great frustration for us when knowledgeable observers do not read our license agreement and do not look at what we do and then lump us with other players who don't adhere to our standards of privacy," said Naider.

He maintained that only a few SaveNow users have complained about the software and that his company collects no information about its users. Pazdan's case was extreme, by any measure. Many users click past SaveNow's windows without a second thought, believing pop-ups and pop-unders are the price of browsing the Internet, like primetime advertising or magazine cards: annoying but inevitable.

"When you lump all adware together and call it spyware, you are doing a disservice to the makers of free software who are looking for a legitimate revenue model that protects consumers at the same time," said Naider.

The adware/spyware argument has even gone to court. Claria, formerly Gator, went as far as to sue PC Pitstop, a creator of antispyware software, for libel.[3] Claria produced a program called Gator eWallet, which holds a user's online identity in one central location. Gator starts up every time the computer is turned on and, allegedly, reports surfing habits back to a central server. Many systems consider Gator a piece of spyware, but Gator officials begged to differ. Ultimately, anti-adware advocates believe that all adware that parasitically installs itself along with other software, with or without the user's permission, is spyware. The definition, however, is as amorphous and unstructured as the Internet itself.

---

[3] *Paul Festa, "See you later, anti-Gators?" CNET News.com, October 22, 2003.* See `http://news.com.com/2100-1032_3-5095051.html`.

Underhanded Ads

The adware marketing model, one of unobtrusive links in pop-under windows, has replaced more effective and more obtrusive advertising systems.

Pop-up windows, in fact, are falling out of favor as users learn how to disable them in their browsers. Pop-unders, which hide under other windows until a user begins shutting other windows, almost seem like a natural fixture on many desktops after a browsing session. A company called X10, purveyors of ubiquitous spy-camera pop-ups and pop-unders, recently lost a $4.3 million lawsuit brought against them by the creators of pop-under technology. This is a testament to the popularity and perceived value of this basic and annoying web bug.[4]

In light of falling revenues and an apparent lack of interest in traditional banner ads, adware creators feel that more intrusive measures are in order. As these programs hit the Internet, a dedicated group of antispyware programmers treat them like viruses released into the wild. Programs like Ad-aware (see Figures 3-2 and 3-3), Spybot—Search & Destroy, and Spy Sweeper, among others, work in the same way antivirus software works. Individual spyware programs have their own distinct signatures, a few special lines of code hidden in the body of the program, or certain files that show up in certain types of spyware.

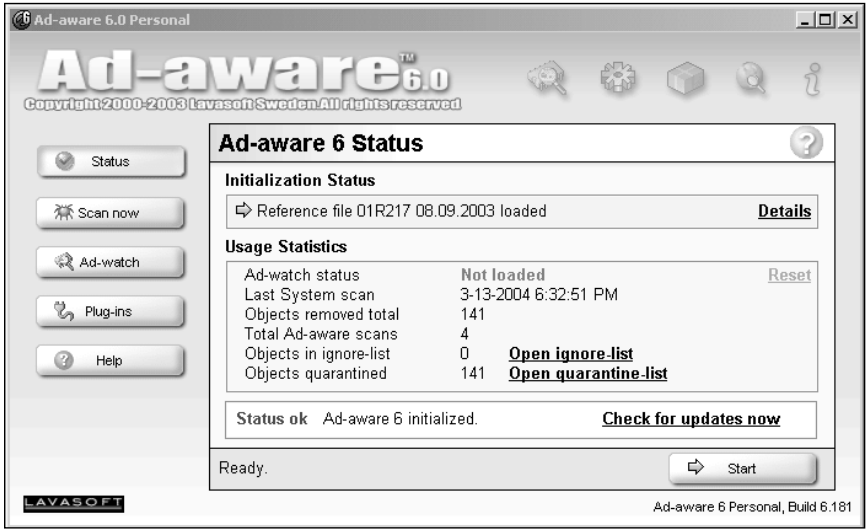

Figure 3-2 Spyware hunter. Lavasoft Sweden's Ad-aware scans your computer for spyware and wipes it out. Some spyware actually deletes programs like Ad-aware.

[4] *Associated Press, "Brothers Win 'Web Bully' Lawsuit," October 20, 2003.*

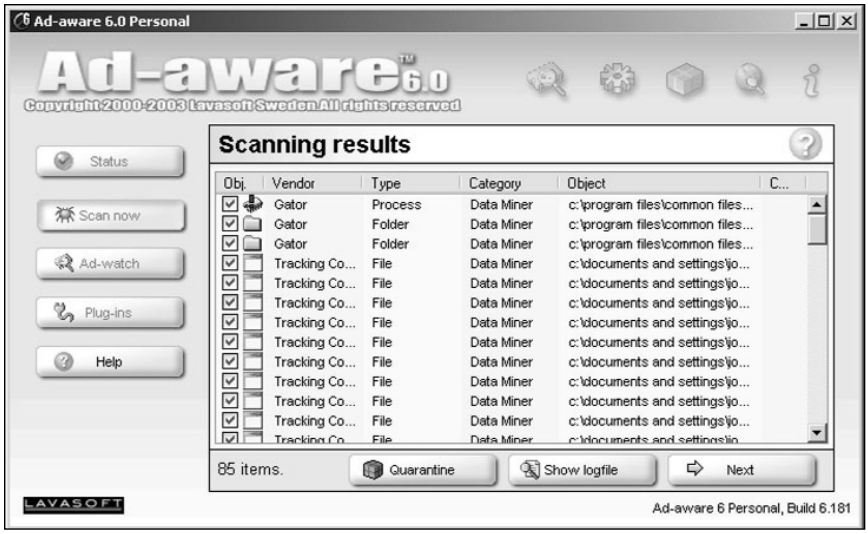

Figure 3-3 A particularly fruitful hunt. After practicing some unsafe browsing (using Internet Explorer, clicking Yes to all possible pop-up windows), I found myself with 85 spyware files. Thankfully, Ad-aware was able to bump them off.

Mike Healan, curator of an antispyware site, `www.spywareinfo.com`, says that the programs are designed to lure users to e-commerce sites and in rare cases pornographic sites, and are churning up debate as companies try to drum up business through adware.

"They are parasites on the body of the Internet," he says.

The most popular carriers of spyware are peer-to-peer networking tools like Kazaa and LimeWire, along with "free" software like MP3 players and games. This form of bundling ostensibly allows programmers to give out software for free, but unfortunately the damage incurred by the spyware usually outweighs the value of the software itself. Lost resources cause other programs to crash, and increased disk space and bandwidth usage slow down the system, sometimes to the point of failure.

Other sources of spyware are porn websites. These sites use Microsoft's DirectX programming framework to push programs onto an unsuspecting, or otherwise occupied, user. These windows appear as legitimate messages that many users accept, thinking they are accepting security certificates and the like.

Figure 3-4 shows a software-acceptance dialog box that allows for Gator's software to be installed automatically upon clicking Yes. Unfortunately, this window also looks similar to any number of web certificates and error screens that appear when browsing. Many users will gloss over this screen, even though it's augmented by information regarding Gator's GAIN ads. The Gator Corporation clearly asserts that this content is safe and this ephemeral certificate exonerates Gator from any responsibility because it clearly states the possible ramifications of installing their software (Figure 3-5).

Figure 3-4 Gator software-acceptance dialog box.

Figure 3-5 Always trust content from GAIN Publishing? Many users ignore these security warnings completely. Clicking Yes will install Gator, which was once one of the most notorious pieces of spyware on the Internet.

Other pieces of spyware insinuate themselves onto a user's browser, placing a special button or text box, ostensibly adding value to a user's browsing experience by leading the browser towards predefined websites and posting ads using pop-under and pop-up windows.

For example, programs like GAIN's DashBar or Weatherbug (Figure 3-6) load into your browser or onto your desktop, obscuring some desktop real estate and hosting ads and other information without your knowledge or permission.

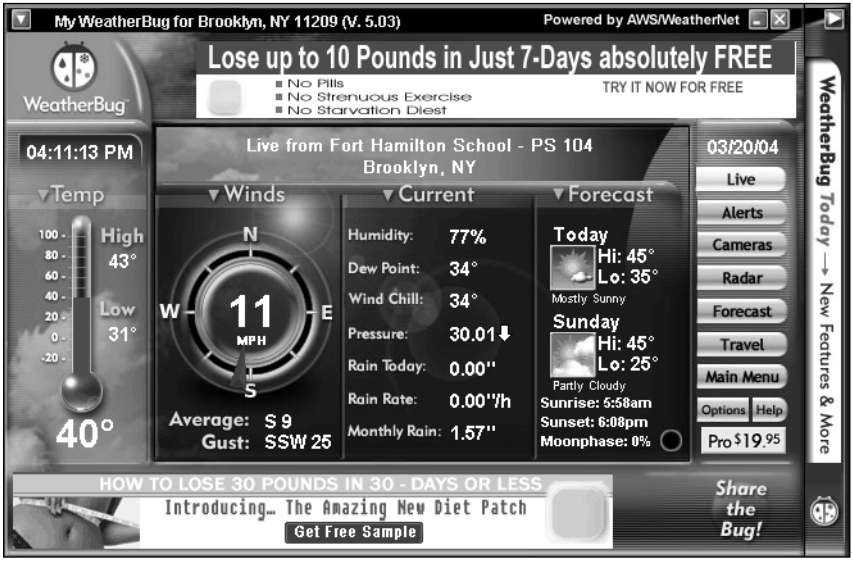

Figure 3-6 Weather, wind speed, humidity—and ads. WeatherBug is considered a particularly stubborn piece of ad-serving spyware.

Removal of these programs is usually a long and complicated process. In fact, my father, a 65-year-old, fairly tech-savvy retiree, fell victim to spyware. As programs like Gator, DashBar, and WeatherBug slowly took over his computer, I was forced to act as a remote troubleshooter, walking him through diagnostic procedures that eventually led to a costly upgrade. In order to avoid another wholesale infection, I decided to give him an entry-level version of Linux. This operating system, completely secure and almost foolproof, has yet to be infected by any of the nasties that plagued him for months.

Spyware vs. Antispyware

RadLight is a small group of developers based in Slovakia who produced a downloadable multimedia player and bundled two programs, New.Net and SaveNow, with their own product. These two products are considered virulent spyware by the antispyware community, which describes them as "parasites."

The software posts ads based on a user's browsing patterns and certain URLs chosen by online marketers. The software reports back to SaveNow's central servers, sending a record that includes the URL that triggered SaveNow to start in the first place, as well as the user's IP address.[5]

Igor Janos, a RadLight developer, said he decided to bundle the adware after he realized that customers weren't voluntarily paying the $10 he charged for his multimedia software.

"Only 45 users have registered for a total of $450," he said. "This amount of money is definitely not enough to run a serious business."

So he augmented his revenue by allowing the producers of New.Net, a program that sells new domain names with endings like .mp3 and .xxx, and SaveNow to bundle their software with his. The companies pay Janos for including the software with his program and record the number of clicks RadLight users register on SaveNow's central ad servers. This shows SaveNow which affiliates have the most active ad clickers.

Janos believes that users are aware that they're installing SaveNow and New.Net and that it was in any case not his company's fault if users didn't read the license agreement.

"RadLight is definitely not the one to blame," he says.

In 2002, the RadLight team also added a function to their program that searched for and deleted Lavasoft's Ad-aware. This is in fact similar to the way some viruses or Internet worms delete antivirus software in order to thwart attempts at disinfection.

"If Lavasoft is right and my programs are indeed dangerous, then I'd like to see proof," he said in defense of his decision. "Until then, I consider Ad-aware an illegal uninstaller."

The problem with most adware, antispyware advocate Healan says, is that it preys on often inexperienced users of the Internet who are prone to accepting attachments and other software without first considering the consequences. Programs like viruses and worms can spread themselves without user intervention, but destructive privacy-eroding spyware is in plain sight, putting the onus on the user to refuse to accept it, which often results in a completely failed installation. RadLight, says Janos, is ad-supported, meaning that the program and the adware cannot be separated. If you refuse one, the other won't load.

Corporations are also concerned by the growth of spyware. Software like SaveNow and Gator post rival advertisements over a company's carefully calibrated and designed website. This intrusion isn't only annoying, it also eats into a company's web-driven sales, and the selective nature of the pop-ups makes users think that the window is actually sponsored by the website they're visiting. This led a number of companies to attempt to sue adware vendors for impinging on their trademarks.

---

[5] *and.doxdesk.com, "SaveNow."* See `www.doxdesk.com/parasite/SaveNow.html`.

Moving giant U-Haul charged that SaveNow broke trademark laws when it showed competing movers' ads over U-Haul's own online ads. In a brief filed at the US District Court in the eastern district of Virginia, U-Haul brought the problem of spyware out of the shadows, just as a number of high-profile cases have increased the visibility of spam and black-hat hackers.

But in September 2003, a federal judge disagreed. Pop-ups and adware were intrinsic parts of the online experience.

District Judge Gerald Bruce threw out the case, stating that, "The fact is that the computer user consented to this detour when the user downloaded WhenU's computer software. While pop-up advertising may crowd out the U-Haul advertisement screen through a separate window, this act is not trademark or copyright infringement, or unfair competition."[6]

This case essentially legitimized the methods of many adware purveyors. Luckily, anti-adware advocates are hard at work creating newer and more impressive systems for stopping adware at the source. Ad-aware and other anti-adware programs can search out and destroy these programs with one click, and online databases of adware programs allow individuals to dig these programs out of their systems through a number of arcane steps, bypassing the protections spyware writers embed in their programs. Luckily, however, most of these programs are innocuous and merely annoying.

In fact, traditional adware is fast becoming a thing of the past. As Internet technologies improve, companies are finding better ways to track users from site to site without the user's knowledge or permission. These backdoor antics are even more nefarious than standard spyware because the user rarely knows he's being watched. Thanks in part to the crash of the dot-coms, companies have become more careful, and more secretive, about their marketing efforts.

Unfortunately, there are far nastier forms of spyware out there, and their numbers are growing.

Sneaky Tricks

Juju Jiang probably has your password.

Jiang, a New York City–area hacker, was caught in July 2003 capturing passwords, credit-card numbers, and private emails from public computers in Kinko's copy stores across Manhattan. Jiang, who used a piece of spyware called a keystroke logger (see Figures 3-7 and 3-8) to capture over 450 logins and passwords, was caught when he attempted to transfer money from a captured user's account through NETeller, an online money-transfer system.[7]

---

[6] *Stefanie Olsen, "Court: Pop-ups burden of using Net," CNET News.com, September 8, 2003. See* `http://news.com.com/2100-1024_3-5072663.html?tag=fd_top`.

[7] *Keven Poulsen, "Guilty Plea in Kinko's Keystroke Caper," Security Focus, July 18, 2003.*

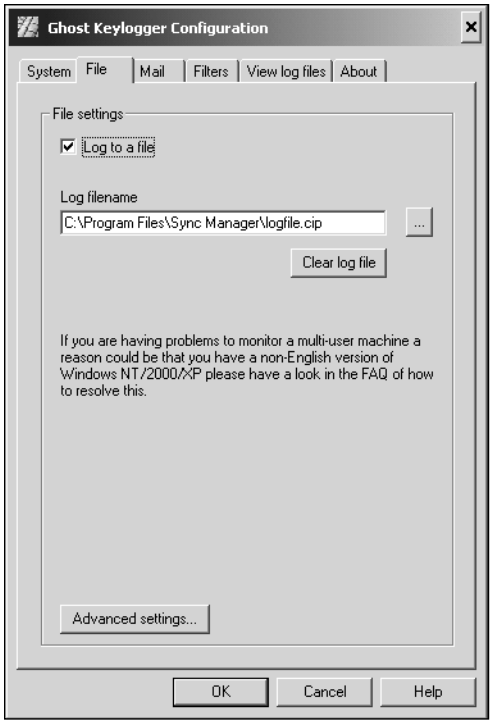

Figure 3-7 A keystroke logger in action. Keystroke loggers usually save logs of keystrokes in innocuously named files on your computer. Many computers can become completely invisible to the average user.

The improbably named Jiang, who was arrested and charged with computer fraud in December 2002 and who could face up to five years in prison and a $250,000 fine, used a simple form of spyware, also called Magic Lantern, to spy on every single keystroke written to Kinko's computers by every user. This virulent form of spyware captured passwords as they were typed and opened up hundreds of computers to attack. Jiang was finally caught when he connected to a captured GoToMyPC-enabled computer that allowed him to completely control the victim's computer. The victim only noticed Jiang on his computer when his computer turned on and his mouse began to move of its own accord on the screen.

This form of spyware is far more dangerous than basic ads appearing on a user's desktop. A keystroke logger like the system Jiang used to steal his passwords could silently capture and transmit keystrokes over the Internet.

Keystroke loggers also come in a hardware form and are about as long as an AAA battery. These loggers, usually attached between the user's keyboard and the computer, can capture hours of keystrokes and can only be unlocked using the cracker's own password.

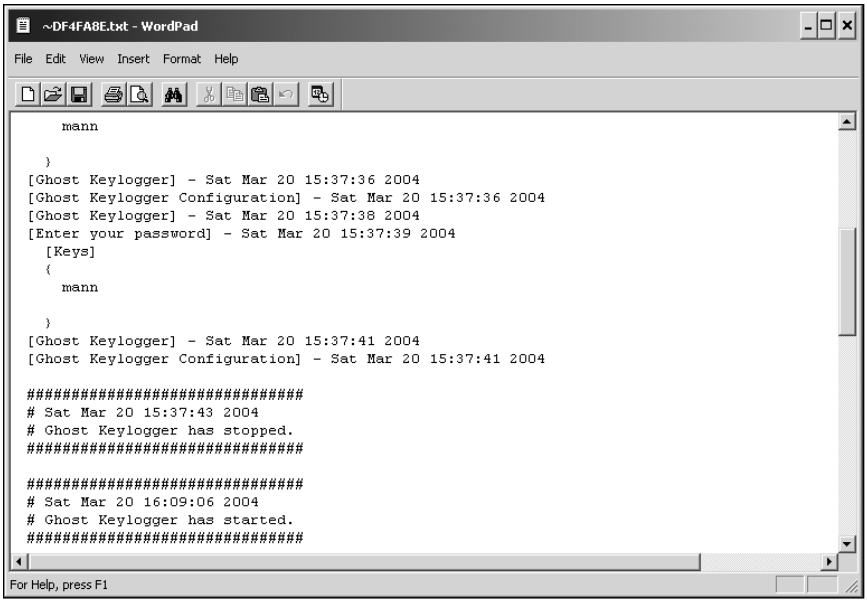

Figure 3-8 The results of a keystroke logging session. Note the password I've collected. Almost every piece of text that appears on the victim's screen is stored in an encrypted file for later playback.

There are also programs, like Spydex, Inc.'s Anti Keylogger, that can detect and prevent keystroke logging, but in most cases, the victim is oblivious.

Many antivirus programs and other systems now consider keystroke loggers dangerous and remove them accordingly. However, they are increasingly used in business environments when an employer is attempting to catch an employee downloading porn or wasting time online. Keystroke loggers are also used by detectives who wish to catch a cheating spouse in a tryst or by hackers like Jiang who use the information to take control of a victim's system.

Other forms of spyware include worms that carry back doors. These programs open up a port into your private computer that allows a programmer, or even someone familiar with the program, to take control of the system completely. These systems, also called rootkits, give remote users full access to a victim's files over the Internet, sometimes even tunneling through firewalls and hiding their tracks in a mishmash of encryption. Many of these programs also take over a system in order to serve pirated files or send out spam.

In some rare cases, even established companies are getting in on the act by adding payloads to their programs that can be used to serve ads from remote computers, essentially stealing a user's processing cycles to process graphics or for other purposes.

Opponents of adware protested this spring when they learned that Altnet, a 3D advertising program, had been bundled with Kazaa. The software came from Brilliant Digital Entertainment, an advertising technology company in Woodland Hills, California that had licensed Kazaa's file-swapping technology.

Brilliant Digital, an Australian company that acquired the popular Kazaa file-sharing program in May 2003, created a program that was designed to piggyback onto the program's capabilities and process 3D graphics in a massive grid computing system. In a grid computer, a full set of computers receives orders to process a data-intensive task like 3D rendering or advertisement serving. Like a bucket brigade, one system processes a tiny part of a file and then passes it on to the next system, which in turn adds its own piece of processing to the finished product. The fastest grid computer in the world, the Earth Simulator in Japan, was created by chaining thousands of low-powered systems together. It can simulate weather patterns, migration, and explosions.

Brilliant Digital originally designed Altnet to activate itself automatically on computers running Kazaa whenever the user's system received a signal from the company. Although the company explained that the activation would occur only with the user's permission, online users were outraged by what they saw as an intrusion. Brilliant Digital quickly scrapped the plan although the technology is clearly in place to create a large-scale grid of nonvoluntary computers. In the same way thousands of volunteers donate spare computer time to worthy causes like SETI and protein folding, an intrepid company could capture thousands of hours of computing time to process anything from high-powered computer animation to ad serving, without the user's knowledge.

Lessons Learned

Spyware is like poison ivy. It can be avoided if you look for the signs, but once you have it, it's a painful ride. Spyware makers depend on user carelessness to spread their software. Much free software, including games and media players, is funded in part by adware. Programs like RadLight, which are usually homegrown, tend to carry the most adware. Addictive puzzle games spread almost virally over the Internet yet don't have quite the draw to get any number of paid users. Companies like SaveNow offer product bundles, a system that automatically installs its own adware along with the partner's software. After SaveNow tabulates the ads displayed, the product producer, in theory, receives a check for the impressions served. This is much like placing a billboard on an apartment building, except that this billboard tends to keep the tenants up all night with huge flashing lights and annoying sounds. Clearly, it may be good for the landlord, but the tenants, or users, would just as soon be rid of it.

The threat of virulent spyware is also growing. The best advice to avoid keystroke loggers is to rarely, if ever, use public-access terminals to check sensitive things like email or credit-card and bank balances. Security experts will say that it pays to be paranoid. In many cases this is true.

Anti-adware programs are currently all the rage, and ironically, even spammers and adware purveyors are getting into the act, offering anti-adware software in the very ads served by adware servers.

A bevy of websites track the rise and fall of spyware in the wild. Sites like `www.SpywareGuide.com` include full lists of regular adware and suspected adware as well as information on how to remove the programs without further damaging your system. Because of the hidden nature of most adware, however, it isn't as visible a problem as spam or worms. Adware is designed to stay under a user's radar indefinitely and only rarely is its true function revealed.

Ultimately, it's up to you, the end users, to become careful software consumers. The long, boring legalese in most EULAs often mentions the types of rights software manufacturers grant themselves when a user accepts one of these licenses. Although most of these rights are innocuous, it only takes one or two spyware-infested programs to turn a brand new computer into junk.