Cyber Criminal Activity: Methods and Motivations

Presented for

Cyber Security and Homeland Security

(University of Washington CSE P 590TU

UC Berkeley PP 190/290-009

UCSD CSE 291 (C00))

by

Elijah Joshua Esquibel

Michael A. Laurenzano

Jing Xiao (James)

Ted Zuvich

December 7, 2005

Introduction

Cyber criminal activity on the Internet is pervasive and increasingly sophisticated. Attackers use a variety of methods (spam, phishing, keylogging, etc.) to steal money and cause harm using the Internet. This paper discusses two major classes of tools used by cyber criminals to accomplish these goals: spyware and botnets. It describes spyware and botnets, why cyber criminals use them, how they use them, and how businesses and individuals can defend themselves from these attackers. In addition, we briefly discuss the current legal situation surrounding the use of botnets and spyware and propose several possible things that could be done to help the situation.

Introduction to Spyware

The term "spyware" covers a broad category of malicious software authored to take control of a computer's operation without the full consent of that machine's legitimate user. While the term literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party. This is still somewhat vague, because it is notoriously difficult to create a useful and fair definition for spyware [1] [2] [3] [4]. Experts have noted that any technical definition of spyware will usually include many non-spyware programs along with the spyware itself[5].

Spyware Before the Internet

---

[1] Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, "Measurement and Analysis of Spyware in a University Environment," *Proc. NSDI 2004*, March 2004.
[2] "Chapter 2: History of Spyware," http://www.pcsecuritynews.com/spyware_history.html
[3] Mary Landesman. "Sly Wares," http://remediator.shavlik.com/e_article000366966.cfm
[4] Steven Gribble. "Spyware,"
http://www.cs.washington.edu/education/courses/csep590/05au/lectures/slides/Gribble_110905.ppt
[5] ibid

This work focuses on modern spyware, which is spyware developed and spread as a result of the increase in the popularity of the Internet since the 1990s. Spyware existed in other forms before this point (such as keyloggers[6] being installed on hard targets), but the landscape of spyware has become much more interesting since the Internet boom. This is because the Internet offers the possibility of continuously reporting and delivering content to and from the target. The Internet also allows attackers to easily perform a much larger number of spyware installations.

Browser Cookies

Around 1996, the Doubleclick[7] network began to use tracking cookies to gather information about users' surfing habits[8]. This was achieved by having web sites save and read browser cookies from other sites that were also on the Doubleclick network. This allowed each Doubleclick site see which other Doubleclick sites the user had previously visited. For a while there was a general sense of panic over the implicit invasion of privacy that these browser cookies presented.

While the apparent threat that browser cookies pose has not changed, it should be noted that users can protect themselves against cookies simply by exerting more control over the download and storage of cookies; they can disallow cookies from untrusted or unknown domains or delete cookies periodically. Cookies could probably be considered the least invasive form of spyware because they are not kept secret from the user and the user has complete control over their use, including the ability to disable cookies

---

[6] Sachin Shetty, "Introduction to Spyware Keyloggers," http://www.securityfocus.com/print/infocus/1829
[7] Doubleclick, http://www.doubleclick.com/us/
[8] David Cole, Symantec Corporation. "Spyware and Adware Fundamentals," http://enterprisesecurity.symantec.com/Content/webcastinfo.cfm?webcastid=200

altogether. For the remainder of this work we will not be referring to browser cookies when we refer to general spyware, unless it is specifically stated.

Spyware Behavior

Unlike viruses and worms, spyware does not usually self-replicate. Like many recent viruses, however, spyware exploits infected computers for commercial gain. Typical tactics includes delivery of unsolicited pop-up advertisements, theft of personal information such as names, addresses and credit card numbers, monitoring of web-browsing habit for marketing purposes, or routing of HTTP requests to advertising sites.

Some spyware can make changes to computers that can be annoying and can cause the computer to slow down or crash. Some spyware has the ability to change the Web browser's home page or search page, or add additional components to the browser that the user does not need or want. They can also make it very difficult for the user to change the computer's settings back to the original state, and they resist detection and un-installation.

From the perspective of anti-spyware makers[9], spyware includes:

- Adware: the most common kind of spyware, adware generates several types of ads, possibly keyed to the sites that the user visits on the Internet. Adware may download programs onto a PC without the user's knowledge or consent.
- Adware cookies: installed without the user's knowledge, these tiny pieces of code store information about surfing habits. Cookies can allow marketing companies to create and sell a profile of the user.

[9] "Spyware's threat to PCs is growing", Dan Richman, Seattle Post Intelligencer.

- Browser hijacker: changes the settings in the Internet browser; can change the chosen home page or redirect searches. A hijacker may render the browser useless.
- Dialer: disconnects the computer from the user's Internet service provider and reconnects to the Internet using an expensive phone line.
- Keylogger: records all the keystrokes made on the computer. A keylogger may allow a third party to access logins, passwords, credit card numbers, and other sensitive information.
- System monitor: records keystrokes plus e-mail, chat room conversations and instant messages. May be accessible to a third party.
- Trojans: programs that let outsiders make changes to the computer. Might create or delete files, or install other programs without the user's knowledge.

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. That does not mean all software, which provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but "pay" for the service by agreeing to receive targeted ads. If you understand the terms and agree to them, you may have decided that it is a fair tradeoff. You might also agree to let the company track your online activities to determine which ads to show you. The key point in all of these cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

Spyware Threat and Damage Analysis

Spyware is pervasive. Most Internet PCs have, or have had, it. According to an October 2004 study by America Online and the National Cyber-Security Alliance, 80% of surveyed users' computers had some form of spyware, with an average of 93 spyware components per computer[10]. Approximately 89% of surveyed users with spyware reported that they did not know of its presence, and 95% reported that they had not given permission for it to be installed. In addition, many websites contain spyware. According to a very recent study by the University of Washington, 1 in 8 executables on the web are piggybacking spyware, and 0.1% of random Web pages are trying "drive-by" installs on the client machine[11].

Nor is spyware confined to home users. The average amount of spyware on business machines is similar to home users – largely because most companies do not have centralized, managed anti-spyware protection in place. Many companies also fail to properly educate their employees to do the basic protection such as timely patch updates. It is a problem that should scare big businesses as they face up to the fact that important data could be leaking out of their organizations daily. Certain spyware – such as that used by P2P networks like Kazaa – is also bandwidth intensive as it communicates a significant amount of data between machines, which can be a burden on corporate networks.

Spyware steals some of the value of the computer from its legitimate users. It slows down the computer and sometimes it even crashes it. It changes the setting of the computer so that they are not easy to recover. Sometimes spyware problems are so severe that they can only be resolved by a re-installation of the whole computer operating

[10] AOL/NCSA **Online** Safety **Study**, http://www.staysafeonline.info/pdf/safety_study_v04.pdf.
[11] Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, "Measurement and Analysis of Spyware in a University Environment," *Proc. NSDI 2004*, March 2004.

system, which consumes time and effort. Sometimes users even choose to discard the computer and totally replace it because they think their computer is just too slow and they are not aware of the existence of the spyware programs on their computer.

Spyware also reduces the reliability of a computer. For example, 50% of Microsoft windows system crashes are caused by spyware based on the results obtained from the Dr. Watson tools. Spyware also increases the support cost for hard ware systems greatly. 30% of product supports calls in Dell, HP and IBM are caused by spyware. Estimated support costs due to the spyware are $2.5 million plus per year[12].

Here we can have a look at an affiliate fraud example to see how spyware might affect different groups of people. WhenU[13] and 180 Solutions[14], have written a "stealware" which aims at affiliate marketing[15]. These programs redirect the payment of affiliate marketing revenues from the legitimate affiliate to the spyware vendor by placing the spyware operator's affiliate tag on the user's activity or replacing any other tag, if there is one. In November 2003, MSNBC reported that during September 2003, 180 had earned more than $100,000 in commissions from more than $4 million of purchases at Dell through this practice[16].

This harms just about everyone involved in the transaction other than the spyware operator. The user is harmed by having their choices thwarted. Having their earned income redirected to the spyware operator harms a legitimate affiliate. Affiliate marketing networks are harmed by the degradation of their reputation. Vendors are

---

[12] David Aucsmith. "Crime on the Internet: Dealing with Spyware, Botnets, and Other Cyber Attacks," http://www.cs.washington.edu/education/courses/csep590/05au/lectures/slides/Aucsmith_110905.ppt, slide 78.
[13] WhenU, http://www.whenu.com/
[14] 180 Solutions, http://www.180solutions.com/
[15] New York Times, Sept 2002, "New Software Quietly Diverts Sales Commissions," http://www.nytimes.com/2002/09/27/technology/27FREE.html
[16] MSNBC, Nov. 2003, "Pop-ups prove profitable, persistent", http://msnbc.msn.com/id/3541497/

harmed by having to pay out affiliate revenues to an "affiliate" who did not contractually earn them.

Spyware is becoming such a sizeable problem in the US that the government voted unanimously in spring 2004 to approve the first ever anti-spyware bill. The Securely Protect Yourself Against Cyber Trespass (Spy Act)[17], approved by the US House of Representatives, would levy fines up to $3 million for those who illegally collect personal information, change a browser's default home page or bookmarks, log keystrokes, or steal identities.

Spyware is also directly affecting government departments. Federal agencies are not prepared to deal with the triple Internet menaces of spam, phishing and spyware, government auditors have concluded. A survey of the largest federal agencies by the Government Accountability Office revealed that most agencies are suffering from junk e-mail and other online detritus -- but not one has a plan in place to deal with the threat and all have received limited guidance on what to do. "Our analysis of the incident-response plans or procedures provided by the 20 agencies showed that none specifically addressed spyware or phishing," says the GAO report that was published June 2005[18].

Attackers and Goals of Attacks

In the spyware arena, attacks can come from any one of a variety of sources. In adware, individuals and businesses can gather your personal information and computing habits for compilation into a database to use for either their own directed marketing

[17] 109th Congress , H.R. 29: Securely Protect Yourself Against Cyber Trespass Act, Spyware Internet Protection bill, http://www.govtrack.us/congress/bill.xpd?bill=h109-29.
[18] INFORMATION SECURITY: Emerging Cybersecurity Issues Threaten Federal Information Systems, United States Government Accountability Office, Report to Congressional Requesters. May 2005, http://www.gao.gov/new.items/d05231.pdf

purposes or to sell to other advertisers. Companies like Claria[19], eZula[20], WhenU, and 180 Solutions distribute the most commonly seen adware. These companies typically make their adware software available to other software developers so that both parties can derive income from the associated affiliate's fees[21]. An advertiser pays affiliate fees to the spyware company that refers the target to the advertiser. The spyware company then pays some of this fee to the party responsible for installing the software on the user's system.

This type of adware is very commonly bundled with free and popular software such as peer-to-peer networking clients, games, and desktop themes/cursors/wallpapers. The nature of these attacks has not really changed in that it will continue to be used by both honest and dishonest software developers and by web sites in order to increase their own revenue. The types of software where adware is found will continue to change with time, with the most popular types of software being more likely to contain adware as well.

In the most destructive types of spyware like keyloggers and browser hijackers, directed marketing can take place, but the larger threat is that the attacker can also obtain information such as the target's banking information and credit card numbers. This information can be used by the attacker or sold to someone else to take money directly from the target.

---

[19] Claria, http://www.claria.com/
[20] eZula, http://www.ezula.com/home.html
[21] "How Affiliate Programs Fund Spyware," http://www.benedelman.org/news/091405-1.html, September 2005.

An interesting anecdote is that a keylogger was pivotal in the largest attempted bank robberies in the world[22]. The keylogger somehow became installed on a system in the London offices of the Japanese bank Sumitomo Mitsui. When the keylogger reported to its owner and the owner realized that it was installed on a bank's system, he sold the keylogger to criminals in Israel who used the keylogger to figure out some inter-bank transfer codes and steal hundreds of millions of dollars. The theft ultimately failed because some required paperwork did not show up, but otherwise they would have succeeded!

Keyloggers also have illegitimate non-monetary uses, including spying on spouses, ex-spouses, neighbors, etc. This type of spying has been going on since before the Internet was popular since many times the keylogger is installed by gaining physical access to the machine in question.

How Do Computers Get Infected with Spyware?

Most spyware does not directly spread in the manner of a computer virus or worm: generally, an infected system does not attempt to transmit the infection to other computers. It is important to understand how these programs become installed on target systems. There are three main spyware installation techniques[23] [24], which can be summarized as tricking the user, piggybacking, and drive-by-downloading[25].

The most direct route by which spyware can get on a computer involves the user installing it. However, users are unlikely to install software if they know that it may

---

[22] "UK police foil massive bank theft," BBC News UK Edition, March 17, 2005, http://news.bbc.co.uk/1/hi/uk/4356661.stm

[23] James Butler and Sherri Sparks. "Spyware and Rootkits: the Future Convergence," ;login: The USENIX Magazine, December 2004.

[24] Steven Gribble. "Spyware," http://www.cs.washington.edu/education/courses/csep590/05au/lectures/slides/Gribble_110905.ppt

[25] Wikipedia: spyware, http://en.wikipedia.org

disrupt their working environment and invade their privacy. So many spyware installations trick the user into doing something that installs the software without realizing it. In one variation of the trick theme, some spyware adapts a Trojan horse method to smuggle in something dangerous. The distributor of the spyware presents the program as a useful utility — for instance as a "Web accelerator" or as a helpful software agent. Users download and install the software, only to find out later that it can cause harm. For example, Bonzi Buddy[26], a spyware program targeted at children, claims that:

> *He will explore the Internet with you as your very own friend and sidekick! He can talk, walk, joke, browse, search, e-mail, and download like no other friend you've ever had! He even has the ability to compare prices on the products you love and help you save money! Best of all, he's FREE!*

Another approach is “piggybacking.” In this case, the spyware comes bundled with shareware or other downloadable software or even on a music CD. The user downloads a program (e.g., a music program or a file-trading utility) and installs it. The installer also installs the spyware. This works very well because most users do not bother to ever read an End User License Agreement (EULA) when they install software because EULA’s are usually so lengthy and complex. There are also actually legitimate reasons for piggybacking software, and many legitimate programs fund their software development efforts by packaging adware with their software.

In some cases, spyware authors have paid shareware authors to piggyback spyware with their software[27], as with the Gator spyware now marketed by Claria. The Kazaa peer-to-peer client installs anywhere from two to seven adware programs during

---

[26] http://www.angelfire.com/apes/bonzi_buddy/
[27] Claria Corporation, http://en.wikipedia.org/wiki/Claria

its own installation. In other cases, spyware authors have repackaged desirable software with installers that add spyware.

Drive-by-downloading (an analogy to drive-by shootings) involves either tricking the user into disabling security features, or exploiting security holes in the Web browser or other software. The security features of the design of the Internet Explorer Web browser are biased against allowing web sites to initiate unwanted downloads. Instead, a user action, such as clicking on a link, must normally trigger a download. However, links can prove deceptive. For example, a pop-up ad may appear like a standard Windows dialog box. The dialog box (which is really a pop-up ad) contains a message such as "Would you like to optimize your Internet access?" with links which look like buttons reading Yes and No. No matter which "button" the user presses, a download starts, placing the spyware on the user's system. Later versions of Internet Explorer offer fewer avenues for this attack.

Spyware authors can also infect a system by attacking security holes in the Web browser or in other software. When the user navigates to a Web page controlled by the spyware author, the page contains code that attacks the browser and forces the download and install of spyware. Common browser exploits target security vulnerabilities in Internet Explorer and in the Microsoft Java runtime. Given that Internet Explorer remains the most widely used browser and that many users neglect to update to more secure versions of their software, Internet Explorer provides an attractive entry point for the less scrupulous advertiser or computer hacker.

Additionally, once a target computer has spyware, it tends to download additional spyware. The first installed spyware instance usually downloads additional spyware

programs. Once a Trojan downloader of this type is installed, it can install other spyware and Trojan downloaders, which can in turn install more of these, and so on and so forth. These types of spyware installations are the most difficult to defend against once they are installed because the user is often unaware of the fact that the Trojan is installing more and more spyware.

A worm or a virus can also install Spyware. For instance, some attackers used the "W32.Spybot.Worm" worm to install spyware that popped up pornographic ads on the infected system's screen. By directing traffic to ads set up to channel funds to the spyware authors, they can profit even by such clearly illegal behavior.

A Specific Example: Gator

As a concrete example of these methods, "Gator" is an interesting piece of spyware that uses three different ways to invade computer system. The visited Web sites frequently install Gator on client machines in a surreptitious manner, and it directs revenue to the installing site and to Claria by displaying advertisements to the user. The user's experience is that their computer begins displaying a large number of pop-up advertisements.

The first way Gator gets installed is through advertising. For example, a web ad may promote Gator's Precision Time utility, which keeps the system clock accurate by synchronizing it over the Internet. Clicking on this ad will initiate a download. Gator also uses drive-by-downloading. The third way is that Gator provides their products to other software makers who bundle it into their downloads[28]. One example of this is DivX Networks' DivX Pro.

[28] "How Did I Get Gator?", PC Pitstop, http://www.pcpitstop.com/gator/Confused.asp

There is a survey on the web that found that an astounding 74% of Gator users did not know that a Gator or GAIN application had been installed on their system, and an additional 15% had not read Gator's license agreement[29]. Compare those results to Gator's assertion that users are "inviting" Gator onto their PC's.

How To Detect and Prevent Spyware Intrusions

First and very importantly, in today's environment, it is largely up to individual computer users to battle spyware. This is the situation today, and it is not likely to change in the near future. So for now, at least, users need to be aware of how to detect and prevent spyware installations.

The following are signs of a computer that has become infected by spyware:

- User sees pop-up advertisements even when not on the Web.
- The home page of user's Web browser or the browser search settings have changed without user's knowledge.
- A new toolbar appears in the browser that user did not want; the toolbar may be difficult to get rid of.
- The computer takes longer than usual to complete certain tasks.
- User experience a sudden rise in computer crashes.

The following are the basic steps that all computer users can take to fight spyware:

1. Update the operating system (OS) software frequently. In many cases, spyware makers can reverse-engineer an exploit for a recently announced

[29] Gator Information Center, http://www.pcpitstop.com/gator/default.asp

vulnerability in a matter of hours or minutes[30]. Therefore, it is very important to make sure you get latest software updates in a timely fashion. Windows users should turn on the automatic update option to get all the latest critical and security updates automatically.

2. Adjust the security settings of the browser to determine how much—or how little—information the user is willing to accept from a Web site. For example, in Microsoft IE, user should set the security settings for the Internet to Medium or higher.

3. Use the protection of a firewall. While most spyware and other unwanted software come bundled with other programs or originate from unscrupulous Web sites, a small amount of spyware can actually be placed on computers remotely by hackers. Installing a firewall provides a helpful defense against these hackers.

4. Surf and download more safely. The best defense against spyware and other unwanted software is not to download it in the first place. Some helpful tips that can protect users from downloading software they do not want include: only download things from trusted web sites; read all security warnings and license agreements (EULAs) before downloading; and never click "agree" or "OK" buttons to close a window, use the red "x" in the upper-right corner instead.

5. Use up-to-date anti-spyware protection.

Although the primary responsibility is currently with the individual user, the software industry is also taking action to fight spyware, at least with regard to providing tools. There are many types of anti-spyware software in the market now. Steve Gibson's

[30] "Crime on the Internet", slide 12, http://www.cs.washington.edu/education/courses/csep590/05au/lectures/slides/Aucsmith_110905.pdf

OptOut[31] is a pioneer product in this area. Other well known anti spyware products include Lavasoft's Ad-Aware SE[32], Patrick Kolla's Spybot - Search & Destroy[33],Webroot Spy Sweeper[34], PC Tools' Spyware Doctor[35], Sunbelt's CounterSpy[36], and Microsoft Windows AntiSpyware[37]. Major anti-virus firms such as Symantec, McAfee and Sophos have also come later to the table, adding anti-spyware features to their existing anti-virus products.

Spyware removal tools work to remove spyware by using signatures for known spyware programs to search the target's system for these signatures, removing any infected files and programs. These tools do a fair job of catching the most popular spyware programs; so frequently using an up-to-date version of one of these tools can dramatically reduce the likelihood that the target system will remain infected. Naturally, this leads to "spyware hardening" as the creators of spyware use different techniques to avoid uninstallation of their products. Techniques used range from hiding files and registry values so that reinstallation will occur at a later date to claiming to have uninstalled the program when it has not actually happened. Another technique that spyware can use to avoid detection is to employ various forms of program polymorphism to make it difficult for removal tools to obtain a consistent signature on them. Spyware removal tools have had to resort to heuristic techniques to find polymorphic spyware items.

---

[31] http://grc.com/optout.htm
[32] Adaware, http://www.lavasoftusa.com/software/adaware/
[33] Spybot: Search & Destroy, http://www.safer-networking.org/
[34] http://www.webroot.com/consumer/products/spysweeper?rc=2180&ac=420
[35] http://www.pctools.com/spyware-doctor/
[36] http://www.sunbelt-software.com/CounterSpy.cfm
[37] Microsoft Windows AntiSpyware (Beta), http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&displaylang=en

In addition to anti-spyware software, there are tools like pop-up blockers introduced to help users to fight spyware and adware. For example Google toolbar[38] and MSN toolbar[39] both have built-in pop-up blocking features.

Recently several tech companies have started a Trusted Download Program[40] designed to protect consumers from adware and spyware. America Online, Yahoo, CNET Networks, Verizon and Computer Associates back the Trusted Download Program. The program is set to begin early next year in a trial version, when the Internet partners will get access to a list of applications certified by online privacy watchdog group Truste, according to a statement from the companies. The Trusted Download Program will not blacklist adware or spyware. Instead, to be certified, makers of the software have to clearly communicate what their product does. The consumer then has to consent prior to download and again when installing the software.

Lastly, the fight against spyware is being waged on the legal front as well. The SPY Act[41], House Resolution 2929, which passed in the House on Oct. 5, would direct the Federal Trade Commission to fine violators as much as $3 million for actions such as changing a Web browser's start page without the user's permission or collecting data on user's keystrokes. The bill is now before the Senate.

Similarly, the I-Spy Prevention Act of 2004, House Resolution 4661, would impose criminal penalties on purveyors of spyware. It, too, passed in the House and is on

---

[38] Google Toolbar, http://toolbar.google.com/?promo=mor-tb-en
[39] MSN Search Toolbar with Windows Desktop Search, http://toolbar.msn.com/
[40] "Group backs program to certify downloads", Joris Evers, Staff Writer CNET News.com, Nov 15, 2005, http://news.com.com/Group+backs+program+to+certify+downloads/2100-1029_3-5954668.html
[41] "House approves spyware legislation", http://news.com.com/House+approves+spyware+legislation/2100-1028_3-5397822.htm

the Senate floor. In the Senate, the Spyblock Bill, sponsored by Sen. Conrad Burns, R-Mont., is awaiting a vote.

The courts are also beginning to clamp down on spyware. In November of 2005, the Federal Trade Commission asked the U.S. District Court in Los Angeles to shut down a company allegedly pushing spyware on the Internet, according to The Washington Post[42]. In this case, the company was accused of bundling spyware along with other downloads.

Spyware Evolution

Experts believe that in the future, spyware will be able to avoid detection by using rootkit techniques[43]. A common rootkit technique that can be used by spyware is to use a browser helper object (BHO), which is an extension of a web browser, to hijack search queries or other web page requests made by the user or to compile detailed information about the user's browsing habits to be sent to a third party. Another technique is to modify the import address table (IAT), which is basically a list of imported functions and their addresses, of an application to point to different spyware-related functions that can be used to modify the program's behavior as the attacker chooses, including the techniques mentioned above. These techniques that can be used to hijack other programs can actually be used to subvert the spyware removal tools themselves. They subvert the spyware removal tool by actually modifying its functionality through the aforementioned rootkit techniques.

---

[42] "Court puts clamp on alleged spyware ring", Dawn Kawamoto, Staff Writer, CNET News.com, November 10, 2005, http://news.com.com/Court+puts+clamp+on+alleged+spyware+ring/2100-7348_3-5945047.html

[43] James Butler and Sherri Sparks. "Spyware and Rootkits: the Future Convergence," ;login: The USENIX Magazine, December 2004.

Botnets

With a solid understanding of spyware, we will now focus attention on another cyber criminal tool, which is often used to aid, enhance, and control spyware: the botnet. A botnet is a network of compromised computers controlled by an outside attacker. Cyber criminals use botnets to perform or assist in certain types of attacks, including Distributed Denial of Service attacks (DDoS), spamming, sniffing, and keylogging. Botnets are a key automation tool used to speed the infection of vulnerable systems.

Botnets are relatively easy to make and come in a variety of forms. In addition most users are ill-positioned to defend themselves against botnet attacks, and ill-equipped to prevent their computers from becoming bots in the first place. These circumstances present an opportunity for attackers to cause serious economic and personal damage.

Introduction to Botnets

A bot is an automated program that is frequently used in the context of the Internet. Examples of bots include the "spider" bots used by search engines to map websites. In the world of botnets, a bot is a specialized program that uses Internet Relay Chat (IRC) networks as a means of communication, so that it can receive commands from a remote administrator. Even a mediocre programmer[44] can easily create a bot or customize an existing one.

Such bots are able to spread rapidly to other computers. The rate of infection is somewhat dependent upon the details of the infection process, and this is definitely an area where the skill of the bot programmer has an impact[45]. A number of bots connected

[44] "Know Your Enemy: Tracking Botnets", The Honeynet Projects & Research Alliance, March 13, 2005.
[45] "Inside the Slammer Worm", David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver, IEEE Security And Privacy, 2003.

to a single IRC channel and awaiting a controlling command is called a *botnet*. A computer infected with a bot is sometimes known as a *zombie*.

IRC was commonly used in the infant sages of Internet. It was originally written by Jarkko Oikarinen of Finland in 1988, and is now used worldwide. IRC provided a simple way for people to chat with each other through the Internet[46]. Microsoft Messenger and AOL Messenger are distant relations of the early IRC programs. Several developments lead to the potential for IRC abuse. The first was in 1993: Eggdrop was written by the then 18 year old Robey Pointer[47]. This program allowed the user to monitor a single channel within the IRC, demonstrating the potential for the combined power of bots. In 1999, the Prettypark worm was distributed as an email attachment[48]. PrettyPark displayed the 3D Pipes screensaver, attempted to mail itself to anyone in the infected computer's email address book, and attempted to join a specific IRC channel. Once connected, it sent information to the IRC channel controller every 30 seconds. This keeps the connection going, and allows the IRC network controller to download an executable file from the IRC server and place it on a target computer. Thus the first botnets were born.

IRC provides an excellent way to launch botnet attacks because it is flexible, easy to use and because public servers can be used as a communication medium. IRC offers a simple method to control hundreds or even thousands of bots at once in a flexible manner. It also allows attackers to cover their identity with the use of simple tricks such as anonymous proxies or simple IP address spoofing. Thanks to this, server

---

[46] Vonck, Tjerk "Introduction to IRC for people using Windows", 27 August 2003, http://www.mirc.com/ircintro.html

[47] "Guide to TCL scripting for Eggdrop 1.6", 05 December 2005, http://www.suninet.org/tclguide/index.php?chap=1&pg=-1

[48] PrettyPark.Worm, http://www.symantec.com/avcenter/venc/data/prettypark.worm.html

administrators have little chance to find the origin of an attack controlled in such a manner.

In most cases bots infect single-user PCs, university servers or small company networks. This is because such machines are not strictly monitored, and often left totally unprotected. The reason for this is partially the lack of a real security policy, but mostly the fact that most PC users with an ADSL connection are completely unaware of the risks involved, and do not use protective software such as antivirus tools or personal firewalls. Experiments with un-patched, un-protected PCs indicate that such a PC can be infected with a virus within minutes of connecting to the Internet, and can become a zombie within a similarly short time span[49].

Botnet Applications

The possible uses for compromised hosts depend only on the imagination and skills of an attacker. Most uses are criminally oriented to some degree. A few of the more popular possible uses are discussed below.

Botnets are frequently used for *Distributed Denial of Service* (DDoS) attacks. An attacker can control a large number of compromised hosts from a remote workstation, exploiting their bandwidth and sending connection requests to the target host. In the height of the dotcom era, many networks suffered from such attacks, and in some cases the culprits were found amongst competition. In the case of Operation Cyberslam[50], in which a company and several individuals were indicted on charges of conspiracy and causing damage to protected computers when they conducted a paid DDoS attack on a

[49] "David Aucsmith: Crime on the Internet", http://www.cs.washington.edu/education/courses/csep590/05au/lectures/slides/Aucsmith_110905.ppt
[50] "Know Your Enemy: Tracking Botnets", The Honeynet Projects & Research Alliance, March 13, 2005.

competitor's website. One study[51] used a technique known as backscatter analysis to observe more than 12,000 attacks on over 5000 distinct Internet hosts in one three-week period.

There are also cases [52] where botnet operators extort money from a website. The attackers first use their botnet to conduct a brief DDoS attack against the target website. They then send a message to the site administrator basically saying, "send us money or we will take down your site permanently." Many smaller websites will capitulate immediately rather than face the loss of revenue caused by a long-term DDoS attack. Interestingly, there is also an underground market for DDoS-for-hire botnet attacks.[53]

Botnets are also an ideal tool for spammers. They are used both for exchanging collected e–mail addresses and for controlling spam streaks in the same way DDoS attacks are performed. Single spam message can be sent to the botnet and then distributed across bots, which send the spam. The spammer stays anonymous and all the blame goes to the owners of the infected computers. More than 70% of all spam may be generated by botnets[54].

Bots can also be effectively used to enhance sniffing and keylogging attacks. Observing traffic data can lead to detection of an incredible amount of information. This includes user habits and TCP packet payloads, which could contain interesting information (such as passwords). The same applies to keylogging – capturing all the information typed in by the user (e–mails, passwords, home banking data, PayPal

---

[51] "Inferring Internet Denial of Service Activity", David Moore, Geoffrey M. Voelker, Stefan Savage.
[52] FIX: Botnet DDOS Extortion reference. FIX THIS FIX THIS FIX THIS
[53] INFORMATION SECURITY: Emerging Cybersecurity Issues Threaten Federal Information Systems, United States Government Accountability Office, Report to Congressional Requesters. May 2005, http://www.gao.gov/new.items/d05231.pdf
[54] "Most spam generated by botnets, says expert", Dan Ilett, ZDNet UK, September 22, 2004, http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm

account info etc.). It is interesting to note that botnet operators can sometimes use these methods to “steal” botnets from one another.

The aforementioned methods allow an attacker controlling a botnet to collect an incredible amount of personal information. Such data can then be used to build fake identities, which can in turn be used to obtain access to personal accounts or perform various operations (including other attacks) putting the blame on someone else.

Last, but not least, bot–compromised computers can be used as a dynamic repository of illegal material (pirated software, pornography, etc.). The data is stored on the disk of an unaware computer user. Imagine the following scenario: an employee of a XYZ Company has an infected computer, which is being used by a botnet to store pornography. Company XYZ has a policy of instant dismissal for pornography on computers. A routine computer audit discovers some of the hidden pornographic materials. Who is to blame? The employee? The computer administrator?

Other applications of botnets include: pay per click abuse, poll-skewing, phishing (and the subsequent identity theft issues), hijacking HTTP/HTTPS connections, spreading new malware and spyware, etc. Bots alone are only tools, which can easily be adapted to any task that requires a great number of hosts under single control.

Different Types of Bots

Many types of ready–made bots are available for download from the Internet. Each of them has special features. Here are a few of the most popular bots, outlining common features and distinctive elements.

GT–Bot

All of the GT (*Global Threat*) bots are based on a popular IRC client for Windows called mIRC. These bots launch an instance of the mIRC chat-client with a core set of scripts, which are used to control the activity of the remote system. This type of bot uses a second application, usually HideWindow, to make the mIRC instance invisible to the user of the host computer. This type of bot allows the attacker to link in additional Dynamic Link Libraries (DLLs) to add new features to mIRC that the scripts can use.

Agobot

Agobot is probably one of the most popular bots used by crackers[55]. It is written in C++ and released on a GPL license. The Agobot source code is widely regarded as a highly refined, well-engineered piece of code. It is highly modular, making it simple to add new functions. Agobot provides many mechanisms to hide its presence on the host computer, including the use of NTFS Alternate Data Stream and rootkit capability. It also includes functions to detect debuggers, to protect against reverse engineering. Agobot offers traffic sniffing and sorting functionality. Protocols other than IRC can also be used to control this bot.

SDBot

SDBot is written in C and also available on a GPL license. Unlike Agobot, its code is poorly written[56] and the software itself comes with a limited set of features. Nevertheless, it is still very popular and available in different variants. For some reason, attackers like it and it is often used. This may be because many botnets are run by young

[55] "Know Your Enemy: Tracking Botnets", The Honeynet Projects & Research Alliance, March 13, 2005.
[56] ibid.

males with limited programming skills and these types of programmers tend to gravitate towards popular programs, rather than well-written ones.

Botnet Attacks

To make a botnet, an attacker first spreads a Trojan horse virus, which infects various host computers. Botnets consisting of 400,000[57] or more compromised hosts have been reported. These hosts become zombies and connect to the attacker's IRC server in order to listen to further commands. The IRC server can either be a public machine in one of the IRC networks or a dedicated server installed by the attacker on one of the compromised hosts. Bots run on compromised computers, forming a botnet.

The activity of the attacker can be split into four distinct stages[58]:

- creation
- configuration
- infection
- control

The nature of the *creation* stage depends on the attacker's skills and requirements. Programmers write their own bot code or simply extends and customizes existing code. A wide range of ready–made bots are available and highly configurable. This is the option most often used by the lowest level of attackers, often known as *script kiddies*.

The *configuration* stage involves supplying IRC server and channel information. Once installed on the compromised machine, the bot connects to the selected host. An attacker first enters data necessary to restrict access to the bots, secures the channel and

[57] "FBI Naps Suspected U.S. Botnet Controller," Greg Keizer, TechWeb News, http://www.systemsmanagementpipeline.com/network/173500118.
[58] "Robot Wars – How Botnets Work", Massimiliano Romano, Simone Rosignoli, Ennio Giannini, for hakin9. October 20, 2005.

finally provides a list of authorized users (who will be able to control the bots). In this stage the bot can be further customized, for example by defining the target and attack method.

The *infection* stage involves using various techniques to spread the bots – both direct and indirect. Direct techniques include exploiting vulnerabilities of the operating system or services. Indirect attacks employ other software for the dirty work – they include using malformed HTML files exploiting Internet Explorer vulnerabilities, or using other malware distributed through peer–to–peer networks or through DCC (*Direct Client–to–Client*) file exchange on IRC. Direct attacks are usually automated with the use of. All worms have to do is search the subnets for vulnerable systems and inject the bot code. Each infected system then continues the infection process, allowing the attacker to save precious resources and providing plenty of time to look for other victims.

The mechanisms used to distribute bots are one of the main reasons for so–called Internet *background noise*. The main ports involved are the ones used by Windows, in particular Windows 2000 and XP SP1. These are favored targets, because it is easy to find unpatched Windows computers or ones without firewalls installed. This is often the case with home PC users and small businesses, which overlook security issues and have an always-on broadband Internet connection.

The *control* stage involves actions after the bot is installed on the target host in a selected directory. The first thing the bot does after it is successfully installed is connecting to an IRC server and joining the control channel with the use of a password. The nickname on IRC is randomly generated. The bot is then ready to accept commands

from the master application. The attacker must also use a password to connect to the botnet. This is necessary, so that nobody else can use the newly formed botnet.

IRC not only provides the means to control hundreds or thousands of bots, but also allows the attacker to use various techniques in order to hide his real identity. This makes it difficult to respond to attacks. Fortunately botnets, by their nature, generate suspected traffic, which is easily detectable due to known patterns. This helps IRC administrators in detection and intervention, allowing them to take the botnet down and report the abuse. This leads to a cycle wherein attackers are forced to refine their techniques, which leads to botnet hardening. This leads to the usage of dynamically mapped hostnames and other obfuscation techniques. Most expert attackers use personalized IRC servers and encrypt all the communication on their botnet channels. They also tend to use customized variants of IRC server software, configured to listen on nonstandard ports and using a modified version of the protocol, so that a normal IRC client cannot connect to the network.

As a simple example of the damage potential[59], a group of teenagers used the Randex worm to establish a 30,000-unit botnet, which was used primarily to boost their scores in an online game. In this case, the primary cost was simply that of cleaning up the infected PCs. Assuming that this takes an average of three hours, this fairly benign attack consumed more than 90,000 hours of labor. The estimated total cost would be on the order of $9,000,000.

Defense Strategies for PC Users

[59] Botnet Used to boost Online Gaming Scores, John Leyden, Dec 21, 2004 http://www.theregister.co.uk/2004/12/21/randex_botnet_fun_and_games.

As previously mentioned, bot infection is done mainly through worms, which browse the net looking for vulnerable machines. Therefore the protective measures outlined for protection against spyware are equally valid for protecting against bot infection. Users should keep personal computer systems updated, downloading patches and system updates for both the OS and all the applications accessing the Internet. Enable automatic updates if they are available. Users should also be careful when opening suspicious attachments in email. Finally, it is fundamental to use antivirus software and to keep it updated. However, many bots are configured to evade antivirus controls, so a personal firewall is a valuable addition to security, especially if the computer is on 24 hours a day.

Unfortunately, a significant number of people do not do these things. Even in a university computing environment, one study[60] showed that roughly 5% of the university's computers were infected with spyware of one sort or another. If these sorts of things exist in a supposedly highly competent university computing environment, imagine the spread percentage in run-of-the-mill personal computers.

In order to make life a little harder for the botnet owners, it might be useful to have a government public service announcement telling people to "get your computer OS patched, get a firewall, and get some anti-virus software." An effort like this would be similar to the government sponsored "put out your campfires" public-service announcements. Other options include making legislation to fine people if their computers become zombies because they failed to keep them up to date.

Defense Strategies for Administrators

[60] "Measurement and Analysis of Spyware in a University Environment", Stefan Saroiu, Steven D. Gribble, Henry M. Levy, Dept of Computer Science and Engineering, University of Washington.

There are fairly simple things that computer network administrators can do to help fight botnet attacks[61]. Administrators should always have up to date information on the latest vulnerabilities, and should read Internet security resources on a daily basis. A subscription to a mailing list such as Bugtraq[62] is recommended. Administrators should also attempt to educate their users and define security and privacy policies.

It is also necessary to study the logs generated by IDS and firewall systems, mail servers, DHCP and proxy servers. This can help spot any abnormal traffic, which could be a sign of bot presence in the network. Once such traffic is noticed, a sniffer comes in handy in order to identify the subnet and the computer generating it. All the above points may seem obvious, but are often forgotten about.

It is also possible to use more sophisticated techniques to study and detect threats. One of these techniques is honeypots. Honeypots are machines built to become an easy target for attacks. Their role is to become infected and allow the administrator to pinpoint the source of the problem and study the attack method.

Following these suggestions would greatly limit the ability of bot "herders" to collect massive botnets. The botnets would be discovered at a higher rate and hopefully prompt action would also help mitigate damages done by reducing time that machines are compromised.

Conclusions

The purpose of spyware has, for the most part, remained constant since the Internet boom of the late 1990s. Its primary purpose is to take something of value from the target and use it for some type of gain for the attacker. In the case of adware,

---

[61] Dittrich, David "Five steps for beating back the bots" Information Security 20 March 2005 <http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1068834,00.html>

[62] http://www.securityfocus.com/archive/1

information and privacy are being taken from the user in order for the attacker to get money from affiliate programs or from selling the target's information to another party. In the case of keyloggers and browser hijackers, it is possible to get banking and credit card information for direct monetary gain in addition to getting the type of monetary gain that is obtained with adware. The implementation of these attacks has changed, focusing on piggybacking on the most popular software and attacking the latest browser vulnerabilities. However, the conceptual means of spyware installation have remained the same.

The ways that users can prevent the installation of spyware has remained fairly constant as well. The primary prevention techniques are reading EULAs (and denying installation permission if necessary), keeping their software up-to-date, and not downloading and installing programs from untrusted parties. The detection and defense of installed spyware has usually been done by third party software that looks for the characteristics of common spyware. Polymorphism has been used by some spyware, and experts believe that spyware will begin to take on rootkit-like features in order to avoid detection and thus removal. If this shift occurs, spyware removal programs will need to use more advanced tactics to detect this more sophisticated spyware.

Botnets are a significant threat to privacy and security on the Internet. Users can help mitigate the threat by making sure they have an up to date OS, installing a firewall, and using anti-virus software. Network administrators can take more steps to monitor and find botnet-infected computers, and cooperate with the legal authorities to track down botnet operators. Most botnet operators are driven by monetary motivations, but

there is at least the possibility of a coordinated, tailored attack that could be used by terrorists[63].

In today's Internet, keeping computers secure is pretty much left to the individual computer user. In the case of a network, there may be one or two network administrators to help, perhaps with a coherent security policy. Relying on this sort of individual action and responsibility is acceptable; the Internet has been compared to the Wild West more than once, and there are many people that like it that way. But even in the Wild West there was the occasional sheriff to tell you to be careful because the bandits were on the prowl. Perhaps its time for the "sheriff" (effectively the U.S. Government) to give people a nudge in the right direction. A large number of people simply do not know what security precautions they should take when using the Internet, or how to implement them. The simple act of sponsoring public service announcements telling people why and how to make their computers secure would be a large step in the right direction and may lead to a decline in the number of spyware and botnet attacks.

[63] "Release: IM Rootkit, BotNet Linked to Hacker Group in Middle East", by Spywareguide.com Staff, Nov 17, 2005, http://www.spywareguide.com/articles/article_show.php?id=95