Cybercriminal Activity

Hemavathy Alaganandam – The Evolution of Cybercrime

Pravin Mittal – Cybercrime Case Study: Internet Bots

Avichal Singh - Cyberforensics

Chris Fleizach – Legal Policies and The Future of Cybercrime

December 6th, 2005

Table of Contents

Introduction

The rapid growth of the Internet, not just in terms of users, but also in terms of functionality has allowed entire industries to move their operations, and importantly their money, onto the Internet. This has lead naturally towards a prolific growth in criminal activity conducting solely through virtual means. Although cybercrime is not a new phenomenon, computers have always proved to be valuable targets, the essentialness of the Internet has necessitated a change in our understanding of security, risks and threats.

Cybercrime started as an insider job, grew into a threat that came from a determined outsider and has morphed again into an autonomous attack platform aimed at compromising any machine in order to leverage the might of the masses. The story of how targets, defenders, attackers, threats and vulnerabilities have changed is illustrative of the current state of cybercrime.

The present-day climate is a multi-faceted window into nefarious activities that scale from small-time pranksters to nationally funded spies, each with their own goals and targets. The entry of organized crime into the arena has raised concern amongst many, along with the exponential growth of botnets that have the power to inflict great damage against potential victims. Understanding and analyzing these various aspects will allow a better grasp at prevention and protection.

One area that many have proposed may be able to stem the tide of criminal activity are legal measures that can effectively deal with many of the situations that are novel and exist outside current legal definitions. But the threat of punishment is useless without the ability to capture and prosecute such criminals. Currently, it is difficult, if not impossible to track those who perpetrate crimes. Cyberforensics is a developing field which aims to solve these inherent flaws in the Internet and allow cybercriminals to face the same risk model that real-world criminals must contend with.

Work in cybersecurity is beginning to take off as more researchers and professionals realize the dire need for more effective systems. What direction will cybercrime turn to as the next generation of security measures are implemented and deployed? In turn, how will the good guys respond to novel threats? These are valid questions that need to be asked in order to plan for future growth and mitigate the potential for massive crises.

The Evolution of Cybercrime

Cybercrime has been an artifact of computer systems for a number of decades. However, the phenomenon of cybercrime did not truly come into being until the advent of the computer network. Information moving from across physical distances was much easier to intercept than that on a standalone system. Moreover, attaching a system to a network provided would-be criminals

an access point into other vulnerable systems attached to the same network. But even in the early days of networked computing, cybercrime was rare. The relative rarity of computers, combined with the highly specialized knowledge needed to use them prevented widespread abuse. The cybercrime problem emerged and grew as computing became easier and less expensive.

Cybercrime evolved from hacking of another system, the public switched telephone network. These phone "phreakers" developed methods of breaking into phone systems to make long-distance calls for free. Perhaps, the most famous of these phreakers was John Draper[1] (aka "Cap'n Crunch"), who discovered that toy whistles given away with Cap'n Crunch cereals generate a 2600-hertz sound, which can be used to access AT&T's long-distance switching system. Draper proceeded onto build a "blue box" which, when used together with the whistle, allowed phreakers to make free calls. Shortly after, wire fraud in the United States escalates. Draper was arrested on toll fraud charges in 1972 and sentenced to five years' probation.

In the 1970's, the first affordable personal computers became available on the market, and it was shortly thereafter that the first bulletin board service, or BBS, was established. Early hackers and phreakers seized on the BBS idea as a way to communicate with one another and share their tricks and techniques. Still, even as the Internet grew, getting online was far from easy. Designers of operating systems at the time had no idea how important the Internet would be. They didn't design software with built-in functionality to connect to an Internet service provider. ISPs were few and far between, and very pricey. For a user to connect to the Internet, they would have to obtain, install and configure a number of settings that could be tricky for the casual user. Online services such as CompuServe, AOL, and Prodigy helped to solve this problem. They provided their subscribers with software that would enable them to connect to their service with relative ease. In 1986, alarmed by the larger numbers of computer break-ins, the US government passes the Computer Fraud and Abuse Act. This made it a crime to illegally break into computer networks. The law did not apply to juveniles. Robert Morris[2] became the first person to be convicted under the new Computer Fraud and Abuse Act of 1986. Morris was punished for his Internet worm, which crashed 6,000 Net-linked government and university computers.

Price was still an issue, though, but in the early 1990's, costs for the user dropped to around $3 an hour, and eventually, to less than $20 a month for unlimited usage, allowing not only the Internet to grow exponentially, but also for criminals to learn how to effectively exploit the system. Computers are now ubiquitous and many tasks performed in the daily lives of users depend on computers and computer networks. The Internet has become a mission-critical infrastructure for governments, companies, and financial institutions. Computers and networks are used for controlling and managing manufacturing processes, water supplies, the electric power grid, air traffic control systems, and stock market systems, to mention a few. A benefit of online services that attracts criminals is the anonymity they offer, making it easier for criminals to change identities and cover their tracks. The rapid growth of the Internet in the mid 1990's gave rise to

cybercrime as we know it today.

Evolution of Motivation

Ten years ago, hackers were dabbling on other systems to only see how they were configured and operated. Most of the time they did not cause any damage. Unfortunately, the circumstances have changed and become incredibly malicious. Instead of being driven by curiosity, hackers today are driven mostly by financial motives. The value of Internet activities and the wealth stored on computers is the source of the attraction. While e-commerce represents only a fraction of total commerce, it reached almost $70 billion in the U.S. at the end of 2004, an increase of 24 percent over 2003[3]. A third of the U.S. workforce is online, roughly 50 million people, an important consideration since more than half of e-commerce transactions are made from work. Sixty million residents of North America, almost half of the Internet user population in Canada and the U.S., have online bank accounts. The combination of banking and commerce draws criminals more than anything else.

Categories of Cybercrime

Cybercrime has manifested itself in many different forms over the years. The following points are illustrative of some of the different categories that criminals have entered.

1) Spam - Although for much of history, spam was not technically a crime, the 2003 CAN-SPAM Act[4] changed legal definitions on what is acceptable. Spam now represents more than 50 percent of all email transmitted over the Internet. It's costs, which Internet service providers (ISPs) pass on to their customers, are enormous. With spam's ubiquity comes a whole culture and industry devoted to fighting it. Large groups of people, such as the Spamhaus Project, spend enormous effort to identify the sources of spam so as to block their activity. New technologies have been created to flag its sources, like blacklists, and spam identification through Bayesian filters, distributed checksum databases, and other advanced heuristics. Increasingly on the defensive, spammers are fighting back by becoming more sophisticated, generating unique messages, and using subverted computers to send messages.

2) Extortion and Damaging Reputations - In the Internet variant of a blackmail, criminal gangs will threaten companies with disruption of their networks, through denial of service attacks, or the theft of valuable information, unless they pay ransom into offshore bank accounts. Defacement of a company's website can cause not just embarrassment but loss of sales. In other cases, spite or a desire to inflict harm means that the attack will be executed without warning.

3) Fraud and Phishing - The anonymity and opportunities for misrepresentation found on the Internet make fraud easy. Consumer Sentinel, a complaint database developed and maintained by the US Federal Trade Commission[5], has recorded more than 390,000 Internet-related fraud complaints regarding transactions involving over US$540 million losses in 2004 alone. Fraud

schemes are usually peddled by individuals who spam potential victims, such as the Nigerian, or 419, scam. But as the number of fraud cases has increased, so has the public's awareness of them; fraudsters are increasingly forced to resort to more intricate schemes. New practices like "phishing" are gaining popularity with fraudsters. Using this scheme, criminals create email messages with return addresses, links, and branding that seem to come from trusted, well-known organizations with the hope to convince victims to disclose sensitive information. This practice originates in attempts to fool America Online users into parting with their screen names and passwords in the mid-1990s. The goal these days is to extract information from a victim that crackers can use for financial gain. A commonly targeted item is victim's credit card information. Criminals also want access to Internet payment systems such as e-Bullion, egold, or PayPal; online transaction services such as Authorize.Net, iBill, and Verotel; and Internet accessible banks which includes almost all major banks today.

4) Service Disruption - A cybercriminal can use an Internet attack to disrupt a key service. Denial of service attacks are one method, worms and viruses containing malicious code are another. A major auto manufacturer was one of many companies that had to shutdown its e-mail network for a few days because of the Love Letter virus.

5) Information Theft - The most damaging category of Internet crime, information theft can take several forms. Cybercriminals can extract personal identification information or credit information from a company's database and affect thousands of consumers. Cybercriminals can also extract a company's own financial information. Finally, cybercriminals can steal valuable intellectual property from a company. While the reported cost of information theft is declining, it remains one of the greatest Internet risks a company can face.

6) Money Laundering - The growth of global financial services makes it easy to conduct banking operations across borders over the Internet. The Financial Action Task Force, a group of national law enforcement agencies, notes that "within the retail banking sector, services such as telephone and Internet banking allow customers to execute transactions on a non face-to-face basis from any location with telephone or Internet access." While use of the Internet provides law enforcement agencies a greater ability to trace transactions through electronic records, the volume of transactions, the anonymity, and the lack of consistent record-keeping make it attractive to criminals and terrorists.

7) Child Pornography – The Internet has become an important tool for sex offenders in order to facilitate the making, collection, trading and distribution of abusive images engaging children. It constitutes a vehicle to simplify the contact between child pornographers mutually, on the one hand, and with their victims, on the other hand. Consequently, the Internet linked with other technological advances has an enormous impact on both the volume and the nature of child pornography.

Cybercrime Tools

Cybercriminals have developed a wide array of potential tools that have had varying degrees of success over the years. The following are a short list of some of these techniques.

1) Bots — A bot (short for robot) is a computer on which a worm or virus has installed programs that run automatically and allow cybercriminals access and control. Cybercriminals use viruses or other bots to search for vulnerable computers where they can load their own programs or store data. A botnet is a collection of these infected machines that can be centrally controlled and used to launch simultaneous attacks. Spammers, hackers, and other cybercriminals are acquiring or renting botnets, making it harder for authorities to track down the real culprits.

2) Keylogging — Keyloggers are programs that covertly recover the keys typed by a computer user and either stores the data for later access or secretly sends the information to the author. The advantage of a keylogger program is that the cybercriminal does not need to trick a user into supplying sensitive information.

3) Bundling — Covertly attaching a virus or spyware to a benign or legitimate download, such as a screensaver or a game. When the computer user downloads and installs the legitimate file, they are unwittingly also giving permission to install the criminal program.

4) Denial of Service — An attack specifically designed to prevent the normal functioning of a computer network or system and to prevent access by authorized users. A distributed denial of service attack uses thousands of computers captured by a worm or trojan to send a landslide of data in a very short time. Attackers can cause denial of service attacks by destroying or modifying data or by using zombie computers to bombard the system with data until its servers are overloaded and cannot serve normal requests.

5) Packet Sniffers — Software programs that monitors network traffic. Attackers use packet sniffers to capture and analyze data transmitted via a network. Specialized sniffers capture passwords as they cross a network.

6) Rootkit — A set of tools used by an intruder after hacking a computer. The tools allow the cybercriminal to maintain access, prevent detection, build in hidden backdoors, and collect information from both the compromised computer.

7) Spyware — Software that gathers information without the users' knowledge. Spyware is typically bundled covertly with another program. The user does not know that installing one also installs the other. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

8) Social Engineering — Social engineering is not limited to cybercrime, but it is an important element for cyberfraud. Social engineering tricks deceives the recipient into taking an action or revealing information. The reasons given seem legitimate but the intent is criminal. Phishing is an obvious example, a certain percentage of users will respond unthinkingly to a request that appears to be from a legitimate institution.

9) Worms and Trojans — A trojan is a malicious program unwittingly downloaded and installed by computer users. Some trojans pretend to be a benign application. Many hide in a computer's memory as a file with a nondescript name. Trojans contain commands that a computer automatically executes without the user's knowledge. Sometimes it can act as a zombie and send spam or participate in a distributed denial of service attack. It may be a keylogger or other monitoring program that collects data and sends it covertly to the attacker. Worms are wholly contained viruses that travel through networks, automatically duplicate themselves and send themselves to other computers whose addresses are in the host computer.
In the past, cybercriminals occasionally use worms and trojans to hijack a victim's Web browsers. They replace the victims' home and search pages with links to Web spam, as well as drop links to the spam in the victims' bookmarks and on their desktops. To make money, they infect computers with malicious code that generates fraudulent ad views.
10) Virus—A program or piece of code that spreads from computer to computer without the users' consent. They usually cause an unexpected and negative event when run by a computer. Viruses contaminate legitimate computer programs and are often introduced through e-mail attachments, often with clever titles to attract the curious reader.
11) Internet message boards – Internet message boards dedicated to stocks are fertile ground for impersonators. A habit of many posters to these boards is to cut-and-paste press releases and news stories from other electronic sources into their posts to alert other posters and visitors to that information. Frequently, posters will paste in a hyperlink to direct a reader to a source directly, as Hoke did in the PairGain hoax.[6] In addition to the rising threat, as national level attacks become more plausible, the vulnerabilities have also increased.

Evolution & Profile of the Attacker

There is a growing convergence of technically savvy computer crackers with financially motivated criminals. Historically, most computer crime on the Internet has not been financially motivated: it was the result of either curious or malicious technical attackers, called crackers. This changed as the Internet became more commercialized. Financially motivated actors, spammers and fraudsters, soon joined crackers to exploit this new potential goldmine. Criminals have fully adopted the techniques of crackers and malicious code authors. These are financially motivated people, who pursue their goals considerably more aggressively than an average cracker. They have the monetary means to buy the required expertise to develop very sophisticated tools to accomplish their goals of spamming and scamming the public.

The perpetrators of these attacks vary considerably. At the low end are script kiddies, who are usually unsophisticated users that download malicious software from hacker web sites and follow the posted instructions to execute an attack on some target. These attacks are often only annoyance attacks, but they can be more severe. At the next level are hackers who are trying to

prove to their peers or to the world that they can compromise a specific system, such as a government web site. Next are insiders, who are legitimate users of a system that either access information that they should not have access to or damage the system or data because they are disgruntled. Insiders are often less knowledgeable then hackers, but they are often more dangerous because they have legal access to resources that the hackers need to access illegally.

Next are organizational level attacks. In this case, the organization's resources are used to get information illegally or to cause damage or deny access to other organizations to further the attacking organization's gain. These can be legitimate organizations, such as two companies bidding on the same contract where one wants to know the other's bid in order to make a better offer. They could also be criminal organizations that are committing fraud or some other illegal activity. At the highest level is the nation state that is trying to spy on or cause damage to another state. This level used to be called "national lab" attackers, because the attackers have a substantial amount of resources at their disposal, comparable to those that are available to researchers at a national lab, such as Los Alamos Laboratory or Lawrence Livermore Laboratory. After the September 11, 2001 terrorist attacks on the World Trade Center, the idea of nation state level cyber attacks being carried out by terrorists became a big concern.

Malware and Threat Evolution

Viruses started appearing on dedicated networks such as the ARPANET in the 1970s. The boom in personal computers, initiated by Apple in the early 1980s, led to a corresponding boom in viruses. In1981 the first virus in the wild came into being even before the experimental work that defines viruses of today. Founded on the Apple II operating system, it was spread on Apple II floppy disks containing the operating system. While the viruses of the 1980s targeted a variety of operating systems and networks, most viruses today are written to exploit vulnerabilities in the most commonly used software: Microsoft Windows. The increasing number of vulnerable users is now being actively exploited by virus writers. The first malicious programs may have shocked users, by causing computers to behave in unexpected ways. However, the viruses which started appearing in the 1990s present much more of a threat: they are often used to steal confidential information such as bank account details and passwords.

Classic file viruses reigned supreme in the 90s; however they have almost totally disappeared today. There are currently about 10 file viruses that are still active. They experience peaks of activity when they infect the executable files of worms: the file virus will then travel as far as the infected worm file. For instance, samples of MyDoom, Netsky and Bagle that are infected by file viruses such as Funlove, Xorala, Parite or Spaces. On the whole, there is very little danger that classic file viruses will cause any major epidemics.

The trends in epidemiology that are observed today have their primary roots in the second half of 2003. Internet worms Lovescan, Sobig, Blaster, Slammer and Sober all not only caused

global epidemics, but also profoundly changed the malware landscape. Each of these malicious programs set new standards for virus writers. In 2003, we witnessed the emergence of an attack type that combines exploitation of server and workstation vulnerabilities with the characteristics of virus and Trojan horses. By using more efficient attack vectors and, therefore, minimizing the human effort required to deliver attacks and use the compromised systems, the risks related to newly discovered vulnerabilities moved up in the risk measurement scale.

Optimizing costs, achieving greater efficiency, and applying the minimum necessary effort to accomplish goal are central concepts to modern day life. Therefore, it is not difficult to identify the same approach in the vulnerability exploitation techniques and attack trends. The appearance of many efficient worms as a result of attackers' attempts to maximize their bang for the "bug" are examples. They compromise a very large number of systems with minimal effort. The steadily increasing amount of cross-site scripting and SQL injection vulnerabilities discovered and disclosed during 2003 point to another path of less resistance into vulnerable networks. These vulnerabilities have rather simple ways of exploitation and they provide casual attackers with a high yield, direct access to internal networks, compromise of database servers and their content, and indirect ways of attacking unsuspecting users of third-party systems. The level of sophistication in worms seen in 2003 and the installation of backdoors and tools with elaborate communication protocols and auto update capabilities indicate that attackers are trying to optimize the management of large amounts of newly acquired assets.

Classic email worms are on the decline, with network and instant messaging worms exploiting relatively lax security to take their place in early 2005. IM worms were at the peak of their development in spring and summer 2005, and showed the highest growth rate among all classes of network worms. In the first six months of this year, an average of 28 new IM worms were detected every month[7]. It should be stressed here that when P2P worms were at the peak of their evolution in 2003, approximately 10 new variants were detected every week.

However, the situation changed afterwards and the flood of IM worms suddenly dried up. AOL and MSN, both of which have proprietary IM clients, were the main targets for such worms. Both companies took measures to protect their users. Firstly, by blocking the transmission of files with names and extensions which were known to be used by IM worms. In spite of the fact that IM worms rarely use file transmission as a propagation method, the move did have a noticeable effect. The next step was to block the worms' main method of propagation, hyperlinks leading to files containing the body of the worm.

These actions closed the majority of security loopholes being exploited by virus writers. And most importantly, they closed the loopholes which IM worms based on source code circulating in the computer underground used. Most of the code used in IM worms is of fairly low quality. The majority of these worms are created by script kiddies who have no significant programming skills. When the off the shelf code was no longer effective, these self styled virus writers were unable to

create new propagation methods on their own, and this led to a sharp drop in the number of new worms.

Improved antivirus technologies, and increased user awareness of security issues are clearly forcing virus writers and hackers to use new approaches to access users' information and systems, mostly in the form of phishing attacks. Malicious users are starting to use viruses which propagate by exploiting vulnerabilities within web applications, particularly Internet Explorer, rather than network and email worms. One consequence of this is an increase in the number of compromised sites. Exploits for IE are placed on compromised sites, which means that users who visit these sites will have trojan programs downloaded to their machines.

To date Linux-based platforms have mainly been the victims of rootkit attacks and simple file viruses. However, the growing number of publicized vulnerabilities means that the increased number of users switching to Linux will not remain untouched by new malware.

Handheld devices, such as PDAs and cell phones are almost household appliances for many people. Virus writers have been quick to take advantage of their growing popularity. The first trojan for Palm OS appeared in September 2000. And finally, the increasing interest in on-line games, with the potential profits to be made in this area, make it more than likely that malicious code designed to steal such information will continue to evolve rapidly. The first Trojan for gaming consoles had also been discovered. Sony PlayStationPortable was the first victim - the Trojan targeting this device deleted system files causing the console to cease functioning correctly. This behaviour is very similar to Trojans for mobile phones. It may be that these new Trojans for gaming consoles signal the start of a new interest among virus writers.

Evolution of Exploit Frameworks

Cybercriminals increasingly rely on powerful exploitation frameworks to launch their attacks. Free tools like Metasploit and commercial tools like CORE IMPACT and Immunity CANVAS have revolutionized the attackers' methodology. Previously, upon finding a vulnerability, the attacker either had to create custom exploit code from scratch or scour the Internet to find such code to exploit the hole. Today, instead of scraping together a bunch of individual exploits, these integrated exploit frameworks include around one hundred or more exploits to compromise target systems.

One property of the exploit tools is the separation of the exploit from the payload. An exploit is the software that takes advantage of a flaw, letting the attacker load and execute a program of the attacker's choosing. The code triggered by the exploit is known as the payload. Old-fashioned attacks tightly bundled exploits and payloads together. An attack might exploit a database buffer overflow with the purpose of adding a user for the attacker to the local administrators group. But, with this tight integration, the attackers were stuck with the given payload attached to the given exploit for the given vulnerability. Taking the payload from one attack and embedding it with

another exploit required some serious machine-language fine tuning, and was often impossibly difficult. To remedy the situation, today's exploit frameworks include an arsenal of different exploits and an arsenal of different payloads, each offering a different effect the attacker wants to have on the victim. So today, the attacker can use a tool like Metasploit to choose an exploit, such as a buffer overflow in lsass.exe, originally used by the Sasser worm last year. Then, the attacker can choose from more than a dozen different payloads. Metasploit packages the payload with the exploit, and then launches it at the target.

The real effect of these frameworks in separating the exploits and the payloads is now reverberating through the industry. Developers who create fresh exploits for new flaws don't have to reinvent the payload wheel every time. Thus, they can focus their time on perfecting their exploits and producing them much more quickly. Moreover, those developers who don't focus on exploits can now zoom in on the production of high-quality payloads.

Defence Evolution

Computer security has been reactive for most part. That is, system administrators and security professionals are usually reacting to the latest attack. After they fix the vulnerability that allowed the attack, the attackers look for new vulnerabilities to exploit for new attacks. Trends in worm and virus delivery mechanisms and infection speed have also changed. Not long ago, a virus warning and the patch to vaccinate computers against it would appear days before the virus began spreading. Today, too often the first sign of a virus is that a part of the network goes down. Flash worms such as SQL Slammer have paved the way for future worms to carry payloads that directly target their victims and wreak havoc on government, business, and societal structures. Existing technologies such as firewalls, intrusion detection systems, intrusion protection systems, virtual private networks (VPNs), and virus scanners provide integrated security solutions. Not surprisingly, security has become a massive industry, and it is now a focal point for virtually every organization. Proactively eliminating just the known threats places an impractical burden on existing server and network infrastructures. Eliminating unknown threats or zero day attacks, which as the name implies reveal themselves only when they first occur, requires real-time solutions that can identify unique attacks without overburdening the network with security and management overhead.

The imagination of social engineers knows no bounds. Social engineers are highly aware of Internet user psychology and are well able to exploit current anxieties. In connection with this it should be stressed that the attempts of some companies to create a browser which is capable of determining the veracity of any site visited, or a browser which protects information stored on the potential victim machine is very hard to be one hundred percent successful.

Cyber Victims

Early exploits were mass attacks which affected the whole Internet community. Between

1996 and 2000, high-profile web sites such as eBay, the U.S. Department of Commerce, UNICEF, the New York Times and Microsoft all fell victim to hackers or defacers. The Melissa virus caused company email servers to shut down. A fraudulent web page that was designed to appear to be a Bloomberg financial news story resulted in the shares of a small tech company increasing 31 percent in response to the "news." As the new millennium began, a huge, distributed DoS attack shut down major Web sites such as Yahoo! and Amazon. Apache, RSA Security, and Western Union were hacked. The Code Red worm attacked thousands of web servers, and the Sircam virus hit e-mail accounts all over the world. As of today, spam accounts for fifty percent of all email sent, a staggering 12.4 billion messages a day, worldwide.

Malicious users are now changing their focus from conducting mass attacks to targeting specific business structures, and these attacks are tailored to each individual case. Identity thefts and credit card fraud are prevalent attacks affecting the public directly. Social engineering remains a threat, and the methods used are continuing to evolve. The biggest mass mailings were comparable in size to the activity shown in December of 2004 through and January, when cyber scammers exploited the tsunami in South East Asia.

Cybercriminals target people who are new to the Internet gullible. With huge numbers of people connecting to the Internet for the first time every year, cybercriminals always have a fresh crop of Net newbies on which to prey. Elderly people, youngster and kids are also among the top targets.

Current Situation

The Computer Security Institute (CSI) announced the results of its 10th annual Computer Crime and Security Survey.[8] The survey showed that virus attacks continue as the source of the greatest financial losses, accounting for 32 percent of the overall reported losses. Theft of proprietary information also showed a significant increase in average loss per respondent, more than double that of last year. Also unauthorized access showed a dramatic increase and replaced denial of service as the second most significant contributor to computer crime losses, accounting for 24 percent of overall reported losses and showing a significant increase in average dollar loss. On a better note the total dollar amount of financial losses resulting from security breaches is decreasing, with an average loss of $204,000 per respondent, down 61 percent from last year's average loss of $526,000. However the percentage of organizations reporting computer intrusions to law enforcement has continued its multiyear decline. Respondents cited the concern over negative publicity as the key reason for not reporting intrusions to law enforcement.

Cybercrime Case Study: The Emerging Threat of Internet Bots

Introduction

Network intrusions, data theft using Trojan horses, viruses and worms are among the threats security experts worry about on a regular basis. However, something more dangerous is emerging. Botnets, with their proliferation, sophistication and criminal use are emerging as the number one security threat. The recent arrest of 20-year old Californian man who made $60,000 by selling access to botnets to spammers[9] and hackers is evidence of the growing menace.
A bot is a malicious software program that invades computer so that it can covertly be controlled by a remote attacker. A bot is seeded by attackers through worms, viruses or other means to exploit desktop and server vulnerabilities. They are then herded into botnets, which can then be controlled from a central command point that can force zombie machines to work together to perform any issued task.

Botnets are evolving and getting nastier. Previously, they were controlled exclusively through Internet Relay Chat (IRC) channels, but are now increasingly being manipulated through other means, such as Web, instant messaging or peer-to-peer systems. Moreover, bots are using rootkits to conceal itself from the user of the machine. "Kernel level rootkits are extremely dangerous as they conceal their malicious code and cannot be removed by most anti-virus or anti-spyware programs," says Martin Overton, security specialist at IBM Global Service.[10] "The state of bot technology has reached the point that the state of Web technology has," says Peter Tipett, CTO at Cybertrust, whose security experts found more than 12,000 people contributing to bots or renting out botnets. "Instead of fighting with each other, these guys are working together and posting their code. It's evil open source. We are getting a rich set of commands and capabilities used by the bad guys."[11]

Apart from evolving as sophisticated security threats, their presence is growing exponentially. Network-security experts identify and shut down botnets with 10 to 100 compromised hosts several times a day. Crackdowns on large botnets with 10,000 or more hosts are rarer, but they still occur weekly, said Johannes Ullrich, chief technology officer for the Internet Storm Center, which detects, analyzes, and disseminates information about Internet-related security problems. "Security investigators have even found one botnet of 100,000 computers,"[12] Ulrich noted. Research conducted by Symantec found that on average more than 60,000 botnets were activated each day in the first half of this year.[13] They also noted that this is an increase of more than 140% from the previous year's semi-annual count.

The following sections discuss how hackers profile and select their victims, attack techniques and their criminal usage and defenses home users and system administrators can undertake to mitigate the risk of these attacks.

Profiling and Target Selection

Hackers are diligently profiling hosts and choosing targets that can provide them with longest survivability and carry out large scale attacks, and prevent their detection.

High Bandwidth: One of the most sought after hosts are the machines connected to the Internet using high-bandwidth broadband. This can provide an attacker with an enormous cumulative bandwidth to carry out large scale DDoS attacks on target severs.

Availability: Hosts with broadband connection are always connected to Internet and thus are the most sought after targets. This ensures hackers can carry out attacks round the clock without depending on whims of the users with dial-up connection which may connect to Internet at irregular intervals.

Low user Awareness and monitoring capability: Attackers prefer hosts where users have low security awareness and do not have access control mechanism like firewalls installed on their computers. The absence of such defenses along with un-patched operating systems create ideal victims for hackers to break into and then install and maintain bots over a long period of time without being identified or traced.

Location: One of the prime goals of these cyber-criminals is to avoid detection after they commit crimes. They achieve this by selecting hosts that are geographically far away from their location. This makes very difficult for law enforcement officers to detect bots back to hackers. Also international prosecution being time consuming, expensive and non-standardized process that varies for each country, unfortunately ends up helping these cyber-criminals to go Scot-free.[14]

The typical profile that fits the above criteria is that of residential broadband connection that has low or no access control mechanism or university subnets connected to Internet with minimal monitoring, high bandwidth with high availability.

Attack Techniques

Bots generally employ one of several attack methods, but sometimes use multiple techniques to create a network of compromised computers. Some of these approaches are quite sophisticated, such as Phatbot, which can generate a new encryption for itself each time it infects a new system. This makes it difficult for the software to find a common code signature for and thus recognize Phatbot. According to Ken Dunham, director of malicious code for Security Consultancy iDefense, Phatbot has successfully evaded detection by mutating itself from spyware to launch vitriolic DDoS attacks on compromised networks.[15] The following are some of the ways that attackers use to create networks of bots for themselves.

Chat: IRC is the most common used technique, including those in the large Phatbot/Agobot and Sdbot/Robot families as a way to communicate and receive commands from hackers.[16] IRC has a built in mechanism for multicast capabilities which let attackers quickly send commands to all parts of a botnet without writing new code for the bot.

Peer-to-Peer: Many bots take advantage of peer-to-peer communication to infect computers with vulnerabilities. They connect to open-source file sharing technology such as Gnutella and work with the WASTE file-sharing protocol.[17] WASTE uses a distributed directory rather than a central server which lets bots easily find each other and communicate with one another. They can thus exchange hacker commands or other attack-related information among themselves. An attacker can initiate the process by serving as a peer in P2P network sending commands to one bot, which can then pass them onto the others. Thus, hackers don't have to communicate to bots via IRC multicasting. Decentralized-based bot systems are harder for security officials to trace or shutdown than systems using a single IRC source.

Email Attachments/Worms: Many hackers use methods such as email attachments or worms to infect computers. Bots don't replicate or spread on their own, but they can use the worms' functionality to do so. In fact, hackers can spread bots more quickly with worms than with other methods. In addition, Botnets can spread worms faster than worms can spread on their own. The Symantec Security Response team said 2004's Witty worm, which infected and crashed tens of thousands of servers, was probably launched by a botnet. According to Huger, "we saw Witty break out more or less at the same time from a hundred or more machines. The machines were all over the world but they had something in common: they were on our bot list of compromised computers," he noted.[18]

Criminal use of Bots and Botnets

Bots can serve several purposes both legitimate and illegitimate. One legitimate purpose is to support the operation of IRC channels by conferring special administrative privileges or designated users. However, most of the common uses are criminally motivated for monetary gains or for destructive purposes.

Distributed Denial-of-Service Attacks: A DDoS attack is an attack on a computer system that causes a loss of service to users, typically the loss of network connectivity and services by consuming of the bandwidth of the victim network or overloading the computational resources of the victim's system. Most commonly implemented and often used are TCP SYN and UDP flood attacks.

One of the most common uses of DDoS attacks is to wrest control of an IRC channel from its founder and founder's delegates. To take over an IRC channel, attackers conduct a DoS attack against one or more of the network's servers. If they can succeed in downing a server they can split the network into two or more disconnected segments. If in a given segment there are no users joined to a particular channel of interest, the attacker can join that channel and seize the founder's privileges.[19]

Apart from the role in taking over IRC channels, attackers can launch successful DDoS attack against Internet sites. Let us assume if a given botnet has around 15,000 compromised

hosts and has an associated bandwidth of 56kbps, a simultaneous attack by the entire botnet would direct almost 850 Mbps at its target – enough to cripple almost all e-commerce sites. These estimates are conservative because most of these compromised machines have cable modem and DSL hosts. Moreover, because bots are widely distributed within the IP address space, filtering or blocking such DDoS attacks is not easy. At best, it requires cooperation between the target and multiple service providers.[20]

DDoS is not just limited to web servers; virtually any service available on the Internet can be a target of such an attack. Higher-level protocols can be used to increase the load even more effectively by using very specific attacks, such as running exhaustive search queries on the victim's website. Recursive HTTP flooding means that the bots start from a given HTTP link and follow all links on the provided website in a recursive way. This is also called spidering.[21]

Further research also showed that botnets are used to run commercial DDoS attacks against competing corporations. Jay R. Echouafni and Joshua Schictel, alias EMP, ran botnets to send spam and carry out paid DDoS attacks to take a competitor's website down. Echouafni was indicted on August 25, 2004 on multiple charges of conspiracy and causing damage to protected computers.[22]

Spamming: Some bots enable SOCKS v4/v5 proxy – a generic proxy protocol for TCP/IP-based networking protocol on a compromised machine which allows them to launch spam attacks. Using bots and thousands of zombies (compromised machines) attackers can send massive amounts of bulk emails. These bots can also add special functionality to harvest email-addresses. Harvested email addresses help them to send phishing mail which appears to victims to come from legitimate sources.[23]

Sniffing Traffic: Bots can be used as a packet sniffer to watch for interesting clear-text data passing by compromised machine. The sniffers are mostly used to retrieve sensitive information like usernames and passwords. They can also provide information about other Internet bots if it has been compromised more than once. This allows one to "steal" another's botnet.[24]

Keylogging: If the compromised machine uses encrypted communication channels (e.g. HTTPS or POP3S), then just sniffing the network packets on the victim's computer is useless since the appropriate key to decrypt the packets is missing. But most bots also offer features to help in this situation. With the help of a keylogger it is very easy for an attacker to retrieve sensitive information. An implemented filtering mechanism (e.g. "I am only interested in key sequences near the keyword 'paypal.com'") further helps in stealing secret data. If the keylogger runs on thousands of compromised machines in parallel, it is easy to imagine how quickly PayPal accounts are harvested.

Spreading new malware: In most cases, botnets are used to spread new bots. This is very easy since all bots implement mechanisms to download and execute a file via HTTP or FTP. But spreading an email virus using a botnet is also attractive. A botnet with 10,000 hosts which acts as the starting base for a mail virus allows very fast spreading and thus causes more harm. The Witty

worm, which attacked the ICO protocol parsing implementation in Internet Security System (ISS) products is suspected to have been initially launched by a botnet due to the fact that the attacking hosts were not running any ISS services.[25]

Attacking IRC Chat Networks: Botnets are also used for attacks against Internet Relay Chat (IRC) networks. Popular among attackers is especially the so called "clone attack." In this kind of attack, the controller orders each bot to connect a large number of clones to the victim IRC network. The victim is flooded by a service request from thousands of bots or thousands of channel-joins by these cloned bots. In this way, the victim IRC network is brought down - similar to a DDoS attack.[26]

Manipulating online polls/games: Online polls/games are getting more and more attention and it is rather easy to manipulate them with botnets. Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.[27]

Mass identity theft: Often the combination of different functionality described above can be used for large scale identity theft, one of the fastest growing crimes on the Internet. Phishing emails that pretend to be legitimate (such as fake PayPal or banking emails) ask their intended victims to go online and submit their private information. These fake emails are generated and sent by bots via their spamming mechanism. These same bots can also host multiple fake websites pretending to be Ebay, PayPal, or a bank, and harvest personal information. In addition, keylogging and sniffing of traffic can also be used for identity theft.[28]

Defending Against Bots and Botnets

Defense against botnet infection and attack can be classified in three stages: prevention, detection and response. These stages need to be treated differently from home and system administrator perspective.[29]

Prevention: The most common way for bots to compromise hosts is by exploiting the known vulnerabilities in the operating system or installed applications. Home users should follow guidelines regarding safe use by updating the installed OS and applications to defend their computers from being infected by attackers. If available, they should activate the auto-patch update facilities included in many popular operating systems and applications. Users should always install the latest version of anti-virus software and practice safe handling of common web applications such as web browsers, email, and instant messaging. In addition to this, every system administrator should be given training on online security and privacy issues. A high level of awareness on these issues is the best course in preventing malicious bots from infecting computers. They should implement access control measures and regularly monitor the generated logs on access control/peripheral devices.

Detection: Home users can use Microsoft Antispyware and Antivirus software, which are able

to detect and respond to known types of bots, but are not effective for new bots on net. Online resources for scanning a system can also be employed, like the Symantec online security checker which will scan the system for commonly used Trojan ports.

In addition to detection techniques used by home users, system administrators can employ network based tools to monitor perimeter defense devices to detect anomalies in Internet traffic. Slow network response, unexpectedly high volumes of traffic, traffic on unusual ports, and unusual system behavior indicate the presence of malicious software including bots.

Tools like network packet sniffers can be used not only to identify but also to isolate the subnet/machine which is generating malicious traffic. Analysis of the logs generated by network sniffer can also be used for finding IRC servers used, the names of the attacker's private channels and authentication keys.

Responses: As soon as the user realizes that his/her computer has been compromised, the computer should be physically disconnected from the network. This denies access to the attackers and helps limit the potential damage both to user's own system and to other systems on the Internet. They should immediately update anti-virus software and check OS and application vendor sites for latest patches. If the user stores bank or credit card information on PC, the user should assume them to have been compromised and contact the appropriate organization. Any passwords or secure data should be no more be used and changed at once. Apart from response measures suggested for the home user, system administrators should isolate infected subnets to prevent the spread of bots. They can asses the damage with the help of a network packet sniffer by identifying the number of machines infected by bots within a subnet. They can assist the incident response team by preserving data on the affected system and relevant system logs like firewalls, mail servers, IDS, DHCP servers, and proxies.

Conclusion

Growth of network models like IRC and easily available tools to edit bots has provided attackers, many whom have very limited knowledge of the underlying technology, the ability to create large botnets that are scalable and automated. Sophisticated bots are incorporating encryption and shape-shifting polymorphism in their code, and finding wider uses for rootkits, code that allows a permanent and undetectable presence of computer, to conceal itself from the user of the machine and creating nightmarish scenarios for security experts. Moreover, hackers are also diligently picking victims with poorly implemented access control mechanisms, minimal monitoring to avoid detection, high bandwidth and software that is easy to infect and that allows for propagation.

Bots are creating difficult challenges; nevertheless, users can fight back by proactively following best practices as recommended by the operating system and application vendors to prevent their machines from getting compromised in the first instance. Some of the reactive

methodologies outlined include using packet sniffers, monitoring firewalls and preserving critical logs to help incident response teams track down the attackers. However, none of these, in isolation are effective. High level security awareness among users and diligent monitoring of the systems are the most effective and real defenses against the growing menace of bots.

Further, much research is being done at universities and institutions using honeynets to learn about attacker's tools, tactics, and motives , while developing ways to track these criminals. Government should encourage these research efforts as they may provide a future arsenal for law enforcement agencies against bots, the fastest emerging threat on net, which if left unchecked may jeopardize the safety of cyberworld in coming years.

Cyberforensics

Introduction

Locks do not deter criminals from breaking into our homes, the fear of being caught and prosecuted does.[30] However in cyberspace, malicious users think little of breaking into systems and wreaking havoc even across international boundaries. Improving security is only part of the solution. In order to eventually deter cybercriminals, efforts need to be increased to catch and prosecute the perpetrators. Cyberforensics and effective legal policies form the cornerstones of such an effort.

Cyberforensics can be defined as the application of forensic science techniques to computer-based material. It is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is acceptable in a legal proceeding.[31]

Ninety-two percent of new information is stored on magnetic media (primarily hard disks)[32] and an estimated 95% of criminals leave digital evidence in some form.[33] The combination of such factors has fueled the recent growth of this field. Cyberforensics is increasingly used in the private industry, for cases such as intellectual property theft, insider attacks and so on. However we will focus on its application in the realm of law enforcement, which is what, brings most cybercriminals to justice. Excellent literature exists covering the actual processes of cyberforensics in detail, thus only a brief summary of the process will be presented, followed by a discussion of the current challenges.

Computer Forensic Process

The computer forensics process is comprised of the following general steps:

Identification: The investigator needs to recognize all potential hardware which could contain digital content. This might be computers, laptops, networks, thumb drives, cell phones, PDAs, even iPods and Xboxes. Damaged media is collected as well; hard disks shot at with an AK-47 have been known to be recovered (sans the data lost in the actual holes).[34] Physical material present on the scene which could aid in data analysis later is also collected, for example software

manuals, books, post-its and printouts.

Preservation: The object of this step is to capture the digital evidence in an unaltered form. The process typically involves rebooting the suspect system using a bypass OS and then proceeding to make an image of the whole disk or retrieving the hard disk from the system casing and connecting it to another computer to make a disk image.

Forensic disk imaging tools (EnCase®, SafeBack, Linux dd etc.) are used, which make an exact bit-by-bit replica of the digital media. This process preserves not only all files but also any deleted files, free space and slack space.[i] A checksum[ii] is often used to verify the integrity of the bit-image. The imaged media is usually write-protected by hardware or software means to ensure its continued integrity.

Principles of preservation also include maintaining a chain-of-custody and proper documentation at all steps. These principles also apply to all other stages of forensic work.

Examination & Analysis: This part of an investigation usually requires the most effort[35], and is comprised of the following main steps:

- Exclude known benign files: this can be done by comparing the checksum signature of files present on the system with a database of known signatures. NISTs National Software Reference Library and NDICs Hashkeeper are examples of such databases.
- Examine obvious files: Look for appropriate evidence depending on the case. For example, email records for cyberstalkers, system/network log files for hackers and images for child pornographers.
- Search for hidden evidence: The data stored in a computer can be analogized to an iceberg.[36] What's above the surface is what can be seen with the normal tools such as file explorer. But what's not visible beneath the surface is all the data hidden in areas like the slack space, swap files, windows registry, meta-data, file headers and unallocated space. Forensic tools, such as EnCase®, help the investigator look for evidence buried in such hidden data.

For the benefit of the forensic investigator it is very hard to permanently remove any data from the disk. Simply deleting the file actually only removes the name of the file from a lookup table, leaving the contents of the file untouched. Even formatting simply overwrites the file allocation table and not the entire disk.[37] Disk wiping software (Evidence eliminator etc.) can help, but even they are not completely effective.

Sometimes data which has in fact been overwritten can be recovered by means such as magnetic force microscopy (MFM)[38] which examines the edges of a track to determine the marks of previously written data.[iii] Such a process is however expensive and is only used for critical cases

---

i Free space is areas on the disk where expectedly no data is stored, while slack space is defined as the area between the end of a file and the end of its cluster

ii Checksum is a computed hash value probabilistically unique for any given input

iii Excellent images of overwritten hard disk tracks at

such as those involving national security.

Presentation: The last step involves sharing the result with the investigating agency, and possibly presenting the collected evidence in an expert testimony to court. Investigators should be ready to defend the procedures and tools used when cross-examined in court.

Network forensics is a special case of investigation in which slightly different processes are followed to collect and examine data. The data collection is done either by a hardware/software wiretap or by analyzing the logs of Internet Service Providers (ISPs) and network equipment such as routers. The challenge in analysis is that collected data - has large extraneous content and it is in the form of discrete packets. Network forensic tools, such as NetInterceptor, help by providing options to filter the data, reconstructing data from individual packets and visually representing data to enable identification of noteworthy trends.

Challenges

Encryption: Some consider encryption to be the Achilles heel of computer forensics. There does exist (and will exist in the foreseeable future) strong encryption which cannot be cracked by brute-force methods.[39] However it is difficult to implement and use encryption correctly. Common mistakes are not securing the decryption key or leaving behind an unencrypted copy of data (in the usual hiding places such as the slack space, swap file etc). Entire-disk encryption tools, PGP Whole Disk and DriveCrypt for example, make it easy to use encryption, but data remains vulnerable while an authenticated user is connected to the system. Other methods, such as the use of hardware or software keyboard loggers, could also be used to side-step encryption.

Use of encryption significantly raises the cost of conducting a forensic analysis, and encrypted data cannot always be recovered. Several legislative measures have been adopted or proposed to address this problem, such as – limitations on export of strong cryptography, the Clipper Chip (Encryption-Key-Escrow mechanism), the proposed Cyberspace Electronic Security (CESA) act and Britain's Regulation of Investigatory Powers (RIP) bill.[iv] However, such measures have remained highly controversial amongst the high-tech sector and the general public, and their effectiveness to address the problem has not been verified.

Ultimately such discussion may be moot, in the light of the increasing use of steganography or data-hiding, which does not rely on encryption. Steganography, which literally means 'hidden writing', can be traced back to 440 BC. A recent pre-computer era example is the use of microdots[v] in World War II. Steganography is a class of techniques and it's applications in computer science include hiding messages in audio, video or image files.

Collaboration: Cybercrimes have been growing at an alarming rate and they tend to

---

http://www.veeco.com/nanotheatre/nano_view.asp?CatID=3&page=2&recs=20&CP=

iv For details, see http://www.epic.org/crypto/

v Microdot - A photographic reproduction of printed materials reduced to the size of a dot or a printed period mark for ease of secret transmittal [Source http://www.pbs.org/redfiles/kgb/inv/kgb_inv_voc.htm]

transgress national and international boundaries. Cybercrime investigations also frequently involve multiple parties such as ISPs, phone companies, local police and FBI. The investigative agencies also have to navigate a quagmire of jurisdictional and legal issues and work with a limited set of resources. In such an environment, the need for collaboration to overcome these obstacles cannot be overstated.

Intra-agency cooperation should be encouraged by setting up of multi-jurisdictional tasks forces. Smaller local units could team up to form regional task forces or form alliances with better equipped state and federal agencies. The Computer Crime Point-of-Contact List (CCPC) maintained by National Association of Attorney Generals is a step in the right direction. The list is meant to provide law enforcement with a nationwide network of state and local contacts who can be used to coordinate interstate investigations and to request assistance.

Central reporting stations should be setup to avoid duplication of efforts and to share the current knowledge of events. An encouraging example of this is the Internet Crime Complaint Center (IC3) which was borne out of a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Private industry and academia needs to be involved in the efforts to curtail cybercrime. A serious problem is lack of reporting of cybercrime incidents to the authorities. By a recent study, only 20% of computer intrusion attacks are reported to law enforcement.[40] Programs such as the FBI's InfraGard, which has 84 local chapters spread nationwide, are attempting to address these issues by gaining support and confidence of the private sector and academia. Other such initiatives have been:

- The US Secret Service's Electronic Crimes Task Force (ECTF) – meant to create a partnership between local, state, and federal law enforcement team with prosecutors, private industry and academia. Thirteen task forces have been formed following the successful example of New York.
- The Department of Justice's Computer Hacking and Intellectual Property (CHIP) Units – Follows a model of units of prosecutors working closely with the FBI, other agencies, and the local high tech community. Following its success in the Northern District of California, it has been expanded to other high-tech cities.

Tapping into the financial and technical resources of the high-tech industry and research capabilities of the academia, such programs could ease the pressure on the often overworked, poorly funded, technologically-deficient law enforcement agencies.

International cooperation needs to be secured in spite of the obstacles such as competing interests, lack of treaties and sovereignty issues. There needs to be a consensus on laws and definitions relating to computer crimes. OECD and Council of Europe committees have done pioneering work in this area. But countries have shown reluctance in adopting the resulting recommendations, citing jurisdictional sovereignty and American influence as their concerns.

A painful fact of international computer crime investigations is the letters rogatory process. If international assistance is needed in an investigation, a letter request is sent from one country's judicial authority to that of another country. Such a process is unworkable in an environment where quick responses are needed to catch the perpetrators. Such difficulties can be alleviated by formal alliances and treaties between law enforcement components of different nations.[41]

A recent successful example of international cooperation was the arrest of two people allegedly involved in the Zotob and Mytob worms, in which the FBI worked with the Turkish and Moroccan law-enforcement agencies to nab the perpetrators.[42] The issue of international collaboration extends not just to the investigative needs of law enforcement but to overall cybercrime prevention efforts and is further discussed in the legal policy section.

Standardization: Interestingly, most cybercriminals confess to their crimes. Cases in which computer forensics evidence has been presented, the testimony has mostly been uncontested. Primarily, since most cases do not hinge on the computer forensic evidence and have other corroborating evidence.[43]

Given the shaky foundations of computer forensics, this can only be described as fortuitous. However it should be expected that the forensic evidence presented and the expert testimony will be increasingly contested in future. The challenges are expected to be focused on the following general areas:

- The procedure for collecting and analyzing digital data: Presently, investigators giving testimony on computer forensic evidence, if contested, have to explain and defend every step of the process that they followed. They also need to explain highly technical terms and concepts such as file slack space, network packet sniffing and so on. This could leave the jury and the judge confused and alienated.

What is required is a general framework, which is agreed upon by the majority of computer forensic community. This would help establish a basic set of standard procedures to be followed. Hopefully this would bring the same kind of acceptance to computer forensics evidence as enjoyed by drug or DNA testing.[44]

The Department of Justice 'Searching and Seizing Computers and Obtaining Electronic Evidence' manual and the US Secret Service 'Best Practices for Seizing Electronic Evidence' could be the starting points for this work. The Digital Forensic Research Workshop (DFRWS) has also done collaborative work on developing a framework for computer forensic investigations.

- Expert testimony challenges: In established fields such as accounting, there exist certifications such as CPA, which provide a seal of acceptance and approval. However the lack of a formal education process or well accepted certification could make it easy to challenge the credentials of a computer forensic "expert" in court. Even though computer forensic is still a nascent field, steps should be taken to set up a nationally or internationally recognized certification. Such a certification could bolster the credibility of an expert

witness.[45]

There is no general agreement and acceptance on standard computer forensic techniques, and there is a scarcity of studies and data on potential error rate of the tools and processes. This could discredit the expert testimony in court, based on the Daubert criteria[vi] which is a legal precedent set by the Daubert v. Merrell (1993) case. The Computer Forensic Tool Testing done by NIST is one of the few reliable studies available.

Demanding Skill Set There is an increasing demand for computer forensic experts. Although many establishments have sprung up offering such services, the skills sought, as outlined below, are hard to find.[46]

Blending of skills required - An investigator needs thorough grounding in cyberforensics, but also needs good knowledge of the legal aspects. These qualities are not always found in the field personnel. Some technical experts do not appreciate the legal nuances, such as the need to maintain a chain-of-custody or evidence preservation, and may thus jeopardize the investigation. A Little knowledge can be a dangerous thing when it comes to law enforcement personnel who are self- anointed 'computer experts'. A simple act of booting up a computer could alter as many as 400 files on modern operating systems[47], and thus destroy potentially valuable information needed to reconstruct the activity on the computer.

Patience is a virtue - Some people perceive that all an investigator does is plug in the image of the suspects hard disk, and click on the "evidence" button, which magically shows the needed output. Others perceive it to be a glamorous binary hunt for the evildoers. Both impressions are in fact far from the truth. Cyberforensics, much like the parent field of forensics, is highly specialized and tedious work.

A big reason for that is that digital evidence has grown alarmingly voluminous. In large cases investigators could deal with multiple terabytes of data.[48] Investigators frequently spend long hours in front of the computer, sifting and analyzing data, looking for that one clue which could inculpate or exonerate the suspect.

Flexibility - Investigators need to be flexible and find creative ways to deal with confounding problems such as:

- Timeline development: given that the system clock could have been tampered with, it's difficult to develop a timeline of events based on modification or access times
- Authorship attribution: even though investigators can show the gathered evidence, it's very difficult to determine with any certainty that who was actually at the keyboard at the time that data was created.

Looking Ahead

---

vi Daubert criteria for admissibility of expert testimony comprises - Hypothesis testing, Known or potential error rate, Peer review and publication, General acceptance
[Source http://www.daubertexpert.com/basics_daubert-v-merrell-dow.html]

The physical and digital world models have merged, criminals, like the rest of us, have adopted the convenience of computers, cellphones and PDAs. It is merely the techniques for investigation that are lagging behind. However going forward we should expect an amalgamation of cyberforensics and the traditional forensics process.

Two contributing factors could precipitate this change:

- Computers are playing an increasing role in traditional forensics, from DNA analysis to crime scene recreation.
- Digital evidence is present in not just computer crimes but in almost every crime scene, from simple harassment to homicide.[49]

Such a merging would be good for the nascent field of cyber forensics, in that there could be a significant transfer of knowledge and best practices from the more mature field of forensics.

Other expected trends within the field of cyberforensics are:

- Live forensics: the ability to forensically analyze live running systems. This coupled with intrusion detection could strongly bolster cyberdefenses.
- Improved forensic tools – New research and resulting tools would address some of the currently perplexing problems such as reliable timeline development and authorship attribution.
- Remote forensic capability: EnCase® Enterprise has already made forays in this direction. Such tools would only become more robust and popular.
- Digital Signature Library – Current efforts, such as Hashkeeper (NDIC) and NSRL (NIST), could grow into a comprehensive library of known benign and malicious code in order to quickly identify and segregate the contents of a system.

On the other hand we should also expect development of anti-forensic tools and techniques, specifically meant to slip through or beat the forensic process.

Legal Policies on Cybercrime

Introduction

In its nascent stages, cybercrime enjoyed a special legal status that belied common practice used in adjudicating crimes. Hacking was commonly perceived as a prank perpetrated by teenagers. Later, the lone, highly skilled attacker working against a high value target was mythologized and revered in some ways. The media and movie industry continued to foster the notion, so that when Kevin Mitnick was arrested in 1995, there was a relative groundswell of support for his release, despite having broken into systems, stolen millions of dollars in proprietary software, "altered information, corrupted system software, and eavesdropped on users, [and] sometimes prevented or impeded legitimate use."[50] (See Appendix). The idea that cybercrime was "different" from regular crime persisted into the dawn of the Internet age, helped along by an

unwillingness among police to get involved in patrolling and investigating cyberspace. Such reluctance may have been due to lack of reference points in law, low rates of successful prosecutions (fewer than 2% of cases resolve with convictions) and international resistance to help track cross-border crimes.[51]

The perception that cybercriminals are different entities has now been thoroughly discouraged. Indeed, "prosecutors are starting to make aggressive use of the Computer Fraud & Abuse Act, which carries penalties of up to 20 years in prison. The lengthiest sentence so far has been nine years, issued in December [2004]."[52] There is no longer any calls to be lenient on a those who use computers to exploit, steal and abuse privileges, such as the Californian software executive who conspired to steal trade secrets from a competitor by illegally accessing network and computer systems.[53]

The change in these commonly held notions happened gradually, but importantly, there is now a strong sense of civic empowerment given to the government to apprehend cybercriminals, which when coupled with the renewed diligence attributed to preventing terrorism, has allowed legislation to evolve rapidly in the past few years. As computers have become more integral to daily life, allowing users to conduct higher value operations, they have naturally become targets for those imbued with the criminal tendency. Most users have recognized the threat and the need for protection, even if they ignore certain precautions, like maintaining the secrecy of passwords (instead of giving them away for chocolate.[54])

If users notice that they can no longer effectively use their workstations, legislation has usually been proposed, albeit after a lengthy period of discussion. For example, a few years ago, spam was threatening to overwhelm the usefulness of email. Subsequently, congress passed the CAN-SPAM Act of 2003, which made certain practices, like harvesting email addresses, illegal, while imposing maximum fines of up to one million dollars.[55] Despite flaws that some detractors have brought up, such as continuing to allow email addresses to be sold to third parties[56], the act has provided a legal threshold to base decisions upon and brought notoriously flagrant spammers to justice.

In a broader sense, the government has reacted to the demand for better enforcement and the need to extend legal jurisdiction over crimes that may have not been crimes before. The Cyber Security Enchancement Act of 2002 (H.R. 5710, Sec. 225), which fell under the Homeland Security Act, and the USA PATRIOT Act both instituted changes to deal with cybercrime. Other, more comprehensive laws, like the Fraud and Related Activity in Connection with Computers, located in the the US Criminal Code (18 U.S.C. § 1030) and Unlawful Access to Store Communications (18 U.S.C. § 2701) have been codified for a longer period of time.

The increase in awareness of cybercriminality has begun to manifest itself with the passage of laws, creation of organizations and advisory committees and powers granted to enforcement agencies. Their application to current cybercrime has found varying degrees of success. What

needs to then be examined and discussed with the aforementioned issues in mind are the crafting of laws, enforcement and effectiveness. These have to be multiplexed across national and international settings, while being interpreted within a framework of technology and trends that are rapidly evolving. Only then can a broad understanding of the legal policies surrounding cybercrime be achieved.

International Cybercrime

A significant problem that arises when working with cybercrime is that most crimes transit data through a multititude of international borders before reaching the final, intended target. Such circuitousness has a deleterious effect on investigating cybercrimes as well as the application of laws. An illustrative example of the legal hurdles faced with international incidents comes from the "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" manual for the United State Department of Justice. The manual reports that when seeking assistance from ISPs overseas, officers must work "with the consent of that country," which means certain formalities need to be resolved before proceeding. First, prior permission of the foreign government must be obtained. Next, approval from the Justice Department's Office of International Affairs, and finally a clear indication that the actions would not be objectionable in the foreign country.[57] The process is long and unwieldy, especially since by the time the necessary paper work is filed, ISPs may have already deleted the information. Or in a worse case, after the information is obtained, it will then be discovered that the attacker went through another country, forcing the process to be repeated. Many developing countries are short on the resources and technical knowledge needed to expedite this process, causing the investigation to fail.

By 1997, the problem was being recognized internationally and the G-8 Justice and Interior Ministers noted that to be "consistent with the principles of sovereignty and the protection of human rights, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes."[58] To aid this process they created a Point of Contact network which required participating countries to specify a specific group that could assist 24 hours a day, 7 days a week. By 2002, twenty countries were participating. These types of mutual legal assistance treaties (MLATs) have been effective where in the past law enforcement has been stymied. For example, in 1992, the US government required assistance from Switzerland regarding an attack in the U.S., but since Switzerland had no such laws regarding hacking on the books, they refused to help.[59]

In devising MLATs, a country can either create bilateral or multilateral relationships, each having its own benefits and drawbacks. Traditionally, sovereign nations have entered bilateral agreements with countries that they trust and are willing to accept each other's legal characteristics. They are quicker to negotiate, produce more detailed documents, are easier to

change and allow nations to feel more comfortable sharing sensitive information.[60] In fact, after the 2001 terrorist attacks, the US was eager to more quickly establish such ties and has concluded over 45 such agreements.[61]

The drawbacks of course are that separate, and perhaps unequal, agreements must be reached, resulting in varying interpretations of crime and legal precedent. Multilateral pacts seem more suited to issues that are global in scale, much like cybercrime. Thus, it was with great fanfare that in November of 2001, thirty countries signed the Council of Europe's Convention on Cybercrime. The convention had been five years in the making and represents the first truly multinational attempt at defining, regulating and providing a framework for the legal issues in relation to cybercrime. Briefly, it established conduct that is prohibited, identified required national legal processes and addressed international cooperation.

At the U.S. Senate hearings on ratifying the treaty, Swartz noted "in the past, if an electronic transmission's trail led to another country, the chances were slim of successfully tracking the communication to its source or securing the evidence before deletion. With the tools provided for under the Convention, however, the ability of U.S. law enforcement to obtain international cooperation in identifying major offenders and securing evidence of their crimes so that they can be brought to justice will be significantly enhanced."[62] Although the Senate Foreign Relations Committee approved the treaty, it has stalled in the Senate for nearly two years, as certain groups have opposed it for reasons related to civil liberties.

The current state of multinational legislation thus remains a patchwork of bilateral treaties put together piece by piece. Establishing transnational treaties is a difficult task and remains as an open policy debate. What can be agreed upon is that all nations need multilateral assistance in a global sense, not just a limited group, as cybercriminals can route through any country. Treaties, then, need to harmonize laws, while building capabilities. Most importantly, such treaties should not be used to violate human rights, even though to do so may be legal in some countries.[63] For example, with the current Convention on Cybercrime, China could ask the U.S. to assist in finding political dissidents and supporters of democracy and the U.S. would be obliged, under the terms of the Convention, to provide assistance.

More often than not, even if a successful conviction can be obtained, extraditing a criminal is still a tough legal battle. For example, in October of 2001, a Pakistani man was charged with defacing an American-Israeli organization's website. The FBI, working with the U.S. Embassy in Pakistan, was able to identify the attacker and get a warrant issued for his arrest in Pakistan, yet three years later he is still at large.[64] Clearly, there is a need for a more comprehensive international plan.

Cybercrime in the United States

Legalistically, cybercrime has had a much richer history, as well as more successful application within the U.S. than through treaties. A bevy of criminal codes are defined specifically dealing with computers, and the PATRIOT Act and the Cyber Security Enhancement Act further expand powers, albeit in the name of foiling terrorism. Furthermore, many computer crimes are dealt with by using traditional laws. For example, on November 17th, 2005, the Shadowcrew group, an online organization involved with credit card theft, identity theft and a number of other illegal activities, all plead guilty to conspiracy to commit fraud and identification fraud. The fact that their actions were committed over the Internet was not a legal obstacle, and all will receive up to five years of jail time.[65]

The United States has an interesting legal structure that allows individual states to create and supplement federal statutes. For example, Ohio specifically notes that one cannot "deny access to a computer," (Ohio § 2913.81), while in Texas they have codified different penalties for the amount of damage caused to a system through "harmful access" (Texas § 33.03). Traditional state laws are generally similar due to the Model Penal Code, which attempts to standardize the separate state legal systems. With the advent of computers, states have been left to their own devices. Attempts have been made to create a Model States Computer Crime Code, but the idea has not advanced greatly as to date. Susan Brenner notes that the perception that cybercrime is a "new" type of crime, conflated with the rapid pace of technology, has caused a confusion amongst state legislatures that has resulted in disparity.[66] She further argues that separate state adoption of laws has created an environment that makes fighting cybercrime, an inherently borderless activity, more difficult to combat. In a further criticism, she asks "if the entities that comprise the United States of America do not, for example, adopt legislation making it a criminal offense to disseminate a computer virus, how can they condemn other nations for their failure to do so?"[67]

With the state levels failing to provide consistency, the federal government has taken the lead, not only in defining cybercrime, but also in its prosecution. Yet, before the Department of Justice and the Federal Bureau of Investigations can investigate and prosecute a crime, there must be evidence of interstate or foreign transmission of data, or the crime must become a matter of national security, a threshold lowered in the wake of the PATRIOT Act passage. One such law included in the PATRIOT Act was the Critical Infrastructures Protection Act of 2001 that defines "critical infrastructure as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security."[68] Thus, an attack, even originating from within a state, that seems to threaten the security of the whole network can be dealt with from a new perspective, equating it in many ways as terrorism. The law signifies a marked departure from just a few years prior. In 1998, when tension was building in Iraq over weapons inspections, over 500 industry and military computer targets were attacked and

compromised. Many were concerned that foreign elements were waging electronic war on the U.S. and that it might be grounds for a physical strike in response. In fact, the perpetrators were teenagers from California and Israel, which subsequently downgraded that threat from war to just a crime committed by "digital outlaws", as Attorney General Janet Reno said at the Cybercrime Summit in 2000.[69]

The national government also plays a crucial role in protecting critical infrastructure through establishing agencies and groups responsible for providing support for the Internet. It is a response that most state governments are not able to pursue. In the National Strategy to Secure Cyberspace, a document within the larger Strategy for Homeland Security, a framework is laid out to create a national cybersecurity threat team. The team is a collaboration between public-private organizations, coordinated through the Department of Homeland Security, that can analyze threats, help with warnings, deal with incidents and effect recovery strategies on a 24 hour, 7 day a week capacity. This organization, within the DHS, superseded the National Infrastructure Protection Center and is now called the National Cyber Security Division. This is the group responsible for protecting the nation's vital virtual resources. In practice, the operating arm is US-CERT.

Of course, there has been criticism that the government has not been doing enough to protect cyberspace. In 2005, the President's Information Technology Advisory committee recommended a large increase in spending in order to secure the future of Internet reliability and security by increasing funding for the DHS to focus on different areas within cybersecurity. Interestingly, they also note the need to support and recruit more security researchers because the current population is too small to deeply investigate security issues.[70]

Whether the current legal system, along with its mandates to create and fund enforcement agencies, has succeeded is still a matter of fierce debate. Most recognize that there is a strong need to upgrade the abilities of our current agencies, unify and systemize laws across states and strengthen the penalties for those causing grievous harm to networks and businesses over the Internet.

Future Trends in Legislation

The direction of legislation has slowly been proceeding to more severe and serious punishments for cybercrime. As mentioned earlier, November 3rd saw the first prosecution for owning and operating a botnet system. It seems probable as legislatures, federal and state, become aware of threat posed by botnets, and as methods become more advanced in discerning botcontrollers, legislation aimed at the problem will follow. Whether it will become an effective deterrent probably rests with the ability to investigate and prosecute. Another area of concern is

identity theft, a process facilitated to a large degree through the Internet. California has been the first to create legislation aimed at companies with lax security regarding the protection of personal information they may store. The California Security Breach Information Act (SB-1386), which went into effect in July of 2003, forces organizations to notify individuals if there is such a security breach. It has been a powerful method for not only making people aware of the issue, but also applying a force for change in policy within many organizations, lest they be branded as uncaring and incompetent. With more sensitive information being stored by a greater number of third parties, more states will come to the conclusion California has and indirectly apply pressure to organizations to reform. In another example, a recent piece of county legislation in Westchester, New York proposed to make it illegal for companies storing personal information to allow insecure access to their networks. In a sense, it would criminalize using a wireless network with no security measures. Although, many have pointed out specific weaknesses in the bill, the idea has been praised as a step in the right direction and an important conduit for educating the public.[71]

Cybercrime presents a challenging position for lawmakers, as they struggle to keep up with changes in technology and in the methods used to exploit those technologies for maliciousness. Unfortunately, legal wrangling leaves the judicial system in a state that can be behind the times. It should be realized that in the end, laws can only do so much to regulate an activity. Proactive security, user education and vigilance, combined with effective forensics and enforcement remain the best remedies for combating cybercrime. Legislation still needs to enact appropriate punishments and establish frameworks, though and in that sense it has a crucial role to play in the mitigation of cybercrime.

The Future of Cybercrime

Introduction

During an eight day period in August of 2003, three separate worms cost the U.S. economy close to two billion dollars in lost production. Later that summer, the east coast of the United States experienced a massive blackout that might have been exacerbated by a worm called Blaster.[72] Robert Cringley believed that same year that "the cost to society of identity theft is in the range of $4-5 billion per year and may be even higher."[73] With the convergence of organized crime and technically savvy cybercriminals, the growing fear of cyberterrorism, the inability to understand security from major software vendors and the slow footedness of the government, the future seems to point to an Internet that is not only vulnerable to major attacks, but also infested with scams, thieves, and ever increasing opportunities for exploitation. Although inherently difficult to predict trends within the field of technology, there are some eventualities that seem certain, like the growth of extortion and fraud though the Internet. These difficulties will of course result in new

responses that better protect customers and force criminals into new realms. Although it is a hackneyed expression, the Internet is still in the Wild West stages. It is important to remember, though, that the Wild West eventually turned into suburbia after successful methods were found to control and police criminals, making their life extremely difficult. An examination of some of the potentialities will help to illustrate how the Internet and cybercrime can be envisioned, at least in the near term future.

Future Trends in Cybercrime

The pace at which cybercrime is growing is one of the most disturbing trends. Valerie McNiven, a U.S. Treasury Advisor, has proclaimed "last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion." She further added that "cybercrime is moving at such a high speed that law enforcement cannot catch up with it."[74] It seems clear that the issue will only become worse in the next few years, now that professionals have realized the potential windfalls if exploited properly.

Recently, there has been significant discussion over the amalgamation of organized criminals and cybercrime. Such a pairing indeed forebodes an ill omen for the near term future. With most of the criminal groups operating out of eastern Europe, Russia and Asia, where laws and enforcement are scanty, there seems little hope in containing and neutralizing the threat through traditional means. Phil Williams, a visiting scientist at CERT, summarized the issue succinctly. "The Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime it is difficult to ask for more."[75]

The result that can then be expected will be an increase in sophisticated phishing attacks and other means for identity theft that may be two pronged. For example, using call centers to notify "customers" ahead of time of some issue, and then following up with emails that request personal information. These types of social engineering attacks can be very damaging and have had a long history of success within cybercrime and fraud related transgressions. The Internet makes it even easier since a degree of authority can be imparted with official looking emails and fraudulent websites that mimic their legitimate counterparts exactly. In the past, such social engineering relied on interpersonal skills like gaining trust. Now, the same idea has been transferred to technology, which can be done with greater ease by a wider group of people.

Another aspect of fraud will result from the aggregation of personal information in many third party data centers, making them valuable targets to infiltrate. It is not hard to imagine criminals using data mining techniques to find the most gullible consumers, or tailoring phishing emails for specific people based on their medical, financial or personal history. Identify theft will also move in more automated directions. For example, botnets will become vehicles not just for denial of service attacks and spam, but also as giant search platforms for finding personal information, like credit cards and social security numbers. Controllers of the botnets will then

receive payment to run queries on their "database."

With professional criminals managing the money laundering and organization of such schemes, it begs to ask where will all the technical know-how come from in order to perform cybercrime? Unfortunately, there are growing numbers of intelligent black-hats with university degrees spread around the globe, many of them operating in countries where legal employment does not pay as well and the chances of being caught are slim. But more troublesome is that it has become easier than ever before to be a hacker capable of inflicting great harm on networks and committing cybercrime. The Internet has created a repository of knowledge where anyone is able to learn the fundamentals of subverting computer systems, with numerous tutorials available that spell out in nearly layman's terms how to perform a buffer overflow or a man in the middle attack. Interestingly, the greatest problem is not those who will take the time to learn and find new exploits. In fact this group will probably remain a small, highly intelligent network of researchers and security groups focused solely on finding holes in software. In this, it is preordained, that even if someone is motivated to learn how exploits work, finding a new exploit takes a degree of investigation, skill and diligence that most are not willing to invest. The real threat comes from the profound ease at which anyone can run a program like "MetaSploit," a framework for running exploits against targets that allows new modules to be imported and run automatically. The attacker literally needs to know nothing about how computers work, besides how to operate one. In fact, for almost all attacks, the hard work is done by a small group of people, and then released into the public domain, allowing almost anyone to just run the attack. Botnets are no longer hand-crafted software made by one group who truly understood the fundamentals, but instead are open-source collaborative efforts that aim to make it as easy as possible to control remote computers, such as BotNET, eggheads and CSharpBot, all available from SourceForge.

Thus, the barrier to entry to the field is so low that it allows almost anyone to experiment and join the swelling ranks of cybercriminals. With the learning curve so low, it should prompt discussion on the need for a new paradigm of thought in how to preempt and deal with criminals, in a way that is no longer tied to traditional methods. For example, for someone to break into a house, not only do they need to plan the opportune moment, but they may also have to be aware of lock picking, security system evasion and possess a degree of gumption to overcome moral thresholds. In opposition, the ease of cybercrime seems inversely proportional to the lucrativeness that it bestows and moreover, these trends show signs of accelerating.

Beyond the "who" and the "why" of future cyberattacks, the "how" will also change as operating systems become more secure and harder to exploit. With the damage that comes with each new security hole released, Microsoft, Apple and open source vendors have finally begun to seriously focus on security. Of course that hasn't stemmed the flow of vulnerabilities discovered, but techniques such as address space randomization to stop buffer overflows, advanced and automatic code reviews and more training will reduce the ability to compromise a machine through

operating system protocols over time. The real danger in the future lies with user applications, which are created by individuals or small groups without the knowledge or training required to implement security correctly. Especially dangerous are web applications that can be installed on web servers. The traditional problem with these types of security vulnerabilities was finding susceptible hosts. But with Google, a program can automatically search for sites with a specific version of a program installed and then launch an attack. If remote code can be executed, the program may not be able to take over the whole system, but it can run programs as the user which may be enough to install bots and automatically replicate. The first instance of such an attack occurred in December of 2004 with the Santy worm that attacked a popular bulletin board system by searching through Google to find hosts with a specific file that was vulnerable.[76] Such attacks aim their weapons at the least secure and vetted of software created. Although the installed base of such systems may be small, with "Google Hacking," they can still be quickly located and exploited.

Another avenue of attack that will open up will be through embedded systems, such as cell phones, mobile devices and other electronics that may connect to the Internet for the most mundane of purposes. Software is usually recreated for each iteration of a device as it is specifically designed for the hardware. This allows for security problems to creep back in over time that may have been eliminated before. As these devices start to allow consumers to make purchases, while storing valuable information, they will become more attractive for criminals. The incentives now to do so are low, so security researchers have only seen "proof-of-concept" viruses, like the one that infected cellphones running a version of the Symbian OS that could spread automatically.[77] It appears organized crime has not moved into this area due to the lack of research and understanding of how such attacks can be made profitable. Much as with the Internet, it will take time to exploit successfully.

In the same vein, eventually automobiles, home electronics devices, refrigerators and almost all devices can and will use the Internet in order to perform maintenance, download upgrades or monitor performance. These will present opportunities for maliciousness and blackmail that doesn't equate in the same way as the purely virtual environment of the Internet. If someone enters their car, controlled by a foreign agent that demands a wire transfer or else the car will be crashed at high speeds, a situation arises that people will no longer accept. Whether such a scenario will occur is debatable, but the possibility will certainly exist.

Mitigating Cybercrime

Although it is inevitable that cybercrime will increase and continue to explore new vectors for undermining privacy, authentication and law enforcement, there will also be valid and useful attempts for mitigating the abilities of criminals, as well as the effects of cybercrime. These solutions will take form in better software, anti-spyware and anti-virus software integrated into

operating systems and more user education regarding phishing and identify theft. These solutions will come primarily from software vendors themselves. On the other side, legislators will work with banks to reduce and prevent fraud, putting some of the liability with those most able to prevent it. Finally, advanced solutions coming out of research and academia will try to inhibit the inherently anonymous and insecure nature of the Internet.

With Microsoft's upcoming release of Vista, the latest version of their operating system, they'll have a new chance to focus on not only improving the general security of the system through fundamental changes, but also in providing methods for eliminating common problems, such as botnets, spyware and phishing attacks. In October of 2005, Microsoft began working together with the FTC to educate customers about botnets and the danger of allowing a computer to turn into a zombie.[78] To deal with the problem of phishing, Microsoft released a program in July of 2005 called the "Microsoft Phishing Filter," which aims to invalidate the ability of phishers to reach Microsoft customers by dynamically notifying them when there is a high chance that what is being viewed is a phishing attack.[79] Finally, Microsoft released their "AntiSpyware" program in January of 2005, to be included with Vista as well, that automatically scans your computer for programs that match spyware signatures or that try to perform suspicious actions, like modifying system functionality or trying to run upon computer start up.

If cybercrime continues to grow to epidemic proportions, as all indications seem to point to, legislation will invariably step in, but more importantly, those with the most to lose will become more involved. This includes credit card companies, banks, lending operations and other organizations dealing with monetary transactions. Paypal.com has quickly come to dominate the online payment industry, while also serving as a bank in many capacities. With only an email address and a password required to send money, this low hanging fruit has been one of the most heavily exploited realms for phishing attacks. In response, Paypal has offered at least a thousand dollars of purchase protection and a supposed one hundred percent protection against unauthorized payments sent from an account. A fraud investigation team responds to queries and according to their website, they have software that automatically monitors every transaction for inconsistencies.

This last measure used by Paypal has also become fertile ground for credit cards companies, as their systems have become powerful at identifying fraudulent purchases though the use of neural networks, a type of software emerging out of the field of artificial intelligence. In some cases, this software has been able to reduce fraud by thirty percent or more.[80] It's important to remember that the systems are not perfect solutions, but do address a large portion of illegal activity. Combined with other efforts, the goal is to reduce the effect of fraud, while making it more difficult to achieve.

Legislation will attempt to do its part as well, even though it has moved notoriously slowly when dealing with cyberthreats. The past few years have seen laws specifically crafted for spam

and dealing with attacks that threaten the integrity of the infrastructure of the Internet. If the botnet problem continues to grow, coupled with identify theft, surely more action will be taken. Although, it is still unclear how effective it will be without a significant contribution to cyberforensic development and funding for the various governmental enforcement agencies responsible for handling cybercrime matters. Another issue discussed in the Legal Policies section is the need for more international cooperation in locating, extraditing and prosecuting foreign criminals when possible, as the current system leaves much to be desired.

Finally, as with any dangerous and difficult problem, there will be new and inventive ways to handle security issues coming out of research. One contribution that has limited, but not eliminated many common security flaws that are exploited, is the use of randomization in dealing with code, data and other programmatic necessities. By introducing a factor of unpredictability, it can make the work of a hacker much more difficult and prone to error, limiting the ability of those who do not posses the skill to effect a novel attack. Other interesting proposals have included traceback systems that can remove the anonymous identity of data traveling through the Internet,[81] devising a system for fast and accurate discovery of the source of even one packet of data. Stopping distributed denial of service attacks and worm discovery has also been proposed as a method that can be automated and integrated into the backbone of the Internet, high speed routers. By analyzing similar patterns coming from separate locations, such detectors can realize an attack while it is in its infancy and isolate infected hosts.[82]

There is also still room for ISPs to actively monitor and and discourage botnets, spam and DDoS attacks from occurring. As the first link in the chain for many zombie hosts, as well as attackers, they are in a prime position for stopping spam, either by blocking outgoing mail, which most users have no need for, or by identifying when one host is sending out a large amount of data that does not match expected behavior. Additionally, if they noticed that a number of hosts were acting in concert, with regards to the data being disseminated from those machines, they may assume with likelihood that they are being controlled remotely. Consequently, the ISPs can examine logs to find who is sending the commands and initiate a complaint with the F.B.I. The problem holding back this kind of proactive approach has not been technical in nature, but rather legalistic, as it can be considered an invasion of privacy. Furthermore, such methods are being used to track down minor copyright violations, instead of focusing on more substantial problems, such as cybercrime and identify theft.

Looking Ahead

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber-apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the

Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect a percentage of possible victims. The others need to be automatically protected through measures that do not stress and require considerable participation. Security needs to be easy and effective if it is do work. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cybercrime will be proportional to real-world crimes, if not better.

Conclusion

Cybercrime has captured the attention of not only law enforcement, but also home users, system administrators and even the government. The history of cybercrime has slowly converged into a state in which large amounts of money are responsible for driving crime rather than respect or youthful experimentation. One such example of its manifestation is through botnets, a scourge to be sure, on the viability and long term success of the Internet. Without successful prevention and recovery from having a computer being taken over, users will find it increasingly difficult to justify the benefits of the Internet, especially if, for example, their identity is stolen every time they connect. Luckily, the burgeoning field of cyberforensics has proved that those who commit such crimes may not escape the reach of the law. Although much work must be done in the field to standardize processes and procedures, it is clear that the majority of criminals will not remain anonymous forever. With successful forensic investigations, it is then up to the law and government to assign punitive measures. This has and will remain challenging for law and policy makers who traditionally move slowly. Moreover, international cooperation is increasingly required to successfully resolve crimes, resulting in the need for comprehensive treaties between nations. Finally, any discussion of cybercrime must discuss what directions it seems to be heading in, as preparations must be made for all contingencies. Certainly, criminals will attempt to increase their use of the Internet to perpetrate acts of fraud and other crimes. The real question though is whether researchers, industry, law enforcement and the government can work together in order to reign in the ability to commit crimes and normalize it to a manageable level. It is still an open debate, though and only time will tell whether cybercrime becomes an unchecked monster or a just another growing pain in a long history of the Internet.

Appendix

The following presents a few real-life cases, highlighting the use of cyberforensics to catch and prosecute cybercriminals (the date indicated is the date of capture or arrest).

I. 1995, Feb 15: Kevin D. Mitnick.

Kevin David Mitnick is one of the most famous criminal hackers to be jailed. "His downfall was his Christmas 1994 break-in to Tsutomu Shimomura's computers in San Diego, California. Less than two months later, Tsutomu had tracked him down after a cross-country electronic pursuit."
The evidence collected to catch and prosecute Kevin D. Mitnick included:

- Network traffic captured, which was used to recreate his online sessions.
- Analysis of Tsutomu Shimomura's machine-state after the break-in: method and time of file access and log files were used to create estimated step-by-step actions of the perpetrator.
- ISPs (Netcom) Login records for a stolen account. These were compared with other login and phone records, in order to trace the path of the attacker.

In August 1999, Kevin Mitnick was given a 46 months sentence by the District Court in Los Angeles.[83]

II. 2001, May: Russian "Carders" (Credit Card Thieves)

Credit card thieves in Russia were using similar names to open multiple Paypal accounts, and then using these accounts to buy high-value computer goods from eBay auctions.
Paypal's team investigating this issue used sniffer tools to capture the network traffic and analyzed it to determine the originating IP address. Using this and other information gathered in investigation, PayPal froze all fraudulent accounts opened by the perpetrators, who, by this time, had managed to purchase goods worth more than $100,000. Following this Paypal actually started receiving phone calls from the perpetrators demanding that the funds in their accounts be released to them. Being in Russia, the brazen perpetrators considered themselves out of reach.
The FBI got involved in the investigation and lured them into custody by offering them security jobs while posing as a high-technology company. Paypal's investigative team then used EnCase®, a forensic investigation toolkit, to gather evidence from their computers which was finally used to convict them.[84]

III. 2005, Aug 26: Farid Essebar (Morocco), Attila Ekici (Turkey) – authors of the Zotob and Mytob worms

The FBI and Microsoft worked closely in this investigation. Microsoft monitored the attacks as they occurred, and used the gathered information to track the perpetrator's electronic trail. Analysis of the code revealed a signature with the nickname Diabl0. Further investigation was able to link the nickname to the author Farid Essebar. Moroccon and Turkish law enforcement agencies are

believed to have played an instrumental role in the investigation.[85]

IV. 2004, May 7: Sven Jaschen (Germany), author of the Sasser worm

Sven Jaschen, a German college student was arrested after authorities were tipped off by his friends following Microsoft's announcement of a $250,000 reward for the capture of Sasser's author. However evidence on the suspect's computer which could have linked him to the crime had been erased. Authorities determined that Sven had sent the source code for the worm to a friend using a US based instant messaging service. US authorities assisting in the investigation, with the help of the messaging service provider were able to gather evidence linking the transmission back to the German suspect. Sven Jaschen eventually confessed his crimes, and was tried as a minor (he was 17 when he authored the worm) and received a 21 month suspended sentence.[86]

V. 2000, Apr 23: Australian hacker responsible for attacking SCADA nodes of a sewage management system.

Vitek Boden, snubbed by the rejection of his job application, attacked the SCADA system of a Queensland Waste management company. Driving around with a laptop fitted with a radio transmitter, he commandeered SCADA systems at various waste treatment centers, and managed to release millions of liters of sewage into parks, rivers and even the grounds of a Hyatt Regency hotel. He was finally caught, when he was pulled over by police on his last mission. Examination of his laptop revealed software which could control SCADA systems, and it's time of use was linked to the time of actual attacks. Boden was convicted in October of 2001 and sentenced to two years in prison.[87]

References

1 Webcrunchers: "John Draper" http://www.webcrunchers.com/crunch/story.html

2 PBS Website. "Notable Hacks." http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html

3 Computer Crime Research Center. "Cybercrime Cost about $400 billion." July 6, 2005. http://www.crime-research.org/news/06.07.2005/1344/

4 Federal Trade Comission. "The CAN-SPAM Act: Requirements for Commercial Emailers." http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm

5 Consumer Sentinel: http://www.consumer.gov/sentinel/

6 United States Security and Exchange Commission. "Litigation Release No. 16266." Aug. 30, 1999: http://www.sec.gov/litigation/litreleases/lr16266.htm

7 SecurityPark.net. "Kaspersky Lab identifies malware and cyber threat evolution." Oct. 10, 2005 http://www.securitypark.co.uk/article.asp?articleid=24493&CategoryID=33

8 Gordon, Lawrence, et al. "CSI/FBI Computer Crime and Security Survey 2005." Computer Security Institute. 2005. http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

9 Messmer, Ellen. "Botnets Getting Nastier." Network World

10 Overton, Martin. Anti-Malware Tools: Intrusion Detection Systems, IBM,UK

11 Tipett, Peter. "Putting Patch Management in Perspective." Cybertrust, October, 2005.

12 Gray, Patrick. "Intenet vulnerabilities caught in Bind." ZDNet Australia. March 2003

13 Espiner, Tom. "Inside Symantec's security bunker." ZDNet UK. November 2005

14 Know your Enemy: Tracking Botnets, The Honeynet Project and Research Alliance

15 Lyman, Jay. "Worm Variant Parade Marches On." TechNewsWorld, April 2004

16 Leiban, Rachel. "Chat 'Bots' may be hacker tool." ZDNet Australia. May 2002

17 Brumme, Stephan. "Monitoring the Gnutella Network", University of Technolgy, Sydney, Australia.

18 Lemos, Robert. "Alarm Growing over bot software." CNET News. April, 2004

19 Houle, Kevin J, Weaver, George M. et al. "Trends in Denial of Service of Attack Technology." October 2001

20 ibid

21 Holz, Thorsten. "Spyware in the forms of Bots." Laboratory for Dependable Distributed Systems

22 Poulsen, Kevin. "Hackers Admit to Wave of Attacks." Wired, September, 2005

23 Ilett, Dan. "Most spam generated by Botnets." ZDNet UK, September 2004

24 Massimiliano Romano, Simone Rosignoli, Ennio Giannini, Robert Wars. "How Botnet Works." WindowsSecurity, November 2005

25 Evers, Joris. "Witty 'probably an ISS inside job'", CNET News, May 2005

26 Geer, David. "Malicious Bots Threaten Network Security." Industry Trends, January 2005

27 Franklin, Curtis. "'Botnets' Taking Control Away from Users, Enterprises." Network Computing,

April 2005

28 McCarty, Bill. "Automated Identity Theft." IEEE Security & Privacy, Sep-Oct 2003 (Vol. 1, No. 5) pp 89-92

29 Dave, Dittrich. "Dissecting Distributed Malware Networks." University of Washington.

30 Lampson, Butler. "Economics and computer security." University of Washington. Accessed Dec 4,2005. http://videosrv14.cs.washington.edu/education/courses/csep590tu/05au/csep590tu_7_3.mp3

31 Solomon, Michael G. et al. Computer Forensics Jump Start. San Francisco: Sybex, 2005. 2

32 "How much information?" UC Berkeley's School of Information Management and Systems. Accessed Nov 28, 2005. http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm

33 Radcliff, Deborah. "Inside the DoD's crime lab." Network World. Mar 8, 2004

34 Ibid.

35 Branigan, Steve. "High Tech Investigations: It Ain't Just Forensics..." 2005. CyanLine. Accessed Nov 29,2005. http://www.cyanline.com/pres/auscert05-run-a-case.pdf

36 Cummings, Richard, and Jake Lowry. "Computer Forensics 101 & Incident Response." 2003. Guidance Software. Accessed Nov 30, 2005. http://www.isacala.org/doc/2003oct1_workshop_pres.pdf

37 Caloyannides, Michael. Privacy Protection nd Computer Forensics. Norwood, MA: Artech House, 2004. 26.

38 Ibid. 31-32.

39 Ibid. 192-193.

40 Mueller , Robert S. "Director Mueller to Cyber Professionals: Report Your Hacks!" Federal Bureau of Investigation. Accessed Nov 30, 2005. http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

41 Britz, Marjie T. Computer Forensics and Cyber Crime. New Jersey: Pearson Prentice Hall, 2004. 94-97, 228-229.

42 Kontzer, Tony. "Collaboration Helps Nab Cybercriminals." InformationWeek Sep 5, 2005

43 Meyeres, Matthew, and Mark Rogers. "Computer Forensics: The Need for Standardization and Certification." 2004. International Journal of Digital Evidence. Accessed Dec 1, 2005. http://www.ijde.org/docs/meyersrogers_ijde.pdf

44 Carney, Megan, and Marc Rogers. "The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction." 2004. International Journal of Digital Evidence. Accessed Dec 1, 2005. http://www.ijde.org/docs/04_spring_carneyrogers.pdf

45 Meyeres, Matthew, and Mark Rogers. "Computer Forensics: The Need for Standardization and Certification." 2004. International Journal of Digital Evidence. Accessed Dec 1, 2005. http://www.ijde.org/docs/meyersrogers_ijde.pdf

46 Berryhill, Jon. "Finding a qualified computer forensic analyst." Law Enforcement Technology. May 2000. See also: Kahan, Stuart. "Bring 'em back intact!" Accounting Today Jun 6, 2005.

47 Solomon, Michael G. et al. Computer Forensics Jump Start. San Francisco: Sybex, 2005.

48 Radcliff, Deborah. "Inside the DoD's crime lab." Network World. Mar 8, 2004

49 Coren, Michael. "Digital evidence: Today's fingerprints." CNN.com. Jan 31, 2005. Accessed Dec 4, 2005. http://www.cnn.com/2005/LAW/01/28/digital.evidence/. See also.
Martin, Judith. "Electronic Crimefighting". Law & Order. Dec 1, 2003.
Radcliff, Deborah. "Inside the DoD's crime lab." Network World. Mar 8, 2004.

50 Takedown website: http://www.takedown.com/

51 Jewkes, Yvonne. Dot.Cons: Crime, deviance and identity on the Internet. Willan Publishing. 2003. p. 16.

52 Grow, Brian. "Hacker Hunters." Business Week, May 30, 2005.
http://yahoo.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

53 Dept. of Justice, California. "Software Executive Admits to Conspiring to Misappropriate Chief Competitor's Trade Secrets." Press Release. Sept. 29, 2005.
http://www.cybercrime.gov/mcmenaminPlea.htm

54 BBC News. "Passwords Revealed by Sweet Deal."Apr. 20, 2004.
http://news.bbc.co.uk/1/hi/technology/3639679.stm

55 Schell, Bernadette and Martin, Clemens. Cybercrime. ABC CLIO. 2004. p. 69

56 CAN-SPAM Act of 2003. Section 3 (1). http://www.spamlaws.com/federal/108s877.shtml

57 U.S. Department of Justice. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." July 2002.
http://www.cybercrime.gov/s&smanual2002.htm

58 Meeting of Justice and Interior Ministers of The Eight, Dec. 9-10, 1997.
http://www.qlinks.net/comdocs/washcomm.htm

59 Westby, Jody. American Bar Association. International Cybercrime Project. Aug. 8th 2002.
http://www.abanet.org/scitech/computercrime/cybercrimeproject.html

60 Litt, Robert and Lederman, Gordon. "Formal Bilateral Relationships as a Mechanism for Cyber Security." Cyber Security: Turning National Solutions into International Cooperation. CSIS Press. 2003. p. 43

61 Shimbun, Yomiuri. "Govt eyes law enforcement treaty with U.S." *Yomiuri Online.* June 20, 2003.
http://www.crime-research.org/news/2003/06/Mess2002.html

62 Swartz, Bruce. Senate Foreign Relations Committee. June 17th, 2004.
http://foreign.senate.gov/testimony/2004/SwartzTestimony040617.pdf

63 Goodman, Seymour. "Toward a Treaty-Based International Regime on Cyber Crime and Terrorism." Cyber Security: Turning National Solutions into International Cooperation. CSIS Press. 2003. p. 71.

64 Schell, Bernadette and Martin, Clemens. Cybercrime. ABC CLIO. 2004. p. 166

65 Dept. of Justice. Press Release. Nov. 17, 2005.http://www.cybercrime.gov/mantovaniPlea.htm

66 Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28 (Winter 2001), *at* http://www.richmond.edu/jolt/v7i3/article2.html.

67 Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28 (Winter 2001), *at* http://www.richmond.edu/jolt/v7i3/article2.html.

68 USA PATRIOT Act of 2001. H.R.3162. http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@@L&summ2=m&

69 Bendrath, Ralf. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." Information and Security. Vol. 7. 2001. pg 80-103.

70 President's Information Technology Advisory Committee. Cyber Security: A Crisis of Prioritization. 2005. pg 30.

71 Myser, Michael. "New York County Proposes Law to Enforce Wi-Fi Security." Eweek.com. Nov. 4 2005. http://www.eweek.com/article2/0,1895,1882081,00.asp

72 Schell, Bernadette and Martin, Clemens. Cybercrime. ABC CLIO. 2004. p. 21

73 Cringley, Robert. "How to Steal 65 Billion Dollars." PBS. Sept. 11, 2003. http://www.pbs.org/cringely/pulpit/pulpit20030911.html

74 Karam, Souhail. "Cybercrime yields more cash than drugs." Reuters News. Nov. 28, 2005. http://labs.news.yahoo.com/s/nm/20051128/wr_nm/cybercrime_dc

75 Williams, Phil. "Organized Crime and Cybercrime: Synergies, Trends, and Response." Global Issues. Aug. 2001. http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

76 Lemos, Robert. "Net Worm using Google to Spread."CNET. Dec. 21, 2004. http://news.com.com/Net+worm+using+Google+to+spread/2100-7349_3-5499725.html

77 Naraine, Ryan. "Cell Phone Virus Ringing." InternetNews.com. June 15, 2004. http://www.internetnews.com/security/article.php/3368811

78 Microsoft Press Release. "Stopping Zombies Before They Attack: Microsoft Teams with Federal Trade Commission and Consumer Action to Promote PC Protection." Oct. 27, 2005. http://www.microsoft.com/presspass/features/2005/oct05/10-27Zombie.mspx

79 Microsoft Press Release. "Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers." Nov. 17, 2005. http://www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx

80 The Guardian. "Mimicking Fraudsters." The Guardian Unlimited. Sept. 9, 2004. http://technology.guardian.co.uk/online/story/0,3605,1299691,00.html

81 Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer. "Single-Packet IP Traceback." In *IEEE/ACM Transactions on Networking (ToN)*, Volume 10, Number 6, December 2002.

82 Sumeet Singh, Cristian Estan, George Varghese and Stefan Savage, Automated Worm Fingerprinting, *Proceedings of the ACM/USENIX Symposium on Operating System Design and Implementation*, San Francisco, CA, December 2004.

83 Takedown Website. "Takedown." Accessed Nov 19, 2005. http://www.takedown.com

84 Deborah Radcliff. "Cybersleuthing solves the case." Computerworld. Jan 14, 2002. http://www.computerworld.com/securitytopics/security/story/0,10801,67299,00.html

85 Kerbs, Brian. "Suspected Worm Creators Arrested." Washington Post. Aug 27, 2005. Accessed Dec 5, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/26/AR2005082601201.html

86 Unknown. "Global Partnership at work – Catching a Cyber saboteur." Federal Bureau of Investigation. Nov 30, 2005. http://www.fbi.gov/page2/sept05/globalpartnerships091905.htm

87 Smith, Tony. "Hacker jailed for revenge sewage attacks." The Register. Oct 31, 2001. Accessed Dec 5, 2005. http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/