International Standard Serial Number (ISSN): 2249-6807

International Journal of Institutional Pharmacy and Life Sciences 2(1): January-February 2012

INTERNATIONAL JOURNAL OF INSTITUTIONAL PHARMACY AND LIFE SCIENCES

Computer Sciences **Original Article……!!!**

Received: 02-02-2012; Accepted: 06-02-2012

ANALYSIS OF THE TYPES OF CYBER ATTACK AND THEIR IMPLICATIONS

Kalpna Midha*, Dr. Vijay Singh Rathore

Keywords:

Cyber attack, Botnet, Peer to Peer, Phishing, Pharming, Spoofing, Spamming

For Correspondence:

Kalpna Midha

Sri Ganganagar

E-mail:

kalpnamidha@gmail.com

ABSTRACT

Cyber attack is a growing problem for the international community. The lack of attention given to cyber attack currently can be attributed to the priority given to "cyber" as a military domain. Over the past decade, cyber attack has caused companies around the world to lose millions, if not billions, of dollars. We apply the general theory of crime and the lifestyle/routine. Activities framework to assess the effects of individual and situational factors on six types of cyber attack victimization. The results indicate that neither individual nor situational characteristics consistently impacted the likelihood of being victimized in cyberspace. Self-control was significantly related to only two of the six types of cyber attack victimizations and although five of the coefficients in the routine activity models were significant, all but one of these significant effects were in the opposite direction to that expected from the theory. At the very least, it would appear that other theoretical frameworks should be appealed to in order to explain victimization in cyberspace.

INTRODUCTION

A cyberattack (also called a computer network attack and CNA) is code or other deliberate act designed to alter, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Cyberattack (CyA) "actions combine computer network attack (CNA) with other enabling capabilities (such as, electronic attack (EA), physical attack, and others) to deny or manipulate information and/or infrastructure."

Cyberattack "refers to the use of deliberate actions — perhaps over an extended period of time — to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programsresident in or transiting these systems or networks. Such effects on adversary systems and networks may also have indirect effects on entities coupled to or reliant on them."

A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Over the past two decades, cybercrime has emerged as a salient area of inquiry for criminologists and a growing concern for public policy. Although there are many definitions of cybercrime, the term generally refers to crimes committed through the use of computers and computer networks.

TYPES OF CYBERATTACK

1. Botnet

A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for “robots”) are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

In order to better understand botnets, we first define some key terms. Then, we present a timeline of the significant events that relate to bots and peer-to-peer protocols in terms of technological developments. Based on this review of historical trends, we believe that peer-to-peer botnets will be one of the most significant threats on the Internet in the near future.

1.1 Definitions

We define peer-to-peer, bot, and botnet below.

- peer-to-peer – A peer-to-peer network is a network in which any node in the network can act as both a client and a server.
- bot – A bot is a program that performs user centric tasks automatically without any interaction from a user.
- botnet – A botnet is a network of malicious bots that illegally control computing resources.

Some definitions of peer-to-peer networks require no form of centralized coordination. Our definition is more relaxed because the attacker may be interested in hybrid architectures. Our definition of a bot is not inherently malicious. However, the malicious nature of a bot is implicit under some contexts. Finally we do define a botnet to be malicious in nature.

1.2 History

The timeline ranges from the one of the earliest bots, EggDrop, through the Trojan Peacomm peer-to-peer bot recently released. More recent years have seen significant developments of malicious bots. In particular, the first peer-to-peer bots are beginning to emerge, such as the Trojan.Peacomm bot.

Worms can serve as one form of a delivery mechanism for bots. Although worms are relevant to the development of botnets they are more relevant to the spread of bots than to the botnet communication after infection. Our work focuses on the communication mechanism in place after the botnet has spread to its victims. Kienzle et al. provide a survey of worms. During the early stages of the Internet, a nonmalicious bot was developed called EggDrop. There were likely many other bots developed prior to EggDrop. However, EggDrop is recognized as one of the first popular Internet relay chat (IRC) bots. Example nonmalicious uses of EggDrop include playing games (i.e., Turing test), coordinating file transfer (legally transferred files), automating channel admin commands, etc. Thus, the early bot developments seem to have been motivated by simply improving automation on the Internet. The GTBot variants are one of the earliest wide-known malicious bots.

2. Pharming

A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.

2.1 Pharming Examples

In January 2005, the Domain Name for a large New York ISP, Panix, was hijacked to point users to a site in Australia. In 2004 a German teenager hijacked the eBay.de Domain Name.

Hushmail, a provider of secure email services, was also attacked with pharming. In April of 2005 a hacker (the "pharmer") -- through inappropriate communications with the domain registrar -- was able to redirect users to a defaced webpage.

While defaced web pages may be a problem, pharming can be leveraged to commit far more sinister crimes. If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to commit a phishing-type crime such as stealing users' credit card numbers, PIN codes, or username-password combinations.

3. Spoofing

Creating a fraudulent Web site to mimic an actual, well-known site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.

When the world has started calling this era as the era of Internet A World Wide Web that connects the every nook and corner of the globe we should never be let behind because of some pestering security problems.

Spoofing of the Web and IP has over the years proved to be annoying as well as dangerous. In this tense scenario it is mandatory that we stick onto the various solutions so far available and at the same time spend our sincere efforts in devising better plans to solve this menace. Indeed techniques like Packet Filtering and Cryptographic techniques help to some extend but their efficiency is limited. We still rely on manual security checks of the status line, location line etc. which indeed are quite ineffective and practical.

The whole problem basically exists in that most of the web applications and tools rely on the source IP address authentication. Alternatives are to be derived and a better safer Internet should solve the problem of Spoofing.

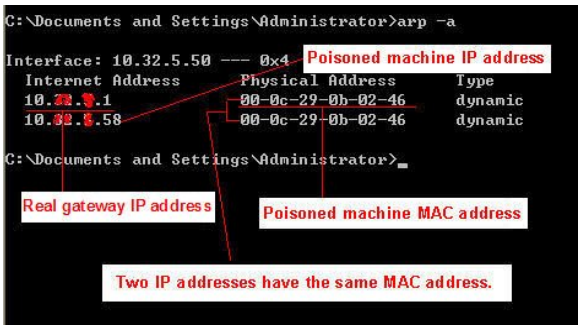
In august 2006 we've seen many ARP spoofing viruses, also known as ARP cache-poisoning viruses. This type of malware comes in many variants and is widely spread in China. Recently, we uncovered an ARP spoofing virus that exhibits several new features.

The new ARP spoofing virus inserts a malicious URL into the session of an HTTP response, thus including significant malicious content, and then exploits Internet Explorer. At the same time, the virus makes a poisoned host act as an HTTP proxy server. When any machine in the same subnet with the poisoned machine accesses the Internet, the traffic goes through the poisoned machine.

Let's take a detailed look at the features of the latest ARP spoofing virus.

This type of virus replaces the MAC address of the Gateway machine with the MAC address of the poisoned machine. The following screen shows the correct Gateway MAC address:

When we run the ARP spoofing virus, the Gateway MAC address is changed, as shown in the following diagram. The real Gateway MAC address is changed by the poisoned machine to the MAC address of the poisoned machine. Please review the following diagram.



4. Phishing

A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial information from the sea of internet users.

With the tremendous increase in the use of online banking, online share trading and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds. Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc) by masquerading as a trusted entity.

The usual scenario is that the victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to "a secure page on the bank's website". The victim believes the web page to be authentic and he enters his username, password and other information. In reality, the website is a fake and the victim's information is stolen and misused.

4.1 History and current status of phishing

A phishing technique was described in detail, in a paper and presentation delivered to the International HP Users Group, Interex. The first recorded mention of the term "phishing" is on the alt.online-service.america-online Usenet newsgroup on January 2, 1996, although the term may have appeared earlier in the print edition of the hacker magazine 2600.

A recent and popular case of phishing is the suspected Chinese phishing campaign targeting Gmail accounts of highly ranked officials of the United States and South Korean's Government, military, and Chinese political activists. The Chinese government continues to deny accusations of taking part in cyber-attacks from within its borders, but evidence has been revealed that China's own People's Liberation Army has assisted in the coding of cyber-attack software.

5. Spamming

Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be sued as a delivery mechanism for malicious software and other cyber threats. Simple program that dial consecutive phone numbers looking for a modem.

5.1 History of Internet spam

The earliest documented spam (although the term had not yet been coined) was a message advertising the availability of a new model of Digital Equipment Corporation computers sent by Gary Thuerk to 393 recipients on ARPANET in 1978. Rather than send a separate message to each person, which was the standard practice at the time, he had an assistant, Carl Gartley, write a single mass e-mail. Reaction from the net community was fiercely negative, but the spam did generate some sales.

Spamming had been practiced as a prank by participants in multi-user dungeon games, to fill their rivals' accounts with unwanted electronic junk. The first known electronic chain letter, titled Make Money Fast, was released in 1988.

The first major commercial spam incident started on March 5, 1994, when a husband and wife team of lawyers, Laurence Canter and Martha Siegel, began using bulk Usenet posting to advertise immigration law services. The incident was commonly termed the "Green Card spam", after the subject line of the postings. Defiant in the face of widespread condemnation, the attorneys claimed their detractors were hypocrites or "zealouts", claimed they had a free speech right to send unwanted commercial messages, and labeled their opponents "anti-commerce radicals." The couple wrote a controversial book entitled How to Make a Fortune on the Information Superhighway.

Within a few years, the focus of spamming (and anti-spam efforts) moved chiefly to e-mail, where it remains today. Arguably, the aggressive email spamming by a number of high-profile spammers such as Sanford Wallace of Cyber Promotions in the mid-to-late 1990s contributed to making spam predominantly an email phenomenon in the public mind.[citation needed] By 2009, the majority of spam sent around the world was in the English language; spammers began using automatic translation services to send spam in other languages.

6. Denial of service

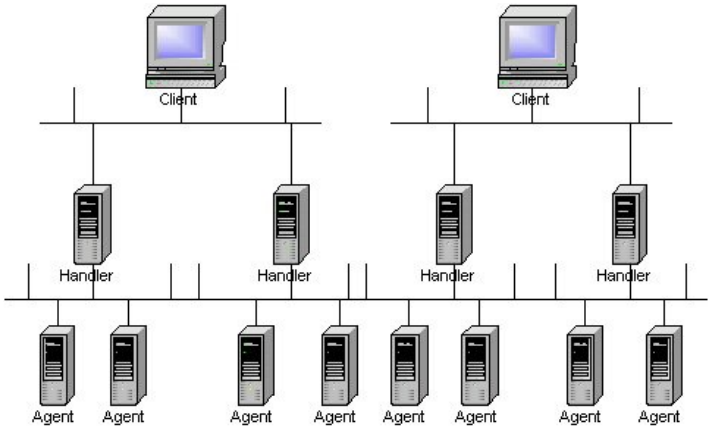
A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.

This white paper contains information in order to help you understand how Distributed Denial of Service (DDoS) attacks are orchestrated, recognize programs used to facilitate DDoS attacks, learn more about host security.

Cyberattacks as a tool for information warfare are not new and have been popular for well over a decade. Their growing prevalence, however, is a disturbing trend that requires study. Distributed Denial of Service (DDoS) attacks are one of the most widely crippling elements of many cyberwarfare campaigns. Designed to overwhelm a victim's infrastructure with junk traffic, their impact has been a significant element in some cyber warfare campaigns. As seen in Georgia, Estonia, and against dissident groups, these attacks can affect much more than just the specific targets. Furthermore, with the growing sophistication of attackers, people see that they can strike key infrastructure elements.

6.1 Understanding the Basics of DDoS Attacks

Refer to this illustration:



Behind a Client is a person that orchestrate an attack. A Handler is a compromised host with a special program running on it. Each handler is capable of controlling multiple agents. An Agent is a compromised host that runs a special program. Each agent is responsible for generating a stream of packets that is directed toward the intended victim.

Attackers have been known to use these four programs to launch DDoS attacks:

- Trinoo
- TFN
- TFN2K
- Stacheldraht

In order to facilitate DDoS, the attackers need to have several hundred to several thousand compromised hosts. The hosts are usually Linux and SUN computers; but, the tools can be ported to other platforms as well. The process of compromising a host and installing the tool is automated. The process can be divided into these steps, in which the attackers:

- Initiate a scan phase in which a large number of hosts (on the order of 100,000 or more) are probed for a known vulnerability.
- Compromise the vulnerable hosts to gain access.
- Install the tool on each host.
- Use the compromised hosts for further scanning and compromises.
- Because an automated process is used, attackers can compromise and install the tool on a single host in under five seconds. In other words, several thousand hosts can be compromised in under an hour.

CONCLUSIONS

In this paper we have attempted to demonstrate how cyberattack mechanism can help us understand how cyberattack work, the threat they pose, and how attackers control them. Our research shows that some attackers are highly skilled and organized, potentially belonging to well organized crime structures. Leveraging the power of several thousand attacks, it is viable to take down almost any website or network instantly. Even in unskilled hands, it should be obvious that attacks are a loaded and powerful weapon. Since cyberattacks pose such a powerful threat, we need a variety of mechanisms to counter it.

REFERENCES

1. Messmer, Ellen (January 22, 2008). "First case of "drive-by pharming" identified in the wild". Network World. pharming.
2. Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*.
3. Cukier, W. & Levin, A. (2009). Internet fraud and cybercrime. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet*. Upper Saddle River, NJ: Pearson Education, Inc.
4. Holt, T. J. & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*.
5. Ranchhod, A., & Zhou, F. (2001). Comparing respondents of e-mail and mail surveys: Understanding the implications of technology. *Marking Intelligence and Planning*.
6. *I. Stoica, R.* Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A service for Internet applications," in *ACM SIGCOMM* August 2001.
7. P. Maymounkov scalable peer-to-peer lookup and D. Mazi`eres, "Kademlia: A peer-topeer information system based on the XOR metric," in *1st International Workshop on Peer-to-Peer Systems*, March 2002.