World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:2, No:8, 2008

Mechanisms of Internet Security Attacks

J. Dubois, and P. Jreije

***Abstract*—**Internet security attack could endanger the privacy of World Wide Web users and the integrity of their data. The attack can be carried out on today's most secure systems' browsers, including Netscape Navigator and Microsoft Internet Explorer. There are too many types, methods and mechanisms of attack where new attack techniques and exploits are constantly being developed and discovered. In this paper, various types of internet security attack mechanisms are explored and it is pointed out that when different types of attacks are combined together, network security can suffer disastrous consequences.

***Keywords*—**DoS, internet attacks, router attack, security, trojan, virus, worm, XSS.

I. Introduction

THE World Wide Web has been the main driving force of the internet. There is about 60 million website reported to be on the internet as of February 2005, according to Netcraft survey [1]. Together with the number of general websites, the number of websites for e-commerce is also increasing. Web sites have always been the honey spots for attackers. Web attacks have been a major problem of information security recently, and are at the top of the 2005 incidents, according to Security Focus analysis [2]. As web sites become more and more important and as their number of users increases, they will expectedly become more exposed to attacks.

Ultimately all attacks are originated by people with a motivation to steal, cause vandalism, prove themselves to be elite hackers, or just for the thrill and "challenge". Most attacks are actually performed by automated tools released on the Internet. Nowadays, different internet attack types are combined such as security exploit, commonly used by malicious hackers, and computer viruses resulting in a very complex attack that, in some cases, is beyond the general scope of anti-virus or security software. In general, a large gap has existed between computer security companies, such as intrusion detection and firewall vendors, and anti-virus companies. For example, many past popular computer security conferences did not have any papers or presentations dealing with computer viruses. Apparently, a few computer security analysts do not consider computer viruses as a serious part of security or ignore the relationship between computer security and computer viruses.

Manuscript submitted June 30, 2006.

J. P. Dubois is with the University of Balamand, Deir El Balamand, Koura, North District, Lebanon (phone: 961-3-841472; fax: 961-6930250; e-mail: jeanpierre_dubois@hotmail.com).

P. Jreije is with the University of Balamand, Deir El Balamand, Koura, North District, Lebanon (phone: 961-3-841472; fax: 961-6930250; e-mail: j.daba@balamand.edu.lb).

II. Internet Attacks

Many types of internet attacks can be prevented, but if combined, they can cause serious problems. Most internet security companies are struggling to try to prevent hackers from attacking web sites by developing new security software and by constantly trying to provide updates and patches when new attack types are discovered, but they realize that this is not feasible because their internet security software is under significant risk. In the next sections, different type of internet attacks will be discussed, noting that some attacks are extremely difficult to discover and prevent.

A. Viruses

Computer viruses have a long history. A virus attempts to install itself on a user's system and to spread directly to other files on that system with the aim that these infected files will be transferred to another machine. The payload of a virus can range from 'comical' pranks to destruction of the system itself. A virus relies on users to spread by sharing infected files either directly or via email. Once launched, a virus is completely independent of its creator. Although it is the most common threat to security, the traditional virus does not attack other systems directly and so is unlikely to be detected.

B. Worms

A worm is very similar to a virus. The key difference is that a worm attempts to propagate itself without any user 's involvement. It typically scans other computers for vulnerabilities which it is designed to exploit. When such a machine is identified, the worm will attack that machine, copying over its files and installing itself, so that the process can continue.

C. Trojans

Trojans take their name from the Trojan horse of Greek mythology. Computer Trojans work in the same way as worms. A game, screen saver, or cracked piece of commercial software is given to a victim. The software may appear to work as normal, but its real purpose is to deliver a payload, such as a virus or a root kit (which will be discussed in the next section).

D. Root Kits

A root kit is a piece of software that, once installed on a victim's machine, opens up a port to allow a hacker to communicate with the machine and take full control of the

system. Root kits are also known as back doors. Some root kits give a hacker even more control of a machine than a victim may have himself. For example, the SubSeven root kit allows an attacker to turn off a victim's monitor, move the mouse, and even turn on an installed web cam and watch the victim without his or her knowledge.

E. Hybrids

Often malware is a dangerous hybrid that can combine the features of the different classifications described above [3 - 5]. Malware should not be confused with defective software, that is, software which has a legitimate *purpose* but contains errors or bugs.

F. Scanners

Scanners are tools designed to interrogate machines on the internet to elicit information about the types and versions of the services that they are running. There are a variety of scanners, some just ping for the presence of a machine, others look for open ports, while others are more specialized in looking for vulnerabilities of a particular type of service, or the presence of a root kit. Scanners are often incorporated into other malware such as worms. Scanners are a favorite tool of hackers, but are just as useful to security professionals trying to detect and close down system vulnerabilities.

G. Internet Domain Name System (*DNS*)

DNS is the distributed, hierarchical global directory that translates names (www.example.com) to numeric IP addresses (192.168.13.2). The top 2 layers of the hierarchy are critical to the operation of the Internet. In the top layer are "root" name servers. Next are the "top-level domain" (TLD) servers, which are authoritative for ".com", ".net", etc., as well as the country code top level domains (ccTLDs – ".us", ".uk", ".ru", etc…) Threats to DNS include:

Cache poisoning: If DNS is made to cache bogus information, the attacker can redirect traffic intended for a legitimate site to a site under the attacker's control. A recent survey by the CERT/CC shows that over 80% of the TLD domains are running on servers that are potentially vulnerable to this form of attack.

Compromised data: Attackers compromise vulnerable DNS servers, giving them the ability to modify the data served to users. Many of the TLD servers run a software program called BIND, in which vulnerabilities are discovered regularly. A CERT/CC survey indicates that at least 20% of TLD domains are running on vulnerable servers, another 70% are considered "status unknown".

Denial of service: A large denial-of-service attack on some of the name servers for a TLD (for example, ".com") could cause widespread Internet slowdowns or effective outages.

Domain hijacking: By leveraging insecure mechanisms used by customers to update their domain registration information, attackers can co-opt the domain registration process to take control of legitimate domains.

H. Attacks Against or Using Routers

Routers are specialized computers that direct traffic on the Internet (similar to mail routing facilities in the postal service). Threats fall into the following categories:

Routers as attack platform: Intruders use poorly secured routers as platforms for generating attack traffic at other sites, or for scanning or reconnaissance.

Denial of service: Although routers are designed to pass large amounts of traffic through them, they often are not capable of handling the same amount of traffic directed at them (one may think of it as the difference between sorting mail and reading it). Intruders take advantage of this characteristic, and attack the routers that lead into a network rather than attack the systems on the network directly.

Exploitation of trust relationship between router: For routers to do their job, they have to know where to send the traffic they receive. They do this by sharing routing information between them, which requires the routers to trust the information they receive from their peers. As a result, it would be relatively easy for an attacker to modify, delete, or inject routes into the global internet routing tables to redirect traffic destined for one network to another, effectively causing a denial of service to both (because no traffic is being routed to them or because they're getting more traffic than they should). Although the technology has been widely available for some time, many networks (Internet service providers and large corporations) do not protect themselves with the strong encryption and authentication features available on the routers.

I. Infrastructure Attacks

Denial of service: Because of the asymmetric nature of the threat, denial of service is likely to remain a high-impact, low-effort modus operandi for attackers. Most organizations' internet connections have between 1 and 155 megabits per second (Mbps) of bandwidth available. Attacks have been reported in the hundreds of Mbps and up, more than enough to saturate nearly any system on the Internet.

Compromise of sensitive information: Some viruses attach themselves to existing files on the systems they infect and then send the infected files to others. This can result in confidential information being distributed without the author's permission (Sircam is an example).

Misinformation: Intruders might be able to modify news sites, produce bogus press releases, and conduct other activities, all of which could have economic impact.

Time and resources diverted from other tasks: Perhaps the largest impact of security events is the time and resource requirements to deal with them. Computer Economics estimated that the total economic impact of Code Red was $2.6 billion, and Sircam costed another $1.3 billion (for comparison, they estimate that the 9/11 attacks will cost around $15.8 billion to restore IT and communication capabilities).

J. Phishing

The term Phishing comes from the fact that Internet scammers are using sophisticated lures as they "fish" for users' financial information and password data. It is the

process of creating a replica of an existing Web page and sending a fake email to fool a user into submitting personal, financial or a password data. It's an identity theft attack that attempts to steal sensitive information using social engineering. Phishing is a such a serious threat that it was quoted by *Jana Monroe, FBI*, July 2003: "Phishing is the hottest and most troubling, new scam on the Internet".

K. XSS Attacks

XSS stands for Cross Site Scripting; an XSS attack is when an attacker manages to inject Java script code or sometimes other code (usually Java Script) into a website causing it to execute the code. Obviously the attack could do some serious damage if an attacker made a specially crafted link and sent it to an unsuspecting victim who unknowingly clicked the link, causing a piece of Java Script code to be executed and sending the victim's cookie away to a CGI Script.

When an attacker creates a malicious link he or she will usually encode the Java Script code in HEX or some kind of encoding schemes in order to try and hide the malicious code. Websites that are vulnerable to XSS attacks are running some sort of Dynamic Content, Dynamic Content is anything that changes due to user interaction or information stored in a database about a user, things such as Forums, Web Based Email and places where information is submitted are vulnerable to XSS attacks.

Many people ask why an XSS attack cannot happen while the user is not at the domain. The reason is that when the victim is on the website, the code is executed under the same permissions as the web applications domain or IP Address.

XSS vulnerabilities have been found in all sorts of websites including fbi.gov, yahoo.com, ebay.com and many other popular and important websites. A lot of administrators fail to pay attention to XSS attacks because they either don't know much about them or they do not see them as a threat. An XSS vulnerability, when exploited by a skilled attacker or even a novice, can be a very powerful attack. The most common attack that is used with XSS vulnerability is the execution of Java Script to allow account hijacking (Cookie Theft). Using Java Script it would be also possible to cause harm to the users account such as change there account details.

III. Combined Attacks

These types of attacks are rated as the most serious and dangerous types of internet attacks [6, 7]. Trying to discover and find a cure for them might take months, while trying to preempt such attacks seem impossible.

Code Red: The Code Red worm first attacked on 18 June 2001. It exploited a buffer overflow vulnerability in the Microsoft Internet Information Server's ISAPI Index Server filter. Even though a patch for this exploit had been released by Microsoft some time before, many administrators had not updated their systems. Once infected with Code Red, a system would scan the Internet searching for unpatched IIS installations and infect them using the buffer overflow. Due to the ineffective way in which Code Red generated random IP addresses, it did not spread as rapidly as it could have done.

Code Red II: A new variant, named Code Red II, quickly emerged a month later on 19 July 2001.This had a much more complex mechanism for selecting random IP addresses and managed to infect 359,000 servers within 14 hours of its release.

Code Red III: Code Red evolved again on August 4, 2001, and its payload was more destructive. It reconfigured the web server to allow access to the entire disk drive and install trojans.

IV. Conclusion

Blended threats have existed for more than ten years and their reappearance today is of greater concern. In the past, the usage of networking and the Internet was limited to governments and university research. Today, Internet usage is main stream and is being utilized in many aspects of business. Blended threats can spread faster and further than classic virus threats and unfortunately, effective solutions are still only on the horizon.

The best line of protection still remains vigilance in applying critical patches. Host and network based vulnerability assessment tools can help to identify outdated systems with security holes inside the internal networks quicker, and thus security patches can be delivered faster. Furthermore vulnerability assessment tools can help to ensure that passwords are set up in accordance to the corporate requirements and they can identify unneeded and insecure system services that need to be uninstalled. Enterprise and personal firewall software can help fight with inbound and outbound attacks reliably [8]. Preventing technologies need to be installed on the workstations, servers and the gateways respectively.

Today and the near future will be composed of blended threats and their damage is still yet unseen. A downed mail server is now the least of our worries when threats can now effectively shutdown Internet backbones. Hopefully, the appearance of threats such as Win32/CodeRed has given security professionals a wake-up call to prepare for the future as the threat could easily have been more damaging.

References

[1] D. Hanson, "ARIS Top Ten 2005 Threats," *Security Focus*, 2005. Available http://www.securityfocus.com/corporate/research
[2] Netcraft, "Netcraft Web Server Survey," 2005. Available http://www.netcraft.com/survey
[3] L. Zeltser, E. Skoudis, W. Stratton, and H. Teall, *Malware: Fighting Malicious Code*, Prentice Hall, 2003.
[4] A. Young and M. Yung, "Cryptovirology: Extortion-Based Security Threats and Countermeasures," *IEEE Symposium on Security & Privacy*, pp. 129-141, 1996.
[5] Z. Tamimi and J. Khan, "Model-Based Analysis of Two Fighting Worms," *IEEE/IIU Proc. of ICCCE '06*, Kuala Lumpur, Malaysia, pp. 157-163, May 2006.
[6] R. Power, "CSI/FBI Computer Crime and Security Survey," *Computer Security Issues & Trends*, vol. 8, no.1, 2002.
[7] AusCERT, "Australian Computer Crime and Security Survey," 2002. Available http://www.auscert.org.au
[8] R. Zalenski, "Firewall Technologies," *IEEE Potentials*, vol. 21, no. 1, pp. 24-29, 2002.