RESEARCH ARTICLE OPEN ACCESS

Analysis of Major Security Attacks in Recent Years

Dr. C.P.Agrawal[#1], Zeenat Hasan[*2]
[#]*Professor Computer Science & Application Department MCNUJC, Bhopal, India*
[*]*Research Scholar Computer Science & Application Department MCNUJC, Bhopal ,India*
*Corresponding Author: *Dr. C.P.Agrawal*

ABSTRACT: The world is becoming digital very rapidly, weight loss programs, books, music, even classes and parties are all available online in digital form, and the technology for these applications continues to grow and innovate exponentially fast.
With this extensive growth in the online industry create an increasing number of threats in internet security. As every part of our lives becomes digital, we are more and more vulnerable to having our information stolen, our files compromised, and our privacy violated There are a lot of obvious threats to online security. Confidentiality, Integrity and Availability (CIA) are major components of security goals. In this paper, the aim is to present the survey of attacks on security goals in recent years and describe in details the nature of attacks and the behaviour of attackers through different scenarios in the network. The paper also provides a better understanding of security goals and finally it provides an analysis and classifies the attacks on the basis of security goals into different threat levels and discussed the solutions to these attacks

Keywords: Phishing Trojan Horse, DDoS, Wiretapping. Key Loggers

---

Date Of Submission: 15-01-2018 Date Of Acceptance: 03-02-2018

I. INTRODUCTION

Many banks and service providers want to encourage people to manage their accounts online and will stress convenience and speed as selling points. However, the fact remains that online fraud is increasing year-on-year with many criminals having a demonstrably greater grasp on technology than many of the institutions they are targeting. Many computer virus and phishing scams masquerade as the emails or websites of legitimate businesses and organizations. Using the logo and good name of reputable charities, non-profits, banks, government agencies and businesses, scam artists send out a variety of legitimate looking, but fake links designed in web pages while clicking on them can install malware in computer or steal private information.

II. ATTACKS ON MAJOR SECURITY GOAL

A. Network Attacks against Confidentiality

Attackers can use many methods to compromise confidentiality. Following are some of the common methods:

1) Packet Capturing (Packet Sniffing): *Packet sniffing,* a network attack strategy captures network traffic at the Ethernet frame level, after capturing the packet sensitive information can be retrieved. This attack starts with a tool such as Wireshark. With Wireshark one can capture and examine data that is flowing across the network. If data is not encrypted properly one can read this. Many types of traffic on the network are passed as unencrypted data — even passwords and other sensitive data.

***2) Password Attacks*:** Password based attacks are used to gain unauthorized access of a computer. In dictionary based attack an attacker tries each of the words in a dictionary or commonly used passwords to hack the user password and in brute force attack an attacker tries every single possible password combinations using Brute Force hacking tools to hack the user password.

***3) Port Scanning and Ping Sweeps*:** Port Scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in[2]. In Port Scanning the attacker tries to discover the services running on a target computer by scanning the TCP/UDP ports. The attacker tries to establish connection to the TCP/UDP ports to find out which ports are open on a target computer. Then he can find which service is running on a target computer. Attacker can attack and hack the target computer negotiating vulnerability in that software product.

A ping sweep is a network attack where the intruder sends ping ICMP ECHO packets to a range of IP addresses to find out which one respond with an ICMP ECHO REPLY . Thus the attacker can identify which computers are up and which computers are down.

4) Dumpster Diving: Dumpster diving is searching through company dumpsters for any information that can be useful for an attacker for attacking the network such as searching for employee names, software application product information, network infrastructure device and models etc.

5) Wiretapping: Wiretapping is a type of network attack where the attacker hacks the telecommunication devices listen to the phone calls of others.

***6) Key logger*:** A key logger is a program that runs in the background of a computer, logging the user's keystrokes. After a user enters a password, it is stored in the log created by the key logger and forwarded to the attacker.

7) Phishing and Pharming: Phishing is an attempt to hack sensitive information (usually financial information like bank user id/password credit card details etc), by sending unsolicited emails with fakes URLs. Pharming is another network attack aimed at redirecting the traffic of one website to another website[3].

8) Social Engineering: Social Engineering is type of attack in which someone with very good interactive skills manipulates others into revealing information about network that can be used to steal data.

B. Network Attacks against Integrity

***1) Salami attacks*:** Salami attacks are a series of minor data security attacks that together result in a larger attack. For example, deducting a very small amount or money from a bank account which is not noticeable. But when the deduct very small amounts from large number of accounts, it become a huge amount.

***2) Data diddling attacks*:** Data diddling is an illegal or unauthorized data alteration. Changing data before or as it is input into a computer or output. Example: Account executives can change the employee time sheet information of employees before entering to the HR payroll application.

***3) Trust relationship attacks*:** Trust relationship attacks exploit the trust between different devices in a network.

***4) Man-in-the-middle attacks*:** A man-in-the-middle attack is a type of network attack where the attacker sits between two devices that are communicating to manipulate the data as it moves between them.

***5) Session hijacking attacks*:** Session hijacking is another type of network attack where the attacker hacks a computer session to gain unauthorized access to information or services in a computer system.

C. Network Attacks against Availability

1) DoS (Denial of Service attacks): DOS Attack is a type of attack to a network server with large number or service requests with it cannot handle. DoS (Denial of Service Attack) can causes the server to crash the server and legitimate users are denied the service.

2) Distributed Denial of Service attacks: Distributed Denial of Service attack (DDoS) is a type of DoS attack, originating from many attacking computers from different geographical regions.

III. RECENT ATTACKS

1) The websites of India's embassies on November 6, 2016 were hacked and some data pertaining to Indian citizens leaked online by the attackers. Indian embassies in South Africa, Malawi, Switzerland, Libya, Mali, Romania and Italy apparently were breached, Personal data on Indian citizens living abroad that was breached included names, home addresses, email, passport numbers and phone numbers [4].

There is an ad hoc system in place to run these websites and the domain names are often owned by the contractor. Because of shared hosting, spoofing the domains and email addresses is cause of this breach.

2) On 7 November 2016 Tesco Bank in UK freezes transactions after cash taken from 20,000 accounts which had been affected by an online fraudster. It was one of the largest cyber-thefts ever to hit a UK bank Thousands of Tesco Bank accounts have been compromised and customers have seen hundreds of pounds wiped from their balances in a wave of fraudulent activity. Account holders reported seeing as much as £600 siphoned from their accounts in a breach. One possible cause under consideration is a compromise at a third party retailer, the bank said. Another is a hack. One customer said that cash had been withdrawn from his account in four separate transactions, all coming from Rio de Janeiro in Brazil [5]. Phishing emails and texts was the cause of this attack.

3) One of the biggest security breaches in the history of India's banks was uncovered on October 2016 placing millions of debit card users at risk. Customers of India's biggest lenders, including the State Bank of India (SBI), HDFC Bank, ICICI Bank, and Yes Bank, were affected, with an estimated Rs1.3 crore already whisked off by hackers. Several victims have reported unauthorized usage from locations in China. Initially, malware—malicious software that targets computer systems—was detected in some ATM

machine systems belonging to Yes Bank, India's fifth-largest private sector bank. These ATMs are operated by Japanese firm Hitachi Payment Services.

The malware presumably allowed hackers to extract money from bank accounts via debit cards, but the exact number of accounts affected is unclear. Media reports suggest it may be around 3.2 million debit cards. The Maharashtra Police, on the other hand, said on Oct. 21 that it could be as high as 6.5 million[6].

4) Internet Service Providers (ISPs) in Mumbai have faced an unprecedented attack by hackers which has reduced surfing speeds in the city on July 24, 2016. The Distributed Denial of Service (DDOS) attack on ISPs was being carried out in an "unprecedented" manner. A DDOS attack involves an attempt by hackers to prevent legitimate users of a service from using that service by either flooding or crashing it[7].

5) On the morning of 26th June 2016 news of a phishing campaign hit the Israeli media. Thousands of Face-book users complained that they had been infected by a virus through their accounts after they received a message from a Face-book friend claiming they had mentioned them in a comment .The message had in fact been initiated by attackers and unleashed a two-stage attack on recipients. The attack was not confined to Israel, but was hitting targets worldwide.

The first stage of the attack started when the user clicked on the "mention". A malicious file seized control of their browsers, terminating their legitimate browser session and replacing it with a malicious one that included a tab to the legitimate Face-book login page. This was designed to lure the victim back into the social network site.

Upon logging back into Face-book the victim's session was hijacked in the background and a new file was downloaded. This represented the second stage of the attack, as embedded in this file was an account-takeover script that included a privacy-settings changer, account-data extractor and other tools that could be used for further malicious activity, such as spam, identity theft and generating fraudulent 'likes' and 'shares'. Further, the malware infection loop began again as malicious notifications were sent to all the victim's Face-book friends[8].

6) On 21 January 2016 Irish lottery site and ticket machines hit by DDoS attack Ireland's National Lottery website and ticket machines were knocked offline after a distributed denial of service (DDoS) attack on Wednesday. Customers trying to buy tickets for the €12m (£9m) draw found themselves unable to do so for nearly two hours. Given the large jackpot involved, the lottery was experiencing high demand for tickets on that day[9].

7) On February 4, 2015, Anthem, Inc. disclosed that criminal hackers had broken into its servers and potentially stolen over 37.5 million records that contain personally identifiable information from its servers. The information stolen from the insurance giant includes names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data. Health insurer Anthem Inc. believes that the attack that compromised up to 80 million individuals' personally identifiable information may have begun with phishing e-mails sent to a handful of its employees. This is just one of several options being investigated as the cause of the breach [10].

8) On 8 and 9 July 2014, an alliance of law enforcement and industry undertook measures against the Internet domains and servers that form the core of an advanced cybercriminal infrastructure attacking online banking systems around the globe using the Shylock Trojan.

Law enforcement agencies took action to disrupt the system which Shylock depends on to operate effectively. This comprised the seizure of servers which form the command and control system for the Trojan, as well as taking control of the domains Shylock uses for communication between infected computers.

The operation, coordinated by the UK National Crime Agency (NCA), brought together partners from the law enforcement and private sectors, including Europol, the FBI, BAE Systems Applied Intelligence, Dell SecureWorks, Kaspersky Lab and the UK's GCHQ (Government Communications Headquarters) to jointly combat the threat[n1]. Shylock – so-called because its code contains excerpts from Shakespeare's The Merchant of Venice - has infected at least 30 000 computers running Microsoft Windows worldwide. Intelligence suggests that Shylock targets the UK more than any other country, nevertheless the US, Italy and Turkey are also being targeted hard by the malicious code. It is thought that the suspected developers are based elsewhere.

Victims are typically infected by clicking on malicious links, and then persuaded to download and run the malware. Shylock will then seek to access funds held in business or personal bank accounts, and transfer them to the criminal controllers [11].

9) In February 2014 Security researchers at Bromium have discovered that hackers were spreading malware onto computers while unsuspecting users were watching YouTube videos. The drive-by-download attack was distributed via adverts shown on the YouTube website, and used an exploit kit to infect Windows PCs with a version of the Caphaw banking Trojan [12].

10) On August 2013 one Sunday morning, part of the Chinese Internet went down in what the government is calling the largest denial-of-service attack it has ever faced. According to the China Internet Network Information Centre, the attack began at 2 a.m. Sunday morning and was followed by an even more intense attack at 4 a.m. The attack was aimed at the registry that allows users to access sites with the extension ".cn,". As originally reported by the Wall Street Journal, the attack is perhaps more an indicator of just how susceptible the global Internet infrastructure is to these types of attacks.[13]
Table I give summary of all the attack described above.

Table I

Victim	Date	Attack type
The websites of seven of India's embassies	6 November 2016	E-Mail and Domain Name Spoofing
Tesco Bank in UK	7 November 2016	Phishing
Debit card users of State Bank of India (SBI), HDFC Bank, ICICI Bank, and Yes Bank	October 2016	Malware
Thousands of Face-book users of Israeli	26th June 2016	Phishing
Irish lottery site and ticket machines	21 January 2016	DDoS attack
Health Insurer Anthem, Inc.	February 4, 2015	Phishing
Computers running Microsoft Windows worldwide	July 2014	Shylock Trojan
You Tube users at Bromium	February 2014	Trojan Horses
Part of the Chinese Internet	August 2013	DDoS attack

IV. SOLUTION TO THESE ATTACKS

Phishing, Distributed denial-of-service (DDoS), Trojan Horses attacks are real and growing threats to businesses worldwide. Designed to elude detection by today's most popular tools, these attacks can quickly incapacitate a targeted business, costing victims thousands, if not millions, of dollars in lost revenue and productivity. By adopting new purpose-built solutions designed specifically to detect and defeat these attacks, businesses can keep their business operations running smoothly.

1) Solution against phishing

Phishing scams are usually presented in the form of spam or pop-ups and are often difficult to detect. Once the fraudsters obtain your personal information, they can use it for all types of identity theft, putting your good credit and good name at risk. There is some tip to prevent phishing attacks:

- Educate your employees and conduct training sessions with mock phishing scenarios.
- Deploy a SPAM filter that detects viruses, blank senders, etc.
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Develop a security policy that includes but isn't limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Do not click on links, download files or open attachments in emails from unknown senders.
- Never enter personal information in a pop-up screen.

2) Defeating DDOS Attacks

DDoS attacks are weapons of mass disruption. Unlike access attacks that penetrate security perimeters to steal information, DDoS attacks paralyse Internet systems by overwhelming servers, network links, and network devices (routers, firewalls, etc.) with bogus traffic. here are some technique to prevent DDoS attacks:

1) Disabling unused services -The less there are applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not needed or unused, the services should be disabled to prevent attacks, e.g. UDP echo, character generation services [14].

2) Install latest security patches -Today, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system [15].

3) Disabling IP broadcast Defence against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. will be successful

only if host computers and all the neighbouring networks disable IP broadcast.

4) Firewalls -Firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Firewalls help preventing unauthorized network traffic through an unsecured network to a private network. They can notify the user when an untrusted application is requested access to the internet [16]. Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. But some complex attack e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DoS attack traffic.

5) IP hopping- DDoS attacks can be prevented by changing location or IP address of the active server proactively within a pool of homogeneous servers or with a pre-specified set of IP address ranges. The victim computer's IP address is invalidated by changing it with a new one. Once the IP addresses change is completed all internet routers will be informed and edge routers will drop the attacking packets. Although this action leaves the computer vulnerable because the attacker can launch the attack at the new IP address, this option is practical for DDoS attacks that are based on IP addresses.

4) Solution to Trojan Horses

The term Trojan horse is applied to malware that masquerades as a legitimate program but is in reality a malicious application. It may simply pretend to be a useful program or it may actually contain a useful function as a cover for a destructive program at the core. Screen savers are often used as a carrier. Trojan horses do not replicate themselves as do viruses and worms. However, a Trojan horse can be part of the payload of a worm and can be spread to many machines as part of a worm infestation. Many Trojan horse are sent out as email attachments. There are following methods for dealing with Trojans:

1) Anti –Virus Programs -Most Trojans are recognized by the major anti-virus programs. However, not all Trojans have characteristics that anti-virus programs do understand so additional software like spyware-removers is recommended. The spyware programs should be considered as well.

2) Firewall-It is essential in the present conditions to have a firewall. The Internet is a two-way street. Unless the computer is properly protected, it is too easy for unwanted visitors or programs to gain access to someone's computer. A cracker can plant a Trojan or worm or do other harm. Good firewall software can make the computer invisible to all except the most determined cracker - the person who has got only one aim - to destroy the computer. Also most firewalls will warn the person if programs on his computer try to connect to the Internet without telling him.

V. CONCLUSION

Internet attacks have been increased dramatically over time, especially in the past few years. This paper discussed some recent attacks and their causes in various places. So many attack like Phishing, DDos ,Trojan Horses are increasing worldwide and targeting Individuals, businesses and Governments for malicious purpose they are gaining unauthorized access to someone's computer without knowledge of him. This paper outlines some technique to prevent these attacks but developing new internet attack detection schemes is necessary because internet attackers develop their strategies continuously too. Information fusion from multiple sources required intelligence techniques to characteristic the internet attackers .To increase the quality of security it is important to adopt technical solutions that proactively address adversaries and establish real-time monitoring systems to detect protect and prepare from these attacks and educate the user about safer access to the internet.

REFERENCES

[1]. (2016) Edwerd tetz [Online].Available:http://www.dummies.com/programming/networking/cisco/common-network-attack-strategies-packet-sniffing/.
[2]. EC Council, *Ethical Hacking and Countermeasures: Attack Phases*, 2nd ed., Cengage Learning New Mexico, 2010.
[3]. (2016) Network tutorial website[Online].Available http://www.omnisecu.com/ccna-security/types-of-network-attacks.php
[4]. (2016) Data Breach Today website. [Online]. Available: http://www.databreachtoday.in/7-indian-embassy-websites-apparently-breached-a-9502The Hacker News reports. http://thehackernews.com/2016/11/indian-embassy-hacked.html
[5]. Robert Booth(2016)[Online]. Available: https://www.theguardian.com/money/2016/nov/06/tesco-bank-blocks-some-customers-cards-suspicious-activity-detected
[6]. (2016) [Online]. Available: http://qz.com/816946/sbi-icici-bank-hdfc-bank-and-yes-bank-may-not-admit-it-but-

they-have-much-to-answer-for-the-great-indian-debit-card-hacking.
[7]. (2016) [Online]. Available http://indianexpress.com/article/cities/mumbai/hackers-target-internet-service-providers-in-mumbai-2932118
[8]. IdoNaor (2016) [Online]. Available: https://securelist.com/blog/incidents/75237/facebook-malware-tag-me-if-you-can/Facebook malware: tag me if you can
[9]. (2016) The BBC news website [Online]. Available: http://www.bbc.com/news/technology-35373890.
[10]. Riley,Charles(2015) [Online]. Available: http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/
[11]. (2014) The Europol website [Online]. Available: https://www.europol.europa.eu/newsroom/news/global-action-targeting-shylock-malware
[12]. (2014) https://www.grahamcluley.com/youtube-malware/
[13]. (2013) The wall Street Journal [Online]. Available http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend/
[14]. X. Geng, A.B. Whinston, Defeating Distributed Denial of Service attacks, IEEE IT Professional 2 (4) , 36–42,2000.
[15]. Neha Gupta, Rajet Veshin, Rajneesh Sharma," Distributed Denial of Service (DDOS) Attacks in Cloud Computing: A Survey", International Journal of Enhanced Research in Management & Computer Applications,, Vol. 4 pp. 22-28, Dec.2015
[16]. Kartikey Agarwal, Dr. Sanjay Kumar Dubey, "Network Security : Attacks and Defence", International Journal of Advance Foundation and Research in Science & Engineering,Vol. 1, Aug. 2014.

*Dr. C.P.Agrawal. "Analysis of Major Security Attacks in Recent Years." International Journal Of Engineering Research And Applications (IJERA), vol. 08, no. 01, 2018, pp. 25–30.