Survey on Cyber Attacks

Roshni Bhandari
Assistant Professor
Computer Department
S. S Agrawal Institute of Engineering & Technology
Navsari

Rathod Swapnil
Student
Computer Department
S.S Agrawal Institute of Engineering & Technology
Navsari

Tailor Vishwa
Student
Computer Department
S.S Agrawal Institute of Engineering & Technology
Navsari

Patel Jaydip
Student
Computer Department
S.S Agrawal Institute of Engineering & Technology
Navsari

Davara Sagar
Student
Computer Department
S.S Agrawal Institute of Engineering & Technology
Navsari

ABSTRACT
It is not possible to make your business wider without using communication. Communication plays an important role in business. Nowadays computer system having internet makes it easy for communication at any level. There are advantages and disadvantages of any object. E-Communication may have different disadvantages. I.e. theft of data, personal information leaking, etc. The present study is an attempt to reveal the varied cyber-attack techniques adopted by cyber criminals to target the selected banks in India where spoofing, brute force attack are found positively correlated with public and private sector banks. Further, the research shows a positive correlation between Intruder Detection and cyber-attacks, i.e., online identity theft, hacking, malicious code, DOS attack and credit card/ATM frauds as well as online identity theft, DOS attack & credit card/ATM fraud are found positively correlated with System Monitoring.

General Terms
Victim, Anomalies , System monitoring, Hacker.

Keywords
Identity Theft, Intruder Detection, Spyware.

1. INTRODUCTION
A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-criminals 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 identify theft.
Their objectives include [1]:

- Gaining or attempting to gain.
- Unauthorized access to a computer system or its data.
- Unwanted interruption or denial of service attacks including the take down of entire web sites.
- Installation of viruses or malware – that is malicious code on a computer system.
- Changes to the characteristics of a computer system, hardware firmware or software without the owner's permission, instruction or consent.
- Unauthorized use of a computer system for processing or storing data.
- Inappropriate use of computer system by employees or former employees.

Table 1. Table of History of Cyber Crime

Year	History records
1988-*1989*	1989 saw the creation of the first computer worm, which was crafted by Robert Morris to test the size of the internet. Unfortunately, the manipulating virus spread aggressively, essentially terminating the internet. The impact of the initial worm was not on the same level of devastation that could be created by harmful malware today. However, it was the first of many to come and shaped how viruses were managed for decades. Furthermore, this meant businesses had to invest in the first defensive security products, such as firewalls. It was cyber security's first step to counter the threats. [2]
1990-1999	Melissa and ILOVEYOU were both fast-spreading macro viruses which were distributed as an e-mail attachment. When the attachment was opened, it disabled a number of safeguards in Word 97 or Word 2000.This was the first issue of cyber-vandalism on a massive scale. [2]
2005	2005-2007 saw cyber-attacks become bigger with end-goals relating to financial benefits. Hacker Albert Gonzalez conducted an operation that stole information from nearly 50 million cards used by customers of US retailer TJX, costing the company $256m. Businesses realized hackers could deceive their existing security tools and operate within their networks for years. [2]
2006	NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest US space launch vehicles were obtained by unknown

	foreign intruders. [3]
April 2007	Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted. The attacks were more like cyber riots than crippling attacks, and the Estonians responded well, launching some services within hours or - at most - days. [3]
June 2007	The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks. [3]
October -2007	China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas. In 2006, when the China Aerospace Science & Industry Corporation (CASIC) intranet network was surveyed, spywares were found in the computers of classified departments and corporate leaders. [3]
August 2008	Computer networks in Georgia were hacked by unknown foreign intruders around the time that the country was in conflict with Russia. Graffiti appeared on Georgian government websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and appeared to be coordinated with Russian military actions. [3]
January 2009	Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization based in a former Soviet state, and paid for by Hamas or Hezbollah. [3]
January 2010	A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. The same "Iranian Cyber Army" had hacked into Twitter the previous December, with a similar message. [3]
October 2010	Subnet, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programmer. [3]
January 2011	The Canadian government reported a major cyber-attack against its agencies, including Defiance Research and Development Canada, a research agency for Canada's Department of National Defiance. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet. [3]
2014	During 2014, there were massive recent data breaches of Target and Sony. Target booked $162 million in expenses throughout 2013 and 2014 related to the **data breach**, in which hackers broke into the company's network to access credit card information and other customer data, affecting some 70 million customers. Moreover, Sony's data breach was inflicted by North Korea, which shows that you don't have to be part of a criminal organization to cause this damage. [2]
2017	This year saw the outbreak of the "biggest ransom ware outbreak". The attack saw the likes of the NHS and FedEx dismantled. Spanish telecommunications company Telephonic was among many targets in the country along with German railway operator Deutsche Bahn. [2]

2. TYPES OF CYBER ATTACK

2.1 Malware Attack

Malware is known as any computer code created for causing malice. Although one may not have known the technical definition of malware, chances are the user has fallen victim of some type of malware. Malware is capable of infecting computer systems slowing or shutting them down and steal valuable information. Malware continues to grow limitlessly along with cyber-attacks and is a popular tool in cyber-attacks. Another problem with malware is the contagious abilities of it. Malware is able to quickly spread across the web since due to its ability to be a small file with capabilities of infecting whole file systems. Malware can cause more harm the longer it exists in the home user's system. For this reason, it is important to protect against, detect, and eliminate malware from home user's computers.

Types of Malware [5]

2.1.1 Spyware

Spyware is the most common form of malware for stealing valuable information. Spyware simply does as the name implies and spies on any information home users enter in the computer or browser through various methods.

2.1.2. Viruses

Computer viruses are similar to biological viruses in terms of survival. Biological viruses need to feed off of a host through the host's cells to live. On the other hand, computer virus, files in the computers system are essentially to the "cell" inside of the computer host. Depending on the severity of the virus, infection can spread to system files effectively slowing or even damaging the computer entirely.

2.1.3 Worms

Worms, although much less common can be more of a threat due to their ability to live on their own. Worms work similar to ways a virus works except worms do not need a host to

live. This is dangerous because without the necessity of a host, infection can spread much quicker. Worms can also be harder to detect due to the fact that no host is needed.

Restriction [6]

- Movie & picture download by the safe website.
- Install the antivirus.
- Install the firewall.

- Give the password to our important files.

2.2 DDOS Attacks [5]

A Distributed Denial of Service attack uses internet traffic to overwhelm servers forcing a shut-down of the system or a slowing of services. This increased traffic denies access and limits usability to legitimate users or systems. Not only is the number of DDOS attacks increasing, but so too is the complexity.

Restricting [7]

The best way to Restriction an additional breach is to keep your system as secure as possible with regular software updates, online security monitoring and monitoring your data flow to identify any unusual or increasing threats in traffic before they become a problem.

2.3 Malvertising [7]

A way to compromise your computer with malicious code that is downloaded to your system when you click on an affected ad. Cyber attacker upload display ad to different sites using an ad network. These ads are then distributed to sites that match certain keywords and search criteria. Once a user clicks on one of these ads, some types of Malware will be downloaded.

Restriction

The best way to Restriction falling victim to advertising is to use common sense. Any ad that promises riches, free computers or cruises to the Bahamas is probably too good to be true, and therefore could be hiding Malware.

2.4 Man in the Middle (MITM) Attacks [9]

In this type of attacks hacker break down original connection between server and client and make a duplicate connection among them. From this connection hacker can get details and data from both sides, from client or server and can monitoring the transaction between client and server.

Restriction [7]

The best way to Restriction them is to only use encrypted wireless access points that use WPA security or greater. If you need to connect to a website, make sure it uses an HTTPS connection or, for better security, consider investing in a virtual private network (VPN).

2.5 Rogue Software [7]

Malware that masquerades as legitimate and necessary security software that will keep your system safe. Rogue security software designers make pop-up windows and alerts that look legitimate. These alerts advise the user to download security software, agree to terms or update their current system in an effort to stay protected.

Restriction

The best defense is to keep an updated firewall. Make sure that you have a working one in your office that protect you and your employee from these types of attacks.

2.6 Cross Site Scripting (XSS) Attack [10]

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database when the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script.

Restricting [8]

To reduce the chances of your site becoming a victim of an XSS attack, it's essential that any Web application is developed using some form of security development lifecycle (SDL). Their aim is to reduce the number of security-related design and coding errors in an application, and reduce the severity of any errors that remain undetected. This applies to any data received by the application data, cookies, emails, files or images even if the data is from users who have logged into their account and authenticated themselves.

2.7 Password Attacks [4]

As computer users, passwords serve as essentially keys to all our private information. When the password is lost, it must be retest quickly to Restriction the risk of theft. For such reasons, it is important to understand how hackers can essentially steal passwords from unsuspecting victims. Some methods of password attacks include: password guessing, password resetting, and password capturing. Password guessing is predicting possible password combinations until the right combination is found. Although this method may seem to take unreasonable lengths of time to accomplish, software's can shorten the process. Since many people still use common passwords such as their birthdays or names for passwords; the process is much shorter than many may think. Another threat is reusing passwords, essentially allowing hackers to access multiple accounts using that one password. Password resetting is not a very common method of password attacks. It requires the hacker to get access in to the file system of the operating system before anything can be done. However, once inside, hackers can modify and crack system files which contain the user's password. Finally, password capturing uses malware which allows hackers to unsuspectingly track all of user's keystrokes. This effectively allows hackers to get the user's passwords right away.

Restriction [7]

Strong password is the only way to safeguard against password attacks. This means using a combination of upper and lower-case letters, symbols and number and having at least eight characters or more.

2.8 Phishing [9]

It is a request which sent via emails or other messages to victim and ask the victim to click on the link and enter required data.

Restriction [8]

Communicate personal information only via phone or secure web sites. In fact: Do not click on links, download files or open attachments in emails from unknown senders.

3. CYBER SECURITY TOOLS

3.1 Nmap [12]

Map your network and ports with the number one port scanning tool. Nmap now features powerful NSE scripts that can detect vulnerabilities, misconfiguration and security related information around network services. After you have nmap installed be sure to look at the features of the included ncat - its net cat on steroids.

3.2 Wireshark[12]

View traffic in as much detail as you want. Use Wireshark to follow network streams and find problems. Tcpdump and Tshark are command line alternatives. Wireshark runs on Windows, Linux, FreeBSD or OSX based systems.

3.3 Nessus [13]

Nessus allows scans for the following types of vulnerabilities:

- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of service against the TCP/IP stack by using mangled packets.

3.4 Snort [12]

Snort is a real time traffic analysis and packet logging tool. It can be thought of as a traditional IDS, with detection performed by matching signatures. The project is now managed by Cisco who use the technology in its range of Source Fire appliances. An alternative project is the Suricata system that is a fork of the original Snort source.

3.5 Safe Browsing [4]

One should be weary of using websites that have no security measures in place for personal information. Most websites will show links to the security certificate if information is encrypted. Home users can simply check for such certificates to assist in deciding whether the organization can be trusted with information.

Here are some tips:

- Disable the use of remembering passwords for sites in all browsers.
- Disable the use of remembering what entered in form in all browsers.
- Make sure browser setting is set to clear data when browser is closed.
- Block pop-ups for all the browsers.
- Set the internet zone security level.
- Do not open unknown e-mail attachments or respond to unknown e-mails.
- Password protects all devices that are connected to the internet.
- Do not respond to online requests for asking personal identifiable information.

3.6 Os Query[12]

Monitors a host for changes and is built to be performing from the ground up. This project is cross platform and was started by the Facebook Security Team. It is a powerful agent that can be run on all your systems (Windows, Linux or OSX) providing detailed visibility into anomalies and security related events.

4. CONCLUSION

Though not all people are victims to cybercrimes, they are still at risk. Crimes by computer vary, and they don't always occur behind the computer, but they are executed by computer. Generally, hacker's identity is ranged between 12 years to 67years. The hacker could live three continents away from its victim, and they wouldn't even know they were being hacked. Crimes done behind the computer are the 21st century's problem. With the technology increasing, criminals neither have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their Device. Their weapons aren't guns anymore; they attack with keyboard, cursors and passwords.

5. REFERENCES

[1] Farhat, Vince, McCarthy, Bridget & Raysman, Richard (Holland & Knight LLP), History of cyber attacks, Published by Practical Law Company on its PLC Intellectual Property and Technology web services.

[2] Energi Group, Fresh01, 2001, History of cyber attacks.

[3] Essay.ws/ History of cyber crime.

[4] Hayder Teymourlouei, 2015, awareness and Restrictionions for home user, World Academy of Science Engineering & Technology.

[5] Coburn, Aw Daffron J, Smith A, Bordeau J, Leverret E, Sweeney S, Harvey T, 2018, Cyber Risk Lookout, University of Cambridge.

[6] Joshua, Indentitytheftkiller, 2018, phishing scam

[7] Jeff Melnick, Netwrix, 2018, 10 most common cyber attacks.

[8] Megan Sullivan, Quickbooks, 2018, types of cyber attacks.

[9] Amarujala Hindi Newspaper , Malware Attack

[10] Neil Dupaul, Veracode, 2012, Common Malware Types.

[11] Checkpoint, 2018, Security Reports.

[12] Waste/awareness and Restrictionion.

[13] Abdullah Saad H. Alqahtani, Mohsin Iftikhar, Semanticsscholar, 2013, Restrictionion Tools