International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229511

Cyber Attacks : Detection and Prevention

Jigar Vakil[1], **Dr. Priya Swaminarayan**[2]
[1]Research Scholar, Parul Institute of Engineering and Technology - MCA, Parul University, Gujarat, India
[2]Director-MCA, Dean-FITCS, Parul Institute of Engineering and Technology - MCA, Parul University, Gujarat, India

Article Info
Volume 9, Issue 5
Page Number : 82-93

Publication Issue :
September-October-2022

Article History
Accepted :09 Sep 2022
Published: 22 Sep 2022

ABSTRACT

Tens of millions of cyber-attacks (Emails, online transactions, live video streaming, online games, and navigation are all examples of fraudulent Internet-based intelligence gathering.) are launched every day against Internet users throughout the world. Various defences have been developed by researchers in response to these attacks. At present, the techniques that cyber attackers use to perpetrate attacks are related to human exploitation. These attacks are more frequent than before, and they are harder to contain. In the area of information management, cybersecurity is essential. In today's world, protecting privacy has been one of the most difficult tasks. "Cyber-crimes" is the first thing that has come to me when I think about cyber security, which are on the rise at an alarming rate. Various governments and corporations are taking various actions to tackle cybercrime. Despite different initiatives, cyber security remains a major issue for many people. Traditional non-confidence counter-measures are unable to prevent violations against individuals. This paper explains the current state of cybersecurity threats, counter-measures and non-confidence tools that are relevant to day-to-day online operations. It offers a valuable cyber-attack taxonomy and classification that aids in the identification of cyber-attacks and cyber-security initiatives.

Keywords : Cyberattacks, Cybercrime, cyberattacks detection, Cyberattack Prevention, Malware, SQL injection, Phishing, Man in the middle attack (MiM), ObURL detection algorithm.

I. INTRODUCTION

Any effort to obtain unauthorized access to a device, operating system, or computer network with the intent to inflict harm is considered a cyber-attack. Cyber-attacks attempt to disable, interrupt, kill, or take control of computer networks, as well as to alter, block, erase, exploit, or steal data stored on them. Any person or group may initiate a cyber-attack from anywhere using one or more different attack strategies. Cybercriminals are people who carry out cyber-attacks. Bad actors, threat actors, and hackers are individuals who work independently and rely on their programming abilities to design and execute malware attacks. They may also be members of a crime gang that collaborates with other threat actors to discover flaws or bugs in computer networks, known as bugs that can be abused for financial gain.

1.1 Reasons for Cyber Attacks

Cyber-attacks are intended to harm people and damage their information. They can have various objectives, including the following:

1.1.1 Financial gain:

The majority of cyber-attacks today, including those targeting commercial institutions, are carried out by cybercriminals for monetary benefit. They also aim to steal confidential information, such as consumer credit card numbers or personal employee information., which cyber criminals then use to access money or items under the victims' names

1.1.2 Disruption and revenge:

The majority of cyber-attacks today, including those targeting commercial institutions, are carried out by cybercriminals for monetary benefit. They also aim to steal confidential information, such as consumer credit card numbers or personal employee information., which cyber criminals then use to access money or items under the victims' names

1.1.3 Cyberwarfare:

Governments all over the world are engaged in cyber-attacks, with many admitting to or suspecting to planning and launching attacks against other countries as part of ongoing political, economic, and social conflicts. Cyber warfare is the term that describes these kinds of attacks.

1.2Working on cyber attack

Depending on whether they're pursuing a targeted or untargeted goal, threat actors employ a range of strategies to carry out cyber-attacks. When bad actors want to hack into as many computers or networks as possible in an untargeted attack, they search for bugs that will allow them to gain entry without being detected or blocked. They could use a phishing attack, for example, sending emails to a large number of people with socially programmed messages designed to persuade recipients to click a connection that will download malicious code. Threat actors threaten a single organization in a coordinated attack, and the tactics used differ based on the attack's goals. In a coordinated attack, hackers craft emails to particular individuals who, if they select included links, download malicious software intended to subvert the organization's infrastructure or the sensitive data it contains.

1.3 Types of Cyber Attacks:

Cyber-attacks most commonly and dangerous involve the following:

1.3.1 Malware:

Malware is a sort of technology (framework, algorithms, integrated data, as well as other programs) that is designed to disrupt or dismiss actions, collect data that can lead to privacy or misuse, obtain unauthorized access to device resources, and engage in other abusive behavior. The word is a catch-all phrase used by programming professionals to describe a wide range of offensive, disruptive, or irritating software or programmed code.

1.3.2 Phishing:

Phishing is the practice of delivering malicious emails that tend to come from a trusted source, usually through email and text messages. Phishing is such social manipulation technology that involves obtaining private data from individuals, such as user credentials and banking details. When an attacker poses as a trustworthy person to trick a victim into clicking a suspicious connection, the victim's computer may be infected with malware.

1.3.3 Man-in-the-middle attack:

A cyberattack that uses a man-in-the-middle technique, in which an unauthorized third party approaches an online conversation between two users and stays unnoticed by the two parties. Individual/classified data that was only found by the two users are often tracked and updated by the malware at the heart of the attack. An outsider within the machine is exposed to a man-in-the-middle assault, which allows the outsider to enter, read, and alter sensitive knowledge without leaving any traces of coercion.

1.3.4 Denial-of-service attack:

A denial of service (DoS) assault is a sort of internet that attacks a networked model and prevents a server from providing services to its customers (DOS). Sending millions of requests to a server to slow it down, overwhelming a server with massive packets of invalid data, and sending requests with an invalid or spoofed IP address are all examples of attacks.

1.3.5 SQL injection:

SQL injection is the greatest threat to web-based systems. The attackers will use SQL queries to trick the server into permitting them to enter the database. This occurs because the developers aren't completely aware of SQL Injection attacks and their origins. SQL Injection is perhaps a methodology for modifying the database besides a piece of software. It's calculated by transferring Database queries as just an input pattern to gain access to the system access permission.

1.3.6 Ping of death attack:

A refusal assault known as PoD (Ping of Death) is a type of dos and ddos attack. in which an attacker uses a basic ping command to transmit malformed or oversized packets to crash, since sending a ping packet greater than 65,535 bytes is a violation of the Internet Protocol, attackers will send malformed packets in chunks. Memory overload can occur as the target device tries to reassemble the fragments and ends up with an oversized packet, which can cause a variety of issues including a crash.

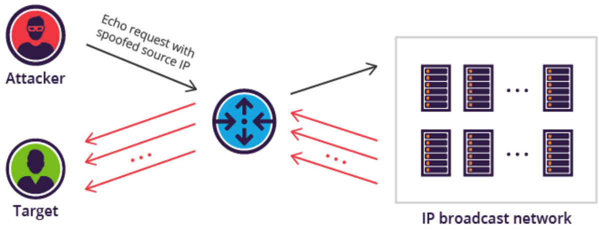

Figure 1. Ping of death attack

II. APPLOCATION AREAS

Cyber-security has a number of advantages, including

1.1Backup and Data Recovery

All of your data is backed up. Are you sure you're safe? Perhaps, however, consider where the backed-up data resides. Maintaining backups is only part of the battle. A hybrid server-based backup model is recommended, in which backups are stored locally and in the cloud. When you have three sets of data manufacturing, central, and off-site, hybrid cloud backups have greater security.

1.2Physical Access Controls

Controlling access to the campus, house, and data-sensitive areas is a top security priority. It's critical that only authorized individuals have actual quicker access. Picture ID cards, least-privilege approvals for badge entry, surveillance cameras, and a protocol that includes visitor check-in are also examples of physical access restrictions that your company should consider enforcing.

1.3Logical Access Controls

Limiting access to full-time staff isn't enough. It's also critical to ensure that even those who require communication network and data access have access. A robust protection strategy should include controls such as least-privilege permissions for end-user network access, annual checks of access permissions, and the automatic revocation of access due to position transition or termination.

1.4Email and Online Protection

A phishing email is used in at least 91 percent of hacking attempts! With this in mind, it's critical to have military-grade email filters in place that can detect and block spoofing emails from outside your jurisdiction. For browsing the web, just use Brave, Mozilla or Google Chrome - sorry, Internet Explorer. Furthermore, using a service like Cisco's Umbrella would block links to established malware pages, because that if one of your customers clicks on a potentially malicious post, the domain will be blocked.

1.5Vulnerability Assessments and Security Training

When we get caught up in the implementation of operations, we can be lulled into a false sense of faith. A third-party vulnerability evaluation and compliance test can reveal security flaws that need to be addressed. The annual security training session that is a one-and-done, check-the-box exercise is no longer sufficient. End-user training, like executive training, is an integral aspect of overall security wellbeing.

III. METHODOLOGIES

1.4Malware Detection:

Malware is malware that is intended to infiltrate a computer or mobile device to damage the machine and compromise the stability, reliability, and privacy of the user. The use of machine learning to identify malicious files has expanded the use of malware detection systems that use data mining techniques. Often, malware creators do not write new code without first preparing it, but rather rewrite existing code with new elements or muddled tactics. Detection of malware there are many algorithms.

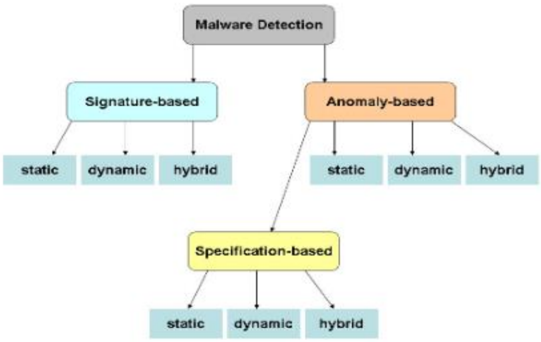

Figure 2. Malware detection algorithms

1.4.1 Signature Based Malware Detection:

Signature-based security tries to predict malware's malicious behavior and uses the model to detect malware. The collection of both of these models represents the experience of signature-based recognition. The term "signature" refers to an approach of harmful behavior. In concept, a signature ought to be able to discern any malware which illustrates the intrusion attempts specified in the verification. Signatures, like all other large-scale data that needs storage, need an archive. It keeps detects malware by matching patterns to the database. The antivirus programmed provider regularly updates and refreshes a library of known code signatures so that this strategy can reliably identify known instances of malware.

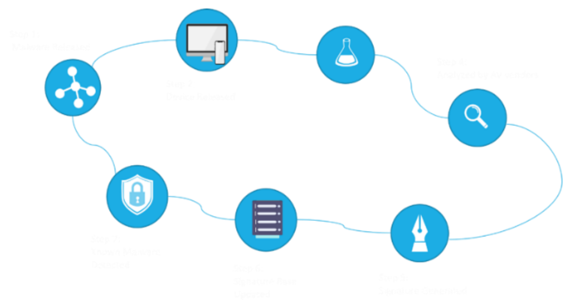

Figure 3. The flow of signature-based malware detection.

1.4.2 Behavior-Based Malware Detection:

Behavior-based malware identification assesses an entity based on the operation it intends to perform. The behavior of an object, or its possible behavior, is examined for irregular activity. Attempts to execute irregular or illegal acts would mean that the target is malicious, or at the very least questionable. A broad set of possibilities suggests the probability of danger. Such examples include attempting to detect a sandbox setting, deactivating security checks, installing rootkits, and auto-start registration. The examination of malevolent activity as it occurs is referred to as dynamic characterization. Static analysis that searches for hazardous functionality in the code and layout of the object may also determine threat risk or malicious intent. While no solution is absolutely stupid, behavioral detection always leads technologies to identify new and unexpected threats in almost real-time today. Such examples of the success of conduct-based systems if signature-based systems fail are:

- Defending against heretofore unimagined malware threats.
- Detecting a single case of malware that has been aimed at a specific person or organization.
- Identifying what the virus does when files are accessed in a certain environment.
- Gaining extensive data on the malware.

1.5Phishing Detection:

Phishing is a persistent trouble, as well as the loss is much larger on social networking sites like Instagram, Reddit, Twitter, and Google. Hackers will develop a website imitation and encourage you to enter your personal information, something you will then send to them by e-mail. Hackers also use these websites to target people who use them at work, at home, or in public to collect information on personal safety and protection that can influence their users or businesses (if in a workplace environment); therefore, as this happens the hacker can obtain sensitive information, including passwords, usernames, security codes, and credit card numbers, from the target user.

1.5.1 Rule-Based Phishing Detection:

Like the IDS signature for a network, a rule is a template we want on a web page. By using a rule-based approach mechanism, phishing attacks can be detected more easily, quickly, and efficiently. One of our and key objectives is to make the framework scalable clear by integrating modern and evolving phishing methods as they meet. Regulations are mostly based on numerous current pieces of literature about phishing attack identification on observations and machine learning features [2]. The section provides an overview of the many rules we evaluate to identify malicious phishing URLs:

IF conditions are met, THEN actions will be taken

- ➢ When a correlation, also widely regarded like a condition, is met, the rule's operations are triggered.

❖ **Search Engine-based Rules**

- ○ **Rule 1:** If the URL of a webpage does not apply in all indexes of search engines, the webpage is potentially phishing
- ▪ Users check whether a Link exists in the search results indexes (Google, duck duck go, and Bing). Our rule generator queries search engines automatically and finds the top 30 answers. This law declares the website to be a phishing attack if the findings do not contain the URL. Once we crawled the URL, we noticed that it was presented as the very first response by all major search engines. This makes sense intuitively because we cannot check the URL ourselves, which is dependent on keywords, for appropriate URLs. But to be sure, we use the 30 best results because it has proved to have little impact, moving beyond the 30 top results.
- ○ **Rule 2:** The web site may phish if the domain of such webpage doesn't really present in all search algorithm indexes.
- ▪ By querying the search engines with a URL domain, rule 2 is created. If there is no domain in the top 30 results, this rule states that the web page must be complete.

❖ **Obfuscation-based Rules**

- **Rule 3:** An IP-based URL (hexadecimal, octal, or decimal) may indicate phishing.
- **Rule 4:** If a URL has most of [-, _, 0-9, @, ",", ;] [-, The website is phishing, or it has a non-standard port.
- **Rule 5:** If a URL's portion of the host is 5 or more points or the URL's size is more than 75 characters OR the host's length is longer than 30, the website could be a phishing threat.
- **Rule 6:** Blacklisted URLs are likely to be phishing websites.
- **Rule 7:** When a URL includes a top-notch target or the domain of the URL's IP, then the website is possibly a phishing attack in statistical reports produced by PhishTank, Stop adware, etc.

❖ **Content-based Rules**

Most criteria in this classification are focused on the HTML components of phishing websites. The look and sound of the legitimate website are similar to the ingenious phishing website. Nevertheless, phishers use the same techniques to find out about our content-based laws. Regulations are created as follows by examining HTML structures of several hundred phishing web pages:

- **Rule 8:** If you have a Web site with the password AND HTML element (for the corresponding form contents, the form contents shall be transmitted in plain text without even using Transport Layer Security (TSL)/Secure Socket Layer (also with assistance of the "get" procedure) (SSL).
- **Rule 9:** An external domain that does not have TLS/SSL can be phished if it has a webpage with password input.
- **Rule 10:** META tags include a target property's URL, which might be blacklisted or in a third-party domain, and the page might be blocked
- **Rule 11:** If a webpage does not have the wrong HTML mark-up, then the webpage might be phishing. IF it includes the password entry field.

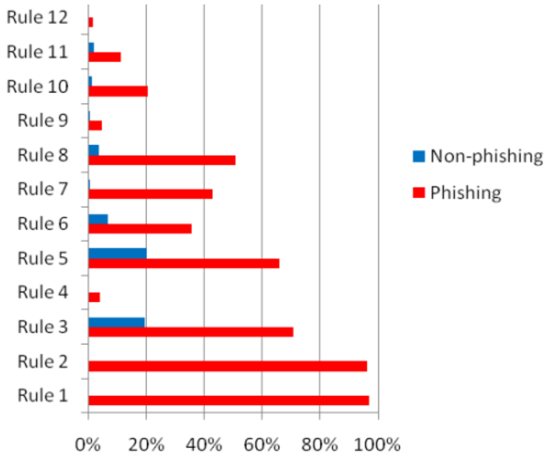

Figure 4. Histogram of Rules

Figure 4 shows the histograms of Rules 1-12

In Phishing websites, rules 1 and 2 are prominent and are high markers of whether the website phishes. These rules will detect more than 97% of the Phish web pages, thus classifying 100% of legal websites correctly.

1.5.2 Detecting Phishing Using Obfuscation URL Detection:

The email has been used for exchanging messages since 1993 from a sender to one or more beneficiaries. This works on the Internet or other network of computers. Before this, all senders and email recipients require the email system to be simultaneously online. Fraud mail is a threat to the SMTP system's purpose of exchanging messages. Mail containing spam or junk mail is unwanted. Spoofing is perhaps a term that describes unsolicited message sent to multicast. Spam mail has a link to phishing pages or malware. Often, money and confidential information can also be obtained indirectly through phishing, such as usernames and passwords.

➢ ObURL Detection :

- The way to spot spam emails is by combining fingerprint technology with large data analysis. Almost every fingerprint is stored in an inbox and directory through using hash functions used to create a footprint for the World Summit on Innovation Systems and Management.

- In phishing assaults, ObURL monitoring is used to recognize the URL. ObURL Algorithm for Detection of URL is the Obfuscated algorithm for URL Detection. The ObURL target acquisition technique provides multilayered defence. Due to the continuously growing usage of internet services, phishing attacks are also on the rise. How do we give users the phishing website and spoofed e-mail? The algorithm for the identification of ObURL would then protect the data from phishing attacks across the Internet. As we all understand exactly, the attacker hides the Address in a variety of ways. As a result, detecting each of these threats is challenging, but even then the ObURL detection method will recognise the maximum URL obfuscation number. As a result, detecting any of these attacks is difficult, nonetheless, the ObURL detection algorithm is capable of detecting the largest volume of URL obfuscation phishing as it examines phishing site addresses using the following test cases:

1. Domain Name System Test
2. Verify your IP address
3. Test to encrypt the URLs
4. Test for shortening URLs
5. White List Test
6. Black List Test
7. Pattern Matching Test

IV. Algorithms / Techniques

❖ Detection Algorithms / Techniques

➢ ObURL Detection Algorithm:-

```
Step 1. Load: Content
Step 2. Output: Discourage users  if URLs appears to be a forgery
Step 3. Alert notification to the User: Phishing is attainable.
Step 4. Safe User: There will be no phishing.
Step 5. DB: Database
Step 6. Within the email content If there is an Input form then
        The user will receive an alert; End
        For each iframe inside of an e-mail which is illustrated does
                // Retrieve the iframe's content
        For each iframe's origin during an e-mail text do
                If There was an input form then Notify User;
        End
        For each, source of the iframe in the E-mail's content    contains a hyperlink do
                // For every one of the six assessments, follow the directions carefully.
        End
        For each Iframe source URL and e-mail content contain hyperlinks
        do
Step 7.
        Test 1: DNS Test
        If text_of_hyperlinks! = text_of_anchor
        Then
        The user will receive an alert;
Step 8.
        Test 2: Verification of IP address
                If the IP address set up in the text of the hyperlink
                Then
                If an IP address is discovered in the White list database
                then
                        User is Safe: There is no Phishing;
        Else The user will receive an alert;
                // an IP address is discovered in the Blacklist DB
Step 9.
```

```
    Test 3: Encryption of URL Test
    If the text of the hyperlink is constructed using ciphered
    Then
        Decipher hyperlink;
        Inform the User;
Step 10.
    Test 4: shortening the URL Test,
    IF is the size of the URL is lessened
    Then
        Notify alert to the user;
Step 11.
    Test 5: hyperlink white list and blacklist test
    IF URL found in safelist (Whitelist) Database
    Then
        User is safe: There is no phishing;
    Else
        The user will receive an alert;
        // URL discovered in Blacklist Database
Step 12.
    Test 6: Pattern Matching Test
    IF the pattern of hypertext and anchor text matches
    Then
        Notify Alert to the User;
```

1.5.3 Prevention Techniques

1.5.3.1 Malware Prevention Techniques:

The quick solution to blocking extortion security breaches is to regulate the activity. Educating your workers about what to do to identify and protect their personal computers and smartphones from malware attacks is a good place to start when it comes to preventing malware attacks in the company. The below are some of the best tactics that we can use to take a constructive way to prevent malware:

- Make doubly sure you already have most of the essential defense security patches applied. – To guard against ransomware and other security threats, Releases and security fixes should be installed as soon as feasible. This is especially important for a program like Java, Adobe, and QuickTime, which are common and commonly used. Where practicable, allow automatic app updates.
- Avoid suspicious links and emails – Avoid clicking on any unsolicited or suspicious-looking attachment or text. These are often phishing emails that claim to be genuine to deceive users into uploading malware or disclosing confidential details. Remember that a company would seldom request your credentials or other private details through email, which is usually a sign of a phishing scam.
- Review software carefully before downloading – Look at the application and its ratings before downloading something for the first time on a machine or smart device, even app versions that are free or trial.
- Make use of strong, one-of-a-kind passwords – The passwords that so many Users opt select the most appropriate passwords that are easy to deduce or should be the same for hundreds of accounts. For every one of your identities, you must create secure and unique credentials.
- Firewalls and security protocols should be turned on– Make absolutely sure that firewall is enabled well and controlled properly all of the time as these rules determine what information can reach your computer.
- Install an anti-virus/anti-malware software – Advanced anti-virus software that monitors the environment will shield you from common ransomware and other security threats. Many infiltrations can be blocked and prevented by using trustworthy anti-virus applications. Anti-virus tools won't catch any bit of malware out there, so it's a good starting point for defending against well-known malware threats.
- Limit application privileges –Since malware also requires complete access to your computer to function properly, account controls can be used to

restrict what a program can do without your permission. Then, when you're alerted to apps or programs that are attempting to alter your device, you should pay heed to the alerts and seek assistance in preventing ransomware from being installed.

1.5.3.2 Phishing Prevention Techniques:

Nobody wants to be a victim of a phishing scheme. However, there is an explanation why those scams will continue to exist: They are lucrative enough for black hat hackers to make a lot of money handsomely from them. Phishing scams have existed almost since the dawn of the Internet, and they aren't going anywhere anytime soon. There are, interestingly, things you can still do to avoid being a victim of a crime. Here are 10 basic safety standards to follow:

- Keep Informed About Phishing Techniques – Phishing scams are constantly being created. You could fall victim to one of these modern phishing tactics if you don't keep up with them. Keep an eye out for updates on the latest phishing scams. You would have a much smaller chance of being snared by one if you learn about them as soon as possible. Continuous threat awareness training and simulated phishing for all users are strongly recommended for IT managers to maintain security top of mind in the organization.
- Think Before You Click! – When you're on a reputable website, it's fine to click on links. Clicking on links in random emails and text messages, on the other hand, isn't such a good idea. Before clicking on any links that you're not sure about, hover over them. A phishing email may appear to be from a reputable organization, and when you click the link to the website, it may appear to be identical to the actual one. If you get a phishing email that begins with "Dear Customer," be cautious. When in doubt, rather than visiting a potentially dangerous website, head straight to the source.
- Install an Anti-Phishing Toolbar – For some of the most modern web browsers, anti-phishing extensions are easily accessible. Using these toolbars, you can quickly verify a website's legitimacy via a rapid test and link it to established phishing websites. You will be notified if you visit a potentially harmful website when using the toolbar. Phishing scams can now be avoided thanks to a secure additional line of defence.
- Verify a Site's Security – It's understandable to be wary of disclosing confidential financial information over the internet. However, as long as you're on a safe website, you shouldn't have any problems... Often look for the site's protection certificate. Do not access a website if you receive a warning that it can contain malicious material. Even search engines can display such links that lead to a phishing website that advertises low-cost goods. If a customer makes a payment on such a website, credit card information is collected.
- Check Your Online Accounts Regularly – Someone might be having a field day with your online account if you don't log in for a bit. Regularly, make sure almost all of your internet accounts is up to date. To stop bank phishing and credit card phishing scams, you should directly check your accounts regularly. Obtain monthly financial account statements and a close review of entry to ensure that unauthorized transactions have occurred without your knowledge.
- Be Wary of Pop-Ups – Pop-up windows are often mistaken for genuine website elements. The vast majority of the time, though, they are phishing frauds. Pop-ups can be blocked in several popular browsers, or you can authorize them on a case-by-case basis. If you do happen to slip between the cracks, don't press the "cancel" button; these buttons often lead to phishing pages. Instead, press the little "x" in the window's upper corner.
- Never Give Out Personal Information – You can never exchange personal or financial information

over the Internet as a general rule. This law dates back to the early days of America Online when users were continuously warned about phishing scams due to their popularity. Where in doubt, go to the company's main webpage, get their phone number, and send them a message. The majority of phishing emails will guide you to a website where you must enter financial or personal details. A account holder of the Internet should never enter top secret information via email attachments. Never give someone personal information via email.

V. TOOLS & TECHNOLOGIES

Cyber-attacks integrate a variety of tools, which are classed as follows:

1.6Operating System:

❖ Kali Linux:

Offensive Confidentiality also keeps up and funds a fully accessible platform called Kali Linux. It's criminal investigations and detection process software designed exclusively for computer forensics.

1.7Attacks Tools:

❖ Ophcrack:

This tool is primarily used to crack hashes that are created by the same Windows files. It offers an user - friendly interface that is durable and can set up on a variety of platforms.

❖ EnCase:

An investigator will use this program to photograph and analyze data from hard drives and removable disks.

❖ SafeBack:

SafeBack is primarily used to visualize the storage media of Intel-based operating systems and restore those images to other hard discs.

❖ KeyLoggers:

The process of having to log (or storing) the keys pressed on a keyboard, Keystroke logging, also known as recordkeeping or keyboard capture, is a method of recording keystrokes in a non-obtrusive manner so that the person using the keyboard is blissfully ignorant that their activities are being recorded.

❖ Spyware:

Spyware is malware that collects information about an individual or organization without their permission and sends it to another party without their approval, or that, without any of the user's awareness, takes ownership or control of the device.

❖ X-Ways Forensics:

This collection is one of the most extensive forensic suites accessible for Windows-based programs. It is supported by nearly every version of Windows, resulting in it being one of the most user-friendly on the marketplace, permitting you to work with versions supporting both 32-bit and 64-bit. One of its most appealing features is the fact that it is entirely compact, allowing it to be run from a memory card and transferred from one machine to another.

❖ SurfaceBrowser:

SurfaceBrowser™ is the ideal tool for identifying a company's entire online infrastructure and extracting useful intelligence information from DNS records, DNS servers and their past and present Registry information, exposed subdomains, Digital certificate files, and more are all available.

VI. CURRENT/LATESTNR&D WORKS IN THE FIELD

Here some of the trends that affect cyber security are listed below.

1.8Web Servers:

Cybercriminals spread their malicious code over their hacked legal web servers. However, data robberies, many of which are media-focused, are also a major threat. Such cybercriminals may steal data on web servers in particular. Therefore, a safer browser must always be used in order not to fall victim to such crimes, particularly during important transactions.

1.9 Cloud computing and its services:

All small, medium-sized, and big businesses now gradually become cloud service providers. This means that the planet progresses steadily to the clouds. This latest development poses a major challenge to cyber safety because traffic can be rounded by conventional checkpoints. In addition, with the increase in the number of cloud applications, policy controls would need to change for web applications and cloud services to ensure that sensitive information is not lost.

1.10 Encryption of the code

Encryption is the encoding (or information) method in such a way that nobody can read it. The message or data is encrypted with an encryption algorithm in an encryption scheme to turn it into an unreadable chip document. This is normally achieved using an encryption key, indicating how to encode the message. Encryption preserves the privacy of data and their confidentiality at an early stage.

1.11 IPv6: New internet protocol

IPv6 is the latest IPv4 (old version) Internet Protocol, which was a backbone to our networks and the Internet as a whole. It is not just a matter of porting IPv4 capacity that we protect IPv6. Though IPv6 is a wholesale substitute in providing more IP addresses, some key improvements to the protocol need to be taken into account in security policies.

VII. CONCLUSION

Overall, several security measures can be enforced to safeguard computers and networks against these types of attacks. The majority of security tools targeted at consumers are designed to protect computers from malware, adware, spam, and different forms of viruses. Despite the fact that many businesses offer these services, cybercriminals are constantly searching for new ways to get around firewalls and anti-virus software, and they are often successful. Since there are so many hackers and spammers all over the world, new ways to get around these obstacles are constantly being built, making it difficult to catch them. Users who take the necessary precautions, such as installing firewalls and anti-malware/virus software, are less likely to fall victim to cybercriminals. Though not all people are victims of cybercrimes, they are still at risk. Computer-assisted crimes are diverse, and they do not all take place in front of a computer, but they are always carried out by one. The hacker's age ranges from 12 years old to 67 years old. The hacker may be on the other side of the world from the victim, and they would have no idea they were being hacked. Computer-assisted crimes are a concern in the twenty-first century. Criminals no longer need to rob banks or be outside to commit any crime, thanks to advancements in technology. On their laps, they have everything they require. Their arms are no longer guns; instead, they use mouse cursors and passwords to strike.

VIII. REFERENCES

[1]. G.NIKHITA REDDY, G.J.UGANDER REDDY A STUDY OF CYBER SECURITY CHALLENGES https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

[2]. Ram B. Basnet. Andrew H. Sung, Qingshang Liu Rule-Based Phishing Attack Detection https://www.cs.nmt.edu/~rbasnet/research/RuleBasedPhishingAttackDetectionFinal.pdf

[3]. Patil, Prajakta & Rane, Rashmi & Bhalekar, Madhuri. Detecting spam and phishing mails using SVM and obfuscation URL detection algorithm. 1-4. 10.1109/ICISC.2017.8068633. https://www.researchgate.net/publication/320651414

[4]. Ammar Ahmed E. Elhadi, Mohd Aizaini Maarof and Ahmed HamzaOsman Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph. ISSN 1546-9239 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.854.2710&rep=rep1&type=pdf

[5]. A. M. Shabut, K. T. Lwin and M. A. Hossain, "Cyberattacks, countermeasures, and protection schemes — A state of the art survey," DOI: 10.1109/SKIMA.2016.7916194 https://ieeexplore.ieee.org/abstract/document/7916194

[6]. G.NIKHITA REDDY, G.J.UGANDER REDDY A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

[7]. Cyber Crime Investigation: Tools and Techniques | Info-savvy.com Copyright © 2021 Infosavvy Security and IT Management Training | Certification Partner InfoCerts.com https://info-savvy.com/cyber-crime-investigation-tools-and-techniques/

[8]. Focus Areas for Cyber Security© ProTech Services Group, Inc. https://www.psgi.net/10-focus-areas-for-cyber-security

[9]. What is Malware? A Definition & Tips for Malware Prevention | Digital Guardian©Digital Guardian All rights reserved. https://digitalguardian.com/blog/what-malware-definition-tips-malware-prevention

Cite this article as :

Jigar Vakil, Dr. Priya Swaminarayan, "Cyber Attacks : Detection and Prevention", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 82-93, September-October 2022. Available at doi : https://doi.org/10.32628/IJSRSET229511
Journal URL : https://ijsrset.com/IJSRSET229511