International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-10 Issue-8, June 2021

A Comprehensive Overview on Cybersecurity: Threats and Attacks

Preetha S, P. Lalasa, Pradeepa R

Abstract: ***In the world of evolving technologies, we are being driven by online transaction, AI technologies and automated processes. With the increased use of technologies in our life, the cybercrimes have amplified. Various new attacks, tools and techniques have been developed which allow the attackers to access more complex and well-managed systems, creating damage and even remain untraceable. The statistics about cyber crime tell that as of 2021 January, google has registered around 2 million phishing websites. In 2019 around 93.6% of observed malware was polymorphic, which means it changes the code continuously to evade detection. According to FBI and internet crime complaint center 2020crime report has doubled compared to 2019. International Data Corporation predicts that global spending on cybersecurity solutions will reach $133.7 billion by 2022 as cyber threats continue to increase. Governments around the world have acknowledged to growing cyber-attacks by providing directions to organizations implementing efficient cybersecurity practices. Cybersecurity protects computer systems and networks from creating damage to hardware and software, information disclosure, theft and from the interference or misdirection of the services they provide. The need to understand different kinds of cybercrime. In order to develop necessary measures against cybercrime, we need to understand different kinds of cybercrime. Our paper gives you an overview of various types of cyber-crime like malware, phishing, zero-day exploit, Advanced Persistent Threat (APT). The study provides an overview to different preventive existing solutions proposal and methods to detect attack. A strong understanding of such attacks would benefit us to be cautious and develop effective solutions.***

Keywords: Attacks, Cybercrime, Cybersecurity, Malware Detection, Preventive.

I. INTRODUCTION

Today's business and communication scenario is changing due to advanced usage of Information technology. To improve the products and services, organizations are increasingly turning to information technology. Organizational and personal data can be stolen in any form at any time, making it difficult to protect. A cyber-attack is a malicious and deliberate attack performed by a person or organization to gain unauthorized access to another person's network or organization for the purpose of damaging, disrupting, or stealing IT assets, computer networks, intellectual property, or other types of confidential information. In the year 1820, the first cybercrime was recorded. In 1978 over Arpanet, the first spam email was sent. In 1982, an apple computer was installed with the first virus. Data breach incidents cost the U.S. 8.64 million dollars, the highest globally, followed by the Middle East at 6.52 million dollars, as per the "2020 Cost of a Data Breach Report" published by IBM. The Cisco Cyber Security Reports show that 50 percent of large organizations, with a workforce of more than 10,000, spend at least $1 million on security every year. The report also found that 43 percent spend between $250,000 and $999,999, while 7 percent spend less than $250,000.

Cybersecurity is also a set of technologies, processes, and methods designed to protect unauthorized access to various networks, computer systems, programs and data from cyberattacks. Computer security includes cybersecurity and physical security. Various techniques have been followed to avoid cybercrime. To develop more effective solutions against cybercrime, a clear understanding of various cybercrime and solutions is essential.

II. LITERATURE SURVEY

Rahna Buch et al. [1] are working to raise awareness of cybercrime, one of the biggest crimes committed by computer experts. This article covers the need for cybersecurity and some of the consequences of cybercrime. While cybersecurity is designed to prevent cybercrime, cybercrime is a set of actions performed by people interfering with networks, stealing data, other sensitive and personal documents, hacking bank details and accounts, and transferring money to themselves. The study provides detailed information on IT security and cybercrime. It covers the types of cybersecurity, the need for cybersecurity, cybersecurity issues, advantages and disadvantages, the history of cybercrime, and the types of cybercrime.

Hamad Al-Mohannadi et al. [2] described cyberattacks as one of the most important issues for most organizations. Governments and businesses work hard to protect valuable information from theft. To protect network, there are many systems like Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Firewall, and Shaper. There are also several attack modeling techniques available to help organizations know the nature of attacks. Defending the network against intruders is one of the organization's top priorities.

People are the front line of defense for any organization to protect their networks from the greatest threats.

Manuscript received on June 16, 2021.
Revised Manuscript received on June 22, 2021.
Manuscript published on June 30, 2021.

* Correspondence Author
Preetha S*, Department of ISE, B.M.S. College of Engineering, VTU, Bengaluru (Karnataka), India. Email: Preetha.ise@bmsce.ac.in
P. Lalasa, Department, department of ISE, B.M.S. College of Engineering, VTU, Bengaluru (Karnataka), India. Email: lalasapunaganti@gmail.com
Pradeepa R, Department of ISE, B.M.S. College of Engineering, VTU, Bengaluru (Karnataka), India. Email: r.pradeepa.bms@gmail.com

Honey pots- are used to find identifiers and collect data in the company to reduce the cybercrime risk of employees. Internal threats-in many cases, a lack of knowledge among employees leads to cyberattacks in an organization's network.

Study safety knowledge and educational effectiveness- they have identified several security awareness barriers in the organization like computer skill, general security awareness and budget. Cyber security communication- is essential for any organization. Studies have shown that mutual security knowledge is better than modified delivery. Many organizations offer basic training to their employees. Such exercises are usually online or introductory. Security alertness is very beneficial because it can provide users with more information about cyber threats. Behavioral change is important with learning. Phishing attacks are very common in all organizations to understand the consumer perception that attackers use primarily through email. As a result, participants were able to avoid phishing much better. Safety Aware Phishing is useful for raising safety awareness.

Satish A.P. Kumar talks about the problems and solutions faced in phishing [3]. It is a serious problem to all internet users and is obviously harmless, making it difficult to track or defend against. Today, society has become online and the security of individual information is at huge risk. It is analyzed as one of the ways to steal information from people and used to obtain a wide range of personal data. Also has a quite simple way to send an email, an email sends the victim to a website, and the site steals information. The proposed system has three approaches to solve the problem. Using a filtering system reduces the number of phishing emails reaching users, which reduces the likelihood of phishing. Blocking and detecting phishing becomes increasingly difficult as attackers continue to update their phishing tactics. In three categories of solution approaches proposed today, automated machine learning defenses can help control phishing. Akarshita Shankar et al. [4] briefly talk about phishing attacks and highlighting measures to overcome them. Phishing is a cybercrime in which users provide confidential information to an attacker. Information may contain credit card information, user-name and password, bank content, and more. Goals can be people, organizations, or clusters within an organization. The article described phishing attack and its affects to increase awareness and provided some countermeasures.

Bhavana Gautam , Jyotiraditya Tripathi and Dr. Satwinder Singh provides a way to prevent SQL injection attacks [5]. SQL injection attacks are considered as the most dangerous threats to the security of web applications. SQL occurs when a hacker successfully injects malicious code into a specific web-application and these injected code successfully communicates with a database query. Attackers can inject these types of infected applications through URLs or web forms. The different types of SQLI prevention techniques are black box testing, combined static and dynamic analysis, infection-based approaches, and more. In this study, they propose a secure encryption method to prevent SQL injection attacks, which can be very appropriate in protecting web-applications from this kind of attack because user information authentication serves as a signal to communicate with the data base queries on the side server.

Sebastian Floderus and Linus Rosenholm conducted educational experiments to detect targeted phishing attacks [6]. Targeted phishing attacks are a major problem that has existed since 1995, and the number of attacks is increasing year by year and seems to be declining sooner or later. The impact of reduced productivity can have a significant impact on individuals and companies. Common people are vulnerable to fraud and fraudulent card theft. At the same time, businesses are much more at risk and the breach of trade secrets can lead to millions of dollars in lost revenue. Due to the small number of participants in this study, the t-test may be more accurate in future studies if performed on a larger scale. Similar studies can be conducted with many university participants and programs. Without human interaction, it's quite difficult to get attention to the subject if people are forced to read on their own. If some of the pedagogical treatments are longer and more detailed, majority of interest may disappear after a while. Hence other learning methods are recommended.

Husin J. Hedzhase, Hassan F. Fayyad-Kazan, and Imad Mukadem say that the organization's leading awareness and presence of leading organizations, technology and information, is the first building block to proactively mitigate cybersecurity threats [7]. In fact, "Administrators have to learn how to use new technologies to actually provide extra protection. Security is responsible for creating the security policy. These policies describe the steps you must take to manage data within your organization's technology infrastructure. However, there are several security flaws and vulnerabilities that an attacker can use to attack your organization." Effectively protecting, detecting and responding to APTs is a rigorous security application for ongoing security and training for the most targeted users. Study Emphasized that governments, businesses, and educational institutions should work together to launch an all-heavy information campaign related to cyber warfare, airbags, cybersecurity and cyber pools. "The threat of cyberattacks" is always present and it is a glossary of everyday words.

Santiago Quintero-Bonilla, OrcID and Angel Martin del Rey provided a comprehensive information on sophisticated targeted, personalized attacks and Advanced Persistent Threats (APTs) [8]. Attackers are often referred to as actors and are classified as public and private actors. These actors use a variety of techniques to perform attacks. As the attack progresses successfully, the method becomes more sophisticated.

Machine learning methods and models commonly used to detect APT attacks are SVM, k-NN, and DT. In addition, the APT attack lifecycle has been analyzed and there are various stages that form these cycles. Steps in different circles have similarities that can be grouped together. However, these measures represent a non-linear system of attack behavior. Finally, a five-phase lifecycle model was described, the most commonly used methods were identified, and potential mitigation methods were proposed. Recommendation of machine learning methods provided good results. The suggested method was advantageous as it simplified the behavior of APT attacks by taking into account the passive and active phases of the lifecycle. The study aims to provide a new approach to APT detection using machine learning techniques and is based on the APT attack lifecycle.

Retrieval Number: 100.1/ijitee.H92420610821
DOI: 10.35940/ijitee.H9242.0610821
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

The proposed model consists of two passive and three active stages to apply the emancipation technique based on machine learning. Taehyun Kim and Douglas Reeves [9] studied vulnerabilities and attacks on domain name systems [DNA]. DNS plays an important role in Internet operation.

Customers get internet service by mapping domain names to transferable internet protocol addresses. DNS provides a flexible name resolution service that can be easily and quickly scaled up. However, DNS was originally designed without security and the information is not secure. The DNS security add-on was released in 1999 to protect against vulnerabilities, but it has not been widely adopted, and DNS is still under a lot of attack. The purpose of this study was to provide a comprehensive overview of DNS security. Result of this study was to introduce fundamental DNS vulnerabilities and classify representative DNS attacks into four categories for effective analysis. Although DNS is an integral part of Internet operations, it is still vulnerable to a variety of attacks because of its weaknesses, low use of available mitigation methods, and limitations to these methods.

A. K. Maurya, N. Kumar, A. Agrawal, and R. A. Khan showed how ransomware works with the development and common features of several popular ransomware programs [10]. In terms of evolution, this article presents a study of the first ransomware program of the day. The study illuminated different types of intrusions caused by ransomware, including data infections and infected systems. Different attackers have chosen targets for diverse attacks. An insight into different types of targeted ransomware was discussed. Case studies illustrating problems and attacks were presented. Behavior of victim after infection, security measures to protect computer systems from ransomware and steps to maintain system and data was elaborated. Saurab Kumar Sen and Nidhi Chouri investigated their organization's ransomware detection and prevention. Ransomware poses a serious threat to the online world [11]. Most software companies, universities, companies and organizations around the world try to make proactive decisions to avoid ransomware attacks. Two U.S. governments issued a joint statement on ransomware attacks and urged consumers to be vigilant and take precautions. Recently, on May 19, 2017, the Swiss government celebrated Ransomware Awareness Day to raise awareness of ransomware and its consequences. Ransomware is also increasing in India, methods to improve detection, prevention and recovery of malicious software should be adopted to reduce the damage caused by ransomware attacks.

Abhishek Kumar Pandey et al. [12] discussed the trend of malicious software attacks. Security issues are constantly evolving in today's scenarios due to the heterogeneous nature of software. Multimedia functions-Interactive and responsive multilingual capabilities and rapid growth of third-party software products. The study focused on the problems and components consumers face on Internet, malicious software research, importance of social technologies and increasing consumer awareness of malicious software attacks. Investigation reviewed the current malicious attacks, and explained measures to control. Cyber-attacks have been the most common problem in recent years and has increased malware threat for security professionals. Hence an urgent need to focus on aspects that help reduce the problems of malicious software attack. Software systems are common in both personal and professional life, security of such systems are essential as they are an important source of sensitive information.

Chanchala Joshi et al. [13] offered an advanced framework for identifying and assessing the risk of zero-day vulnerabilities. A proposal of a new security approach to assess the security risk of zero-day vulnerabilities that compromise network assets was done. Network's ability to protect against zero-day vulnerabilities was measured. The proposed method developed a probabilistic attack diagram that encodes the possible and current data on the attacker's behavior and determined the risk of dissection. An experiment was designed to test effectiveness of the proposed method using various standard parameters. Experiment resulted 96% for best detection rate and 0.3% for false positive frequency.

C.P. Patidar and Harshita Handelwal in the discovery of no-day attacks through machine learning [14]. The rapid growth of malicious software designed to infiltrate and damage computer systems poses a rather large threat to the integrity and security of computer systems without consciously exploiting system software vulnerabilities. It is required to detect malicious software for zero-day attacks, which exposes a variety of malicious code, opening up a platform to perform an attack or overload the system. The rapid growth of malicious software has forced most researchers to implement new methods to mitigate attacks and develop countermeasures, so they have adopted machine learning algorithms to detect routine attacks.

III. VARIOUS CYBER-ATTACKS AND THREADS

Cybercrimes are categorized into several types.

A. Hacking

Hacking is simply an act committed by an attacker and access the computer system without user's permission. Hackers are mostly computer programmers (hackers) who use computers frequently with advanced knowledge and misuse for defamatory reasons. Viruses are computer programs that attach or infect a system or file and tend to spread to other computers on the network. It interferes with the operation of the computer and affects the stored information by completely altering or deleting it.

B. Denial-of-Service Attack

A denial of service (DoS) attack is a type of cybercrime where the attacker does an obvious attempt to deny service to an intended user of a service. A computer resources are overloaded with more applications than can be handled by the available bandwidth, resulting in server overload.

C. Phishing

Phishing is defined as a form of malware in which a random email is sent to a victim by masquerading as a legitimate enterprise to obtain personal information about the victim.

D. Bombing and Spamming

Electronic bombing is characterized by an attacker sending a large number of email to a target address, causing an error in the victim's email account or email server.

E. Jacking

A hackers takes control of websites fraudulently. The attackers can also modify the content of the original site or redirect the user to another similar page.

F. Data Diddling

An unauthorized modification of data before or during access to a computer system and then altered again after processing is complete.

G. Slicing Attack

In Salami slice attacks or salami scams, cybercriminals steal money or resources in pieces, so there is no noticeable difference on the overall scale.

H. SQL Injection

SQL injection tricks the server to perform malicious SQL commands by injecting SQL commands into a submitted web form query string or specifying a domain name or page request.

I. Zero Day Exploit

A zero-day attack is a type of malware which occurs when software or hardware vulnerability is announced and before a patch or solution is implemented, the cybercriminals exploit the vulnerability.

J. Ransomware

Ransomware is a kind of crypto virology software that threatens to post or permanently block access to victim's data if they don't pay a ransom.

IV. EXISTING METHODS

In [3] questionnaires were distributed to various cyber threat handling teams to understand the knowledge and perceptions of IT security staff and conducted survey on different teams. Several professionals' staff working directly or indirectly on the cybersecurity team were a part of the survey. Survey was conducted primarily with Security Operations Center (SOC) employees who were involved in cyberattacks directly on the organization's network, and other employees who do not directly handle and participate in cyberattacks, but who support them. Actions to alleviate problems, focus was on three areas of cyber threat analysis: Knowledge, Monitoring and Prevention. Investigation showed that there is an information gap between the security team and other IT professionals. Interestingly less than half (48.4%) of non-SOC teams and only 68.1% of SOC teams knew about Indicator of Compliance (IoC). Similarly, only 65% of SOC teams know and use access control lists (ACLs), and 41.9% of non-SOCs. In addition, only 75% of SOC teams and 45.2% of non-SOC teams control privileged consumer activities.

Additional serious threats are attacks like zero-day attack, Advanced Persistent Threat etc. which are difficult to identify and defend against. Results showed a large difference between SOC and non-SOC, which needed to be decreased. Only 32.80% of SOC teams and 16.10% of non-SOC teams scan their databases for weaknesses and performance.. Finally attaining SOC and non-SOC working together is a challenge that organizations must address by generating daily reports, weekly meetings to discuss the latest cybersecurity threat issues. The results of the Predictive Response and Prevention survey do not reflect good knowledge of these workers. It showed that only 31.9% of SOC team members are familiar with penetration test results, while only 22.6% of non-SOC employees are aware of this report. In case of multi-factor authentication in both SOC and Non-SOC team scored very low as 41.2% and 32.3% as demonstration of knowledge. From the survey it was also noticed that only 61.3% of SOC staff has knowledge of patch and vulnerability management. In order to overcome the knowledge gap in awareness among IT employees within an organization they proposed the use of security assessment services. Some common assessment scenarios were proposed to support organizations to keep in par with cyber security knowledge. Each type of assessment is impacted by the number of targets like application, servers, etc. and therefore takes varying amounts of time. The various type of assessments based on targets are as follows:

A. Network-Based Attack & Prevention

Network-based attacks like denial of service attack can be prevented by using design decision. To prevent cyber-attack, organizations need to check the network vulnerabilities through Penetration testing. It includes components of application vulnerability assessment, security best practices and host vulnerability assessment. To perform these type of test, detailed prior knowledge of the environment is not required.

B. Host Based Assessment

An assessment to check health and security of a given workstation or server. Automatic scanning equipment (e.g. Nessus2) is the most important evaluation tool of this kind. This assessment will answer questions like "Is patching up to date?"

C. Application

It is an assessment to test the resilience and functionality of an application to known threats. This valuation emphasis on the components that are built and installed throughout the system, such as how application components are used, interaction with user and server environments. This assessment answers questions such as "Basic server attacks and software applications."

D. Compliance

This may include an audit of the Department of Information Security on the system for specific rules (or assistance with audit coordination if ISO is not proficient to perform specific audits).

E. Physical Security Assessment

This assessment usually includes interviews with significant personnel, document review to evaluate suitable physical and environmental controls to protect computer resources. Such assessment replies questions like "Are there appropriate physical access controls in place for securing servers and desktop machines".

In [4] authors proposed three ways by which a solution for phishing can be approached, they are prevent phishing, detect phishing and stakeholder training. Each technique has both pros and cons.

The best way is to approach utilizing a mix of all three ways and to increase the chances to find phishing and stop it. The steps are explained as follows

Step 1 – *Prevent phishing:* By listing or blocking phishing sites, or use phishing filtering phishing can be prevented before reaching the user.

First way is to use machine learning to check the URL and the website it claims. Features used to classify phishing emails in the article "Classify Phishing Emails Using Random Forest Machine Learning Technology" were discussed. Some examples are the use of URLs containing an IP address with unique "href" attribute, and a URL containing the domain name's link text and domain name verification for the sender of the email. The program also looks for a few simple keywords like urgency, update, delay and confirmation. Experimental resulted with an accuracy of 99.7%, with few false positives of about 0.06%. It demonstrates to be a very effective anti-phishing technique, especially since it allows users to develop machine learning techniques alongside web phishing attacks.

Step 2 – *Detect phishing:* Many browsers already have phishing protection with passive or active indicators. Active indicators will show pop-up warnings that the website they are on is suspected of being tampered with or unsafe, whereas passive indicators do not disturb user's actions. According to the Suggested solution to the phishing problem, as expected, the active indicator was much more effective and many users ignored or did not notice the passive indicator. However, some users believe that the sites they visit are original and trusted. To prevent this, it can be useful to use a website verification system that are trusted and secure. If users sees this check each time they visit a real site, they're more likely to know they're not on a fake site which help the users to know that they are using a secure site.

Step 3 – *Stakeholder training:* The third approach is teaching the users to prevent phishing attacks. Most modern common phishing courses are broad and do not cover more sophisticated phishing attacks of today, depending on whether the user interacts with and reads the material. Hence to overcome these problems, solution was proposed to learn anti-phishing through games or embed an education system in an email server. Researchers are working on developing and improving similar games. One among the most successful examples of these format games is a micro game named Anti-Phishing Phil, which educates users to spot suspicious URLs and various components of scams. This method is interesting and beneficial for users. In built-in training method, users are trained default by sending mock phishing emails. Another approach is to use comics to outline the key point which helps the user to maintain their personal details secure. Both groups outperformed the control group that only received security alert emails. This is a useful technique because when users use an email server and click on fraudulent emails, they are greeted by training emails and are more risk aware to turn premium phishing victims into trained consumers.

An overview to various ANTI-PHISHING TECHNIQUES was discussed in [5]. “Anti-phishing based on Individual Whitelisting” by Ye Cao proposed a solution in which Automated Individual White-list (AIWL) attempts to maintain a whitelist which includes all known login interfaces (LUIs). When a user submits their confidential information to an unlisted LUI, AIWL warns the user of potential trap and subsequent attacks. In Computer Vision Techniques for Phishing Attack Detection, Routhu Srinivasa Rao [15] proposed a solution to protect against phishing attacks by combining visual similarity-based technique and whitelist.

The computer viewer (CV) tool called the SURF (Robust Feature Speed) sensor which use square filters to highlight discriminative key point. Features were collected from both suspicious and legitimate websites. Later compared the features downloaded from website and calculated similarity. Degree of similarity helps to decide whether the site is legitimate or not. Madhusud Khanan Chandrasekaran [16] proposed an alternative solution to detect phishing emails based on a structured feature that uses Support Vector Machines (SVM) to determine if an email is harmful or not.

SVM extracts common email features such as the language used, layout, structure, etc. To check similarity accuracy, extracted details are compared with data from the system. If accuracy crosses a certain threshold, then email is identified as malicious. In [17] Rakesh Verma's study on “automatic detection of phishing emails based on natural language processing technology”, used a unique NLP (Natural Language Processing) technology to determine whether messages were harmful. NLP tools were used to draw and compare common features. Natural language technology with all information in the email like subject, link and body text is used by PhishNet-NLP. Phishing is being detected by the information extracted from emails by PhishSang. NLP and statistical analysis is being used by Phish-Sem to mark email as phishing or non-phishing.

In Yi-Shin Chen’s [18] “Detect Phishing by Checking Content Consistency” used more advanced filtering and classification methods. Study tested whether the URL is harmful or not. An automated method was used to detect phishing which consisted of two stages: preliminary filtering and classification. The URLs are blocked using the URL domain section from the black list in the pre-filtering phase. If the URL was on this list, it is classified as harmful and will not proceed to the next phase. In the next step, two key features are identified: randomness of the URL (RU) and the location of the domain token. Depending on the result of the classification step, the URL was classified as malicious or not. “Intelligent Computing, Communication, and Devices: Advances in Intelligent Systems and Computing” by Masuma Zareapura [19], extracted different features of email using text mining. Strategy used was to first transform emails to a vector representation and then use selection techniques for classification. Using datasets collected from HamCorpus (legitimate email) of SpamAssassin project and publicly available PhishingCorpus (phishing email) assessment was done.

Extraction and classification methods were further developed in Sankhvar S [20] "A Novel Anti-phishing Effectiveness Evaluator Model, Smart Innovation, Systems and Technologies" where vulnerabilities were categorized into three types, depending on the email’s structure. The three categories were page content vulnerabilities, domain vulnerabilities, and code script vulnerabilities. Effectiveness of anti-phishing which was implemented as an evaluation model was analyzed using the Anti-Phishing Effectiveness Evaluator Model (APEE model).

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

Three categories of vulnerability are checked to determine whether the message is phishing. In "Anti-phishing protection" by Xavier Joseph [21], categorization of emails was done based on spam filters as junk or non-junk. When an email is received by the user, filtering function is performed by the spam filter and checks whether the message is spam.

Based on the URL reputation of the email Spam filtering is done. The email is identified as spam, if the URL is unclear or suspicious. Email goes to spam after the URL in the email is disabled. If the email is valid, it will be moved to your inbox. In Okunoye's [22] "A Web Enabled Anti-Phishing Solution Using Enhanced Heuristic Based Technique", anti-phishing technology was developed using an advanced heuristic approach. In this method, if a suspicious website is found, it will be added to blacklist immediately. When a legitimate website is found, it will be updated on the whitelist. Hence, when a user opens a website, it first checks if it's phishing website. The method supports two lists using the PHP programming language with a database. According to this method, 2519 URLs were tested and 2510 were classified correctly.

"A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection" by Anna L Buczak [23], discussed about the reusable component of the anti-phishing layer component. By using reusable components web pages can be converted into feature vectors using heuristic methods and external repositories. Vector machines are provided input with finite features vectors machines and trained. Based on the provided training by these inputs, the Machine classifies and identifies different web pages as legitimate or not.

Studies in [6] explained HOW TO PREVENT SQL INJECTION. Reasons for SQL injection attack are either due to not properly written statements or the special characters are missed in the program development process. In such case, client will be able to execute any SQL query through global variables POST and GET. To prevent SQL injection, the following methods can be followed: In the configuration file, Open the magic_quotes_gpc and magic_quotes_runtime settings, convert the SQL statement using add slashes on when executing the SQL statement, filter out few keywords at SQL queries such as Update, select,. *, without omitting small and single quotes as much as possible when writing the SQL statement. Naming skills for table and data fields should be improved, and based on characteristics of the program naming critical fields that is hard to guess Close the global variable registration by setting the register_globals parameter tp off in the php configuration file. Control error information, error information to be written in the log file and not output it in the browser.

In [7] a solution was proposed to prevent sql injection which focuses on research of following topics:

A. Input and URL validation- It is one of the most common loophole in web applications security. This means that user input cannot be verified prior to use. This causes serious web based vulnerabilities such as cross site script and SQL injection. Therefore, to prevent such situations, "All Input is Evil" rule was imposed. To verify user input, validation should be performed to check the length, format, and characters of valid user input. For example, mobile number field in form should accept numbers and not characters. Therefore to prevent SQLIA, all user input must be validated and sanitized before interaction with database query.

B. Data Sanitization- Well advised way to prevent SQL injection is to clean up every input before placing them as queries. Sanitization is a way to make user input valid (e.g. single quotes and spaces). This basically filters out all the characters you don't need from data. For example a username/password should contain only alphanumeric characters. An apostrophe should not be present in the username value. Sanitization of the input helps us to ensure it contains only valid characters. Preferable method to remove unwanted characters is regular expressions and can be stripped outside of the predefined "legal" characters. String parsing and pattern matching can be done by powerful tool "regular expression". It is not only enough to sanitize the data from the form fields, it should also be applied to fields like hidden, disabled and cookies. It's completely not right to assume that client-side authentication works fine, since attackers can bypass this and make changes to cookies. Therefore, data cleansing is a very significant step to block SQLIA.

Prepared Statement (or PDO) for query execution- Prepared statements are functions used efficiently to execute the same SQL statement repeatedly. PHP is one among the majorly used user-friendly and common programming languages, but it also leads to unsecure code. PHP Data Object (PDO) is a database abstraction layer which allows to work quickly and securely with diverse types of databases for the developers. The database abstraction layer hides the database interactions. It provides all features through API, complexity, processing and database communications are handled by the layer. Basically, prepared statements work with the following three steps-1.

Preparation: First, a template for the SQL statements are generated and sent to the database. Some unspecified values are called parameters (marked with "?"). Example: INSERT INTO Login VALUES index (?,?,?). The database analyzes, compiles, and optimizes queries in SQL query templates and the results are stored without executing them.

Execute: when you need the application later, it binds the value to the parameter and the statement is executed by the database. The statement can be executed as many times by the application with different values as it wants. Advantages of comparing the prepared statements with SQL prepared statements are: analysis time is reduced because the query is prepared only once. Limited parameters only need to send each time and not the whole query, consequently reducing server bandwidth. Prepared statements are advantageous for SQL injection since later transmitted parameter values which use a different protocol, need not be correctly escaped. SQL injection cannot be done unless the original statement template is received from external input.

Query and session tokenization: Query tokenization is a way to convert incoming queries into different tokens. Tokens are indicated by a string line before a single quote, before the double dashes, and before the space.

This method handles the original and injection query differently. Working scenario for the proposed method: In this technique, following steps are taken at the time of coding to some extent to protect the web application from this type of attack. It uses regular expression at client side to verify inputs and URLs.

Retrieval Number: 100.1/ijitee.H92420610821
DOI: 10.35940/ijitee.H9242.0610821
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

A token is generated that is used on the server side for query to interact with the application database. Data sanitization is applied to all variables before sending them to the server. Token mapping happens on the server side. If the tokens match, interaction with the database is allowed.

Otherwise, the variable will not be able to communicate with the database request for further server-side operations and will be redirected to a default page. Form item validation serves as an indication to interact with database request. For example, if some variable interacting with the database through a query is marked "$a" and a value is passed to that variable in a custom format, there is a validation record on the client side for that particular variable. Thus client-side authentication for a specific variable "$a" acts as a token to communicate with the server-side database query, and without "$a" variable cannot connect with the database. Thereby reducing the chances of SQL injection attack.

Proposed model in [11] enables early and efficient detection of APT attacks. Machine learning (ML) techniques are used in detection solution suggested from the beginning to the end of the active attack. The model's stages are discussed below:

A. Target discovery

This step involves manual investigation of the network organization to obtain extensive details about the attacked IT structure. To achieve this, an attacker can use port search methods, services indexed on the Internet, profiles of officials in social networks, and OSINT intelligence tools (for example, "Spider Poor"). Communication is not modified or interfered by the passive attackers but rather taps or monitors the information that is being transferred. Dark net may be used to collect the information found on the Internet. Such attacks may require the use of several specialized devices over a long period of time. Hence it's a good idea to close unused ports, use firewalls, IDS and secure virtual private connections (VLANs and VPNs), create password policies and increase awareness among users.

B. Exploitation toolset

Aims to gain access to network targeted through attacks discovered in target discovery. Variety of machine learning techniques are created for automated solutions that detect potential attacks early. For example, create a module that checks emails for malicious links or files. A different solution is to scan the network traffic for dial-up packages from unauthorized servers, analyze logs to detect unusual network activity, and finally update the software. Implementing these machine learning solutions requires training datasets for the normal flow of your organization and other datasets with unusual network flows. Next step is to choose a machine learning algorithm that provides the highest accuracy. Finally, testing should be done in a controlled environment. The machine learning algorithms k-NN and SVM provided the best results. At the initial training or retraining of the algorithm, the amount of data can be added along with the stream of other attack methods to improve detection.

C. Internal intrusion

Attacker should be able to maintain endurance for a long time because it's the longest. Online persistence can be achieved through unnecessary access, account management, or a web shell. Addresses may be accessed by reference search, brute force etc. Another important phase for an attacker is to bypass the security system (IDS, IPS, firewall, etc.). This can be done through proxy links and files or information abuse. The solution includes using ML techniques like NB, K-means and SVM to analyze logs generated by IDS/IPS to detect the possible APT attack patterns, analysis of system logs.

D. Set data extraction channels

This step creates a connection to the attacker's command-and-control (C&C) server and sends all the collected information, typically in compressed and encrypted form to limit packet size. Data is usually transferred for several hours when low network bandwidth is used. Attackers use quick flow techniques to make connections. Network stores target data and sends to the C&C server when the target is ready, or it can be sent in a small package at different time. Data collection methods include automatic collection, email collection, and data entry in the browser. A solution for detecting data transfers to C&C servers with data encrypted using machine learning methods. Connections to random IP addresses and DNS encrypted data flow to unknown or unauthorized servers. APT can be detected using the k-NN and k-mean algorithms.

E. Eliminate footprints

Once the mission is completed by the attacker, next step is to eliminate all traces of network attacks and threatened systems. Traces are maintained as compressed files, logs, or malicious files to be recovered. When an attacker reaches this phase, organization may not be aware that they have been hacked and attacked using APT. As a result, it becomes difficult to determine what level of information an attacker has extracted and the duration it remains on the network. Therefore, the attack needs be detected early.

The proposed Five-step model is well suited to APT attacks. Passive phase are the initial and final steps in the proposed model since in majority cases they do not represent an actual attack. The three active phases of the model are identified as the most commonly used attack techniques and possible mitigation measures. It is significant to know that any organization should contain security policies in their infrastructure of cybersecurity plans, given the need to notify users regularly. Another benefit of the proposed solution is that at all levels attacks are considered. Unlike other models studied, where the studies proposed a life cycle, but APT detection occurs only at one stage of the life cycle. Also, this phase does not always coincide with the first phase of the cycle. Step-by-step identification of potential attacks in the model can help predict such anomalous behaviors in the network, making it easier to detect APTs.

In [14] few suggestions are given to use before and after ransomware infection happens, they are:

- Create backup
- Avoid all spam links. Protect yourself from malicious ads with an ad blocker. Disable plug-ins like Java and JavaScript.
- Capture and block All operating systems, browsers and security systems must be constantly updated and update third-party plugins such as Java and Flash.

- Discharge and scroll when system detects any signs of infection, it is necessary to immediately turn off the infected system to reduce the infection, and if this system is online, the network should also be disconnected. Very few case studies confirm ransomware attack.

Based on the case study, few suggestions were made to deal with ransomware, such as

- To prevent ransomware attack, the first step is, the operating system needs to be updated.
- Do not use an unsupported operating system.
- If you do not have an updated anti-virus program on your system, the information from step 1 is meaningless, so it is better to use a good quality anti-virus for your system.
- After removing all malware/spyware, cleaning of spam folder is required.
- Opening JavaScript files and websites is dangerous, so disable them once all security measures are done.

In [15] several best practices to prevent ransomware attacks are mentioned.

- Update with the latest operating system, third-party software (MSOffice, browsers and browser plug-ins). Disable remote desktop connection.
- Turn on personal firewall on your workstation.
- Keep your anti-virus software up to date on all systems.
- Strict policy for external devices (USB devices).
- Restricts user rights to install and run inappropriate programs. Block attachment types: exe/pif/tmp/url/vb/vbe/scr/reg/cer/pst/cmd/bat/dll/hlp/hta/js/wsf
- The contents of the database backup files are checked daily for unauthorized encrypted content from data records or external elements, trunks, and malicious scripts.
- Set up access control with fewer privileges to access files, directories, and network resources.
- Configure the Enhanced Mitigation Experience Toolkit installation for a similar level of protection at the host level.
- Microsoft product macros are disabled.

Some of the specific counter measures to prevent Ransomware attack are:

- Symantec and Trend Micro offices are not supported on Windows XP. Update to the latest version of the operating system.
- Use Microsoft security solutions to prevent ransomware infections like Microsoft Security Bullet in MS17-010.
- Back up of important data regularly to avoid data loss. Disable SMBv1 or block SMB ports (UDP 137138 and TCP 139445). Activate the anti-virus IDS/IPS function to prevent attacks.

Research Studies in [24] proposed a solution using hybrid technologies to detect zero-day malware. The methodology consists of four steps. First, we collect samples of known malware related to our data set and analyze the data collected. In the second step, correlation algorithms were used to create relationships between malware and predict future malicious software variants. Final step used malicious software detection methods to train and detect malware. The four steps are detailed as follows 1. Malware data sets: To train the system, they needed to collect a dataset of corrupted or previously detected malware. Malware datasets were collected from a variety of online sources. 2. Machine Learning/Artificial Intelligence tools are used to analyze data sets collected by malware. 3. Correlation Algorithm: Correlation between different datasets of malware allows to predict or estimate future outcomes. 4. Detection method: Detection algorithm is used to detect patterns and train the system to detect the unknown like zero-day exploit. 5. Rstudio Desktop: Integrated development environment (IDE) is a free open source for R, a programming language for statistical data processing and graphics. To search and load datasets it has graphical tools like add-in include datasets. load. This helps to analyze malware data sets.

V. CONCLUSION

This survey paper summarizes, analyzes, categorizes and compares the data set, algorithm and methodologies of several types of cyber –crime attacks. The existing solutions may have flaws due to the sophisticated and complicated cyber threads, in order to overcome these attacks a clear understanding of crimes and solutions are required. Cyber security is the practice of protecting sensitive systems and confidential information from attacks and cybercrimes. Cybersecurity is designed to counter threats to systems and network applications, whether these threats come from inside or outside the organization. The study provides knowledge of various types of cyber-attacks such as malware, phishing, zero-day exploit, Advanced Persistent Threat (APT), methods to detect attacks and preventive solutions to avoid them.

ACKNOWLEDGMENT

The authors would like to acknowledge BMS college of Engineering and TEQIP III phase for their immense support in carrying out and encouraging this research work.

REFERENCES

1. Buch, Rachna, et al. "World of Cyber Security and Cybercrime." (2017).
2. Al-Mohannadi, Hamad, et al. "Understanding awareness of cyber security threat among it employees." 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE, 2018.
3. Vayansky, Ike, and Sathish Kumar. "Phishing–challenges and solutions." Computer Fraud & Security 2018.1 (2018): 15-20.
4. Shankar, Akarshita, Ramesh Shetty, and B. Nath. "A Review on Phishing Attacks." International Journal of Applied Engineering Research 14.9 (2019): 2171-2175.
5. Gautam, Bhawana, Jyotiraditya Tripathi, and Satwinder Singh. "A Secure Coding Approach For Prevention of SQL Injection Attacks." International Journal of Applied Engineering Research 13.11 (2018): 9874-9880.
6. Floderus, Sebastian, and Linus Rosenholm. "An educational experiment in discovering spear phishing attacks." (2019).
7. Hejase, Hussin J., Hasan F. Fayyad-Kazan, and Imad Moukadem. "Advanced persistent threats (APT): An awareness review." Journal of Economics and Economic Education Research 21.6 (2020): 1-8.

8. Quintero-Bonilla, Santiago, and Angel Martín del Rey. "A New Proposal on the Advanced Persistent Threat: A Survey." Applied Sciences 10.11 (2020): 3874.
9. Kim, Tae Hyun, and Douglas Reeves. "A survey of domain name system vulnerabilities and attacks." Journal of Surveillance, Security and Safety 1.1 (2020): 34-60.
10. Maurya, A. K., et al. "Ransomware: evolution, target and safety measures." International Journal of Computer Sciences and Engineering 6.1 (2018): 80-85.
11. A Study of Ransomware Detection and Prevention at Organizations Saurabh Kumar Sen1, Nidhi Chourey2
12. Pandey, Abhishek Kumar, et al. "Trends in Malware Attacks: Identification and Mitigation Strategies." Critical Concepts, Standards, and Techniques in Cyber Forensics. IGI Global, 2020. 47-60.
13. Joshi, Chanchala, Umesh Kumar Singh, and Dimitris Kanellopoulos. "An enhanced framework for identification and risks assessment of zero-day vulnerabilities." International Journal of Applied Engineering Research 13.12 (2018): 10861-10870.
14. Patidar, C. P., and Harshita Khandelwal. "Zero Day Attack Detection Using Machine Learning Techniques." (2018).
15. Rao, Routhu Srinivasa, and Syed Taqi Ali. "A computer vision technique to detect phishing attacks." 2015 Fifth International Conference on Communication Systems and Network Technologies. IEEE, 2015.
16. Shankar, Akarshita, Ramesh Shetty, and B. Nath. "A Review on Phishing Attacks." International Journal of Applied Engineering Research 14.9 (2019): 2171-2175.
17. Verma, Rakesh, Narasimha Karpoor Shashidhar, and Nabil Hossain. "Automatic phishing email detection based on natural language processing techniques." U.S. Patent Application No. 14/015,524.
18. Chen, Yi-Shin, et al. "Detect phishing by checking content consistency." Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014). IEEE, 2014.
19. Zareapoor, Masoumeh, and K. R. Seeja. "Text mining for phishing e-mail detection." Intelligent Computing, Communication and Devices. Springer, New Delhi, 2015. 65-71.
20. Sankhwar, Shweta, Dhirendra Pandey, and R. A. Khan. "A Novel Anti-phishing Effectiveness Evaluator Model." International Conference on Information and Communication Technology for Intelligent Systems. Springer, Cham, 2017.
21. Shankar, Akarshita, Ramesh Shetty, and B. Nath. "A Review on Phishing Attacks." International Journal of Applied Engineering Research 14.9 (2019): 2171-2175.
22. Okunoye, O. B., N. A. Azeez, and F. A. Ilurimi. "A Web enabled Anti-phishing solution using enhanced Heuristic based technique." (2017).
23. Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications surveys & tutorials 18.2 (2015): 1153-1176.
24. Patidar, C. P., and Harshita Khandelwal. "Zero Day Attack Detection Using Machine Learning Techniques." (2018).

AUTHORS PROFILE

Preetha S, working in the capacity of Assistant Professor, in the Department of Information Science and Engineering. She obtained her B.E. in Computer Science and Engineering from BMS College of Engineering. She is an Alumni of BMSCE serving for the institution since 2007. She also received M.Tech in Computer Network Engineering from Dayanand Sagar College of Engineering, affiliated to Visvesvaraya Technological University, Belgaum. She has over 13 years of Teaching Experience and have registered for Ph.D.,(VTU). Her research area is Biometric Authentication for Wireless Sensor Networks. She has several publications to her credit in her research area as well as IoT, Networks and Block chain.

P. Lalasa, final year student of Information Science and engineering, BMS College of Engineering, Bangalore affiliated to Visvesvaraya Technological University, Belgaum .She pursued her per-university from Shri Bhagawan Mahaveer Jain college, vv puram Bangalore, under Karnataka State Secondary Education Examination Board and completed her schooling in Sree Rama Vidyalaya. She has worked at Peacock solar with Web Developer role as an intern .She has worked on various projects throughout the academics of Engineering. The projects were based on various programming languages like Java, C++, C .She is Certified and appreciated for "Eco-Club Generation" 2017 .Her interests include Computer Networks ,Machine learning, data mining and software engineering.

Pradeepa R, final year student of Information Science and engineering, BMS College of Engineering, Bangalore affiliated to Visvesvaraya Technological University, Belgaum. She finished her schooling from ST. Mira's High School, Rajajinagar, Bangalore. She obtained her NCC A certificate during schooling. She pursued her per-university from MES PU college, Malleshwaram, Bangalore under Karnataka State Secondary Education Examination Board. She has worked on various projects throughout the academics of Engineering. The projects were worked on various programming languages like Java, C++, C. Her interest to publish this paper came up as the cyber threats are increasing and becoming more sophisticated day by day. Her interests include Computer Networks, Machine Learning.