TITLE: REVIEW PAPER ON PHISHING ATTACKS

Aathi oli .S Mohammed Raeesul irfan C. Vijayalakshmi
oliaathi@gmail.comphilosuave@gmail.comvijayalakshmi@crescent.education
B. S. Abdur Rahman CrescentB. S. Abdur Rahman Crescent B. S. Abdur Rahman Crescent
Institute Of Science Institute Of Science Institute Of Science
And Technology. And Technology.And Technology.

ABSTRACT

Phishing may be a cybercrime, which involves luring the user into providing sensitive and confidential informa- tion to the attacker. the data could include mastercard details, username and passwords, bank details, etc. After obtaining the knowledge, the attacker could commit crimes like financial losses and identity thefts. The target might be a private, a corporation or a cluster in a company. This paper provides an evidence on phishing attacks to make awareness and several other countermeasures to beat them.

Keywords: Phishing, deceptive and spear phishing, whaling, pharming, anti-phishing techniques.

1.INTRODUCTION

A field of knowledge Technology is Cyber Security that aims at the protection of knowledge, systems, network, etc., from the varied attacks. Cyber Security is one in all the key concerns in today‘s information technology world. It also aims at the prevention of unauthorized access to sensitive data. Data is prone to various attacks while in transit and while stored. These attacks, both existing and upcoming, pose a wonderful threat to industries and individuals. Since, industries rely heavily on computers for his or her functionalities, confidential and sensitive information must be protected. Various Cyber Security techniques and tools provide this protection of knowledge while it's stored and in transit.

The threats and vulnerabilities, together with the value of detecting and fixing the bugs, have consistently been increasing over the past 20 years. This has led to loss of holding, loss of reputation and revenue, transmission of security vulnerabilities, etc. the price encountered for overcoming such security attacks have escalated from $27.4 billion to $66 billion in eight years.

The attackers use various methods like loophole in applications as gateway to require advantage of the vulnerabilities, which help them to understand unauthorized access to sensitive data.

Phishing involves sending fraudulent emails to a target that appear to come back from a creditable source. a private or several individuals called phishers or attackers orchestrate the attack. The individuals who are stricken by the attack are called victims or targets. The goal of phishing is to collect sensitive data, like login credentials or checking account details or install malware into the target‘s system. Investigating such a fancy attack is extremely challenging to the cybersecurity experts. Phishing attacks are often performed manually but to over- come the attack and to reply effectively to the attack requires a lot of some time , intelligence and manpower. this could take days or perhaps weeks to reply and analyze the attack thorough. Manual investigation has lot of dependency on the safety analyst‘s talents and tools avail- able for investigation. Moreover, these manual investigations get it wrong because of human errors.
Commonly called the Amazon Prime Day phishing attack, the knowledge of the shoppers of Amazon was compromised by a phishing attack. All the Amazon Prime members received an email that consisted of seemingly legitimate deals to them. On trying to get the ’deals‘, the transaction would fail, promoting the attackers to achieve sensitive information on the user.

Another common example is Google Docs invitation. In May 2017, attackers sent fraudulent invitations to google users across the globe to edit documents. When the recipients clicked the invitation, it led to a third party app that facilitated attackers to urge tip .

2. PHISHING MECHANISM

The motive of phishing attack is to govern the attacker into providing lead about him/her. To perform such an attack, the attacker or phisher mimics a legitimate website. To mimic the web- site, he/she constructs a malicious site employing a phishing website. This phishingwebsite would gather all the in- formation on the target and provide it to the attacker [11]. Usually, the targets are unable to differentiate between genuine and phishing websites causing them to constitute the traps set by the phisher.

Phishing attacks have several steps that attackers follow to get information. this may be explained in six steps. The steps are as follows:
Plan
Compose email
Attack
Gather data
Fraud

The attacker starts the strategy by planning the attack. This step involves when deciding the legitimate website that must be imitated and also the victim whose information should be gathered. Followed by planning, is composing an email that should appear genuine for the victim to be lured into providing his/her data. The third part is sending the composed email to the target followed by gathering the knowledge on the victim. The gathering of in- formation phase occurs as long because the victim has been tricked by the phisher. Using the victim‘s information, the attacker commits cybercrimes like mastercard fraud, theft, etc.It shows several steps involved within the attack.

This email consists specified it appears to be genuine and legit. In step 2, the attacker sends this composed email to the victim (target). Step 3 indicates that the victim, unable to differentiate between genuine emails and phishing emails, tends to open the e-mail . the e-mail then directs her to the phishing website. The victim enters her login credentials within the webpage oblivious of the actual fact that it is a malicious site. The phishing website then pro- vides the login credentials to the attacker. this is often illustrated in step 4. within the last step, the phisher, using the information he has obtained from the phishing website, logs into the target website. Now, he would be able to access all the data of the victim. Thus, the method of phishing is completed.

3.SORTS OF PHISHING ATTACKS

The attack may be performed in several ways. The mo- tive for all the kinds are the identical. the sole variation amongst the categories are the quantity of targets and also the mechanism accustomed obtain the info.
The various forms of phishing attacks are [12]:
Deceptive Phishing
Spear Phishing
Whaling
Pharming

3.1 Deceptive Phishing

Deceptive phishing is that the most prevalent kind of phishing attack. It involves imitating a legitimate website and sending an email to the target appearing it to be genuine. the e-mail sent would contain a malicious URL or link. it might instruct the target to click on the URL. Upon following the instruction, the phishing website gathers all the login credentials and other sensitive information about the target and forwards it to the attacker [11].

For example, testuser@amazon.com uses a lowercase ’a ‘that might be removed. Hence, testuser@mazon.com could trick the target and thereby obtain data.

3.2 Spear Phishing

This sort of phishing is almost similar to deceptive
phishing. the sole difference is that the target. Unlike deceptive phishing, spear phishing targets one individual only. The attacker aims at one person and lures him/her into providing confidential data. The fraudsters customize the e-mail consistent with the individual. the e-mail would consist a number of the target‘s information like the person‘s name, company he/she is functioning in, designation, etc. the foremost common platforms where spear phishing takes place is social media sites like LinkedIn where it's easy for them to get
information on the individual‘s profession [2].

3.3 Whaling

Whaling attacks occur when the phisher targets a private at an executive position like CEO. The attacker would be profiling the victim for a substantial period before performing the attack. The attacker, almost like other types, would send an email to the target and manipulate him/her into providing information to the attacker. Whaling is taken into account a really dangerous attack since the people in executive bands have access to the organization‘s most hint.

3.4 Pharming

Pharming is another variation of phishing. Unlike, the opposite techniques, it's not necessary to focus on individuals. The attack can victimize an oversized number of individuals with- out having to be targeted individually.

Pharming is performed in two ways:

The first method involves a code that's sent to the target via email that modifies all the local host files within the system. The URLs would be converted by the host files to number strings, utilized by the system to access websites. This causes the target to be redirected to the malicious site in spite of entering the right URL.

The second method of performing pharming is thru a method called DNS Poisoning. during this method, the system‘s local host files aren't corrupted but the name system table is modified. This leads to the target being redirected to malicious websites without their knowledge. The target would be assuming they're accessing the legitimate websites, but thanks to DNS Poisoning, they might be accessing the malicious website.

Thus, the motive for all the variations of phishing are the identical. Only the tactic and therefore the technique accustomed obtain the data varies from one type to a different.

4. ANTI-PHISHING TECHNIQUES

In [1], an answer was proposed where Automated Individual White-List (AIWL), an automatic list, attempts to keep up a white list that consists of each familiar Lo- gin User Interfaces (LUI) of the user‘s. When a user submits his/her login credentials or sensitive information to a LUI that's missing from the white-list, AIWL will warn the user of the possible trap and can warn him/her of the ensuing attack.

In [2], the authors proposed an answer to defend phishing attacks employing a combination of visual similarity based techniques and white list. the pc Vision (CV) tool called Speed up Robust Features (SURF) detector. This detector uses square shaped filters for extracting discriminative key point features. These features are extracted from both – suspicious and genuine web- sites. The features extracted from the websites are then compared for calculating a similarity degree. The similarity degree then helps in determining if the web site is legitimate or not. If the similarity degree was high, it had been considered malicious since the legitimate website was trying to be imitated.

In [3], a special solution was proposed by the employment of Support Vector Machines (SVM) to detect if the mail is malicious or not. The SVM extracted common characteristics of the mail like language used, layout of the mail, structure of the mail, etc. It then compares the extracted details with the small print present within the system to test the similarity accuracy. If the accuracy exceeds a specific threshold, it marks the e-mail as malicious.

The study conducted in [4] used a singular technique of language Processing (NLP) to work out if the mail was malicious or not. during this paper, they extracted and compared common characteristics using NLP tools. PhishNet-NLP utilized tongue techniques together with all information present in an email, namely the header, links, and text within the body. PhishSnag used information extracted from the e-mail to detect phishing. Phish-Sem used NLP and statistical analysis on the body for labelling the mail as phishing or non-phishing.

A more advanced technique of filtering and classification was utilized in [5]. during this paper, the authors tested the URLs and verified whether it absolutely was malicious or not. They used an automatic approach for detecting phishing. It had two phases- Pre-filtering and Classification phase. within the pre-filtering phase, the URL was compared against a black list using the domain a part of the URL. If the URL was present in this list then it absolutely was classified as malicious and wouldn't be proceeding to the Classification Phase. within the next phase, two main features were checked for consistency- Randomness of the URL (RU) and therefore the Position of the domain token. supported the results of Classification Phase, the URL was classified as malicious or non-malicious.

In [6], the authors used text mining to extract distinct features from emails. The emails could be phishing or genuine emails for better detection of the attack. The strategy followed was an initial conversion of the email to a vector representation followed by feature selection techniques for classification. The evaluation was per- formed using data sets accumulated from the HamCorpus of SpamAssassin project (legitimate e-mail) and the publicly available PhishingCorpus (phishing e-mail).

The extraction and classification method was further developed in [7]. In this paper, the vulnerabilities were differentiated into three categories based on the structure of the email. The three categories were Page-content vulnerability, Domain vulnerability and Code-scripting vulnerability. The evaluator model used was Anti-Phishing

Effectiveness Evaluator Model (APEE Model) which is used to analyze the effectiveness of the Anti-Phishing Mechanisms that have been implemented. The reputation of the vulnerabilities from the three categories are tested which help in determining whether the mail is a phishing email or not.

The method used in [8] is marginally different from the other techniques. In [8], they classify the mails as junk or not junk based on the spam filter. When an email arrives to the mailbox, the spam filter performs its filtering function and verifies if the mail is spam or not. The spam filtering is performed based on the reputation of the URL present in the mail. If the URL seems to be unsafe or suspicious, the filter marks the mail as 'junk'. The URL(s) in the mail are deactivated and the mail is then moved to junk. If the mail is genuine, the mail is moved to inbox for the user to open it safely.

In [9], Anti-phishing technique was developed with the help of advanced heuristic approach. In this technique, when a suspicious website was encountered, it was immediately updated in the black list. If a legitimate web- site is found, it updates the same in the white list. There- fore, when the user open a website, it was first verified if the website was a phishing website or not and accordingly provided access to the same. This technique used PHP Programming Language along with a Database to maintain the two lists. According to this technique used, 2519 URLs were tested and 2510 were correctly classified.

The authors talk about reusable components for anti-phishing components layer in [10]. These reusable components are used for converting webpages to feature vectors using heuristic methods and external repositories. The finite feature vectors that provide as input to these vector machines train the support vector machine. With the training provided by these
inputs, the support vector machine classified and determined various web pages as legitimate or a phishing web page. This was experimented with the mixture of heuristics in identifying a phishing webpage.

5. CONCLUSION

Phishing is a technique to gather sensitive information about the target using malicious links and emails. It is one of the most dangerous cyber-attacks that occurs in organizations, personal devices, etc. It is often difficult to distinguish between genuine emails and phishing emails. There are several methods that can be used to avoid this attack. Periodical updating of anti-phishing tools and platforms can prove to be very powerful. This study provides an in-sight to phishing, the mechanism of the attack, various forms it can occur in and the possible solutions to overcome them.

REFERENCES

[1] Ye Cao, Weili Han and Yueran Le - Anti-phishing based on automated individual white-list, Proceed- ings of the 4th ACM workshop on Digital Identity Management, pp. 51-60, October 2008.

[2] Routhu Srinivasa Rao and Syed Taqi Ali - A Com- puter Vision Technique to Detect Phishing Attacks, 5th International Conference on Communication Systems and Network Technologies, IEEE, October 2015.

[3] Madhusudhanan Chandrasekaran, Krishnan Narayanan and Shambhu Upadhyaya - Phishing E- mail Detection based on Structural Properties, IEEE, November 2015.

[4] Rakesh Verma, Narasimha Karpoor, Nabil Hossain and Nirmala Rai - Automatic Phishing Email De- tection based on Natural Language Processing Techniques, Research Gate, 2016.

[5] Yi-Shin Chen, Huei-Sin Liu, Yi-Hsuan Yu and Pang- Chieh Wang, Detect Phishing by Checking Content Consistency, IEEE, 2017.

[6] Masoumeh Zareapoor, K.R. Seeja, Text Mining for Phishing E-mail Detection, Intelligent Computing, Communication and Devices: Advances in Intelli- gent Systems and Computing, vol. 308, pp. 65-71, August 2016.

[7] Sankhwar S., Pandey D., Khan R.A - A Novel Anti- phishing Effectiveness Evaluator Model, Smart Innovation, Systems and Technologies, Springer, vol 84, Cham, 2018.

[8] Xavier Joseph, Mitchell Aime M, Tsang Brian J, Herbert, George A, Savastano, Hernan I, Khandel- wal Lubdha, Pengelly Robert C. J, Novitskey Robert, Grant Stanley - Anti-phishing protection, United States Patent 10,069,865 B2, Sept 4th, 2018.

[9] Okunoye, O.B, Azeez, N.A, Ilurimi F.A - A Web Enabled Anti-Phishing Solution Using Enhanced Heuristic Based Technique, FUTA Journal of Re- search in Sciences, vol. 13 (2), pp. 304-321, Octo- ber – 2017.

[10] Anna L. Buczak, Erhan Guven - A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communica- tions Surveys & Tutorials, vol. 18, pp. 1153-1176, June – 2016.

[11] Dr. Radha Damodaram - Study on Phishing Attacks and Anti-Phishing tools, International Research Journal of Engineering and Technology (IRJET), vol. 3, pp. 700-705, January – 2016.

[12] Gaurav, Madhuresh Mishra, Anurag Jain - Anti- Phishing Techniques: A Review, International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 350-355, April – 2012.

[31]Akbarzhon Madaminov, “Recommendation Systems”, Engpaper Journal

[32]Aathi oli.S , “REVIEW PAPER ON PHISHING ATTACKS”, Engpaper Journal

[33]Rania Fernando, “IoT based – Street Light Controlling System”, Engpaper Journal

[34]K. SAI BHARGAV, V. RAJENDRA, “Study on Data Structures for Machine Learning”, Engpaper Journal

[35]Brundha P, Guruprasad K N, Amith V Hiremath,Sirisha R, Chandrakanth G Pujari , “Face Detection Based Smart Attendance System Using Haar Cascade Algorithm”, Engpaper Journal

[36]Afsana Nadaf , “RFID BASED LIBRARY MANAGEMENT SYSTEM”, Engpaper Journal

[37]Mr. Vedant Thube, Neha Thakur, Mr. Siddhesh Balsaraf,Ms. Priyanka Hanchate, Dr. S. D. Sawarkar , “Accident Prevention using Eye Drowsiness & Yawning Detection”, Engpaper Journal

[38]Abhishek A Hishobkar, Rutuja Gaonkar, Jagdish Chintamani , “DIGITAL DIARY”, Engpaper Journal

[39]Pooman Suryavanshi, Aryan Ghadge, Manali Kharat , “TAXI SERVICE for VISUALLY IMPAIRED”, Engpaper Journal

[40]Mr. Pankaj yadav, Shila Jawale, Mr. Ashutosh Mahadik, Ms. Neha Nivalkar, Dr. S. D. Sawarkar , “NEWS ARTICLES CLASSIFICATION”, Engpaper Journal

[41]Rahul Chavan, Manvee Bhoir, Gaurav Sapkale, Anita Mhatre, “Smart Tourist Guide System”, Engpaper Journal

[42]Rutik Desai, Akash Jadhav,Suraj Sawant ,Neha Thakur , “Accident Detection Using ML and AI Techniques”, Engpaper Journal

[43]Anagha Vishe,Akash Shirsath, Sayali Gujar, Neha Thakur , “Student Attendance System using Face Recognition”, Engpaper Journal

[44]Ms.Sayali Patekar, Shila jawale, Ms.Pranali Kurhade, Mr.Shubham Khamkar , “Smart Classroom Application”, Engpaper Journal

[45]DOSHI SAKSHI, DEVYANI CHAUDHARI, POOJA GAIKWAD, RUTUJA CHABUKSWAR,MRS. SUJATA KOLHE, “TOURISM SIMPLIFIED THROUGH VOICE”, Engpaper Journal

[46]Afreen Fathima,Samreen Jameel, Pathan Ahmed khan , “ACCIDENT DETECTION AND ALERTING SYSTEM”, Engpaper Journal

[47]Suman Zareen, Tuba Masood, Pathan Ahmed khan, “E-Commerce Web Application with Augmented Reality”, Engpaper Journal

[48]Lok Shan CHAN, “Selection of Waterfall and Agile Methodologies in Software Testing”, Engpaper Journal

[49]Barve Rutu, “CLOUD COMPUTING SYSTEM FOR GAMING”, Engpaper Journal

[50]Harshvardhan Singh, “Machine Learning: Fake News Blocking”, Engpaper Journal

[51]M.Al Batahari, “SERVERS ROOM MONITORING SYSTEM USING IOT”, Engpaper Journal

[52]AYUSHI ANKITA RAKSHIT, “VIRTUAL MASTER USING PYTHON”, Engpaper Journal

[53]Baldeep Kaur, “REAL TIME SLEEP DROWSINESS DETECTION USING FACE RECOGNITION”, Engpaper Journal

[54]Suchitav Khadanga, “Two Stage CMOS Operational Amplifier From Specification to Design”, Engpaper Journal

[55]nidhi sharma, “Introduction to Remote Sensing”, Engpaper Journal

[56]Rohith N Reddy, “COVID-19 Detection using SVM Classifier”, Engpaper Journal

[57]Swapnil Kole, “COVID-19 Database on Consortium Blockchain”, Engpaper Journal

[58]TejalLengare, PallaviSonawane, PrachiGunjal, ShubhamDhire, Prof.Shaikh.J.N , “Accident Detection & Avoidance System in Vehicles”, Engpaper Journal

[59]Abhishek Pawshekar, Deepti More, Akash Khade, Pratiksha Wagh, Ganesh Ubale, “Augmented Reality: to converting and placing object into 3D model”, Engpaper Journal

[61]Prof.Ubale.G.S, Pranjal Adhav,Pooja Gaikwad, Sushama Nadavade ,Pooja Kale , “Iot based Bridge Monitoring System”, Engpaper Journal

[62]Divya Deewan, Priyanka Maheshwari, Sanjay Jain, “A REVIEW OF BATTERY-SUPERCAPACITOR HYBRID ENERGY STORAGE SYSTEM SCHEMES FOR POWER SYSTEM APPLICATION”, Engpaper Journal

[63]Prof.Ansari.M.B, Pranjal Adhav,Pooja Gaikwad,Sushama Nadavade,Pooja Kale, “Survey on MyHelper IOT based Bridge Monitoring System”, Engpaper Journal

[64]Shreyas.S.J, Saddam hussain, Chaithra E, “COMPARATIVE STUDY ON SEISMIC RESPONSE OF MASONRY INFILLED RC FRAME BUILDINGS AND MIVAN BUILDINGS WITH DIFFERENT PERCENTAGE OF WALL OPENINGS”, Engpaper Journal

[65]Yusuf Ali Hassan, “Somali Power-Grid Significant Challenges”, Engpaper Journal

[66]Ahmed N. Elhefnawy, “Refractive IR Objective Optical Design Operating in LWIR band For Military Observation Applications”, Engpaper Journal

[67]S MANJULA, D SELVATHI and SUCHITAV KHADANGA, “Design of low-power CMOS transceiver front end for 2.4-GHz WPAN applications”, Engpaper Journal

[68]Suchitav Khadanga, “Fabrication of MEMS Pressure Sensor on thin film membrane”, Engpaper Journal

[69]Suchitav Khadanga and Dr. K.R.Suresh Nair, “An Introduction to Bluetooth”, Engpaper Journal

[70]Suchitav Khadanga and S. Ahmad, “DESIGN AND FABRICATION OF LOW COST MICROWAVE OSCILLATOR”, Engpaper Journal

[71]Ameen Ahmed, Noushad S, Suchitav Khadanga, K.R.Suresh Nair, P.K.Radhakrishnan, “DEVELOPMENT OF LOW PHASE NOISE SMALL FOOT PRINT SURFACE MOUNT VOLTAGE CONTROLLED OSCILLATOR”, Engpaper Journal

[72]Suchitav Khadanga , “Synchronous programmable divider design for PLL Using 0.18 um cmos technology”, Engpaper Journal

[73]Kavya.G.R, Shivaraju.G.D, Dr. T V Mallesh, S R Ramesh, “PROGRESSIVE COLLAPSE RESISTANCE OF FLAT SLAB BUILDING”, Engpaper Journal