WEB PHISHING DETECTION A LITERATURE SURVUY

ABSTRACT

This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyberattacks are spread via mechanisms that exploit weaknesses found in end users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process. Phishing URL is a widely used and common technique for cybersecurity attacks. Phishing is a cybercrime that tries to trick the targeted users into exposing their private and sensitive information to the attacker. The motive of the attacker is to gain access to personal information such as usernames, login credentials, passwords, financial account details, social networking data, and personal addresses. These private credentials are then often used for malicious activities such as identity theft, notoriety, financial gain, reputation damage, and many more illegal activities. This paper aims to provide a comprehensive and comparative study of various existing free service systems and researchbased systems used for phishing website detection. The systems in this survey range from different detection techniques and tools used by many researchers. The approach included in these researched papers ranges from Blacklist and Heuristic features to visual and content-based features. The studies presented here use advanced machine learning and deep learning algorithms to achieve better precision and higher accuracy while categorizing websites as phishing or benign. This article would provide a better understanding of the current trends and existing systems in the phishing detection domain.

KEYWORDS: Phishing, Phishing Websites, Detection, Machine Learning

LITERATURE SURVEY

A phishing attack is one of the most serious threats for any organization and in this section, we present the work done on phishing attacks in more depth along with its different types. Initially, the phishing attacks were performed on telephone networks also known as Phone Phreaking which is the reason the term “fishing” was replaced with the term “Phishing”, *ph* replaced *f* in fishing. From the reports of the anti-phishing working group (APWG) [1], it can be confirmed that phishing was discovered in 1996 when America-on-line (AOL) accounts were attacked by social engineering. Phishing turns into a danger to numerous people, especially individuals who are unaware of the dangers while being in the internet world. In light of a report created by the Federal Bureau of Investigation (FBI) [2], from October-2013 to February-2016, a phishing attack caused severe damage of 2.3 billion dollars. In general, users tend to overlook the URL of a website. At times, phishing tricks connected through phishing websites can be effectively prevented by seeing whether a URL is of phishing or an authentic website. For the situation where a website is suspected as a targeted phish, a client can escape from the criminal’s trap The conventional approaches for phishing attack detection give low accuracy and can recognize only about 20% of phishing attacks. Machine learning approaches give good outcomes for phishing detection but are time-consuming even on the small-sized datasets and not scale-able. Phishing recognition by heuristics techniques gives high false-positive rates. Client mindfulness is a significant issue, for resistance against phishing attacks. Fake URLs are utilized by phisher, to catch confidential private data of the targeted victim like bank account data, personal data, username, secret password, etc Previous work on phishing attack detection has focused on one or more techniques to improve accuracy however, accuracy can be further improved by feature reduction and by using an ensemble model. Existing work done for phishing attack detection can be placed in four categories Presenting a literature survey of anti-phishing detection techniques, which incorporates software detection techniques as well as user-awareness techniques that enhance the detection process of phishing attacks. Presenting a comparison of the various proposed phishing detection techniques in the literature Presenting evaluation metrics that are commonly used in the phishing domain to evaluate the performance of phishing detection techniques. This facilitates the comparison between the various phishing detection techniques.

MITIGATION OF PHISHING ATTACKS

Due to the broad nature of the phishing problem, we find important to visualize the life-cycle of the phishing attacks, and based on that categorize anti-phishing solutions. Based on our review of the literature, we depict a flowchart describing the life-cycle of phishing campaigns from the perspective of anti-phishing techniques, which is intended to be the most comprehensive phishing solutions flowchart When a phishing campaign is started (e.g. by sending phishing emails to users) the first protection line is detecting the campaign. The detection techniques are broad and could incorporate techniques used by service providers to detect the attacks, end-user client software classification, and user awareness programs. More details are in Section IV-A. The ability to detect phishing campaigns can be enhanced whenever a phishing campaign is detected by learning from such experience. For example, by learning from previous phishing campaigns, it is possible to enhance the detection of future phishing campaigns. Such learning can be performed by a human observer, or software (i.e. via a machine learning algorithm). Once the phishing attack is detected, a number of actions could be applied against the campaign. According to our review of the literature, the following categories of approaches exist: Offensive defense — these approaches aim to attack phishing campaigns to render them less effective.

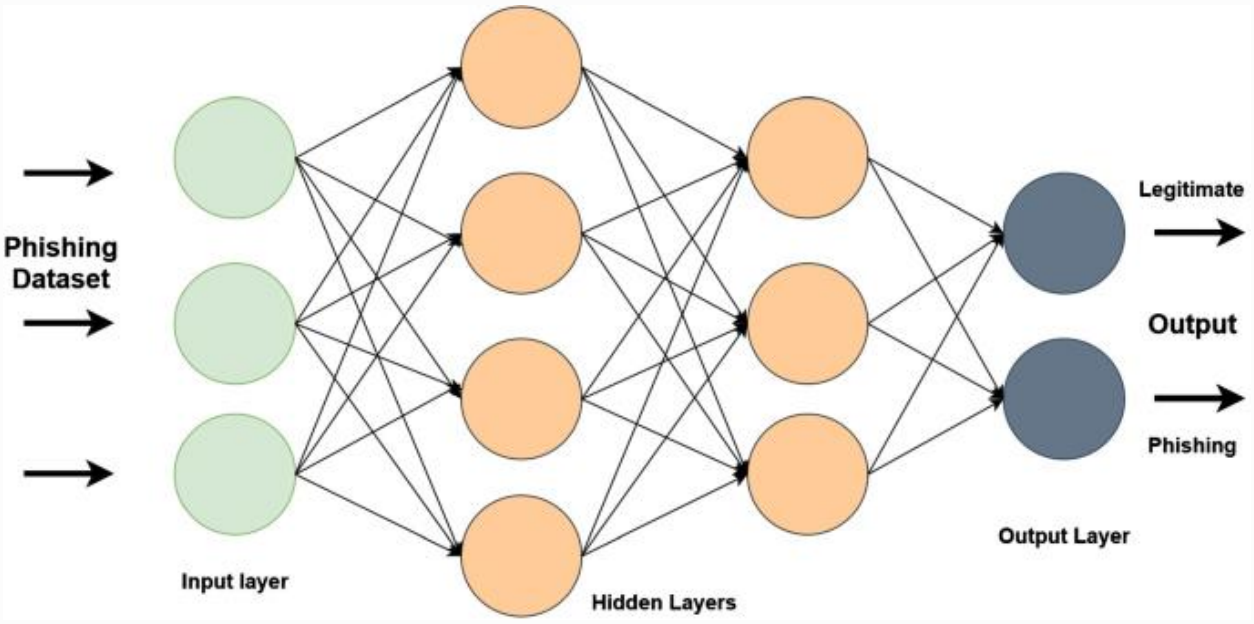

Fig:1.1 Phishing Dataset

EDUCATIONAL NOTICES

The evaluation in [3] also compared multiple approaches in educating users, such as text, annotated figure and comics. The study concluded that embedded comics were the most effective approach. The proposed system functions as follows:

• The e-mail administrator prepares a number of fake phishing emails.

• The phishing emails are communicated to the victims. No warnings are shown at this stage.

• Once the victim interacts with a phishing email, such as by clicking on a phishing link, the user is then shown a security warning teaching him the risks of phishing attacks.

• Training messages to be embedded into the daily activity of the user, without the need to read external sources (e.g. other websites or SMS).

• The warning message should clearly and concisely explain the causes; warning messages can fail if they have too much of textual data.

• The warning message should clearly and concisely explain proper actions to be taken by the end-user to enhance his/her security.

• The warning should not be delayed, but be shown immediately following the moment when the user falls as victim and clicks on an email link.

• The fake phishing messages used for training purposes should mimic closely phishing messages in the wild.

• Enhancing the security warning text with story-based comics enhances readability. However, the drawbacks of the proposed embedded training system are:

• The system requires a human administrator to craft the messages. This adds delay and increases the maintenance cost of the solution.

• Version 2 of the protocol divides the URL data into chunks and allows partial updates. Such partial updates were not available in version 1 of the protocol.

• Version 2 of the protocol does not always send full 256- bit hashes of blacklisted URLs to web browsers, instead it initially sends a list of 32-bit truncated forms of the hashes.

COLLABORATIVE INTRUSION DETECTION

Many phishing detection and prevention mechanisms are based on finding the source IP address of the attacker. Fast-flux [31], on the other hand, enables attackers to frequently change their IP addresses. By having a sufficient number of infected hosts (usually home users), hosts can behave as front-end proxies for phishing websites. Multiple front-end proxies relay the traffic back to a main phishing site to fetch the content from (also known as mothership). Load balancing is achieved by means of low Time to live (TTL) DNS A RR, which enables a quicker change of mapped IP addresses than if higher TTL values were used. Low TTL also helps in reducing the downtime when dead front-end proxies are removed. The DNS A RR are updated by the attacker through a fixed DNS NS RR. Although fast-flux has a fixed NS record pointing to the attacker's real IP address, double fast-flux complicates the task further by relaying DNS RR update to front-ends as well. A proposed solution to this is through the use of Collaborative Intrusion Detection System (CIDS) to exchange phishingrelated data among a number of Intrusion Detection Systems (IDSs). The distributed system should be installed globally. Each local CIDS should monitor its local DNS cache, and list DNS zones with a high number of DNS A RR that are combined with low TTL values. The list of IP addresses and domains are sent to global CIDS for further analysis. The proposed mechanism counts the number of connections to the front-end proxies (infected hosts), and distributes such numbers to global CIDS. If the threshold reaches a certain number, it would then be assumed that it is a connection to the mothership (since the mothership has one-to-many connections, it is assumed to have a high number of accumulated connections is toward the mothership. Connection count is not a definitive criteria since many phishing networks could also be globally This proposed solution has not been implemented yet due to difficulty in studying fast-flux or double fast-flux attacks due to their unrepeated nature so far. It also faces challenges in determining which connection connected to other legitimate networks (such as Internet Relay Chat (IRC) or game networks), from which they initially appeared. Thus, doing a simple connection count could lead into false positives.

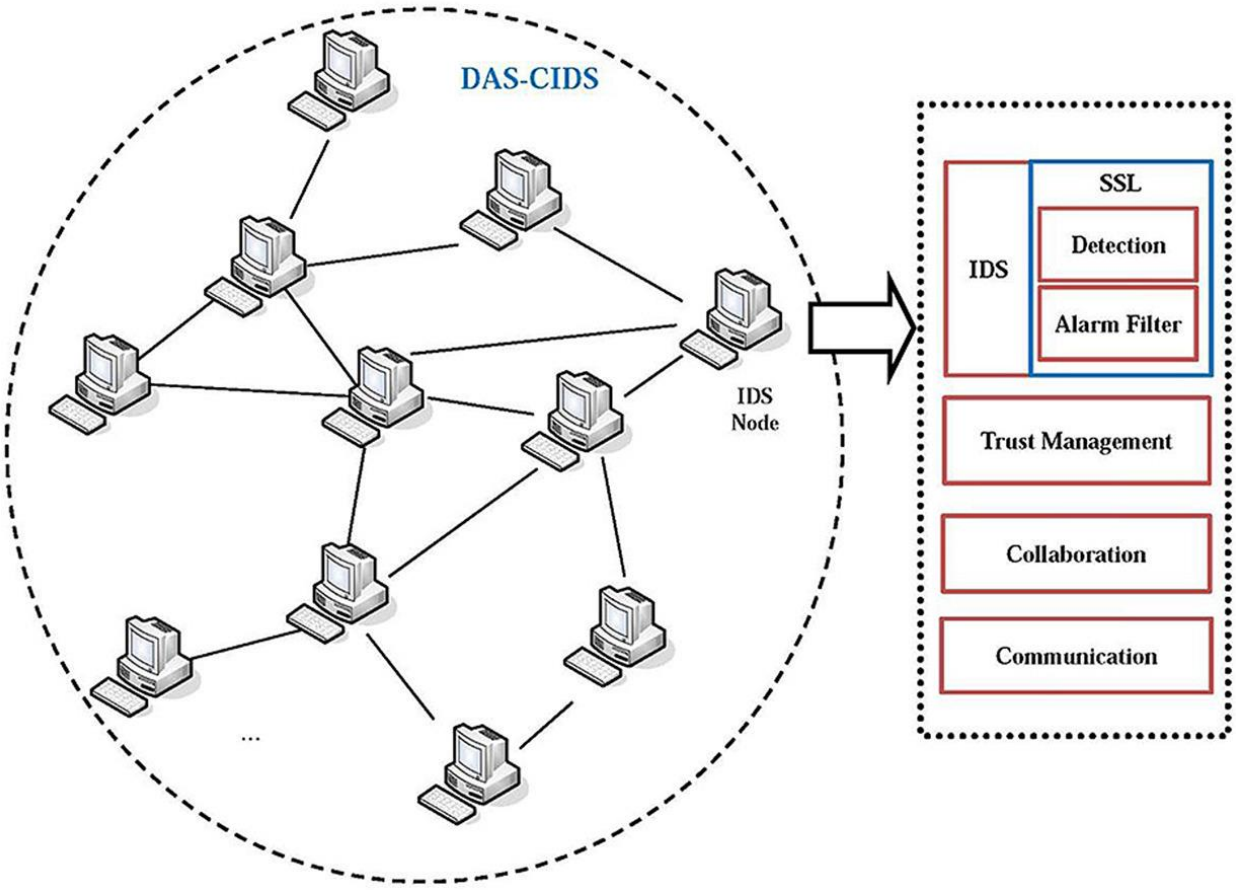

Fig:1.2 DAS-CIDS

The goal of the work in [39] is detecting phishing sites based on visual similarity without the need of whitelisting pictures of all legitimate websites, and is based on the fact that most phishing websites aim at being visually similar to their target websites (e.g. PayPal phishing websites aim to look visually similar to the legitimate PayPal website in order to maximize their chances of persuading more victims). To achieve the above objectives, the following steps are performed:

1) A list of previously known legitimate WL and phishing WP websites are processed to function as baseline for the classifier. Each of the sites are processed and stored in a database that presents each website by the following elements:

• A label (legitimate/phishing) that determines the class of the website.

• A screen-shot of the website as rendered by a web browser.

• The domain name of the website.

2) Each suspect website's (Ws) screen-shot (as rendered by a web browser) is taken and then used to find other websites in the database that have similar visual appearance. The visual similarity

search is performed by imgSeek16, which returns a number that reflects how similar an input image is compared to other images in the database. Using a threshold function, a crisp classification decision can be made.

3) Based on the outcomes of image Seek, Algorithm (2) is executed.

4) To reduce false positives, a whitelist of domain names is used.

LEVEL OF PHISHING RATES

According to APWG, phishing attacks were in a raise till August, 2019 when the all-time high of 90,364 unique1 phishing reports were submitted to APWG. The total number of submitted unique phishing websites that were associated with the 90,364 in between the month of **(January-September)** As justified by APWG, Global Phishing Rates overtime in the years 2004 and 2012 compared to that of the year 2019 was due to the disappearance of the Avalanche gang4 which, according to APWG's 2004 report, was responsible for 0.10% of world-wide phishing attacks in the 2nd half of 2012 [4]. In the 1st half of the year 2011, the total number of submitted phishing reports to APWG

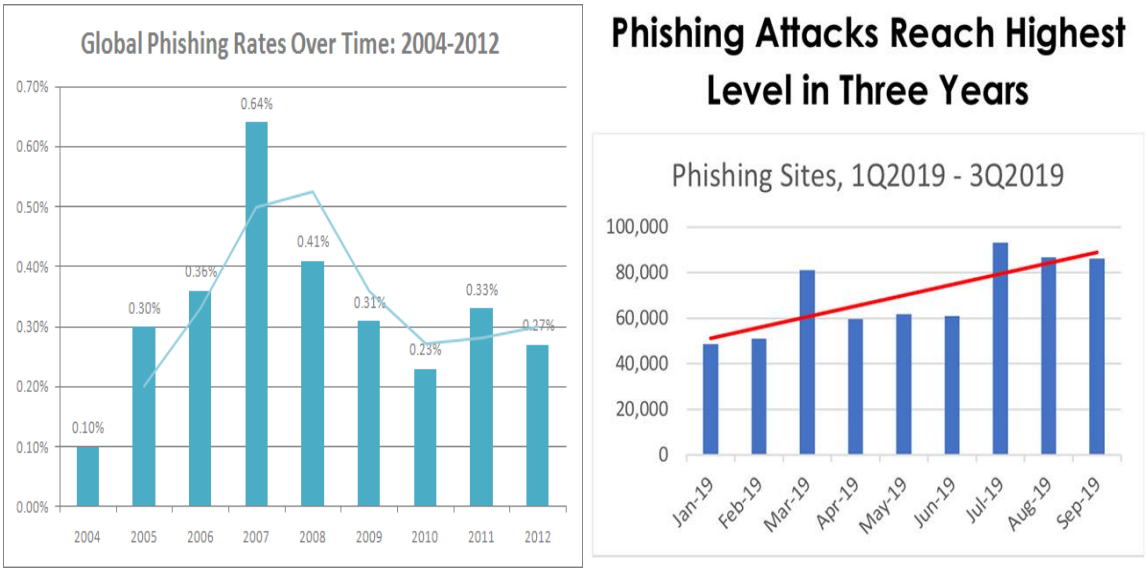

Fig:1.3 Overall Rates of Phishing Attack Scenario

• User education; the human is educated in an attempt to enhance his/her classification accuracy to correctly identify phishing messages, and then apply proper actions on the correctly classified phishing messages, such as reporting attacks to system administrators.

• Software enhancement; the software is improved to better classify phishing messages on behalf of the human, or provide information in a more obvious way so that the human would have less chance to ignore it.

• Phishing is a semantic attack that uses electronic communication channels to deliver content with natural languages (e.g. Arabic, English, French, etc. . .) to persuade victims to perform certain actions. The challenge here is that computers have extreme difficulty in accurately understanding the semantics of natural languages

CONCLUSION

User education or training is an attempt to increase the technical awareness level of users to reduce their susceptibility to phishing attacks. It is generally assumed that the addition of user education materials compliments technical solutions (e.g. classifiers). However, the human factor is broad and education alone may not guarantee a positive behavioral response. As shown in the previous sections, most of the educational materials were also associated with a decrease in the T N rate, with an exception of only one educational material, namely: Anti-Phish Phil. This shows that the addition of user training approaches is not always the right answer

• Low false positives. A system with high false positives might cause more harm than good. Moreover, end-users will get into the habit of ignoring security warnings if the classifier is often mistaken. Generally, software detection solutions are:

• Blacklists.

• Rule-based heuristics.

• Visual similarity.

• Machine Learning-based classifiers