Enterprise Credential Spear-phishing Attack Detection

Yuosuf Al-Hamar [1], Hoshang Kolivand [1,2], Mostafa Tajdini [2], Tanzila Saba [3], Varatharajan Ramachandran [4]

[1] Department of Computer Science, Liverpool John Moores University, L3 3AF, Liverpool, UK; Yalhamar@hotmail.com
[2] Staffordshire University, UK
[3] Prince Sultan University, Riyadh, Saudi Arabia
[4] Bharath University Chennai, India

* Correspondence: h.kolivand@ljmu.ac.uk

Abstract:
The latest report by Kaspersky on email Spam and targeted Phishing attacks, by percentage, highlights the need of an urgent solution. Attachment-driven Spear-phishing struggles to succeed against many email providers' malware-filtration systems, which proactively check emails for malicious software. In this paper, we provided a solution that can detect targeted Spear-phishing attacks based on required similarities in the specific domain which it has been targeted. The strategy is to figure out whether the domain is genuine or a forgery, which is to be evaluated by multi novel grading algorithms. Therefore, this research addresses targeted attacks on specific organisations by presenting a new enterprise solution. This detection system focuses on domain names, which tend to be registered domain names trusted by the victims. The results from this investigation show that this detection system has proven its ability to reduce email phishing attacks significantly.

Keywords: Spear-phishing, phishing attacks, phishing detection, anti-phishing

1. Introduction

Neutralising the threat of phishing for cybersecurity is not easy; over the years, the attacks have exponentially gained sophistication, adapting to the ever-more stringent parameters and new techniques applied by anti-phishing strategists [1], [2]. By using a variety of social engineering methods and hoodwinking web-surfers, phishing poses a risk to the cyber-security of users, often extracting crucial, confidential information using these methods [3]. Even web-surfers who are not naïve to the risk of phishing can still be vulnerable to these attacks [4], because their ability to discern between legitimate and illegitimate pages may be confounded by a false web page that is designed by phishers to accurately emulate the features of the legitimate site it is imitating.

In the last half of 2014, the anti-phishing working report discovered 132,972 unique phishing attacks between July and December, globally [5]. The industries which are most likely to come under attack are e-commerce, banks, and money transfer companies, for an obvious reason- these promise the most lucrative reward for phishers. The following top-tier domains were utilised by 75% of phishing pages: .net, .cf, .pw, .tk, and .com.

The report also found that during the given time period, the median uptime for phishing sites (i.e. uptime) increased to 10 hours and 6 minutes. In 2015's first three quarters, the financial service sector and banking sector ceased to be the most vulnerable sector, falling into third and second place respectively. Evidently, attackers began to prioritise Internet Service Providers (ISPs) during this time-frame, with them taking first place as the most commonly targeted industry sector [6].

The reason for this change of tactic becomes clear when we consider the opportunities ISP accounts offer phishers for gleaning confidential information such as credit card and identification data [7]. Once gained, this personal information can even be utilised for further phishing endeavors; for example, attackers are able to use hacked accounts to send spam mail. The Business Email Compromise (BEC) fraud of 2015 exemplifies a serious case where a successful phishing attack cost industries large amounts of money [6]; with the use of Spear-phishing methods, the phishers were able to dupe their targets into making transfers and fraudulent transactions. Blacklisting, as previously mentioned, is commonly used to guard users against phishing. Often, these mechanisms are embedded within web browsers as plug-ins which perform a check on every URL and operate on the basis of phishing identification measures which include user votes. This then alerts users of the malicious nature of pages they are trying to visit when a domain appears in the blacklist and blocks the connection to protect them. Some examples of this type of anti-phishing plug-in are as follows:

Google-safe browsing for Firefox [8], phishing filter for Internet Explorer [9]. The blacklist, though, needs to be constantly updated for these measures to be effective, and the update process is often not as speedy as it needs to be, especially considering the fact that many phishing websites typically have short life-spans, with up-times of only a few hours.

Our approach is designed to detect Spear-phishing attacks by analysing the sender domain name. Ransom-ware attack is categorised as drive-by-download attacks and it is beyond the scope of this paper as we have focused on targeted attacks.

This paper is organized as follows. Overviews of existing literature is presented in Section 2. Section 3 presents the proposed method which is divided into two subsections. The results obtained from the proposed method is presented in Section 4. Section 5 reveals some related discussions and comparisons with existing methods. The paper ends with complete collusion based on the outcomes of the presented method.

2. Background

Spear-phishing refers to an attack targeted specifically against a group, organisation or individual [10], [11]. This method has grown in popularity [12], superseding that of more conventional techniques like random and mass email phishing. The reason for this is that Spear-phishing has a far higher success rate than the other, more generalised methods [12]. This is because the content of the phishing email is tailored to the receiver, therefore it is less likely to arouse suspicion.

Spear-phishing is much more successful because people generally trust communications which come from entities whom they already hold an account with or are familiar with [13]. Phishing sites that imitate organisations which users have previously interacted within their legitimate forms are less likely to arouse suspicion and cause them to check the authenticity closely. Some phishers even impersonate specific users' friends [14] or colleagues [15] to ensure a higher success rate. Phishers can, for instance, contact a staff member in an organisation whilst pretending to be a colleague from another department, who for legitimate-seeming reasons asks the victim to respond with important login details or open malicious attachments.

This technique can yield great success and lead to entire data networks being compromised in an institution [16]. This is the preferred method for phishers carrying out what is described as an Advanced Persistent Threat (APT) attack [17], which is an attack targeted at a specific organization, with specific goals. The personalised nature of Spear-phishing makes it an ideal means of attaining this goal. APT attacks are typically carried out over a long time, and care is taken to avoid drawing any attention to the infiltration before the set objectives are achieved. Making use of malware or zero-day vulnerability exploits, phishers launch APT attacks in order to achieve goals such as sabotage or espionage [18].

To create personalised Spear-phishing emails, it is first necessary to obtain some data about the target. One means of achieving this is browser sniffing [14], which is a technique of "sniffing" out the websites that a target has visited by viewing access times for certain cache cookies, DNS caching, and URL [19]. If access time for a certain DNS lookup or URL is brief, this is evidence that the user has accessed the website before, since a DNS cache already exists for the DNS entry, or the browser has created a cache for quick access to the site. Cache cookies also allow phishers to monitor which sites are frequently accessed by their victims. This enables the development of a personally targeted attack which draws on what the phisher knows to be the victim's established network of interests and affiliations. This sniffing technique can be deployed by embedding JavaScript containing malware into websites, web-ads, HTML emails, or search engine optimisation, and sending links to these in emails [20]. Once installed, the malware will report back to the phisher all of the victim's access times, allowing a personalised attack to be devised.

3. PROPOSED METHOD

3.1 Attack Taxonomy

Spearfishing differs from attacks which use software and protocol weaknesses and technical vulnerabilities to infiltrate machines. The engineering that goes into a Spear-phishing attack can be described as social rather than technical. Spear-phishing entails sending specially designed emails which are bespoke to the victim, intended to hoodwink victims into carrying out an action which benefits the predator. Due to the nature of the attack, very little technical knowledge is necessary on the part of the attacker. Unlike other types of phishing, Spear-phishing does not prey on the functional vulnerabilities of machines and software but rather relies on the gullibility of users, which means attacks are difficult to deflect through automated technical defense systems.

The relatively high success rate of Spear-phishing results from the fact that emails are easy to spoof and the considerable time attackers invest in creating emails designed specifically for a particular victim. Hence, as of yet, effective measures or tools for identifying or defending against Spear-phishing do not exist.

whilst Spear-phishing emails are made bespoke to victims with particularly valuable information, capabilities, or access to resources. The attacks are designed with a very specific aim in mind, which makes it possible to tailor every detail in such a way as to increase convincingness.

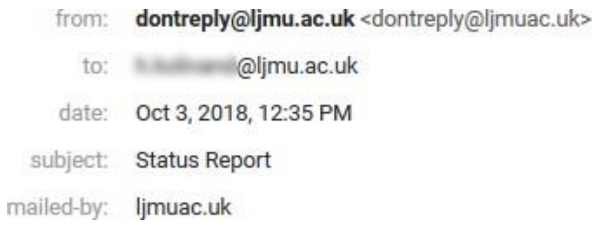
Phishers are forced to carry out expensive zero-day exploits in order to succeed against meticulous technical defense systems. Conversely, the barriers set up against credential Spear-phishing are very low; phishers need only to cleverly construct a bespoke email and host a spoof website in order to hoodwink their victims.

To hoodwink targets into performing actions on behalf of the phisher, Spear-phishing emails must instill trustworthiness by a demonstration of authority or legitimacy. Usually, this is attained by impersonating trusted entities who are already known to the target. Then, the phisher impersonating the authority figure will ask the target to carry out an action which benefits the phisher, such as transferring funds or breaching sensitive data.

3.2 Threat Model

In this work, we specifically focus on an “Enterprise Credential Spear-phishing” threat model, where the attacker tries to fool a targeted enterprise’s victim into revealing their credentials.

In the tests that we did on the Liverpool John Moores University email system, we found that the attacker can bypass detection by changing one character of a legitimate domain name. In this test, we register the domain “ljmuac.uk”. The only difference between our registered domain name and the legitimate Liverpool John Moores University domain name “ljmu.ac.uk” is that ours has one less full stop or dot. As shown in Figure 1, we sent an email from **dontreply@ljmu.ac.uk**<dontreply@ljmuac.uk>.



from: **dontreply@ljmu.ac.uk** <dontreply@ljmuac.uk>

to: [redacted]@ljmu.ac.uk

date: Oct 3, 2018, 12:35 PM

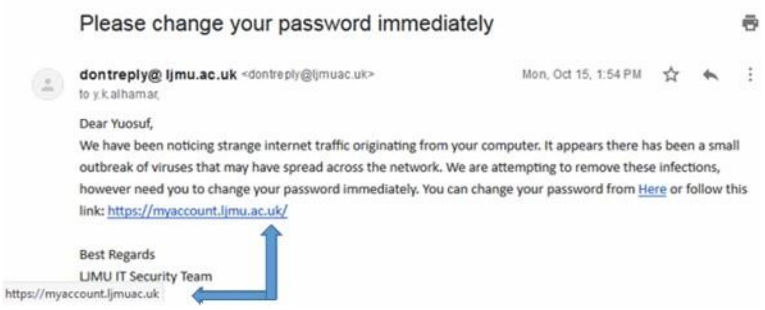
subject: Status Report

mailed-by: ljmuac.uk

Figure 1: Registered domain name

In our threat model, the real email is xxx@ljmu.ac.uk, where “xxx” can be any name such as dontreply, ITHelpDesk, or even a person’s name.

The adversary can send arbitrary emails to the victim and convince the recipient to click on URLs embedded in the adversary’s email (Figure 2). To impersonate a trusted entity, the attacker may set any of the email header fields to arbitrary values.



Please change your password immediately

dontreply@ ljmu.ac.uk <dontreply@ljmuac.uk> Mon, Oct 15, 1:54 PM

to y.k.alhamar,

Dear Yuosuf,

We have been noticing strange internet traffic originating from your computer. It appears there has been a small outbreak of viruses that may have spread across the network. We are attempting to remove these infections, however need you to change your password immediately. You can change your password from Here or follow this link: https://myaccount.ljmu.ac.uk/

Best Regards

LJMU IT Security Team

https://myaccount.ljmuac.uk

Figure 2: Send email to user

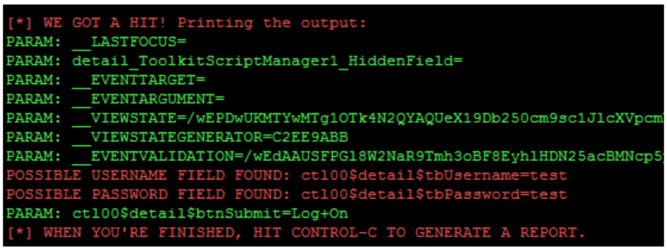
This paper is focused on attacks which entail masquerading as a trusted entity, with the payload being a link to a credential harvesting phishing page.

Figure 2 shows an email we sent to LJMU students, informing them of strange internet traffic originating from their computers, and telling them that there appears to have been a small outbreak of viruses that may have spread across the network. We reassure the user that we are attempting to remove these infections, however, the user must change their password immediately. Then, the user is asked to click on a link. The link redirects the user to a cloned website where we present a cloned version of a legitimate website.

To gain more trust, we placed ''https://myaccount.ljmu.ac.uk/'' over the hyperlink text which sends users to our cloned website ''https://myaccount.ljmuac.uk/''.

We asked 50 different people (40 students and 10 staff) to read the email and click on the link. Once they read it and opened the link, we asked if they noticed anything wrong with the email and the page. Only 2 people (1 student and 1 staff member) noticed that firstly, the sender of the email is not Liverpool John Moores University, and none of them spotted that the web page they browsed is a cloned version of a legitimate page

As shown in Figure 3, we were able to obtain user usernames and passwords. Once the user clicks on the login button, they are redirected to the legitimate address, which in this case is ''http://stureg.ljmu.ac.uk'', and they think that they might have inputted their username and password incorrectly without even realising that their username and password has been stolen. Therefore, this Spear-phishing attack was successful in stealing the victim login credentials.



```
[*] WE GOT A HIT! Printing the output:
PARAM: __LASTFOCUS=
PARAM: detail_ToolkitScriptManager1_HiddenField=
PARAM: __EVENTTARGET=
PARAM: __EVENTARGUMENT=
PARAM: __VIEWSTATE=/wEPDwUKMTYwMTg1OTk4N2QYAQUeX19Db250cm9sc1JlcXVpcm
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAAUSFPG18W2NaR9Tmh3oBF8Eyh1HDN25acBMNcp5
POSSIBLE USERNAME FIELD FOUND: ctl00$detail$tbUsername=test
POSSIBLE PASSWORD FIELD FOUND: ctl00$detail$tbPassword=test
PARAM: ctl00$detail$btnSubmit=Log+On
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 3: Sniffed username and password

During our test phase, we successfully bypassed the email protection that the university put in place to protect users. A dialogue was established with the university IT department, to find out what types of protection they employ and how they tackle phishing attacks.

Unfortunately, they had no idea what we were talking about. There is a difference between spam and phishing emails. Spam emails can be phishing emails, but Spear-phishing emails cannot be spam and will bypass the spam scoring system if the attacker crafts the email carefully. Therefore, the "Trend Micro Email Protection" system is impractical in guarding against Spear-phishing attacks on

Liverpool John Moores University staff or students, as demonstrated by the fact that we successfully launched a Spear-phishing attack and bypassed the detection system.

During the literature review phase, we could not find any solution that tackles “Enterprise Credential Spear-phishing”, where attackers carefully plan attacks. These types of attacks normally deploy by the following steps:

Step 1: Identifying the victim: *At the beginning of each phishing attack, an attacker needs to find a target. Since Spear-phishing is a targeted attack, the attacker must specifically identify the victim.*
Step 2: Gathering information about victim: *Once the attacker identifies the victim, they need to gather intel about the victim using search engines or social networks such as name, location, place of work, close friends, favourite brands, and favourite things to do.*
Step 3: Choosing techniques: *Based on the information gathered from the previous step, now the attacker will choose their attack techniques. In our threat model, the attacker has chosen Spear-phishing, typosquatting and credential harvesting.*
Step 4: Preparing tools: *Based on techniques selected in step 3, the attacker now prepares the tools that are suited to the planned attack.*
Step 5: Register domain(s): *In this step, the attacker will register a domain name designed to establish the victim’s trust. For example, for a victim working in a company with the web address www.abcd ef.co.uk., the attacker will register a domain name similar to that with 1 or 2 characters different, e.g. www.abcedcf.co.uk.*
Step 6: Craft email template: *To gain more trust, the attacker must construct an email template carefully. Once a victim cannot identify anything suspicious in a spoofed email, 99% of their trust is established.*
Step 7: Clone targeted website: *Because of the nature of the techniques chosen, the attacker needs to clone the targeted website that he wants to send to the victim in order to extract their credentials.*
Step 8: Send email
Step 9: Credentials Obtained

Therefore, to tackle this type of attack, we proposed a solution that can detect an “Enterprise Credential Spear-phishing” attack, where the attacker uses a similar domain name to gain the victim’s trust and to trap the victim into the attack. The proposed solution, at a high level, has four stages as illustrated in Figure 4.

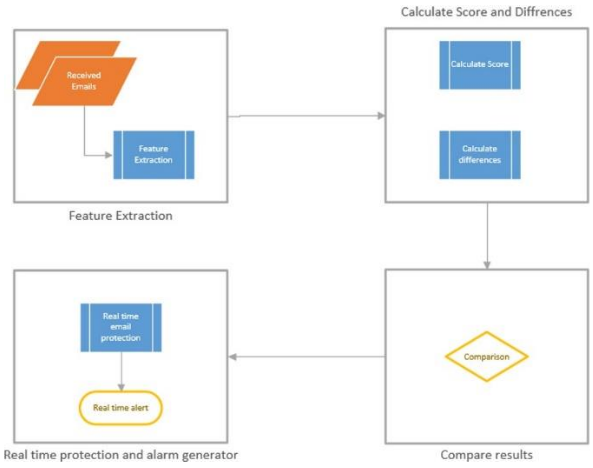


Figure 4: Overview of the proposed protection system

As shown in Figure 4, the first process is feature extraction, then the extracted features are processed to calculate scores and differences. These two processes are the most important parts of our proposed solution. Once the scores and differences are calculated, the result will is compared with the database and threshold values. If there is a match, an alert is created and the email is quarantined for further investigation.

3.2.1Feature Extraction

In this process, the proposed system extracts the following features from the received email domain: **Count number of characters** (Cnoc), **Count number of unique characters** (Cnouc), **Count number of dots** (Cnod), **Count number of numeric values** (Cnonv), **Count number of hyphens** (Cnoh), **Extract domain extension after** (Ede), **Count number of charter before the first dot** (Cnocb f d), **Incoming mail IP address** (INi p), **Valid IP address** (VI P), **Similar characters place** (SCP), **Similar domain name** (Sdomain**), Number of common characters** (NCC), **Similar domain name length** (SDNL)

As shown in Figure 5, the proposed solution starts to work once the email is received by the system. At the first stage, the email domain is whitelisted through the first process, which is the "whitelisting" process.

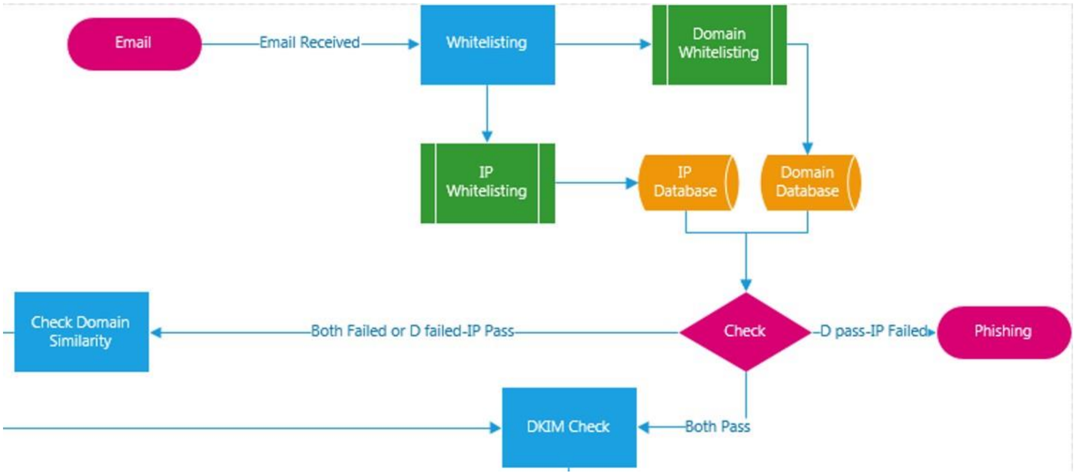


Figure 5: Whitelisting processes

This process has two sub-processes to check whether the incoming email can be whitelisted or not. The first sub-process is to check the domain against a valid domain database. This process will check if the incoming email domain name (i.e. ljmu.ac.uk) exists in the domain database. Then, the next sub-process will check the sender IP address (i.e. 1.1.1.1) against the IP database to see if the sender IP address exists in that database.

Afterward, the results are compared to make a decision about the email. In the “Check” process, the system will mark the email as phishing if the domain name is the same (result pass), but the IP address is different (result fail). This means an attacker is trying to spoof a valid domain name to send the phishing attack, but the IP address is not similar to the valid IPs.

If both checks fail, then the email is forwarded to another process, which is “Check Domain Similarity”. This is because neither the domain nor the IP is valid.

If the domain check result is failed but the IP address is valid, the email is still sent to the “Check Domain Similarity” process again for further examination. If both the domain and IP pass, the proposed solution sends the email to another process named “DKIM and SPF” checker.

3.2.2 Algorithm 1: Whitelisting

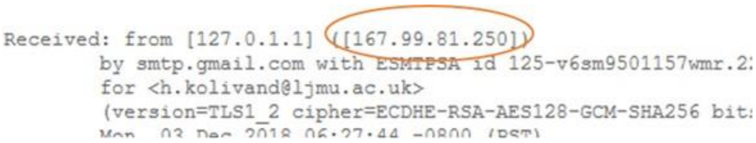
In this part, we propose an algorithm for whitelisting the incoming email domain name. The proposed algorithm has two parts, “Function Domain Whitelisting” and “Function IP address Whitelisting”.

Function Domain Whitelisting

This function whitelists the domain name using the valid domain database, where INdomain is the incoming email domain name and Vdomain is a whitelisted domain in the valid domain database.

Function IP address Whitelisting

This function whitelists the sender IP address(Figure 6) using the valid IP address database, where $IN_{I\ P}$ is the sender IP address and $V_{I\ P}$ is the whitelisted IP address in the valid IP address database.



```
Received: from [127.0.1.1] ([167.99.81.250])
        by smtp.gmail.com with ESMTPSA id 125-v6sm9501157wmr.2:
        for <h.kolivand@ljmu.ac.uk>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bit:
        Mon, 03 Dec 2018 06:27:44 -0800 (PST)
```

Figure 6: Send IP address

Once an email is received, the process starts to work by checking and validating two factors. The first factor is the domain name and the second one is the sender IP address. If the result is pass, then the email is valid and moves to the next layer of processing, which is the Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF).

This is because if INdomain = Vdomain, then it means the sender domain is the same as the domain in the whitelisted database. To avoid address spoofing, we check the sender IP address against the valid IP address. If INI P = VI P then it means the email was sent from one of the trusted domains. In this case, we send the email for future checks to the DKIM and SPF process. If both fail, then the email is sent to the next function, "Check Domain Similarity".

3.2.3 Algorithm 2: Check Domain Similarity

This process starts to work by evaluating the incoming email domain name. As shown in Figure 7, this process has two sub-processes, Similar Character Place (SCP) and Number of Common Characters (NCC).

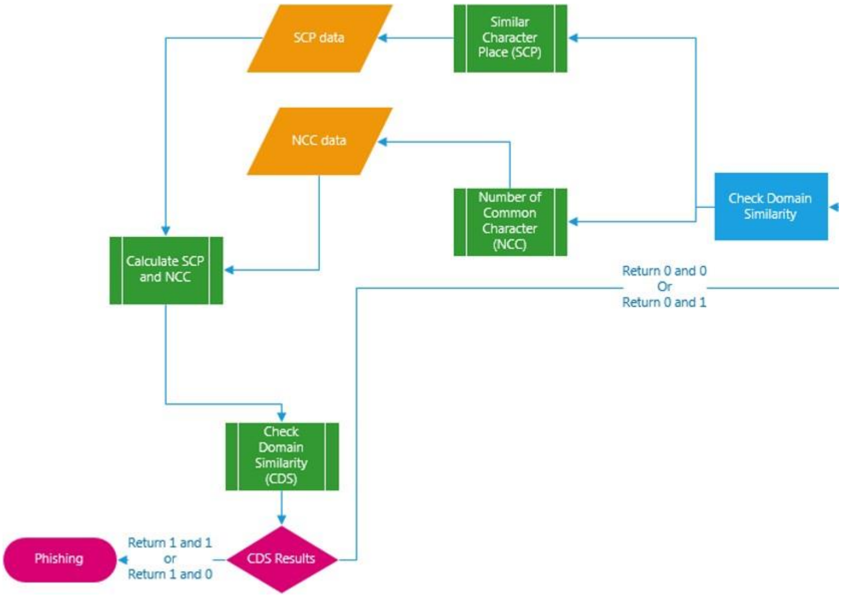

SCP data
Similar Character Place (SCP)
NCC data
Number of Common Character (NCC)
Check Domain Similarity
Calculate SCP and NCC
Return 0 and 0 Or Return 0 and 1
Check Domain Similarity (CDS)
Phishing
Return 1 and 1 or Return 1 and 0
CDS Results

Figure 7: Check domain similarity process

Similar Character Place (SCP) looks for common character placements between incoming the email domain name and valid domain addresses. In theory, this will help to prevent attack techniques such as "Typo squatting". In "Typo squatting", attackers use a similar domain to a legitimate domain.

For example, an attacker might use "ljmuac.uk" as the email domain name to send an email to the victim, which is close to "ljmu.ac.uk".

To achieve this, we proposed an algorithm named "Similar Character Place (SCP)" to find similar character placements in both domains. If the "SCP" is more than the threshold value, it is given a "1" score, if it is less the score is "0". The threshold value is half of the valid domain name.

As an extra security precaution, we proposed another algorithm named "Number of Common Character". This sub-process counts the number of common characters in both domains, minimising the risk of the attacker evading detection. The idea behind this is that normally, attackers use words similar to a target address. For example, an attacker might send an email from "insatgarm.com", trying to pretend that the email is from "instagram.com". This domain has eight common characters with the domain "Instagram.com". As with SCP, if the threshold is met, then the system gives a score of "1", and if it is not met then the score is "0". The threshold value for this process is one-third of the number of characters in the valid domain address.

Once both Similar Character Place and Number of Common Character are calculated based on the following presented algorithms:

```
Function Similar Character Place (SCP) () {
        $\boldsymbol{def1: Find\ SCP}$
        $\boldsymbol{Read\ From}\ (\boldsymbol{V_{domain}})$
        $\boldsymbol{Input\ IN_{domain}}$
        $\boldsymbol{String}\ [\ ]\boldsymbol{SP1};$
        $\boldsymbol{String}\ [\ ]\boldsymbol{SP2};$
        $\boldsymbol{Counter\ Index = 0};$
        $\boldsymbol{For\ I = 1\ to\ V_{domain}.length}[\ ]$
            $\boldsymbol{For\ J = 1\ to\ IN_{domain}.length}[\ ]$
                $\boldsymbol{IF\ V_{domain}[I] = IN_{domain}[J]}$
                    $\boldsymbol{SP1.append(I)};$
                        }
Function Number of Common Character (NCC) () {
    $\boldsymbol{def2: Find\ NCC}$
    $\boldsymbol{s1 = set(Read\ From\ Database(V_{domain}))};$
    $\boldsymbol{s2 = set(Input\ IN_{domain})};$
    $\boldsymbol{common_{char} = s1\ \&\ s2};$
```

```
        $\boldsymbol{remove_{dots}} = ([\boldsymbol{s.strip}('.')\boldsymbol{for\ s\ in\ s2}])$
        $\boldsymbol{IF\ len}(\boldsymbol{common_{char}}) <' \mathbf{1}'$:
            $\boldsymbol{return}\ \left(\boldsymbol{list}(\boldsymbol{set}(\boldsymbol{s1}).\boldsymbol{intersection}(\boldsymbol{remove_{dots}}))\right)$
        $\boldsymbol{else}$:
            $\boldsymbol{return}\ \mathbf{0}$
                                }
```

Then the result is forwarded to another sub-process called "Check Domain Similarity". If the result of both is "1", then the incoming email is classified as "Phishing". This is because the proposed sub-processes, Similar Character Place and Number of Common Character, detected a high chance of similarity to the valid domain; therefore, the email is marked as phishing.

If the Similar Character Place score is "1" and the Number of Common Character score is "0", again the proposed system has detected a high chance of the incoming email having a Similar Character Place to the valid email.

If one of the SCP or both of them return "0", then the domain will forward the email to DKIM for further examination of the domain.

DKIM and SPF Process

This process was designed and added as an extra layer of security to make sure that the emails reaching users are 99% clean and valid.

Once an email is received, first the process checks the Domain Keys Identified Mail (DKIM) with a public DNS server. Once the result comes back from the Public DNS Server, the next process checks the Sender Policy Framework (SPF) with a Public DNS Server to hinder the ability of attackers to send email spoofing a domain name, as shown in Figure 8.

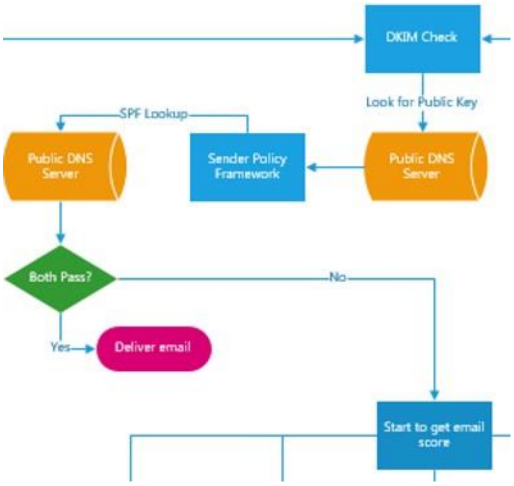


Figure 8: DKIM and SPF proceSS

If both the DKIM and SPF check pass, then the system will deliver the email. This is because, after the previous processes and this one, the proposed system believes that the email is 99.9% clean. However, if both of the checks or one of them failed, then an extra layer of filtering and checks are put in place to make sure that the email sender is legitimate.

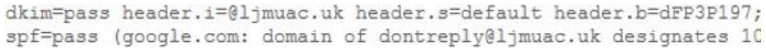
***Step 1:** Read "DKIM" and "SPF" from DNS Domain Check with Public DNS Server to see if SPF record is valid and authorised*
Retrieve Public Key with Public DNS Server to verify sender key
***Step 2:** IF Both Pass = yes => Deliver Email*
Step 3:** IF Both Pass = No => Check Domain Similarity IF either of them pass = NO => Check* ***Domain

Similarity Domain Keys Identified Mail (DKIM): is a protocol used by email systems to verify the sender and integrity of a message and prove that spammers did not modify an incoming message while in transit.

The DKIM key is used by recipient mail servers to decrypt the message's signature and compare it against the domain DNS record. If the values match, then it will prove that the message is authentic and unaltered in transit, therefore, not forged or altered.

Sender Policy Framework (SPF): SPF prevents spammers or attackers from sending emails with a spoofed domain name as the sender. SPF adds IP addresses to a list of servers that are authorised to send email from your domain. It verifies that messages sent from your domains originated from the listed server, which reduces the amount of backscatter that you receive.

An example of received email by Gmail with DKIM and SPF results is shown in Figure 9.



```
dkim=pass header.i=@ljmuac.uk header.s=default header.b=dFP3P197;
spf=pass (google.com: domain of dontreply@ljmuac.uk designates 10
```

Figure 9: Example from received email by Gmail

Complimentary Filtering and Checks

In this process, we used an existing solution which was designed to prevent spam emails, because we believe that the same system to prevent spam can be used in conjunction with the proposed method to increase the detection rate.

If the results of DKIM and SPF failed, then the incoming email is forwarded to this process. This process has five sub-processes. An incoming email is passed to each of these five sub-processes for further checks. Each of these sub-processes has a scoring limit, which if exceeded, will categorise the email as phishing. Each filter below contributes to a SPAM/Phishing scoring. If the received email returns a total score greater than the "Pre-defined Scoring Limit", then the message will be blocked. Compared to the Bayesian option, the Hidden Markov Model (HMM) produces results that are more exact.

Step 1: Check with RBL Filter

This filter extracts the sender IP address from the email header and checks it with the configured RBL one at a time. If the check returns a positive result, it means the sender IP address is listed by one of the RBL servers and a spam score equal to the RBL server's assigned confidence level is assigned to the email.

Calculate Score:

IF Pre-defined Score Exceed = No => Send to Total Pre- defined Score

IF Pre-defined Score Exceed = Yes => Label Email as Phishing

Step 2: Check Bayesian Filter

This scoring filter adds to a message's score if contains specific words, and when it exceeds a pre-defined score, it categorises the message as phishing/spam. An example is "Share Password", which would surely give a high score.

Calculate Score:

IF Pre-defined Score Exceed = No => Send to Total Pre- defined Score

IF Pre-defined Score Exceed = Yes => Label Email as Phishing

Step 3: HMM Filter Calculate Score:

IF Pre-defined Score Exceed = No => Send to Total Pre- defined Score

IF Pre-defined Score Exceed = Yes => Label Email as Phishing

Step 4: Suspicious HELO Calculate Score:

IF Pre-defined Score Exceed = No => Send to Total Pre- defined Score

IF Pre-defined Score Exceed = Yes => Label Email as Phishing

Step 5: Invalid HELO Calculate Score:

IF Pre-defined Score Exceed = No => Send to Total Pre- defined Score

IF Pre-defined Score Exceed = Yes => Label Email as Phishing

4. Test and results

This chapter has two parts, which provide an evaluation of the proposed solution and the awareness-training framework by performing different tests. The first part covers the proposed technical solution, which we call ECSPAD (Enterprise Credential Spear-phishing Attack Detection) and the second part covers the evolution of the proposed awareness- training framework. At the end of the tests, by comparing the results, we have validated that the proposed solutions achieved the main aim of this paper, which is to develop a solution that can detect an Enterprise Credential Spear-phishing Attack. The other aim of this paper is to develop an awareness-training framework for the state of Qatar, to train users to reduce the impact of phishing attacks. There is a proverb saying, "Prevention is better than a cure".

ECSPAD – (Enterprise Credential Spear-phishing Attack Detection)

Test – ljmu.ac.uk

In this part, we performed a series of tests to evaluate the proposed method. In Table 1, we have a valid domain name set to "ljmu.ac.uk". The Similar Character Place (SCP) Threshold Value and Number of Common Characters (NCC) are calculated based on the valid domain name.

TABLE 1 SCP and NCC for ljmu.ac.uk

Valid Domain	Ljmu.ac.uk
SCP Threshold value	2
NCC Threshold value	2

Once the SCP and NCC Threshold value was calculated, we then used the domain "ljmuac.uk" as the phishing domain name. As the results show in Table 2, we assume that the attacker registered the domains to perform the "Credential Spear-phishing Attack" by choosing the same domains as the victim domain name.

Once an email is received from "user@ljmuac.uk", the proposed system starts to work. In the beginning, the system extracts the following features from an incoming email domain name.

TABLE 2
RESULT OF THE PROPOSED METHOD

Incoming email domain	Classified as Phishing?
ljmuac.uk	Yes
Ljmu.acuk	Yes
Limu.a.c.uk	Yes
Ljm.ac.uk	Yes
Ljmuu.a.c.u.k	Yes
Ljmuacuk	Yes

Valid Domain = LJMU.AC.UK

Incoming mail Domain = LJMUAC.UK

Step 1: Whitelist domain: Verify if the incoming email domain name is the same as the valid domain name.

Step 2: Whitelist IP: Verify if the incoming email IP is the same as the valid IP.

The result for this process will be “fail” as “INi p 192.168.1.11” is not the same as “Vi p = 192.168.1.10”

of Common Characters extracted from “Step4” and it will compare to TVNCC (threshold value) which is calculated previously. Because both “Step1” and “Step2” result came back as “fail”, the email will forward to the next step to perform further examinations.

Step 3: Find Similar Character Place (SCP): Find similar character places between Vdomain and INdomain. As shown in Figure 10 (top), the SCP between Vdomainand INdomain is just 4 characters. The result of this process is “4”.

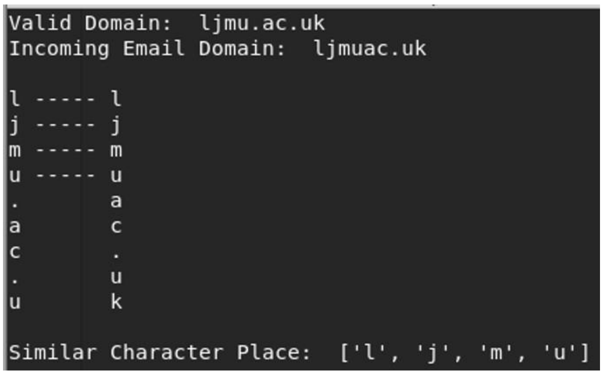
Step 4: Find Number Common Character (NCC)

The result from this step is shown in Figure 10(middle), and the result of this process is “7”.

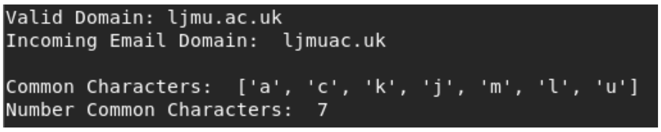
Step 5: SCP and NCC Calculation

To calculate the SCP, we propose the following algorithm which the results is shown in Figure 10(buttom).

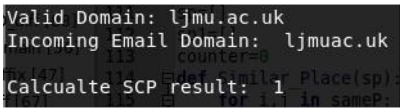
```
def 3: Calculate SCP
IF RSC ≥PTVSC P Then:
Return 1
Else:
Return 0
```



```
Valid Domain:  ljmu.ac.uk
Incoming Email Domain:  ljmuac.uk

l ----- l
j ----- j
m ----- m
u ----- u
.       a
a       c
c       .
.       u
u       k

Similar Character Place:  ['l', 'j', 'm', 'u']
```



```
Valid Domain: ljmu.ac.uk
Incoming Email Domain:  ljmuac.uk

Common Characters:  ['a', 'c', 'k', 'j', 'm', 'l', 'u']
Number Common Characters:  7
```



```
Valid Domain: ljmu.ac.uk
Incoming Email Domain:  ljmuac.uk

Calcualte SCP result:  1
```

Figure 10: (top): SCP result, (**middle**): NCC result, (**buttom**): Calculate SCP result

We need to calculate the TVsc p. The TVsc p is half of the length of the valid domain name (Sdomain = ljmu). Therefore, TVsc p is "2". Based on the result from "Step 3" which is "4", the result of Calculate SCP is "1".

Now, it is time for the NCC calculation process to begin. The following algorithm has been proposed, where RNCC is the Number of Common Characters that were extracted from "Step4", and is compared to the TVNCC (threshold value) which was calculated previously.

```
def 4: Calculate NCC
IF RNCC ≥TV NCC Then:
Return 1
Else:
Return 0
```

The RNCC is "7", and the TVNCC is "2". Therefore, the result of this should be "1", as the Number of Common Characters is greater than the threshold value.

Step 6: Check Domain Similarity

Based on the results from previous processes, the domain is now classified as Phishing, Suspected as Phishing, or send to the next step, which is DKIM and SPF check. Based on the results, the proposed system classified the email as phishing, because the SCP score is "1", the NCC score is "1", and the proposed algorithm calculated a high similarity between the incoming domain name and the valid domain name. Table 3 shows the results of the tests we did with different domains that we registered for the presented Spear-phishing targeted attack.

TABLE 3
VALID DOMAIN EXTRACTED FEATURES

Feature Name	Ljmu.ac.uk	Ljmuac.uk	INSTAGRAM.COM	insatgarm.com	ALPINA.QA	ALPNIA.QA
VCnoc	10	9	13	13	9	9
VCnouc	7	7	10	10	6	6
VDomain	ljmu.ac.uk	*ljmuac.uk*	*instagram.com*	*insatgarm.com*	*alpina.qa*	*alpnia.qa*
SDomain	ljmu	*ljmuac*	*instagram*	*insatgarm*	*alpina*	*alpnia*
VCnod	2	1	1	1	1	1
VCnonv	0	0	0	0	0	0
VCnoh	0	0	0	0	0	0
V Ede	ac.uk	*ac.uk*	*com*	*com*	*qa*	*qa*

VCnocb f d	4	6	9	9	6	6
Vi p	192.168.1.10	192.168.1.11	192.168.12.100	192.168.15.15	192.168.20.100	192.168.22.100

Table 4 shows that the only detection system that detected all of the tests is the proposed method. However, from the result, we can see that the Gmail email server detection was able to detect our “Instagram.com” phishing attack and the motc.gov.qa was able to detect the attack that we sent from our registered domain “motcgv.qa”.

TABLE 4
TARGETED SPEAR-PHISHING ATTACK TEST RESULTS

Domain	TrendMicro	Outlook	Gmail	Yahoo	Live	ESCPTAD
ljmuac.uk	pass	pass	pass	pass	pass	detected
instagram.com	pass	pass	detected	pass	pass	detected
motcogv.qa	pass	pass	pass	pass	pass	detected
alpina.qa	pass	pass	pass	pass	pass	detected

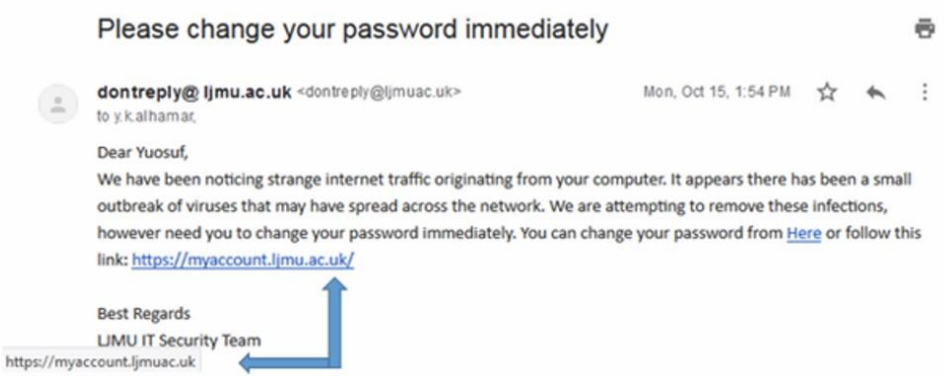
5 Discussion

In this part, we made a comparison between the results of ECSPAD and other enterprise solutions and research solutions. Because the nature of the attack is targeted, and the victim will be selective rather than mass email sending, we performed a target test rather than analysing a database to find the phishing. Based on the conducted research, we could not find any solution exactly designed for Credential Spear-phishing attacks.

Liverpool John Moores University uses TrendMicro Email Security as the enterprise approach to provide a secure environment for email. As mentioned by TrendMicro on their website, “A good technique for hunting and detecting suspicious domains is to also use a similar modus that cybercriminals typically employ: patterns. DNS data (i.e., a passive system of record of DNS resolution data), for instance, provides information security professionals and system administrators insight on how a particular domain changes over time. Not only does this help them correlate indicators of compromise, but also provides the context needed for identifying related or additional suspicious domains. Domain registration information also helps unmask a cybercriminal’s infrastructure by correlating a specific suspicious domain to others registered using similar information.”

Trend Micro InterScan Messaging Security claims that it can stop email threats in the cloud with global threat intelligence, identify targeted email attacks, social engineering attacks, and identify targeted attack emails by correlating email components such as the header, body, and network routing. Our research proves that those claims are not valid, at least for Enterprise Credential Spear-phishing attacks, by comparing the results of an email sent to a user in Liverpool John Moores University with TrendMicro as their email security system versus ECSPAD.

As shown in Figure 11, an email was sent to users saying “Please change your password immediately”. In the content, we asked users to change their password due to strange internet traffic originating from their computers.



Please change your password immediately

dontreply@ ljmu.ac.uk <dontreply@ljmuac.uk> Mon, Oct 15, 1:54 PM
to y.k.alhamar,

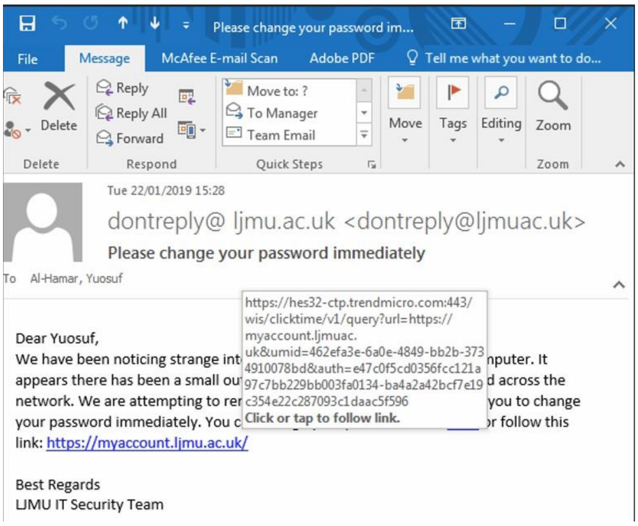
Dear Yuosuf,
We have been noticing strange internet traffic originating from your computer. It appears there has been a small outbreak of viruses that may have spread across the network. We are attempting to remove these infections, however need you to change your password immediately. You can change your password from Here or follow this link: https://myaccount.ljmu.ac.uk/

Best Regards
LJMU IT Security Team

https://myaccount.ljmuac.uk

Figure 11: Targeted Spear-phishing email

Then we asked them to follow a link to reset their password. As shown in Figure 12, the embedded TrendMicro email security system has a feature named “Unknown URL protection” that blocks emails with malicious URLs before delivery and re-checks URL safety when a user clicks on it.



Tue 22/01/2019 15:28

dontreply@ ljmu.ac.uk <dontreply@ljmuac.uk>

Please change your password immediately

To Al-Hamar, Yuosuf

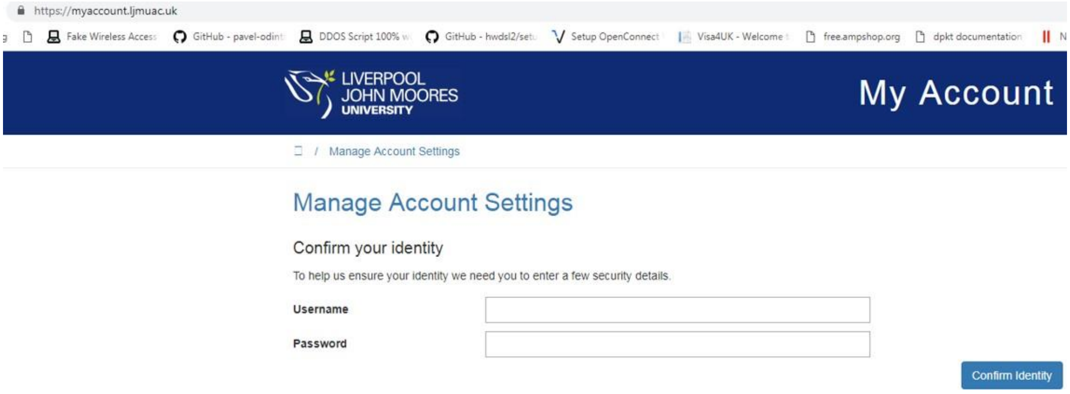
https://hes32-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https://myaccount.ljmuac.uk&umid=462efa3e-6a0e-4849-bb2b-3734910078bd&auth=e47c0f5cd0356fcc121a97c7bb229bb003fa0134-ba4a2a42bcf7e19c354e22c287093c1daac5f596
Click or tap to follow link.

Dear Yuosuf,
We have been noticing strange int nputer. It
appears there has been a small ou d across the
network. We are attempting to rer you to change
your password immediately. You c or follow this
link: https://myaccount.ljmu.ac.uk/

Best Regards
LJMU IT Security Team

Figure 12: TrendMicro security email analysis

Once we clicked on the URL, the TrendMicro cloud threat intelligence system analysed the URL and opened it without any warning or block as shown in Figure 13.



My Account

Manage Account Settings

Confirm your identity

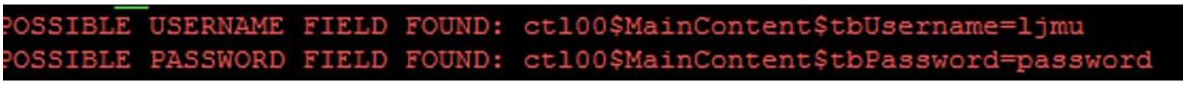
To help us ensure your identity we need you to enter a few security details.

Username

Password

Figure 13: Cloned website

For the proposed test, we used the test username "ljmu" and password "password" on the cloned website to get user credential details (Figure 14).



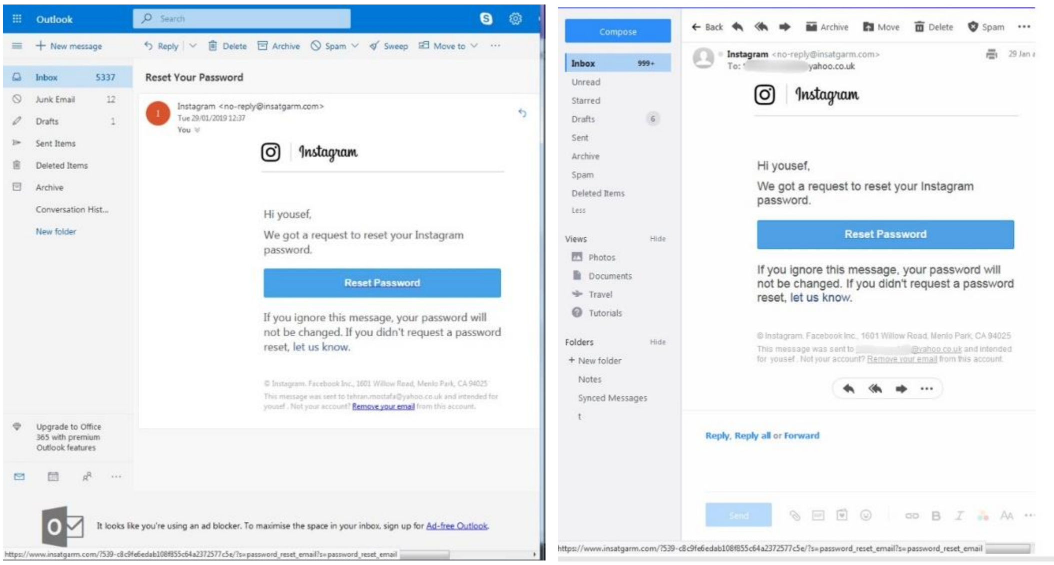
```
POSSIBLE USERNAME FIELD FOUND: ctl00$MainContent$tbUsername=ljmu
POSSIBLE PASSWORD FIELD FOUND: ctl00$MainContent$tbPassword=password
```

Figure 14: User credential

In this test, we registered a new domain, "insatgarm.com", to attack Instagram users. This domain has been carefully chosen, as it is very similar to the original domain name, which is "Instagram.com".

We sent an email to Instagram users to reset their password. The emails asked the user to click on a link to go to a password reset page.

As shown in Figure 15(left), the email successfully bypassed the Microsoft Email Phishing Detection system. As shown in Figure 15(right), it also successfully bypassed the Yahoo Email Phishing Detection system. Therefore, the user would receive this email as a genuine email.



Reset Your Password

Instagram <no-reply@insatgarm.com>
Tue 29/01/2019 12:37
You

Instagram

Hi yousef,

We got a request to reset your Instagram password.

Reset Password

If you ignore this message, your password will not be changed. If you didn't request a password reset, let us know.

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

This message was sent to tehran.mostafa@yahoo.co.uk and intended for yousef . Not your account? Remove your email from this account.

It looks like you're using an ad blocker. To maximise the space in your inbox, sign up for Ad-free Outlook.

https://www.insatgarm.com/?539-c8c9fe6edab108f855c64a2372577c5e/?s=password_reset_email?s=password_reset_email

Instagram <no-reply@insatgarm.com>
To: [redacted]yahoo.co.uk
29 Jan

Instagram

Hi yousef,

We got a request to reset your Instagram password.

Reset Password

If you ignore this message, your password will not be changed. If you didn't request a password reset, let us know.

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

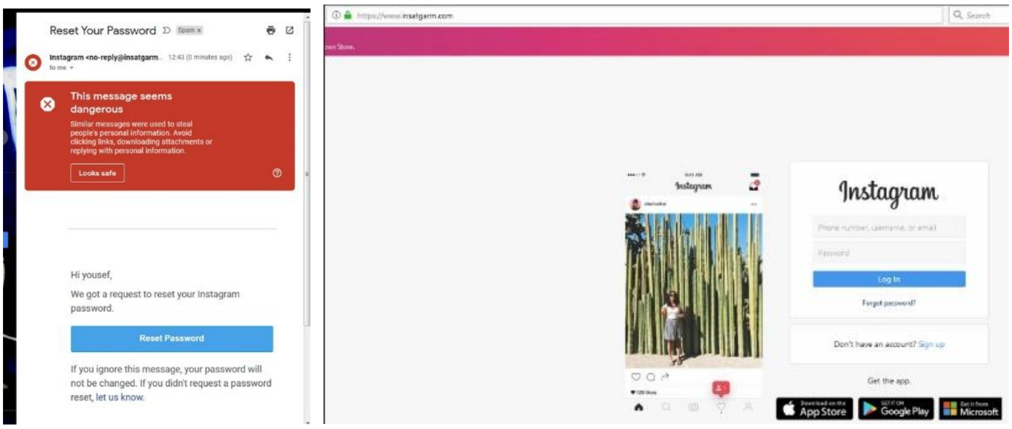
This message was sent to [redacted]@yahoo.co.uk and intended for yousef . Not your account? Remove your email from this account.

Reply, Reply all or Forward

https://www.insatgarm.com/?539-c8c9fe6edab108f855c64a2372577c5e/?s=password_reset_email?s=password_reset_email

Figure 15: (left) Instagram phishing to live, (**right**): Instagram phishing email to yahoo

However, as shown in Figure 16(left), Gmail detected the email that was sent to our victim. By doing further tests and analysis, we found that Gmail uses content analysis; therefore, it found "Instagram" in the content and classified the email as phishing. As has been shown in Figure 16(right), we cloned Instagram's main page on our host to get the victim's usernames and passwords.



Reset Your Password

Instagram <no-reply@insatgarm... 12:43 (0 minutes ago)
to me

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments or replying with personal information.

Hi yousef,

We got a request to reset your Instagram password.

Reset Password

If you ignore this message, your password will not be changed. If you didn't request a password reset, let us know.

https://www.insatgarm.com

Figure 16: (left) Instagram phishing to Gmail, (right): Cloned Instagram page

6. Conclusion

This paper presents a real-world example of targeted Spear-phishing attacks, where attackers use a mixture of different techniques such as Spear-phishing, Typosquatting, and Credential harvesting to bypass detection and perform successful attacks.

To detects and combat such attacks, a multi-layered method, called ECSPAD (Enterprise Credential Spear-phishing Attack Credential), is presented in this chapter which has provided multiple-layered algorithms for the complex task. The presented method was developed specifically to detect "Enterprise Targeted Spear-phishing Attacks", where attackers select their targets and launch personalised attacks to harvest personal information from social networks.

Our research displays the results of our original study on how well users and email hosts can detect and prevent spear-phising attacks. We spoof an email, claiming to be from Instagram, while changing one letter, which our research showed is common phishing technique, to evaluate the relative success of ECSPAD. The results were then compared to existing Spear-phishing defense methods, especially LJMU's Trend Micro, which failed to capture our spoofed email. Our results were also compared to popular web hosts' defense mechanisms. A successful Spear-phishing attack on the Liverpool John Moores University email system could be a catastrophic event potentially leading to credential theft, identity theft, Malware download, and Ransomware attack. The attack method proposed in this paper showed how an enterprise security system like TrendMicro could be vulnerable to Spear-phishing attacks. The proposed method can be used to detect whaling attacks when attackers use a similar domain name to bypass the email security system and gain the target's trust.

This study's goal is to design a solution that can detect a targeted attack based on the domain it has used. Our research has shown that the success rate of SpearPhishng/whaling attack when attackers use a similar domain is significantly high, therefore we worked to provide a solution that can overcome this issue, and our tests showed that the current email security system and email providers are vulnerable to such attacks.

The enterprise email phishing detection system has been tested successfully both in the UK, and Qatar. We continuously sent those emails on 4 months intervals from Oct 2018, with an average of 10 emails per month. The last test was carried out on 22/01/2019, which clearly shows that the TrendMicro intelligence security system is unable to even determine the pattern of these attacks, while ECSPAD did successfully detect them.

Our investigation show ECSPAD performs an excellent detection result as compared to five standard and widely used email system (built-in with Phishing Detection Mechanism).

Conflicts of Interest: We confirm that there is no conflict of interest for this paper.

Reference

[1] A. G. Mishra and B.B., “Hybrid solution to detect and filter zero-day phishing attacks,” 8 2014, pp. 373–379.

[2] K. Parsons, A. McCormac, M. Pattinson, M. J. Butavicius, and C., “The design of phishing studies: Challenges for researchers,” Computers & Security, vol. 52, pp. 194–206, 2015.

[3] A. Almomani, B. B. Gupta, S. Atawneh, A. A. Meulenberg, and E., “A survey of phishing email filtering techniques,” IEEE communications surveys &, vol. 15, no. 4, pp. 2070–2090, 2013.

[4] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. N. Hong, and E., “Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish,” 7 2007, pp. 88–99.

[5] “APWG report available at,” Accessed, vol. 30, 11 2015. [Online]. Available: http://www.antiphishing.org/download/document/ 245/APWG_Global_Phishing_Report_2H_2014.pdf.

[6] “APWG Q1-Q3 2015 Report available.” [Online]. Available: http:

[7] R. M. Saad, A. Almomani, A. Altaher, B. M. Gupta, and S., “ICMPv6 flood attack detection using DENFIS algorithms,” Indian Journal of Science and Technology, vol. 7, no. 2, pp. 168–173, 2014.

[8] E. Alomari, S. Manickam, B. B. Gupta, P. A. Singh, and M., Design, deployment and use of HTTP-based botnet (HBB) testbed. IEEE, 2 2014.

[9] F. Schneider, N. Provos, R. Moll, M. Chew, and B. Rakowski, “Phishing protection design documentation,” 2007. [Online]. Available: https://wiki.mozilla.org/Phishing_Protection

[10] N. P. Singh, “Online frauds in banks with phishing,” The Journal of Internet Banking and Commerce, vol. 12, no. 2, pp. 1–27, 1970.

[11] K. Krombholz, H. Hobel, M. W. Huber, and E., “Advanced social engineering attacks,” Journal of Information Security and applications, vol. 22, pp. 113–122, 2015.

[12] F. S. Rietta, “Application layer intrusion detection for SQL injection,” 3 2006, pp. 531–536.

[13] J. S. Downs, M. C. Holbrook, and L.F., “Decision strategies and susceptibility to phishing,” 7 2006, pp. 79–90.

[14] T. N. Jagatic, N. A. Johnson, M. M. Jakobsson, and F., “Social phishing,” Communications of the ACM, vol. 50, no. 10, pp. 94–100, 2007.

[15] T. Halevi, N. N. Memon, and O., “Spear-phishing in the wild: A real- world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks,” 2015.

[16] A. Elledge, Phishing: An analysis of a growing threat. GIAC Security Essentials Certification. GSEC) Practical, SANS Institute, 2007.

[17] T. Micro, “Spear-phishingemail: Most favored APT attack bait. Research Paper . Trend Micro Incorporated,” 2012. “Symantec,” Symantec Corporation, 2011.

[18] E. S. Felten and M.A., “Timing attacks on web privacy,” 11 2000, pp. 25–32.

[19] E. E. Bursztein and V., "Internet-wide efforts to fight email phishing are working. Google Security Blog, https://security," 2013, googleblog. com/2013/12/internet-wide-efforts-to-fight-email. html.

[20] D. P. Patil and J.B., "Survey on malicious web pages detection tech- niques," International Journal of U-and E-service, Science and Tech- nology, vol. 8, no. 5, pp. 195–206, 2015

Yousef Al-Hamar received his MSc from Loughborough university and his PhD from Liverpool John Moores University, UK. He is currently working in Qatar Foundation. His current research interest social engineering attacks , cyber security, user behavior impact on security and user training awareness.

Hoshang Kolivand is a senior lecturer at LJMU. His recearh interest is HCI, Computer Graphics and cyber security.

Mostafa Tajdini is a lecturer at University of Staffordshire, UK. His research interest is Cyber Security and Network Security. He is working on the IPv6 Evasion Detection System, which can detect IPv6 Advanced Evasion Techniques.

Tanzila Saba is serving as a Research Professor and Associate Chair of Information Systems Department in the College of Computer and Information Sciences Prince Sultan University Riyadh KSA. Her primary research focus in recent years is medical imaging, pattern recognition, data mining, MRI analysis, and Soft-computing.

Ramachandran Varatharajan received his B.E., M.E. and Ph.D. degrees all in Electronics and Communication Engineering from Anna University and Bharath University, India. His main area of research activity is Medical Image processing, Wireless Networks, Network security and Green engineering.