Identifying Methods of Web Attacks towards Minimizing their Effects on Websites

Joshua John
Institute of Computing &
Information Communication Technology
Ahmadu Bello University, Zaria, Nigeria

S. Z. Bugi, Ph.D
School of Science and Technology
National Open University of Nigeria
Kaduna Study Centre, Kaduna, Nigeria

Muripshaka Yibis
Department of Printing Technology
Kaduna Polytechnic, Kaduna, Nigeria

ABSTRACT

This study set out to identify methods that phishers employ to attack unsuspecting internet users. The aim was for the purpose of minimizing their effects on websites as well as users. Eleven statements, namely, Emails, Web based, Malware based, Internet Relay Chats (IRC's) Man in the middle (MITM) Domain Name Server (DNS) based, Impersonate, Forward Attack, Pop-up attack, Voice Phishing and Mobile Phishing, depicting methods used by phishers to carry out their attacks against unsuspecting victims who are the internet users were presented to respondents to indicate their level of agreement. The result showed that only two, (MITM and Web based) out of the eleven were not significant while the remaining nine were significant. That means only the two strategies of attacks are not really dangerous as such can be ignored. This also indicates a high level of danger posed by phishers. Suggestion for further studies was made.

General Terms

Your Web Attacks, Websites, Internet Relay Chat, Man in the Middle, Forward Attack, Voice Phishing, Mobile Phishing.

Keywords

Botnets, Bucket bridge attack, Cyber Espionage, Phishing, web spoofing.

1. INTRODUCTION

Numerous cyber-attacks otherwise referred to as web attacks have been designed by criminals with the sole aim of causing problems for internet users. Cybercrimes encompass a broad range of activities. Generally they can be classified as the kind of attacks that target the computer devices or networks directly and the ones whose prime target is independent of the computer device or network. Online applications have been plagued with problems since their inception and this study examines one of these problems: The lack of user trust in online applications created by the risk of phishing. The growth and advancement of technology has not only benefitted honest Internet users, but has enabled criminals to increase their effectiveness which has caused considerable damage to this budding area of commerce. Moreover, it has negatively impacted both the user and online business, by breaking down the trust relationship between them.

The severity of this problem can be seen in the statement that phishing has increased by 8000% over the period January 2005 to September 2006 [1]. Also, the Anti-Phishing Working Group (the leading, worldwide, anti-phishing law enforcement association) reported that in August 2009, the number of unique phishing websites detected by the Anti-Phishing Working Group reached an all-time high of 56,362, this being a 1.3 percent increase on the previous record of 55,643 in April 2007[2] .

The types of crimes that target particular network or devices are Denial of Service attacks (DoS), Malware or malicious code, computer viruses, Trojans and so on. Apart from such a classification there are several methods of attacks which emanate from the types of phishing employed. These have to be identified before their methods of attacks can be known and described. They are:

i. **Web Vandalism**
ii. **Cyber Espionage**
iii. **Denial of Service Attack(DoS)**
iv. **Spams**
v. **Malware/Crime ware**
vi. **Botnets**
vii. **Web Based**
viii. **Man in the middle (MITM)**

All of the cybercrimes listed above are very much with us each time we access the internet and more of them are invented daily by the cyber criminals. It is therefore important to explain how each and every one attacks the internet so that the unsuspecting internet user can guard against it in the course of browsing the net.

2. LITERATURE REVIEW

2.1 Web Vandalism: Is the willful, voluntary, and malicious destruction or damage of the property of others. In this attack a cyber- criminal gets the access to the target website, and changes the visual appearance of the target website. This is also known as website defacement, and is generally harmless; however it can be used to cover up more evil actions like uploading malware [3].

2.2 Cyber Espionage: Is the act or practice of obtaining secrets without the permission of the holder of the information. This is an act of acquiring secret from individuals, rivals, governments, rivals and so on using certain exploitation methods. It is usually carried out for unethical and illegal strategic advantage and or psychological, political and physical subversion activities and sabotage [4].

2.3 Denial of Service Attack: *(DoS):* DoS or Distributed DoS (is an effort to make one or more computer systems unavailable) an attempt to make a computer resource unavailable to the intended user. The most common method of carrying out this attack involves saturating the victim machine with excessive external communication requests, so that it cannot respond to legitimate traffic or responds so slowly that is rendered effectively unavailable. The most common victims of such an attack are servers hosted on high profile web servers such as banks, credit card payment gateways and even root name servers [5].

2.4 Spams: Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Spam accounts for over 100 billion messages each day, which is approximately 85 percent of email sent worldwide. Such a huge number definitely eats up a lot of computer resources. Spammers continue to improve the design and content of the spam e-mails, to make it appear more legitimate and professional. Spammers hardly use computers in their physical possession to send out the bulk of spam, instead they rent botnets [6].

2.5 Malware/Crimeware: Computer programs designed to infiltrate and damage computers without the users consent. Most modern malware is designed to help attacker gain control over victim's computer, device or a network. Certain malware changes the way the infected computer works. It might force the terminal to connect to the internet and download additional malware. In addition it might also search for sensitive information [7, 8].

2.6 Botnets*:* Is a large number of compromised computers that are used to generate spam, relay viruses or flood a network or Web server with excessive requests to cause it to fail. Most of the current malware is used to deploy the huge botnets. Botnets consist of thousands of compromised computers and have become the basis of the of large scale online criminal activity. People controlling the botnets typically rent out the botnets to send out bulk of spam or carry out other online crimes [9].

2.7 Web based: The web based attacks generally involve embedding malicious scripts that exploit vulnerability in the browser. Other approach to web based phishing involves using pop up's to hide the warnings generated by anti-phishing toolbars, that often mark the address bar with red color for a suspected phishing website. Some of the attacks provide a replica of the login page of the spoofed website directly in the email, targeting the HTML email readers, eliminating the need to click the link and activate the web browser [10].

2.8 Man in the middle (MITM): This attack is also referred to "Session hijacking", "Monkey in the middle" or "Bucket bridge attack". It is one of the most dangerous of all the attacks, as this victim doesn't have a clue that he is been phished. In this particular attack the attacker places himself between the victim and the legitimate website. Thus, victim's every request goes to the genuine website through attacker and there is no way that the victim suspects anything, since for him the website is genuine and the entire process is perfectly normal. [11]

Key Exchanging: Phishers normally target financial institutions for this particular attack, reason being lately all banking websites use public key encryption for all transactions. The public key exchange over HTTP to assure the user about trustworthiness, the web server of a secure site sends a digital certificate to the browser, on requesting for that URL. Once the browser receives this certificate it checks various parameters in the certificate to ensure that the certificate is original. After verification the further transaction with the website continues by encrypting all traffic with the public key of the server, embedded in the digital certificate. This process protects against snooping and eaves dropping. However, MITM thwarts this.

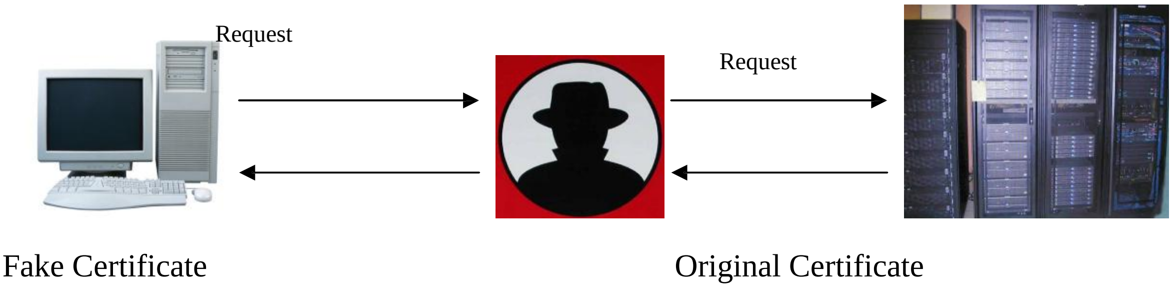

Figure 1: Man in the middle with fake certificate

As the above figure 1 show, in an MITM the Phisher forwards the user request to the desired website; however when the website sends original certificate the Phisher replaces that certificate with his own self signed certificate and sends it as a response to the victim. If the browser doesn't alert the user about the legitimacy of the certificate then the entire transaction proceeds with the encryption by the public key of the Phisher. When the Phisher receives this data he decrypts it using his private key and re-encrypts it using public key of the genuine server thus, creating a pipe between the user and the legitimate website. The response from the server is sent to the user in similar fashion. The user is unaware of dubious activity since the flow of events appears normal [12].

4. METHODOLOGY

This study was a descriptive survey type where interviews were conducted with some stake holders who are selected members of academic and non-academic staff, students, ICT staff of Ahmadu Bello University, Zaria, as well as questionnaires administered on same stakeholders of the same University. The population of the research comprises of the above listed stake holders of the portal for Ahmadu Bello University, Zaria who are directly involved in either the design and development, or usage, of the Students' Registration Portal.

The sample for the study is 250 comprising of 120 male students and 100 female students selected from the faculties of the University where the study was conducted, 10 members of academic and non-academic staff who are not working in the ICT section and 20 ICT staff. A Purposive Random sampling Technique was used to select among males and females.

The selection of the students was based on computer and internet literacy in order to actually involve those students who have the capacity to use the Internet. This is because a good number of students interact with the portal by proxy, since they do not have the requisite computer knowledge to use the portal. As for the ICT staff, only those involved in the design and development of the portal were included in the sample. The sample size for students was limited to 220 students for easy administration of the questionnaire. Ten (10) members of staff involved in the design and development of the portal were also interviewed and likewise, 20 ICT staff were interviewed.

Purposive sampling was utilized for the purpose of this research, as it targets a particular group of people (those that use computers and the internet). This is a form of non-probability sampling in which decisions concerning the individuals to be included in the sample are taken by the researcher, based upon a variety of criteria which may include specialist knowledge of the research issue, or capacity and willingness to participate in the research. Some types of research design necessitate researchers taking a decision about the individual participants who would be most likely to contribute appropriate data, both in terms of relevance and depth as already explained in the section above. In selecting the sample for the students, (male & female) simple purposive random sampling technique was used. In this method, each member of the population, has equal chances of been selected in the sample.

A Structured Questionnaire which is a series of written questions a researcher supplies to subjects, requesting their response was used for soliciting information from respondents regarding Exposing Ways and Means of Carrying out Phishing attacks towards Ensuring Confidence in the use of University Portals. . It is an inexpensive method that is useful where literacy rates are high and respondents are co-operative. Questionnaires can be open or close ended. Open ended questions allow for a space for the respondent to make any comments he or she wishes to make on the course while a close ended question restrict responses to prescribed ones. A second method that was employed along with structured questionnaire was Interview Guide, which are forms that are completed through an oral interview with the respondent. More expensive than questionnaires, but they are better for more complex questions, low literacy or less co-operation.

5. RESULT

Table 1: Which are the different methods of web attacks? - Males

S/N	Statement	5	4	3	2	1	Mean	Remarks
1	Emails	30 (25%)	40 (33%)	20 (17%)	20 (17%)	10 (8%)	3.50 (70.0%)	Significant
2	Web based	15 (13%)	20 (17%)	25 (21%)	50 (42%)	10 (8%)	2.83 (56.7%)	Not significant
3	Malware based	40 (33%)	60 (50%)	10 (8%)	6 (5%)	4 (3%)	4.05 (81%)	Significant
4	Internet Relay Chats (IRC's)	50 (42%)	35 (29%)	25 (21%)	10 (8%)	0 (0%)	4.04 (80.8%)	Significant
5	Man in the middle (MITM)	15 (13%)	20 (17%)	25 (21%)	50 (42%)	10 (8%)	2.83 (56.7%)	Not significant
6	Domain Name Server (DNS) based	40 (33%)	20 (17%)	30 (25%)	10 (8%)	20 (17%)	3.42 (68.3%)	Significant
7	Impersonate	30 (25%)	40 (33%)	20 (17%)	20 (17%)	10 (8%)	3.50 (70.0%)	Significant
8	Forward Attack	50 (42%)	20 (17%)	10 (8%)	30 (25%)	10 (8%)	3.58 (71.7%)	Significant
9	Pop-up attack	60 (50%)	40 (33%)	16 (13%)	10 (8%)	0 (0%)	4.4 (88%)	Significant
10	Voice Phishing	25 (21%)	35 (29%)	50 (42%)	5 (4%)	5 (4%)	3.58 (71.7%)	Significant
11	Mobile Phishing	40 (33%)	20 (17%)	30 (25%)	10 (8%)	20 (17%)	3.42 (68.3%)	Significant

Field Survey, June 2013

Table 2: Which are the different methods of web attacks? - Females Responses

S/N	Statement	5	4	3	2	1	Mean	Remark
1	Emails	25 (21%)	35 (29%)	50 (42%)	5 (4%)	5 (4%)	3.58 (71.7%)	Significant
2	Web based	40 (33%)	20 (17%)	30 (25%)	10 (8%)	20 (17%)	3.42 (68.3%)	Significant
3	Malware based	30 (25%)	40 (33%)	20 (17%)	20 (17%)	10 (8%)	3.50 (70.0%)	Significant
4	Internet Relay Chats (IRC's)	50 (42%)	20 (17%)	10 (8%)	30 (25%)	10 (8%)	3.58 (71.7%)	Significant
5	Man in the middle (MITM)	50 (42%)	35 (29%)	25 (21%)	10 (8%)	0 (0%)	4.04 (80.8%)	Significant
6	Domain Name Server (DNS) based	40 (33%)	20 (17%)	30 (25%)	10 (8%)	20 (17%)	3.42 (68.3%)	Significant
7	Impersonate	30 (25%)	40 (33%)	20 (17%)	20 (17%)	10 (8%)	3.50 (70.0%)	Significant
8	Forward Attack	15 (13%)	20 (17%)	25 (21%)	50 (42%)	10 (8%)	2.83 (56.7%)	Not significant
9	Pop-up attack	60 (50%)	40 (33%)	16 (13%)	10 (8%)	0 (0%)	4.4 (88%)	Significant
10	Voice Phishing	15 (13%)	20 (17%)	25 (21%)	50 (42%)	10 (8%)	2.83 (56.7%)	Not significant
11	Mobile Phishing	40 (33%)	60 (50%)	10 (8%)	6 (5%)	4 (4%)	4.05 (81%)	Significant

Field Survey, June 2013

Table 1 that seeks to answer research question. It reveals statements 1, 3, 4, 6, 7, 8, 9, 10 and 11 are significant and the rest are not. While in table 2 statements 1, 2, 4, 6, 7, 9, and 11 are significant and statements 8 and 10 are not significant.

6. HYPOTHESIS

$H1_0$: Phishers and other cyber criminals do not only use emails to perpetuate their atrocities

$H1_1$: Phishers and other cyber criminals only use emails to perpetuate their atrocities

6.1 Test of Hypothesis

The chi square calculation for the eleven statements of research question is tabulated in Tables 3 and 4.

Table 3: Observed Contingency Table

Statement	Male (O)	Female (O)	Total
Statement 1	84	86	170
Statement 2	68	82	150
Statement 3	97	84	181
Statement 4	97	86	183
Statement 5	68	97	165
Statement 6	82	82	164
Statement 7	84	84	168
Statement 8	86	68	154
Statement 9	106	106	212
Statement 10	86	68	154
Statement 11	82	97	179
Total	**940**	**940**	**1880**

Level of Significance: 5% Level of significance

Critical value: Number of degrees of freedom

(v) = (r - 1) (c - 1)

(v) = (11 - 1) (2 - 1) = 10 x 1 = 10

Test statistic $$\sum \frac{(O-E)^2}{E} \quad \text{--------------------------- (1)}$$

Table 4: Expected Contingency Table

Statement	Male (E)	Female (E)
Statement 1	85.0	85.0
Statement 2	75.0	75.0
Statement 3	90.5	90.5
Statement 4	91.5	91.5
Statement 5	82.5	82.5
Statement 6	82.0	82.0
Statement 7	84.0	84.0
Statement 8	77.0	77.0
Statement 9	106.0	106.0
Statement 10	77.0	77.0
Statement 11	89.5	89.5

Using equation 1,

Chi-square (Test statistic) = 13.47
degrees of freedom = 10
Level of significance = 0.05

Critical value =18.31

Conclusion: Test statistic < Critical value therefore accept H_0.

Emails: All respondents agree that phishers generally send out such specially crafted emails to millions of legitimate users, having live email accounts, within a few hours.

Web based: Female respondents agree that the web based attacks generally involve embedding malicious scripts that exploit vulnerability in the browser. Other approach to web based phishing involves using pop up's to hide the warnings generated by anti-phishing toolbars, that often mark the address bar with red color for a suspected phishing website.

Malware based: All respondents agree that malware is malicious software which is designed to damage a computer. Malware is often installed on a user's computer by tricking the user into believing the attachment or the software on the web is a legitimate one.

Internet Relay Chats (IRC's All respondents agree that many IRC clients allow embedded dynamic content, in such a scenario it's a trivial task to launch phishing attacks.

Man in the middle (MITM): Female respondents agree that in MITM the attacker places himself between the victim and the legitimate website. Thus, victim's every request goes to the genuine website through attacker and there is no way that the victim suspects anything, since for him the website is genuine and the entire process is perfectly normal.

Domain Name Server (DNS) based: All respondents agree that t the DNS contains key value pairs in which each IP address is mapped to an alphanumeric name. Thus, the user no longer needs to memorize the IP address, but just the corresponding alphanumeric name which is called a Uniform Resource Locator (URL).

Impersonation: All respondents agree that the phishing email falsely claims to be from a legitimate business where victims might have an account.

Forward Attack: Male respondents agree that the phisher collects personal information through a scam email that includes harmful code or script.

Pop-up attack: All respondents agree that this technique launches a hostile pop-up in front of the legitimate website asking the victim to login through a secured pop-up window. Once the user logs in to the pop-up, the phisher captures the victim's credentials and forwards him/her to the official website.

Voice Phishing: Male respondents agree that that this is a new technique, improved nowadays by phishers. It is believed to be one of the newest breakthroughs in telecommunications; it uses VOIP – Voice over Internet Protocol - to conduct it.

Mobile Phishing: All respondents agree that GSM devices are used in sending text messages to mobile users trying to trick them into following a malicious mobile Internet link.

7. CONCLUSION

The aim of this research was to investigate a rising lack of user trust and confidence between both the user and the E-Commerce business created by escalating information security breaches such as phishing attacks or its modifications, such as pharming. The study first attempted to provide a better understanding of the threat of phishing that created online risk and a lack of confidence in E- Commerce by digging deep into relevant literature. The thrust of the research has been to instill a sense of trust and confidence in the Students' Registration Portal of Ahmadu Bello University, Zaria through cybernetic management of phishing as well as spoofed websites. Table 1, that seeks to answer research question: Which are the different methods of web attacks? It reveals statements 1, 3, 4, 6, 7, 8, 9, 10 and 11 are significant and the rest are not. While in table 2, statements 1, 2, 3, 4, 6, 7, 9, and 11 are significant and statements 8 and 10 are not significant.

8. RECOMMENDATION

This study has brought to the fore the ignorance of most students to criminal activities that do take place on the internet, especially on sites that commercial activities take place.

Most students are unaware of the fact that the internet is a double-edged sword that could be used for good or bad and as such ignorantly assumed that what they see written on the webpages mean exactly what they are said to be doing. This has, more often than not, led them into the dens of internet robbers. Hence, this study has succeeded in highlighting the need for more computer education for all students of the Ahmadu Bello University, Zaria, and many other similar institutions. The University should do more to educate and inform students on all the services offered by the University. This is made them to be wary of any attempt by scammers to cash on their ignorance.

It is observed that a good number of students have their registration done to them by others, mostly in public internet cafés where they sublet some key information about themselves and their records to people they do not know and whose character they cannot vouch for. The University should do more to make all students computer literate and also provide internet services to all nooks and crannies of the University.

The University should sustain and improve on the current feedback mechanisms they have put in place. Prompt and courteous response to inquiries and complaints will go a long way in increasing the trust of students on the use of the Students' Registration Portal.

The University must ensure that its personnel charged with the design, development and maintenance of the portal are properly taken care of and motivated to be doing their jobs promptly.

9. REFERENCES

[1] Something Vishy, Be Aware of a New Online Scam FBI (2007).

[2] Anti-Phishing Working Group, 2009, p. 2.

[3] Christine E. D., Jonathan J. O. and Eugene J. K. (2004). "Anatomy of a Phishing Email", First Conference on Email and Anti-Spam (CEAS). *2004* Proceedings.

[4] Christine, et-al 2004. "Anatomy of a Phishing Email", First Conference on Email and Anti-Spam (CEAS). *2004* Proceedings.

[5] FBI (2007). *Something Vishy, Be Aware of a New Online Scam* 2007.

[6] Gunter, O. (2009). "The Phishing Guide, Understanding & Preventing Phishing Attacks", Next Generation Security Software.

[7] James, L. (2005) Phishing Exposed. Oct, Syngress.

[8] Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Malware#Characteristics_of_data-stealing_malware. Retrieved on 30th April, 2014

[9] Rachna, D., Tygar, J. D. (2005). "Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks", In Human Interactive Proofs: Second International Workshop (HIP 2005).

[10] Rob T., and Jerry, M. (2010). "The underground economy: priceless"

[11] Shah, J. (2007) Online Crime Migrates to Mobile Phones. Sage, April. 1(2).

[12] Yue Zhang, S.E., Lorrie C., and Jason H. (2007). Phinding Phish Evaluating Anti-Phishing Tools. In 14th Annual Network & Distributed System Security Symposium (NDSS 2007). San Diego, CA.