www.gphjournal.org
Gph-International Journal
Computer Science Engineering

Original Research Paper Vol. 04 Issue 06 June - 2021 Manuscript ID: #0450

EFFECT OF PHARMING ATTACKS ONTHE FUNCTIONALITIES OF THE UNIVERSITY WEBSITES IN NORTHERN STATES OF NIGERIA

ABDULRASHID ABUBAKAR
Department of Library and Information Science, Federal University, Dutsinma-Nigeria.
e-mail:abubakarabdulrashid@rocketmail.com
ZAKARI MOHAMMED
Department of Library and Information Science, Ahmadu Bello University, Zaria-Nigeria.
e-mail:zakmoh2000@yahoo.com

Corresponding author: *ABDULRASHID ABUBAKAR
Email : abubakarabdulrashid@rocketmail.com

ABSTRACT

This paper investigates 'the effects of pharming attacks on the functionalities of the University websites in Northern States of Nigeria. Two research objectives were stated: to find out the types of pharming attacks University websites are exposed to; and to identify the effects of pharming attacks on functionalities of the websites of the Universities in Northern States of Nigeria. The literature was reviewed based on research questions raised. Quantitative research methodology was adopted in the study. Multistage sampling technique (i.e. purposive, stratification, cluster, proportionate and simple random sampling) was used to select 9 Universities (3 each Federal, State and Private) with 127 ICT personnel which comprised of the Directors, the staff of the Software Development Units and the staff of the Networks Infrastructure and Security Units from a population of 61 Universities with 713 ICT personnel of the Universities in Northern States of Nigeria. Questionnaire was the instrument used for data collection. The data collected were presented and analysed using mean, standard deviation, frequencies and percentages. The study found that human factors attacks, local host and local networks attacks, domain configuration attack and domain registration attack among others were the types of pharming attacks University websites in Northern States of Nigeria are exposed to; and pharming attacks do affect the functionalities of the websites of the Universities studied by causing existing administrative settings to be incorrectly configured, poisoning an entire Domain Name System server, manipulating legitimate website's traffic and hijacking search result. Other effects include making communication system to become vulnerable, loss of confidence by stakeholders, tarnishing institution image and tricking unsuspecting individuals into revealing sensitive data among others. The paper concludes that if security safeguards are not adequate, pharmers run little risk of getting caught. They can attack a system using techniques the designers never even considered. The study recommended that Policy statements should be enforced to reduce the effects of pharming attacks on the websites of the Universities. The authorities of the Universities should also provide insurance covers for their ICT technologies and trust worthy Internet Service Providers should be maintained.

KEYWORDS

Pharming Attacks, University, Websites, DNS Server, Functionality.

INTRODUCTION

Organisations' websites handle users' personal sensitive data like banks credentials, passwords and other vital information like credit card details. University Website is a central point of information about a University where one can find information about its faculties, directorates/units, mission and vision, latest news and links to University portal, e-mail and other services. Talalaev (2018) proposed several tips that a good functional website should have. These include:

- Password Management Tools: Every account should have different passwords, so an evil-minded attack can't access all account when one of them gets compromised. Let the password manager calculate a strong password for users so that it would be extremely hard to brute force them. And of course, Use Two-Factor Authentication where ever possible.
- Avoiding Running Multiple Site on One Server: Create a separate database for each site instead of using different prefixes. This will help in keeping the sites isolated and will save a lot of money if one of them gets hacked by intruders such as pharmers.
- Backing up the Websites Regularly: Some hosting providers do it for their client but no matter how secured the websites is, there is always room for improvement. At the end of the day, keeping an off-site backup somewhere is perhaps the best antidote against pharming attacks no matter what happens.

Pharming is the fraudulent practice of tampering with Domain Name System (DNS) server in order to redirect a website's traffic to bogus or spoofed sites. According to Norton (2016), the term "pharming" is based on the words "farming". In their contribution, Patel & Panchal (2013) remarked that pharming is an attempt to change/exploit the DNS server settings of a server so that when one enters the address of a legitimate website, it redirects him/her to a fake/copy of the original site hosted somewhere else. It is a classy edition of phishing attacks endeavour to take users' identification like username and password by redirecting them to a fake website using DNS server based techniques. Pharming attacks can be performed at the client-side - by corrupting the user/company computer or the border router. It can also be in the Internet Service Providers (ISP) network or at the server-side - by intercepting, modifying or spoofing DNS exchanges as well as using content-injection code techniques. Such attack can affect large group of computers in a single instance. As compared to phishing attack, in pharming attack, attacker need not target individual user. Whenever pharming is performed by modifying the DNS server entries, it affects all the users accessing the web page through that DNS server.

Pharming attacks are a major concern for preserving Internet users' privacy. Oshinsky, Masters, Lee, Briggs & Block (2010) remarked that pharmers can cripple the day to-day operations of organisations. Viruses from hackers or disgruntled employees can disable computers or overload the network, leading to business interruption. Organisations also risk the loss of valuable intellectual property if the security of their computer network is breached.

It is of necessity that public and private Institutions implement the necessary controls to ensure that the information and technology assets are protected from all types of threats (whether internal or external), deliberate or accidental, using Institutional ICT Security Policy Document. Kessler (2013) is of the opinion that prevention, detection, and mitigation of pharming attacks involves continuous improvements to built-in security features which include port scanning and remediation, perimeter vulnerability scanning, Operating System (OS) patching to the latest updated security software, network-level DDOS (Distributed Denial-of-Service) detection and prevention, and multi-factor authentication for service access.

Statement of the Problem

Due to progressive advances and it is important to invest in security. Having a website has become easier than ever due to proliferation of great tools and service in the web development space. Content Management System (CMS) like wordPress, Joomla, Drupal, Magento and others allow business owners to build on online presence rapidly. The CMS' highly extensible architectures, rich plugins and effective modules have reduced the need to spend years learning web development before starting to build a functional website. The ease of lunching an online business or personal websites is great. However, there are some negative effects of pharming attacks on the functionalities of organisations' websites. Many webmasters do not understand how to make sure their website is functional and secured. Pharming is one of the most organized crimes of the twenty-first century requiring very little skill on the part of the fraudster to exploit. The challenge of keeping sensitive information like bank accounts and passwords of users' safe from the hands of pharmers becomes more important day after day. Users are becoming accustomed to accessing wireless routers in airports, restaurants, conferences, libraries, and other public spaces. Pharmers can set up malicious wireless routers in the areas that offer free Internet access but redirect users to spoofed websites. Thus, in light of these shortcomings, it is expedient to investigate the effects of pharming attacks on the websites 'functionalities of the Universities in Northern States of Nigeria.

Research Questions

This study sought to provide answers to the following research questions:

1. What type of pharming attacks are the websites of the Universities in Northern States of Nigeria exposed to?
2. How do pharming attacks affect the functionalities of the websites of the Universities in Northern States of Nigeria?

Objectives of the Study

The objectives of the studies are:

1. To identify the type of pharming attacks the websites of the Universities in Northern States of Nigeria are exposed to.
2. To determine how pharming attacks affect the functionalities of the websites of the Universities in Northern States of Nigeria

Literature Review

Today, pharming attacks have become the fastest growing form of cybercrime. It mostly involves unauthorized access, modification and erasure to personal and sensitive information of individuals or organisations. The examples of pharming attacks are probably limited by each individual's imagination but expandable by the escalation of technology advancement. Several scholars revealed different types of pharming attacks. For example, Ollman (2005); and Jakobsson, Yang & Wetzel (2006), Afroz & Greenstadt(2009); Nikiforakis, Invernizzi, Kapravelos, Van Acker, Joosen, Kruegel, Frank Piessens, & Vigna (2012);Patel& Panchal, (2013);in their separate studies found the presence of DNS server hijacking, domain hijacking, DNS cache poisoning, pharming attack via sending email, human factors attacks, static domain name spoofing, drive by pharming, dynamic pharming attack, growing zombies attack, page rank escalation, the "New DNS" attacks, the birthday attack, DNS ID spoofing without sniffing, DNS Identification Device (ID) spoofing with sniffing, DNS spoofing attacks, poorly managed DNS servers attacks, DNS wildcards, domain configuration attacks, botnet name server registration, similar domain name registration, traffic observation and modification, modification of lookup processes, local host and local networks attacks and the insider edge attacks as types of pharming attacks on websites.

These types of pharming attacks vary in their sophistication leading gullible users to their trap. By implication, University's website may be subjected to variety of pharming attacks in such a manner that the DNS server adheres is constantly affected depending on the situation and circumstances. Financial Institutions, especially banking institutions, and educational institutions place greater emphasis on cyber risks and cyber threats due to its nature of information intensive industries. As such, pharmers could have more opportunity and incentive to gain access to institutions' sensitive information through these web applications. This observation corroborates with the findings of Oshinsky, Masters, Lee, Briggs & Block (2010) who depicted that technology has increased the productivity of Universities and businesses, but it comes with many potential risks and liabilities. As organizsations rely more heavily on the Internet, e-mail, and electronic devices, pharmers mishap could loom as serious threats. Universities frequently found themselves in the spotlight as victims of pharming attacks. For example:

- In December 2009, pharmers inserted a malware into Pennsylvania State University's computers, exposing the Social Security numbers of about 30,000 people.
- Pharmers accessed the personal data of approximately 160,000 women who had enrolled in a mammography project conducted by the University of North Carolina at Chapel Hill. The school learnt of this data breach in July 2009, but the intrusion may have occurred as early as 2007.
- In February 2009, the University of California, Berkeley announced that pharmers infiltrated sensitive databases that included Social Security numbers, birth dates, and medical records of 160,000 students and Alumni. Some of the data breached back to 1999.
- Pharmers hacked into Eastern Illinois University's admissions database, exposing personal data of nearly 10,000 current, past, and prospective students dating back to almost a decade.
- Studies addressing phishing and pharming threats on websites of Universities in Federal University, Oye Ekiti-State, Nigeria that is phishing in the education sector identify cyber-plagiarism, cyber-pornography (Michael, 2014) and that 88% of the students that participated in the study were victims of phishing and pharming, majority reported receiving false mails and text messages which in turn led to the loss of money and disclosure of private information in some cases (Michael, 2014).

Pharming attacks are very dangerous to users who are dealing with sensitive accounts like user name, password and credit card number, since it is important information relating to personal and financial data. That's why keeping users aware of forgery websites is an important issue. Even as companies and Universities work to reduce their vulnerability to technology-related risks, new technology advances can lead to new problems that could arise more quickly than defenses can be geared up. In response, organisations have to heightened need for stringent risk management and insurance coverage for mishaps related to these technologies.

Methodology

Quantitative research methodology was adopted for this study. The target population of this study consisted of all the 61 Universities in the Northern States of Nigeria recognised by the National University Commission (NUC). However, the study population (subjects of this study) was the

Information and Communication Technology (ICT) personnel of the Universities studied. They comprised of the Directors, the staff of the Software Development Units and the staff of the Networks Infrastructure and Security Units. This gives a total number of seven hundred and thirteen (713) personnel. A sample of 9 Universities was used for the study with 127 respondents (ICT personnel).The data collected were analysesd using quantitative technique (mean, standard deviation, frequencies and percentages) to answer the research questions raised in the study.

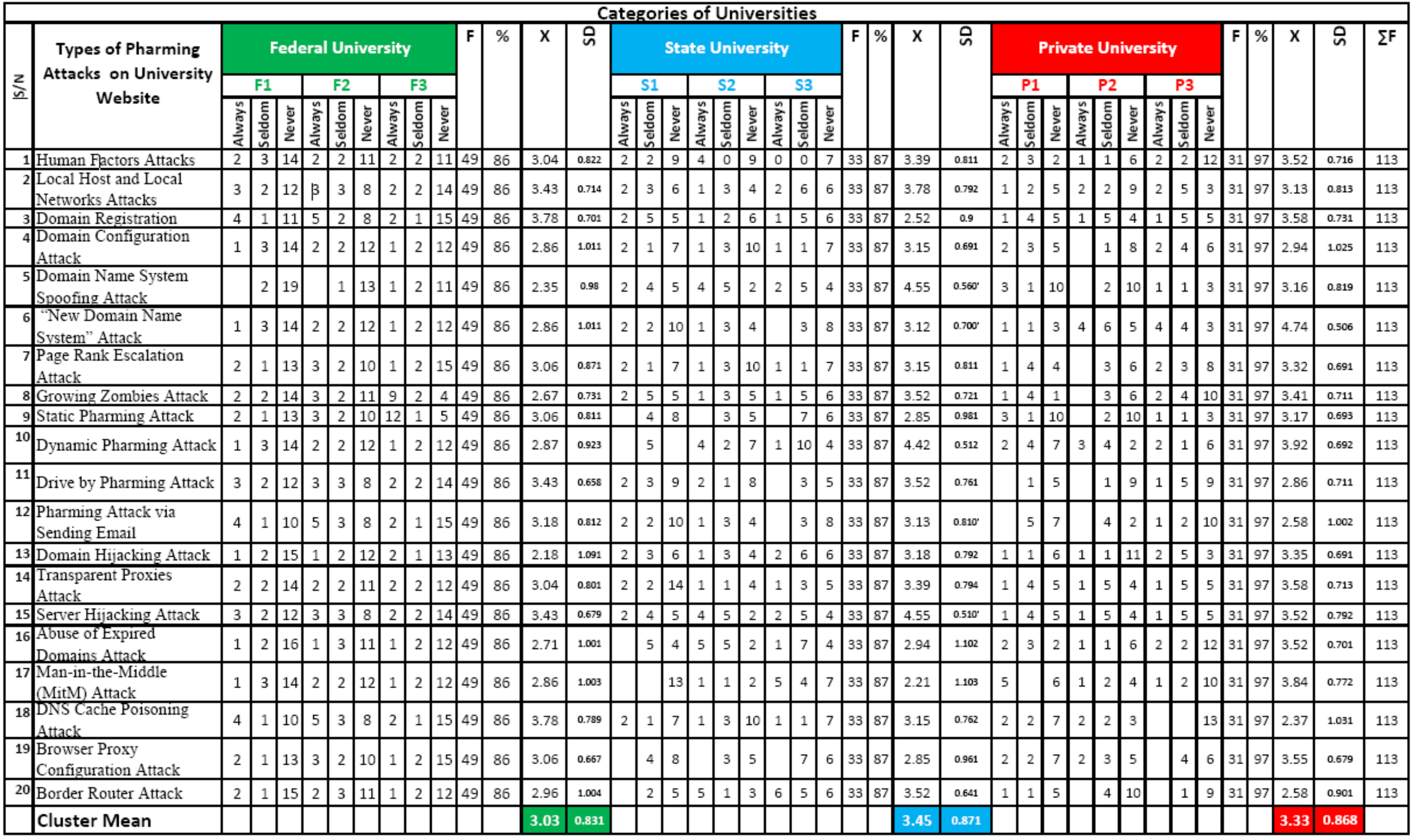
Findings and Discussions

The data collected and analysed were presented and discussed as follows:

Type of Pharming Attacks the Websites of the Universities Studied in Northern States of Nigeria are exposed to

The first research question of this study was raised to identify the type of pharming attacks the websites of the Universities studied in Northern States of Nigeria are exposed to. In order to achieve this objective, a list of types of pharming attacks was outlined for the respondents to indicate as many types of pharming attacks applicable to their respective University websites being exposed to. The data collected in this regard were analysed and presented in Table 1. The acceptable yardstick (benchmark) was 3.0 responses mean score. Thus, any item less than 3.0 mean score was not accepted as really acceptable type of pharming attacks.

Table 1: Types of Pharming Attacks on the Websites of the Universities Studied in Northern Sates of Nigeria



S/N	Types of Pharming Attacks on University Website	Categories of Universities																																							
		Federal University									F	%	X	SD	State University									F	%	X	SD	Private University									F	%	X	SD	ΣF
		F1			F2			F3							S1			S2			S3							P1			P2			P3							
		Always	Seldom	Never	Always	Seldom	Never	Always	Seldom	Never					Always	Seldom	Never	Always	Seldom	Never	Always	Seldom	Never					Always	Seldom	Never	Always	Seldom	Never	Always	Seldom	Never					
1	Human Factors Attacks	2	3	14	2	2	11	2	2	11	49	86	3.04	0.822	2	2	9	4	0	9	0	0	7	33	87	3.39	0.811	2	3	2	1	1	6	2	2	12	31	97	3.52	0.716	113
2	Local Host and Local Networks Attacks	3	2	12	β	3	8	2	2	14	49	86	3.43	0.714	2	3	6	1	3	4	2	6	6	33	87	3.78	0.792	1	2	5	2	2	9	2	5	3	31	97	3.13	0.813	113
3	Domain Registration	4	1	11	5	2	8	2	1	15	49	86	3.78	0.701	2	5	5	1	2	6	1	5	6	33	87	2.52	0.9	1	4	5	1	5	4	1	5	5	31	97	3.58	0.731	113
4	Domain Configuration Attack	1	3	14	2	2	12	1	2	12	49	86	2.86	1.011	2	1	7	1	3	10	1	1	7	33	87	3.15	0.691	2	3	5		1	8	2	4	6	31	97	2.94	1.025	113
5	Domain Name System Spoofing Attack		2	19		1	13	1	2	11	49	86	2.35	0.98	2	4	5	4	5	2	2	5	4	33	87	4.55	0.560'	3	1	10		2	10	1	1	3	31	97	3.16	0.819	113
6	"New Domain Name System" Attack	1	3	14	2	2	12	1	2	12	49	86	2.86	1.011	2	2	10	1	3	4		3	8	33	87	3.12	0.700'	1	1	3	4	6	5	4	4	3	31	97	4.74	0.506	113
7	Page Rank Escalation Attack	2	1	13	3	2	10	1	2	15	49	86	3.06	0.871	2	1	7	1	3	10	1	1	7	33	87	3.15	0.811	1	4	4		3	6	2	3	8	31	97	3.32	0.691	113
8	Growing Zombies Attack	2	2	14	3	2	11	9	2	4	49	86	2.67	0.731	2	5	5	1	3	5	1	5	6	33	87	3.52	0.721	1	4	1		3	6	2	4	10	31	97	3.41	0.711	113
9	Static Pharming Attack	2	1	13	3	2	10	12	1	5	49	86	3.06	0.811		4	8		3	5		7	6	33	87	2.85	0.981	3	1	10		2	10	1	1	3	31	97	3.17	0.693	113
10	Dynamic Pharming Attack	1	3	14	2	2	12	1	2	12	49	86	2.87	0.923		5		4	2	7	1	10	4	33	87	4.42	0.512	2	4	7	3	4	2	2	1	6	31	97	3.92	0.692	113
11	Drive by Pharming Attack	3	2	12	3	3	8	2	2	14	49	86	3.43	0.658	2	3	9	2	1	8		3	5	33	87	3.52	0.761		1	5		1	9	1	5	9	31	97	2.86	0.711	113
12	Pharming Attack via Sending Email	4	1	10	5	3	8	2	1	15	49	86	3.18	0.812	2	2	10	1	3	4		3	8	33	87	3.13	0.810'		5	7		4	2	1	2	10	31	97	2.58	1.002	113
13	Domain Hijacking Attack	1	2	15	1	2	12	2	1	13	49	86	2.18	1.091	2	3	6	1	3	4	2	6	6	33	87	3.18	0.792	1	1	6	1	1	11	2	5	3	31	97	3.35	0.691	113
14	Transparent Proxies Attack	2	2	14	2	2	11	2	2	12	49	86	3.04	0.801	2	2	14	1	1	4	1	3	5	33	87	3.39	0.794	1	4	5	1	5	4	1	5	5	31	97	3.58	0.713	113
15	Server Hijacking Attack	3	2	12	3	3	8	2	2	14	49	86	3.43	0.679	2	4	5	4	5	2	2	5	4	33	87	4.55	0.510'	1	4	5	1	5	4	1	5	5	31	97	3.52	0.792	113
16	Abuse of Expired Domains Attack	1	2	16	1	3	11	1	2	12	49	86	2.71	1.001		5	4	5	5	2	1	7	4	33	87	2.94	1.102	2	3	2	1	1	6	2	2	12	31	97	3.52	0.701	113
17	Man-in-the-Middle (MitM) Attack	1	3	14	2	2	12	1	2	12	49	86	2.86	1.003			13	1	1	2	5	4	7	33	87	2.21	1.103	5		6	1	2	4	1	2	10	31	97	3.84	0.772	113
18	DNS Cache Poisoning Attack	4	1	10	5	3	8	2	1	15	49	86	3.78	0.789	2	1	7	1	3	10	1	1	7	33	87	3.15	0.762	2	2	7	2	2	3			13	31	97	2.37	1.031	113
19	Browser Proxy Configuration Attack	2	1	13	3	2	10	1	2	15	49	86	3.06	0.667		4	8		3	5		7	6	33	87	2.85	0.961	2	2	7	2	3	5		4	6	31	97	3.55	0.679	113
20	Border Router Attack	2	1	15	2	3	11	1	2	12	49	86	2.96	1.004		2	5	5	1	3	6	5	6	33	87	3.52	0.641	1	1	5		4	10		1	9	31	97	2.58	0.901	113
	Cluster Mean												3.03	0.831												3.45	0.871												3.33	0.868	

Table 1 depicts the responses mean scores and standard deviation of the types of pharming attacks on the websites of the 3 categories of the Universities (Federal, State and Private) studied in Northern States of Nigeria. It shows that, for the Federal Universities, items 1, 2, 3, 7, 9, 11, 12, 14, 15, 18 and 19 respectively have mean scores and standard deviation above the acceptable response benchmark of 3.00. Thus, it can be said that, they are the real types of pharming attacks on the websites of the Federal Universities studied. However, items 4, 5, 6, 8, 10, 13, 16, 17 and 20 are below the acceptable response benchmark of 3.00. Hence, they are not indeed really accepted as the types of pharming attacks on the websites of the Federal Universities studied in Northern States of Nigeria.

On the other hand, for the State Universities studied, items 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 18 and 20 respectively also have responses mean scores and standard deviation above the acceptable benchmark of 3.00. This indicates that, they are indeed the real types of pharming attacks on the websites of the State Universities studied in Northern States of Nigeria. However, other items 3, 9, 16, 17 and 19 are below the acceptable benchmark of 3.00. This means that the State Universities studied did not accept them as really the type of pharming attacks on the websites of their respective Universities.

Similarly, for the Private Universities studied, items 1, 2, 3, 5, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17 and 19 respectively have response mean scores and standard deviation above the acceptable benchmark of 3.00. Hence, it can be said that, they are the most prevalent types of pharming attacks on the websites of the Private Universities studied in Northern States of Nigeria. On the contrary, other hand, items 4, 11, 12, 18 and 20 are below the acceptable benchmark of 3.00. This implies that the Private Universities studied did not considered them as really the prevalent types of pharming attacks on the websites of their respective Universities.

A close analysis of the cluster response mean scores for the 3 categories of the Universities studied indicated that, the Federal Universities have cluster mean scores of 3.03, StD=.831, State Universities with the cluster mean scores of 3.40, StD = .871 and Private with the mean scores of 3.33, StD =.868. This implies that the State Universities have higher pharming attacks with higher cluster response mean scores. By implication, the State Governments must make efforts to fund and periodically upgrade the websites of their Universities.

From the foregoing, it can be concluded that all the 3 categories of Universities studied are exposed to different types of pharming attacks such as: human factors attacks; local host and local networks attacks; domain configuration attack; domain registration attack; domain name system spoofing attack; static pharming attack; pharming attack via sending email; and domain hijacking attack among others. The findings of this study is consistent with the similar studies of Afroz & Greensand (2009), Rader & Sayed (2013),Ollmann (2015) and Jakobsson, Yang & Wetzel, (2016), who found the presence of border router attacks, pharming attacks through sending e-mails, presence of local host and local networks attacks, presence of transparent proxies attacks, respectively as types of pharming attacks on websites. This finding is not surprising because the advances in technology and the human wicked nature have compelled many people to maliciously attack individuals as well as organisations such as Universities that have larger markets for students in order to frustrate their effort to meet the goals of education. Additionally it has been observed that most Universities are negligent in security practices and thus fall prey to variety of pharming attacks on their websites. It is imperative for all Universities to take effective safeguard measures to curtail the incidence of pharming attacks on their websites to ensure their functionalities all the times.

Effects of Pharming Attacks on Functionality of the Websites of Universities Studied in Northern States of Nigeria

The second research question of this study was asked to determine the effects of pharming attacks on the functionalities on the websites of the Universities studied in Northern States of Nigeria. In order to ascertain this objective, the responses of the respondents were rated using five Points Likert Scale of Measurement in the following order: Always, Often, Occasionally, Seldom, and Never. But, for the Researcher's convenience, the options were merged into 3 to ease comprehension in the discussion as shown in Table 2. The acceptable benchmark was 3.0 response mean score. Thus, any item less than 3.0 response mean score was not accepted as indeed the real expected component of the functionality of the website of the Universities studied.

Table 2: Effects of Pharming Attacks on the Websites of the Universities in Northern States of Nigeria

		Categories of Universities																																							
S/N	Effects of Pharming Attacks on the Functionality of University Websites Studied	Federal University									F	%	X	SD	State University									F	%	X	SD	Private University									F	%	X	SD	ΣF
		F1			F2			F3							S1			S2			S3							P1			P2			P3							
		Always	Seldom	Never	Always	Seldom	Never	Always	Seldom	Never					Always	Seldom	Never	Always	Seldom	Never	Always	Seldom	Never					Always	Seldom	Never	Always	Seldom	Never	Always	Seldom	Never					
1	Causing existing administration settings to be incorrectly configured	1	2	16	1	3	11	1	2	12	49	86	3.95	0.991	7	2	4	1	3	5	1	3	7	33	87	3.39	0.711			7	2	2	3	4		13	31	97	2.37	0.911	113
2	Poisoning an entire Domain Name System server	1	2	11	3	2	13	3	2	12	49	86	3.11	0.893	2	2	7	1	3	4	2	6	6	33	87	3.73	0.631		1	5		1	9	1	5	9	31	97	2.84	0.891	113
3	Manipulating legitimate website's traffic	4	1	10	5	3	8	2	1	15	49	86	3.18	0.679	2	1	7	1	3	10	1	1	7	33	87	3.15	0.811		5	7		4	2	1	2	10	31	97	2.58	0.100'	113
4	Hijacking search result	1	13	4	2	2	12	1	2	12	49	86	2.88	0.931	2	3	6	1	3	4	2	6	6	33	87	3.78	0.611	1	4	4		3	6	2	3	8	31	97	3.32	0.911	113
5	Making communication system to become vulnerable	3	2	14	2	2	11	2	2	11	49	86	3.04	0.931	2	2	9	4		9			7	33	87	3.39	0.811	1	1	6	1	1	11	2	5	3	31	97	3.35	0.911	113
6	Loss of confidence by stakeholders and tarnishing of institution image	2	1	13	3	2	10	1	2	15	49	86	3.06	0.811	1	5	4	4	2	5	1	7	4	33	87	4.42	0.573	1	4	4		3	6	2	3	8	31	97	3.32	0.911	113
7	Tricking unsuspecting individuals into revealing sensitive data	3	2	13	3	3	8	2	2	13	49	86	3.43	0.711	2	1	6	3	1	9	0	3	8	33	87	3.52	0.671	1	2	5	2	2	9	2	5	3	31	97	3.12	1.001	113
8	Accessing private financial accounts	2	2	14	3	8	1	2	2	15	49	86	3.67	0.713	1	2	5	2	2	11	2	3	5	33	87	3.71	0.713	3	1	10		2	10	1	1	3	31	97	3.17	0.993	113
9	Exploiting security flaws	3	2	12	3	3	8	2	2	14	49	86	3.48	0.712	2	3	6	1	3	4	2	6	6	33	87	3.78	0.771	1	4	4		3	6	2	3	8	31	97	3.32	0.811	113
10	Installing malicious software on visitors' computers	2	1	13	3	2	10	1	2	15	49	86	3.06	0.811	2	2	10	1	3	4		3	8	33	87	3.12	0.821	1	3	2	1	2	6	2	2	12	31	97	3.52	0.711	113
11	Redirecting victims towards a false website	2	2	14	2	3	8	1	2	15	49	86	3.67	0.771	2	2	14	1	1	2	1	3	7	33	87	3.39	0.811	2	2	6	2	3	6		4	6	31	97	3.55	0.671	113
12	Crippling the day to-day operations of institution's website	3	2	14	2	2	11	2	2	11	49	86	3.64	0.713	2	4	5	4	5	2	2	5	4	33	87	4.55	0.676	1	1	6	1	1	11	2	5	3	31	97	3.35	0.781	113
13	Compromising login information	3	5	1	12	3	13	8	2	2	49	86	3.43	0.716	2	2	10	1	3	4		3	8	33	87	3.12	0.812	1	4	4	0	3	6	2	3	8	31	97	3.32	0.821	113
14	Spying victims web traffic and abusing user account privilege	1	2	11	3	2	13	2	2	13	49	86	3.10'	0.813	2	5	5	1	3	6	1	5	6	34	87	3.52	0.700'	3	1	10		2	10	1	1	3	31	97	3.16	0.911	113
15	Loss of valuable intellectual property	4	1	10	5	3	8	2	1	15	49	86	3.18	0.791	1	5	4	4	2	5	1	7	4	33	87	4.42	0.611	1	2	5	2	2	9	2	5	3	31	97	3.13	0.941	113
16	Disrupting service and causing nuisance	3	2	12	3	3	8	2	2	14	49	86	3.43	0.671	2	1	7	1	3	10	1	1	7	33	87	3.15	0.831	1	4	1		3	6	2	4	10	31	97	3.39	0.991	113
17	Subterfuge of routers setting	3	2	14	2	2	11	2	2	11	49	86	3.04	0.851	2	3	9	2	1	5		3	8	33	87	3.52	0.667	1	4	4		3	6	2	3	8	31	97	3.32	0.911	113
18	Causing financial impacts on the targeted victims	3	2	12	3	3	8	2	2	14	49	86	3.43	0.671	2	3	6	1	3	4	2	6	6	33	87	3.78	0.711	1	2	5	2	2	9	2	5	3	31	97	3.12	0.999	113
19	Causing firmware misconfiguration	3	2	14	2	2	11	2	2	11	49	86	3.04	0.852	1	4	5	4	2	5	1	7	4	33	87	4.39	0.651	2	3	2	1	1	6	2	2	12	31	97	3.52	0.771	113
20	Undermining user confidence	4	1	10	5	3	8	2	1	15	49	86	3.78	0.712	1	2	5	2	2	11	2	3	5	33	87	3.91	0.689	3	1	10		2	10	1	1	3	31	97	3.16	0.999	113
	Cluster Mean												3.18	0.639												3.69	0.634												3.20'	0.841	

Table 2 indicated the response mean scores and standard deviations of the effects of pharming attacks on the functionalities of the websites of the 3 categories of the Universities (Federal, State, and Private) studied in Northern States of Nigeria. It reveals that, for the Federal Universities studied, items 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 and 20 respectively have response mean scores above the acceptable benchmark of 3.00. It can be said that, pharming attacks indeed affect the functionalities of the websites of the Federal Universities studied in Northern States of Nigeria. On the other hand, only items 1 and 4 were below the acceptable benchmark of 3.00. Hence, they were not accepted as really having major effects on the functionalities of the websites of the Federal Universities studied.

For the State Universities studied, all the items 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 and 20 respectively were above the acceptable benchmark of 3.00 response mean scores. Thus, it can be said that, pharming attacks indeed affect the functionalities of the websites of the State Universities studied.

However, for the Private Universities studied, items 1, 2 and 3 were below the acceptable benchmark of 3.00 response mean scores. Thus, they were not accepted as indeed the components of the real effect of pharming attacks on the functionalities of the websites of the Private Universities studied. Nonetheless, majority of the items 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 and 20 respectively were above the acceptable benchmark of 3.00. Hence, it can be accepted that, pharming attacks indeed affect the functionalities of the websites of the Private Universities studied in Northern States of Nigeria.

A further analysis of the cluster response mean scores for the 3 categories of the Universities studied revealed that, the Federal Universities have mean scores of 3.18, StD=.639; State Universities have the response mean scores of 3.69, StD = .634; and the Private Universities have the response mean scores of 3.20, StD =.841. The implication of this finding is that, the State Universities have the highest cluster response mean scores of 3.69 and StD=.634 as it relates to pharming attacks on their websites. The state of effects of pharming attacks on the websites of the State owned Universities in Northern States of Nigeria studied, in a way confirmed the inadequate funding of the Universities. There is need to enhance their annual budgetary allocation so that they can effectively manage their websites and meet up to expectations.

Based on the analysis, it is evident that pharming attacks affect the functionalities of the websites of the Universities studied in Northern States of Nigeria. The effects of pharming attacks include: causing existing administrative settings to be incorrectly configured; poisoning an entire Domain Name System server; manipulating legitimate website's traffic; and hijacking search result. Other effects of pharming attacks that have negative effects on the websites of the Universities include: making communication system to become vulnerable; loss of confidence by stakeholders and tarnishing institution image; and tricking unsuspecting individuals into revealing sensitive data; accessing private financial accounts; exploiting security flaws; installing malicious software on visitors' computers; redirecting victims towards a false website; and crippling the day to-day operations of institution's website among others.

The findings of this study is in conformity with that of Oshinky, Lorelie, Kenneth, Cherylyn, Briggs, Jenner & Block (2010) who found that technology has increased the productivity of Universities and businesses, but it comes with its potential risks and liabilities. Oshinsky et- al (2010) remarked that pharmers can cripple the day to day operations of organizations including websites of the Universities. Thus, it is expedient for Universities to provide defensive strategies topredict and prevent a security breach before it happens on their websites. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS detection and prevention, and multi-factor authentication for service access.

The major findings of the study include:

1. The websites of the Universities studied in Northern States of Nigeria are exposed to varying degrees of pharming attacks which include such as human factors attacks; local host and local networks attacks; domain configuration attack; and domain registration attack among others.

2. Pharming attacks do affect the functionalities of the websites of the Universities studied by causing administrative settings to be incorrectly configured; poisoning an entire Domain Name System server, manipulating legitimate website's traffic; and hijacking of search result. Other effects on the websites include making communication system to become vulnerable; loss of confidence on the websites by stakeholders; tarnishing institutions' image; and tricking unsuspecting individuals into revealing sensitive data among others.

CONCLUSION

From the analysis and findings of the study, it is clear that the ICT staff of the Universities studied have realised the need for application of mitigative and detective mechanisms as part of defense-in-depth strategy for providing reasonable protection of sensitive information vis-à-vis the means of detection and remediation of security breaches. However, the ICT staff does not explore, to a large extent, the advantages of preventive mechanisms to prevent the occurrences of most pharming on the websites of their Universities. This paved way for cyber-crimes. When security safeguards are not adequate, trespassers run little risk of getting caught. They can attack a system using techniques the designers never even considered. Hence, the need for constant improvement to secure vital information in the Universities.

Recommendations

1. University authorities should evolve more secured techniques or methods of document security which should include username, password, and access control policy as well as filtering out fake redirects sites vis-à-vis understudy the different types of pharming attacks. There is need to regularly train the operators of the websites on advanced ICT skills competences and knowledge.
2. Security policy statements should be enforced to reduce the effects of pharming attacks on the websites of Universities. The authorities of Universities should also provide insurance covers for their ICT technologies. Trust worthy Internet Service Providers should be maintained.

Referees

Afroz, S., & Greenstadt, R. (2009). “PhishZoo: An Automated Web Phishing Detection Approach Based on Profiling and Fuzzy Matching".

Jakobsson, M., Yang, L & Wetzel, S. (2006). “Warkitting: the Drive-by Subversion of Wireless Home Routers.” The Journal of Digital Forensic Practice.

Michael, E. J. (2014). “Data Breaches: Recent Developments in the Public and Private Sectors,” A Journal of Law and Policy for the Information Society: 556, 567.

Nikiforakis, N., Invernizzi, L., Kapravelos, A., Van Acker, S., Joosen, W., Kruegel, C., Frank Piessens, F., & Vigna, G. (2012). You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions. In Proceedings of the ACM Conference on Computer and Communications Security (CCS). 736–747.

Ollman, G. (2005). “The Pharming Guide”. Understanding and Preventing DNS-Related Attacks by Phishers. Retrieved on 5th, August, 2018 from www.ngssofotware.com

Oshinsky, J., Masters, S.L, Lee, K., J. Briggs, C.J, & Block, J (2010). Fighting Phishing, Pharming, and Other Cyber-Attacks: Coverage for High Tech Liabilities. RMIA Journal.

Patel, J. & Panchal S.D. (2013). A survey on Pharming attack Detection and Prevention Methodology Journal of Computer Engineering (IOSR-JCE). Volume 9, Issue 1. PP 66-72. India. Gujarat Technological University, India.

Talalaev, A. (2018). 12 Web Security Tips from Experts. Retrieved 16th June, 2018 from https://medium.com.