INTERNATIONAL JOURNAL OF SOFT COMPUTING

Effects of Backdoor Awareness on Cyber Hygiene Culture of Nigeria's Civil Servants

Comfort Olebara
Department of Computer Science, Faculty of Physical Science, Imo State University, Owerri, Imo State, Nigeria

Key words: Espionage, cyber security, e-waste, information system, backdoor, cyber hygiene

Corresponding Author:
Comfort Olebara
Department of Computer Science, Faculty of Physical Science, Imo State University, Owerri, Imo State, Nigeria

Page No.: 1-5
Volume: 17, Issue 1, 2022
ISSN: 1816-9503
International Journal of Soft Computing

Abstract: In the advent of surreptitiously inserted or embedded codes on software and hardware for the espionage purposes, the threat faced by developing countries cannot be over-emphasized. This research is geared towards understudying importation of cheap, fairly-used (Tokunbo) mobile devices, PCs and other consumer electronics, with a view to ascertaining the effect they have on the cyber hygiene of Nigerian civil servants and in turn, on Nigerian Information system. A survey was used to collect self-reported data on the backdoor awareness level and cyber hygiene practices of civil servant. Collected data is used to test hypothesis that predicts backdoor awareness level has effect on cyber hygiene practices of Nigerian civil servants. ta of general backdoor awareness, while section2 collected data on participants' cyber hygiene practice. A measurement scale of 1-5 which assumes equidistance is used to assess the participants' level of backdoor awareness and level of cyber hygiene. This method hides behind existing literature on robustness of statistical methods such as logistic regression, to perform parametric data analysis on interval measurement scale chosen. Categorized data on backdoor awareness and cyber hygiene were subjected to logistic regression. The result showed model to be statistically significant at 0.001 and that the odds of having good cyber hygiene was 2.276 more likely for people with high backdoor awareness than those with low backdoor awareness. Regression weight (B) agrees with the outcome, as a positive regression weight of 0.823 showed that there exists a positive relationship between the independent and dependent variables (Increase in backdoor awareness results in increased cyber hygiene culture. The alternative hypothesis is accepted and Null hypothesis rejected. The researcher recommends: Backdoor awareness campaign among civil servants and ministerial heads, Sensitizing and training organizational heads in information security best practices, National measures to ensure ministerial heads are provided with secure PCs and mobile devices by the organizations they represent, frequent software updates, installing browser security software, anti-keyloggers, anti virus software, together with good cyber hygiene will provide some level of Information system protection.

INTRODUCTION

In recent years, malwares, trojans, key loggers and various methods deployed by cyber attackers are no longer limited to software, but has been extended to hardware, through the use of hardware backdoors. Also, the use of cloud-based services has made it possible for installed software or hardware backdoors to be activated and various forms of espionage activities carried out remotely. The risk users face extends to organizations they work for, as most users connect to the organization's network with their PC, or other mobile devices. This works aims to provide insight into the effects fairly used mobile devices and consumer electronics have on the cyber hygiene of a developing nation.

Cyber hygiene is the level of carefulness exhibited by an internet userin order to keep their devices free from various cyber-attack patterns. Some cyber hygiene good practices include but not limited to: Keeping PC firewall on, not opening e-mail whose source is unknown, scanning through flashes before attaching to PC or mobile phones, updating system software often, installing good anti-virus software. These best practices however, work only when the threat faced is software inclined. Hardwaresystem of attack requires physical exposure of the device to an attacker, which implies that an attacker must have physically installed the threat. These come in the form of microcontrollers, or microprocessors, which may be part of the original hardware, or installed for espionage, by manufacturer or other people who have had physical contact with the device. Fairly used Mobile devices, PCs and consumer electronics fall in the second category. These are products either traded-in by their users, stolen and sold, or discarded by owners when obsolete. The importation and dumping of sub-standard consumer electronics into third world countries has been adjudged lucrative to importers from different countries. This is necessitated by the level of poverty, unemployment and dire need to close the digital gap, as made possible by privatization of telecommunication. Knowledge gap is constantly thinning out as a result of remote learning infrastructure, yet affordability of required hardware resources seem far-fetched. Quartz Africa[1] reports that about 21 million Nigerians are unemployed, this has further been compounded by the outbreak of COVID-19, which has caused many employers to shed work force, with many resorting to remote workers. The need for connectivity therefore, has led the citizens in third world countries into resorting to buying mobile phones, PCs, Switches, Routers, Repeaters, from thepopular "Tokunbo" market.

MATERIALS AND METHODS

Conceptual framework

Malware: The word "Malware" is an acronym for Malicious Software. It is a set of instructions injected into ainformation systems, networks or computing devices with the sole aim of carrying out an attacker's intent. A person who carries out the act of injecting malicious software for personal gain is known as an attacker and the act, which results in compromising the integrity of the information system, hardware, network, embedded computers, or computer embodiment, is known as a cyberattack. Types of Malware (Table 1).

Attacker: An attacker is someone who tries to gain access to a device or network unlawfully, with the intention of stealing information, causing harm.

Cyber-attack: Cyber-attacks may be engaged in by individuals, organizations, or nations and for reasons ranging from fraud, espionage, recipe theft and other reasons for which an attacker considers it necessary.

Backdoor: Backdoor is a means of stealthily gaining access to computer, embedded system, or associated devices such as IoT devices. Backdoors, as the name imply, bypass system passwords, encryption algorithms,authentication algorithms and various security protocols, to gain access into the targeted system. Two main backdoor methods are recognized: Software backdoors and hardware backdoors.

Software backdoors are those codes injected into source codes, object codes or compilers. Those inserted into source codes,which are the high-level human readable codes, may be discovered through inspection of

Table 1: Common malware (Baker, 2021)

Type	Action	Example
Adware	Presents in advertisements	Fireball
Spyware	Surreptitiously collects data	Dark-Hotel
Trojan	camouflages as legitimate file, email	Emotet
Ransomware	Denial of Service (DOS) until ransom is given	RYUK
Keyloggers	steals keystrokes such as Pins and passwords	Olympic vision
Bots	Uses AI to launch multiple attacks	Echobot
Worms	Replicates through victim's network	Stuxnex
Rootkits	Used by hackers to take control of victim's device	Zacinlo
Fileless malware	Alters system software files, not application software files	Astaroth
Mobile malware	Used in Mobile phone attack	Triada

the source code. Object code software backdoors are those inserted into the machine-readable object code either during compilation or on the disk-based object code, hence they are difficult to detect through physical examination. Detection of anomaly in object code can be achieved through checking program length, "Checksum analysis" or "object code disassembling".

Hardware backdoors are the codes burned to computer hardware or firmware. These are usually used to compromise integrated circuits, which are silicon wafer fabricated materials. The integrated circuits may be any of capacitors, Microprocessors, Microcontrollers, oscillators, magnifiers, resistors.

ICs are manufactured for a specific purpose, Microprocessors and Microcontrollers, though IC, are programmable and the embedded codes can be reprogrammed to carry out any task the programmer chooses. Programming microcontrollers are carried out using a device called "chip programmer". The chip programmer is attached to a PC through a USB port and installed into the PC. Microcontroller chip legs are attached to the programmer in programmer IDE. Microcontrollers differ in make, shape and size. Some of the legs areinput, some for output, some are for storage (memory), while the others are for processing.

Backdoor discoveries: A developer of "Replicant Project", Paul Kocialkowski reported the discovery of a backdoor in Android Operating system running on Samsung Galaxy devices. The backdoor, a technical issue in the Android Radio Interface Layer (RIL), runs in the devices' processor baseband that controls communication with modems. RIL and Inter Process communication protocol (IPC protocol) in the Samsung device allow modem to carry out input/output operations on file systems throughReceive Flow Steering (RFS) commands. RIL, while allowing the user perform read, write, update, delete operations on phone storage,provides a backdoor for the same operations to be remotely carried out[2] To investigate the open modem port, the researcher added some codes to the modem kernel driver. The patch program, when implemented will: Open data/radio/test file, read its content and then close it.

Another celebrated backdoor find is the research outcome at university of Michigan.The researchers in 2017, inspired by a previous vulnerability in Linux kernel, called 2015 BAIDU SDK BAIDU SDK is an app which opened a port on the devices of users who have any app using it installed and had over 100 million smart phones infected. Inspired by that discovery, the researchers developed a tool they called OPAnalyser, with which they scanned over 100,000 Android-based apps, classified them according to ports they opened for data sharing, proxy, remote execution, VoIP and PhoneGap code signature. Out of the 100,000 Android apps that were subjected to usage test, 410 apps were found to contain 956 backdoors. And the 410 apps had already been downloaded from official Google play store10 to 50 million times by different users.

Backdoor attack examples: Some cyber espionage attacks as reported by techtarget's Alexander Gillis in include, U.S. organizations and government agencies attack in 2020 through a backdoor discovered in Solar Winds' IT management product. The company had over 300,000 customers who use the vulnerable IT product, including various U.S. government agencies. Russian state-sponsored hacking group called Cozy Bear, was suspected to be behind the cyberattack.

The same Russian-state sponsored hacking group (Cozy Bear) was fingered in the attack on Norwegian Police Security Services in 2017. In this attack, emails of nine members of the Ministry of Defense and Ministry of Foreign Affairs and Labor party were phished.

Attempts to hack int Dutch ministries and Ministry of General Affairs were made. The attack targeted sensitive information concerning government documents. Fancy Bear and Cozy Bear were suspected hacking bodies.

Cyber espionage attacks against South Korea, Japan and Vietnam have pointed to North Korea as the suspected attacked. The country was also named in hacking Sony pictures; a state sponsored cyberattack that used malware and Server Message Block worm tool to carry out an attack considered at economic espionage.

Empirical framework

E-Waste in Nigeria: Aniyie[3] described electronic waste as expired electronics, or those that have reached their life span. The author studied the materials with which these electronics are made and presents a categorization of these materials, as well as their toxicity effects at degraded state. Brown *et al*.[4] observed the threats to mobile devices and infrastructure. The authors identified threats to mobile phones, through the operating system and network stacks and recognized mobile phones as major contributor to enterprise threats. Basel group in their network report presented images of imported used IT equipment as shown in Fig. 1.

Methodology

Purpose of research: The purpose of this study is to ascertain the level to which civil servants in Nigerian ministries are aware of the risk factors associated with buying used electronics, with respect to the backdoors they provide to enterprise information system. The cyber hygiene culture of the civil servants is also assessed. The result will help in awareness creation of backdoors in fairly used communication devices and PCs.

Study area: Civil servant in Imo state were identified as target group in the pilot study.

Fig. 1: Ibru Warehouse at Westminister near the Port of Apapa in Lagos. 50, Containers a week of used IT equipment arrive here, Source: Basel Action Network Report (2005)

Questionnaire was generated using google form and distributed to civil servants. The questionnaire consisted of two sections consisting of close ended questions. Section 1 collected data of general backdoor awareness, while section 2 collected data on participants' cyber hygiene practice. A measurement scale of 1-5 was used to assess the participants' level of backdoor awareness and level of cyber hygiene. This method hides behind existing literature on robustness of statistical methods such as logistic regression to perform parametric data analysis on measurement scale chosen. Hence the researcher reiterates that a scale of 1-5 which assumes equidistance is used. The measurement type can be said to be interval which allows parametric statistical testing.

Research question: Does backdoor awareness level amongst Nigerian civil servants affect their cyber hygiene practices?

Hypothesis: H1: Backdoor awareness level amongst Nigerian civil servants affect to the cyber hygiene practices

Data analysis: Data collected from the survey was coded using SPSS version 20 and analyzed.

RESULT AND DISCUSSION

Hypothesis testing: H1: Backdoor awareness level amongst Nigerian civil servants affect to the cyber hygien: Participants total backdoor awareness (TBA) was calculated by summing their scores on the seven questions that made up the domain, average total score was also calculated (ATBA) and run through descriptive statistics to obtain a mean value. Mean value is used to categorize scores (CatATBA). Participants who score below the mean value are categorized as having poor backdoor awareness, while those with scores from the mean and above are categorized as having high backdoor awareness. Total Cyber Hygiene score (TCH) of participants was also calculated by summing up their scores on 5 questions that made up the domain. The total score was averaged (ATCH), ran through descriptive statistics and the resulting mean used to categorize (CatATCH) participants with low cyber hygiene and those with high cyber hygiene culture.

Table 2: Descriptive statistics for Average Total Backdoor Awareness (ATBA)

Variable	ATBA	Valid N (Listwise)
N statistic	300	300
Range	1.43	
Minimum	0.0.00	
Maximum	1.43	
Mean	0.7997	
Std. deviation	0.29739	
Variance	0.88	
Skewness		
Statistic	-234	
Std. Error	0.141	
Kurtosis		
Statistic	0.439	
Std. Error	0.281	

Mean cut off is 0.7997

Table 3: Descriptive statistics for Average Total Cyber Hygiene (ATCH)

Variable	ATCH	Valid N (Listwise)
N Statistic	300	300
Range	1	
Minimum	1	
Maximum	2	
Mean	1.23	
Std. Deviation	0.405	
Variance	0.164	
Skewness		
Statistic	-0.269	
Std. Error	0.141	
Kurtosis		
Statistic	-0.899	
Std. Error	0.281	

Mean cut-off is 1.23

In order to test for the effect backdoor awareness has on cyber hygiene of civil servants, the categorized values of backdoor (CatATBA) awareness and cyber hygiene (CatATCH) culture were subjected to binary logistics regression, which is a statistical technique used to predict relationship between participants' backdoor awareness and their cyber hygiene culture. Backdoor awareness is the independent variable while cyber hygiene is the dependent variable.

Descriptive statistic result is shown in Table 2 and 3.

Interpretation of result: Table 4 presents result of logistics regression analysis which was carried out to find the effect participants' backdoor awareness has on their cyber hygiene culture. Reference category is high

Table 4: Binary logistics regression result

							95% C.I. for exp (B)	
	B	S.E	Wald	df	Sig.	Exp (B)	Lower	Upper
Step 1a CatATBA (1)	0.823	0.237	12.065	1	0.001	2.276	1.431	3.621
Constant	-0.275	0.171	2.581	1	0.108	0.759		

backdoor awareness. The model was statistically significant at 0.001 (< 0.05 maximum significance level). Odds of having good cyber hygiene is 2.276 times greater for people with high backdoor awareness than those with low backdoor awareness. This is also reflected in the regression weight (B = 0.823), as positive regression weight shows a positive relationship between Independent and dependent variables. As backdoor awareness amongst civil servants increases, their cyber hygiene culture also increases.

CONCLUSION AND RECOMMENDATION

The study revealed a medium level of backdoor awareness amongst Nigerian civil servants and also showed that the higher one understands the risk factors associated with various means through which information system may be compromised, the more they increased practices geared towards keeping the safe. The researcher therefore recommends:

- Backdoor awareness campaign among civil servants and ministerial heads
- Sensitizing and training organizational heads in information security best practices
- National measures to ensure ministerial heads are provided with secure PCs and mobile devices by the organizations they represent
- Frequent software updates, installing browser security software, anti-keyloggers, antivirus software, together with good cyber hygiene will provide some level of Informationsystem protection

REFERENCES

1. Yomi Kazeem, 2021. Africa's Largest Economy has Suffered its Worst Contraction in Over a Decade. https://qz.com/africa/1895582/nigeria-economy-gdp-drops-6-1-percent-in-q2-2020/
2. Paul, K., 2014. Replicant developers find and close samsung galaxy backdoor. https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor
3. Azuka, A.I., 2009. The influx of used electronics into africa:a perilous trend. http://www.lead-journal.org/content/09090.pdf
4. Brown, C., S. Dog, J.M. Franklin, N. McNab, S. Voss-Northrop, M. Peck and B. Stidham, 2016. Assessing threats to mobile devices & infrastructure. https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf