Leveraging on Cyber security For Digital Economy: Analysis of Emerging Cyber security Threats and Attacks

Abasiama G. Akpan
Dept. of Computer Science & Mathematics
Evangel University, Akaeze, Nigeria.
email: abasiama.akpan@evangeluniversity.edu.ng

John O. Ugah
Dept. of Computer Science
Ebonyi State University, Nigeria.
email:ugahjohn@gmail.com

Victoria N. Ezeano
Dept. of Computer Science & Mathematics
Evangel University, Akaeze, Nigeria.
email: drmrsezeano@evangeluniversity.edu.ng

Abstract
The rapid growth of the internet has led to a significant growth of cyber threats and attacks incidents with disastrous and grievous consequences. Malware is the main weapon to carry out malicious intents in the cyberspace, either by exploration into existing vulnerabilities or utilization of unique characteristics of emerging technologies. The design of an innovative and effective malicious code (malware) defense mechanism has been regarded as an urgent requirement in the cyberspace. In this paper, we present a survey of the most exploited vulnerabilities in existing hardware, software, and network layers. We also discuss different types of emerging Cyber threats and new attack patterns in emerging technologies such as deep fakes, disinformation in social media, cloud jacking, ransomware, SQL injection attack, cross-site scripting, birthday attack and critical infrastructure. It has been established that these Cyber criminals are exhibiting common level of sophistication and advancement as the advances in Computer and mobile technologies. The available countermeasures are found to be satisfactorily effective, yet Cyber criminals are creating new measures to overcome security mechanisms. This paper has proposed several recommendations including the fact that the National Orientation Agency should shift focus to national re – orientation of the psyche of the whole population and particularly the youths in post – primary and tertiary institutions and to parents, towards raising crop of children with strong religious training, brief and trust in God as well as the infusion of religious training in the curriculum.
Keywords: Cyber Security, Cyber Attacks, Cyber Threats, Malware, Vulnerabilities.

I. INTRODUCTION

Our society, economy, and critical infrastructures have become largely dependent on computer networks and software solutions. We use cyberspace to exchange information, buy, sell product and services and enable various online transactions across a wide range of sectors, both nationally and internationally. Cyber attacks become more attractive and potentially more disastrous as our dependence on information and communication technology increases. Hence, a secure cyberspace is critical to the heath of the Nigerian economy and to the security of the global economy [1]. According to Symantec [2], a cyber attack is any type of offensive action that targets computer information systems, information system infrastructures, computer networks or system devices using various techniques to steal, alter or destroy data or information systems. Cyber attacks become lucrative because attacks are cheaper, convenient and less risky than physical attacks [3]. As discussed by Tatum [4], Cyber Attack can be defined as an attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission. Attacks of this type may be undetectable to the end user or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks [5].

Cyber criminals only require a few expenses beyond a computer and an internet connection. They are unconstrained by location and distance; they are difficult to identity and prosecute due to anonymous nature of the internet. Given that attacks against information and communication technology systems are very attractive, it is

expected that the number and the sophistication of cyber attacks will keep growing. In the other hand, cyber security threats is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

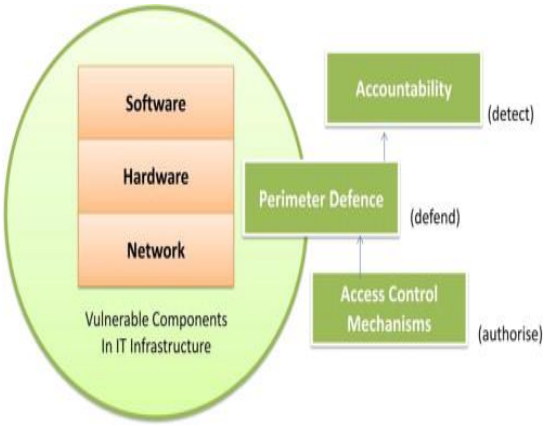

Figure 1: Vulnerabilities and defense strategies in existing systems [6]
Source: Julian jang – Jaccard *et al.* (2014)

Cyber security encompasses industry and government defense strategies adopted to curb cyber criminality in the super highway. It also involve the understanding of surrounding issues of diverse attacks and devising defense strategies (i.e. countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies [7].

- *Confidentiality:* It is the term used to prevent the disclosure of information to unauthorized individuals or systems.
- *Integrity:* It is the term used to prevent any modification/deletion in an unauthorized manner.
- *Availability:* It is the term used to assure that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

In the words of Kosutic [8], Cyber security is the body of technologies, practice with coordinated series of actions, designed to defend networks, computers, system application programs and data from an attack, damage or unauthorized access. Cyber Security professionals classified Cyber emerging threats as malicious attacks, network attacks, or network abuse. Malicious attack is any effort to exploit another person computer and infect the system resources through Virus, Trojan horses, Spyware etc. Network attacks are intended actions meant to damage or disturb data flow of the computer system on a network service, which causes effects such as Denial of Service (Dos), Session Hijacking, Email Spoofing, etc [7]. Network abuse is fundamentally an exploit to the point of interaction of a network, and it could be utilized by actions such as spam, phishing, pharming, etc [8]. Cyber attacks are widely viewed as criminal action led by means of the Web. These exploits can incorporate taking an Organization's intelligent property, seizing online bank accounts, designing and circulating Viruses on different Computers, posting secret Business Data on the Web and destroy a nation's basic national Infrastructure. Internet threats are seen as the highest failure to business and revenue loses of all Organizations [9].

A lot of cyber security professionals believe that malware is the key alternative to carry out malicious intends to breach cyber security efforts in the cyberspace [10]. Malware refers to a broad class of attacks that is loaded on a system, typically without the knowledge of the legitimate owner to compromise the system to the benefit of an adversary. Some exemplary classes of malware include viruses, worms, Trojan horses, spyware, and bot executables [11]. Malware infects systems in a variety of ways, for examples, propagation from infected machines, tricking user to open tainted files, or alluring users to visit malware propagating websites. More concrete example of malware infection is that malware may load itself onto a USB drive inserted into an infected device and then infect every other system into which that device is subsequently inserted. Malware may propagate from devices and equipments that contain embedded systems and computational logic. In short, malware can be inserted at any point in the system life cycle. Victims of malware can range anything from end user systems, servers, network devices (i.e., routers, switches, etc.) and process control systems such as Supervisory Control and Data Acquisition (SCADA). The proliferation and sophistication of fast growing number of malware is a major concern in the Internet today [12].

II NATURE OF CRIME IN THE CYBER SPACE

Cyberspace refers to the interdependent network of information and communication technology

components that underpin many of our communication technologies in place today. This component is a crucial entity of the Nigeria's and global economy critical infrastructure. We use cyber space to exchange information, buy, sell products and services, and enable many online transactions across a wide range of sectors, both nationally and internationally. The primary targets of cybercrimes are on data, network, and access [5, 13]. Cybercrimes under the heading of data crimes include *data interception, data modification, and data theft*. Data interception is the interception of data on transmission. Data modification is the alteration or destruction of data on transmission [14]. Data theft is the taking or copying of data, regardless of whether it is protected by other laws such as US copyright and privacy laws, Health Insurance Portability and Accountability Act (HIPAA) or the Gramm Leach - Billey Act (GLBA) (Electronic Privacy Information Centre, 2004). Cyber crimes include access crimes such as unauthorized access and virus dissemination. Unauthorized access is the hacking or destruction of a network of system [14].

A. *Demography and characteristics of Cyber Criminals*

According to a study by ChiChao Lai *et al.* [15], the demographic characteristics of cybercriminals is revealing as well as disturbing and calls for concerted effort by all to avoid an impending catastrophe. The report findings show that 81.1% were male; 45.5% had some senior high school; 63.1% acted independently; 23.7% were currently enrolled students; and 29.1% were in the 18-23 age bracket, which was the majority group. For those enrolled student cybercrime suspects, the findings show that the percentage of junior high school and senior high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004) of cybercrime suspects in their respective years. The high rate shows that the number of currently enrolled students suspected of involvement in cybercrime is cause for concern. The following groups of people easily fall prey or perpetrate cyber- criminality is:

- Disgruntled employees
- Teenagers
- Political Hacktivist
- Professional Hackers
- Business Rival
- Ex-boy or Girl friend
- Divorced Husband or Wife
- Political enemies

The victims are gullible, desperados and greedy people, unskilled and inexperienced and perhaps unlucky people too can fall victim [16].

B. *Top 20 Countries with the highest rate of Cybercrime*

Symantec [2] has ranked 20 countries that cause the most cyber threats and attacks. In compiling such list, Symantec was able to quantify software code that interferes with a computer's normal functions, rank zombie systems, and observe the number of websites that host phishing sites, which are designed to trick computer users into disclosing personal data or banking account information [17]. Symantec was also able to obtain data including the number of bot-infected systems which are those controlled by cybercriminals, rank countries where cyber attacks initiated and factor in a higher rate of cybercrime in countries that have more access to broadband connections. The highest rate of cybercrime was found to be in the United States which contributes to the broad range of available broadband connections, which are those that allow uninterrupted internet connectivity [18].

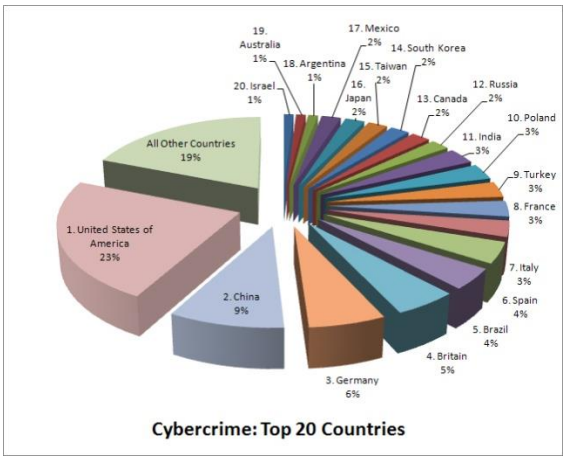

Figure 2: List of Top 20 Countries with the highest rate of Cybercrime
Source: Business Week/ Symantec

C. *Top list of countries with lowest malware infection rates in computers*

Sweden - 19.88%, Finland - 20.65%, Norway - 21.63%, Japan - 22.24%, Belgium - 22.78%,

United Kingdom - 23.38%, Switzerland - 23.94%, Germany - 24.12%, Denmark - 24.34%, Netherlands - 24.86% [18].

D. Corporate security Concerns

Denis [19] reported top three computer security concerns as:
(a) Embezzlement 30% (92), (b) intrusion or breach of computer systems 22% (67), and (c) computer viruses and denial of service attack 11% (33). These top three computer security concerns reflect the thinking of 63% of the organizations reporting. Figure 2 depicts in ranking order all the variables identified.

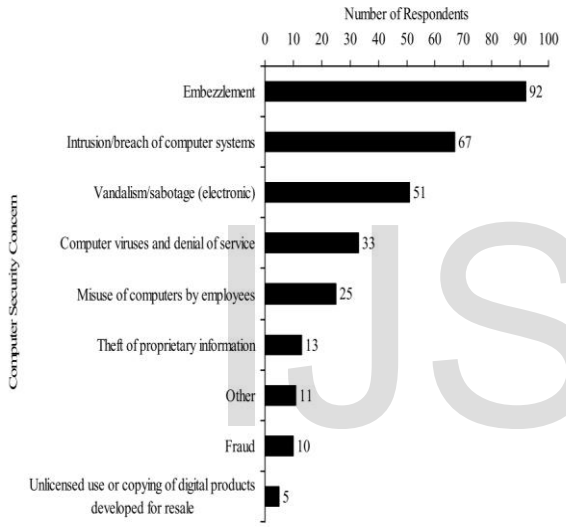

Figure 3: Ranking of computer security concerns by organizations [1].

E. Malware as attack took

In early days, malware was used to underline security vulnerabilities or in some cases to show off technical abilities [20]. Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. For example, malware is often used to target government or corporate websites to gather guarded information or to disrupt their operations. In other cases, malware is also used against individuals to gain personal information such as social security numbers or credit card numbers. Since the rise of widespread broadband Internet access that is cheaper and faster, malware has been designed increasingly not only for the stealth of information but strictly for profit purposes. For example, the majority of widespread malware have been designed to take control of user's computers for black market exploitation such as sending email spam or monitoring user's web browsing behaviors and displaying unsolicited advertisements [21]. Based on Anti-Phishing group report, there was a total of 26 million new malware reported in 2012. Figure 4 describes relative proportions of the types of new malware samples identified in the second half of 2012 reported by the Anti-Phishing group [22].

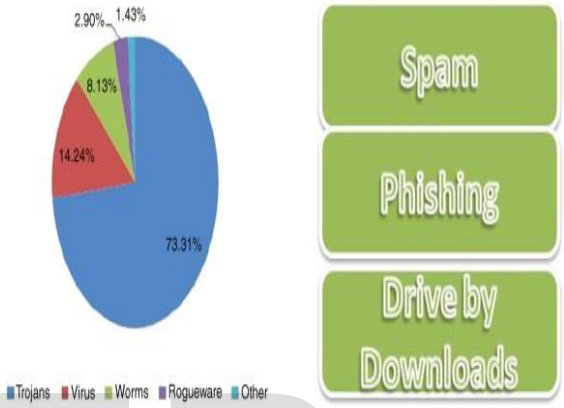

Figure 4: Types of malware and medium to spread them
Source: Julian jang – Jaccard *et al.* (2014)

III. RESEARCH METHODOLOGY

The data for this research were resultant of secondary sources, previous researches and analyses of scholars, books, Journals, Conference proceedings, white papers and Government publications on cyber security that are related to the current trend of cyber emerging threats and attacks. The study involved an extensive literature review which critically analyzed the present state of cyber security. It lay policies to enhance cyber security and the critical steps in acquiring the techniques on how to deal with the emerging cyber threats and attacks through content analysis approach.

IV. EMERGING CYBER SECURITY THREATS AND ATTACKS

Cyber threats and attacks have become routine as the internet itself. Each year, industry reports, media outlets and academic articles emphasize this increased occurrence, spanning both the amount and variety of threats and attacks [23]. In this

study, we seek to further advance discussions on some of the emerging cyber threats and attacks as follows:

- **Deepfakes:** Is a combination of the words "deep learning" and "fake". Deepfakes happen when artificial intelligence technology creates fake images and sounds that appear real. Examples of deepfakes are: creating a video in which a politician's words are manipulated, making it appear that the politician said something he never did. To minimize the risk, have strict verification procedures enforced.

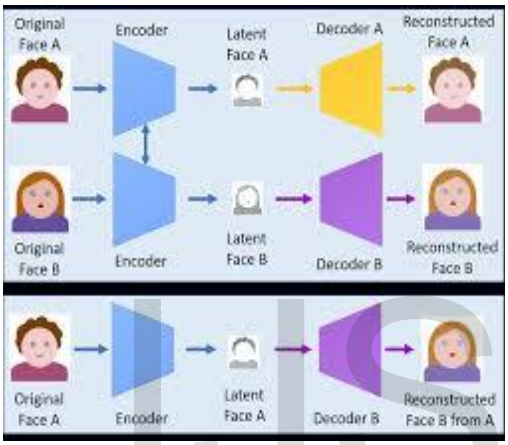

Figure 5: Deepfakes attack

- **Synthetic identities:** They are forms of identity fraud in which scammers use a mix of real and fabricated credentials to create the illusion of a real person. Example, a criminal might create a synthetic identity that includes a legitimate physical address. The social security number and birth date associated with that address, though, might not be legitimate. To minimize risks, ensure that your social security number, both physical and digital, is safe from thieves. Shred old documents that contain personal information.

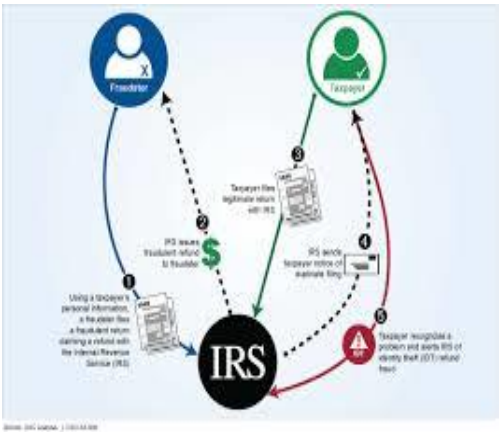

Figure 6: Synthetic identities

- **AI - Powered Cyber attacks:** Uses artificial intelligence. Hackers are able to create programs that imitate known human behaviors. These hackers can then use these programs to trick people into giving up their personal or financial information. To minimize the risk, machine learning algorithms is use to learn from historical data and detect anomalies to enable organizations to prevent and manage cyber attacks effectively and efficiently.

Figure 7: AI - Powered Cyber attacks

- **Poisoning attacks:** Artificial intelligence evolves. In these attacks known as poisoning attacks, cybercriminals can inject bad information into AI program. This bad information can cause the AI system not to function appropriately. Example, getting around spam detectors. To minimize the risk, DNS servers are subject to vulnerabilities. Staying on top of the latest patches can safeguard against attackers looking to exploit these well-known vulnerabilities.

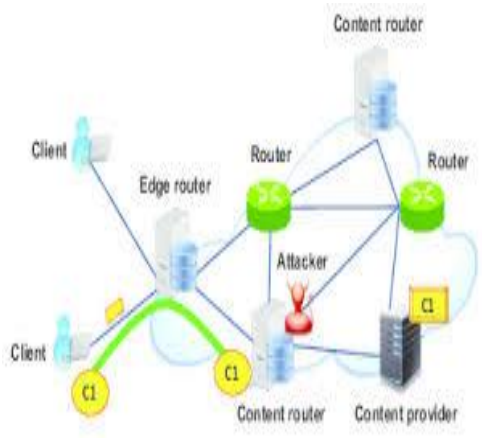

Figure 8: Content poisoning attacks

- **Disinformation in Social Media:** This is also known as disinformation, the deliberate spreading of news stories and information that is inaccurate and designed to persuade people - often voters - to take certain actions or hold specific beliefs. Examples, social disinformation spread through social media such as facebook, twitter, etc. To minimize the risk, limit profile information shared.

- **Advances in quantum computers pose a threat to cryptographic systems:** The threat is that quantum computers can decipher cryptographic codes that would take traditional computers far longer to crack if they ever could. To minimize the risk, implement strong cryptosystems with redundant encipherment and implement long key spaces.

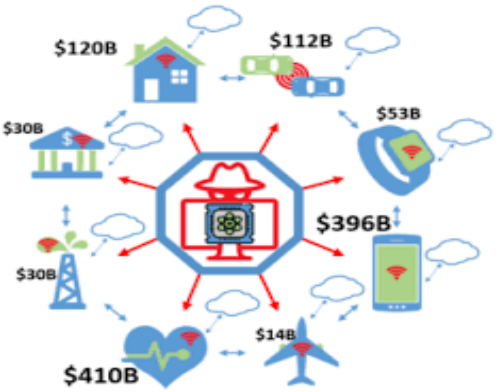

Figure 9: Quantum Attacks on Cryptographic

- **Vehicle cyber attacks:** As more cars and trucks are connected to the internet, the threat of vehicle-based cyber attacks rises. The worry is that cybercriminals will be able to access vehicles to steal personal data, track the location or driving history of these vehicles, or even disable or take over safely functions. To minimize the risk, a risk-based prioritized identification and protection process for safety-critical vehicle control systems should be put in place.

Figure 10: Vehicle cyber attacks

- **Cloud Jacking:** Is a form of cyber attack in which hackers infiltrate the programs and system of businesses, stored in the cloud, and use these resources to mine for crypto currency. To minimize the risk, restrict the IP addresses allowed to access cloud applications. Some cloud apps provide tools to specify allowable IP ranges, forcing users to access the application only through corporate networks or VPNs.

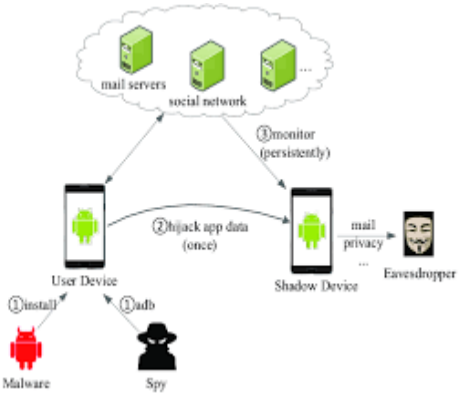

Figure 11: Cloud Jacking Attacks

- **Ransomaware attacks:** In a ransomware attack, the attacker infecting a victim's systems with a piece of malware that encrypts all of their data. The victim is then presented with an ultimatum – either pay the ransom or lose their data forever. To minimize the risk, strong perimeter security, such as firewalls to prevent malware from uploaded to your systems.

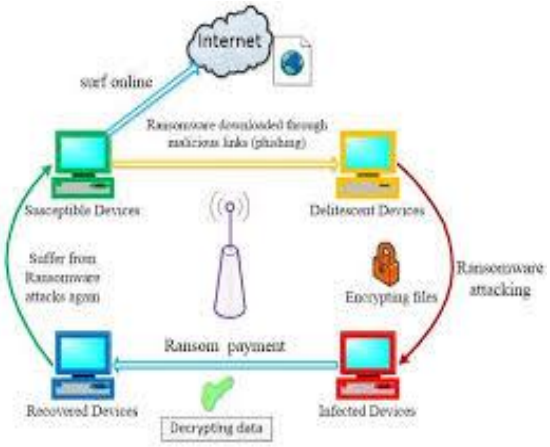

Figure 12: Ransomaware attacks

- **IOT – Based Attack**s: Is any Cyber attack that leverages a victim's use of internet – connected smart devices (Such as Wi – Fi enabled speakers, appliances, alarm clocks, etc) to sneak malware onto a network. To minimize the risk, keep the firmware for these devices up – to – date, as this can help resolve exploits that have been patched by the manufacturer.

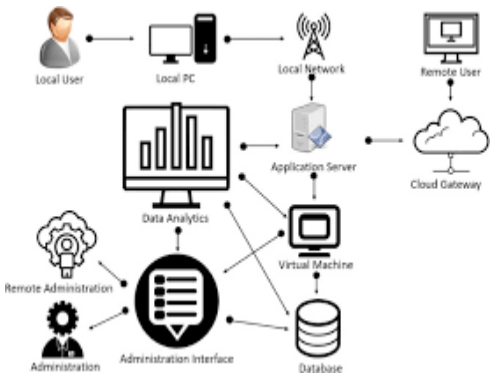

Figure 13: IOT – Based attacks

- **Denial-of-Service (DOS) and Distributed denial-of-service (DDOS) attacks:** A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDOS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker. Examples are, TCP, SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and bonnets. To minimize the risk, blacklist IP addresses that are identified as being part of a DDOS attack.

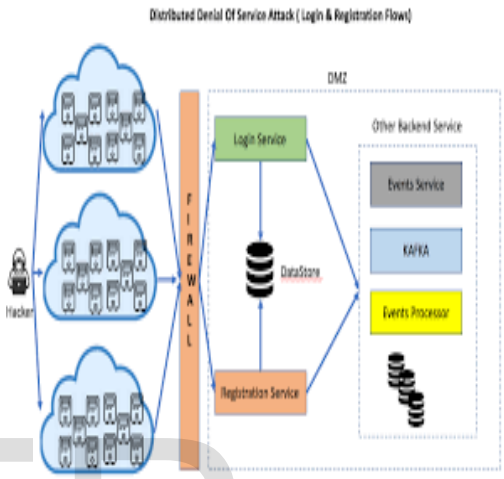

Figure 14: Distributed denial-of-service (DDOS) attacks

- **Man-in-the-middle (MitM) Attack:** A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Examples are session hijacking, IP Spoofing and Replay. To minimize the risk, don't allow employees to use public networks for any confidential work, or Implement virtual private networks (VPNs) to secure connections from your business to online applications and enable employees to securely connect to your internal private network from remote locations.

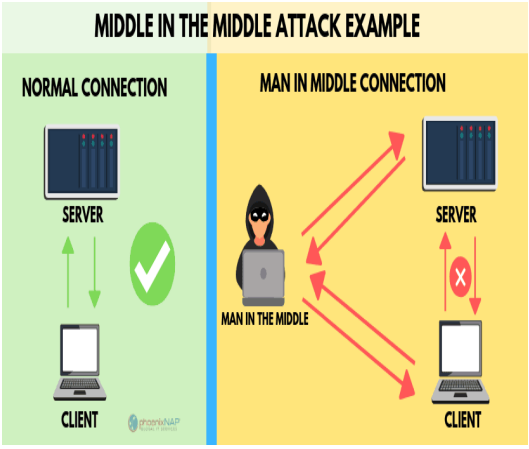

Figure 15: Man – in – the – Middle

Source: Google (2020)

- **Phishing and Spear phishing attacks:** Phishing attack is the practice of sending, emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering technical trickery.

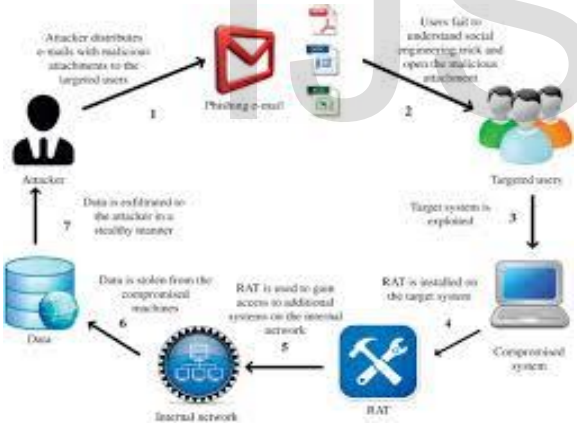

Figure 16: Phishing Attack

- Spear phishing is a targeted type of phishing activity attackers takes the time to conduct research into targets and create messages that are personal and relevant. To minimize the risk, develop a security policy that includes but isn't limited to password expiration and complexity and deploy a web filter to block malicious websites.

Countries	Number of Phishing Sites
Korea	87
China	75
India	25
Thailand	25
Japan	9
Chinese Taipei	18
Australia	4
Hong Kong	5
Malaysia	3
Singapore	2

Figure 17: Countries with phishing sites
Source: eBay

Figure 18: Ten Top Phishing Sites Hosting Countries
Source: Anti – Phishing Working Group

- **Drive-by Attack:** Drive by download attacks are common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP codeon one of the pages. To minimize the risk, one additional security control for preventing a drive-by virus infection is using different Web browsers, and only using vulnerable versions of IE on the specific applications that require it. General purpose Web browsing could be done using an alternative Web browser like Firefox, Chrome, Opera, etc. All of these browsers usually have different security vulnerabilities than IE, and will also require periodic security updates.

Figure 19: Drive - by Attack

- **SQL Injection attack:** SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the data base via the input data from the client to server SQL commands are inserted into data-plane input (for example, stead of the login or password) in order to run predefined SQL commands. To minimize the risk, input validation, parameterized queries, stored procedures, escaping and web application firewall should be apply.

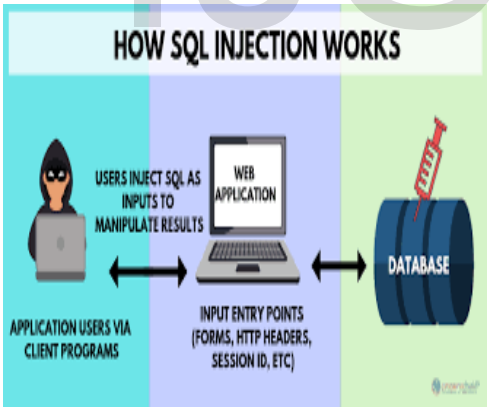

Figure 20: SQL Injection attack

- **Cross-site scripting (XSS) Attack:** XSS attacks use third-party web resources to run scripts in the victims' web browser or scriptable application. Specifically, the attacker injects a play load with malicious JavaScript into a website's database. When victim requests a page from the websites, the web site transmits the page, with the website transmits the page, with the attacker's play load as part of the HTML body, to the victim's browser, which executes the malicious script. To minimize the risk, an effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures filter input on arrival, encode data on output, content security policy and Using appropriate response headers.

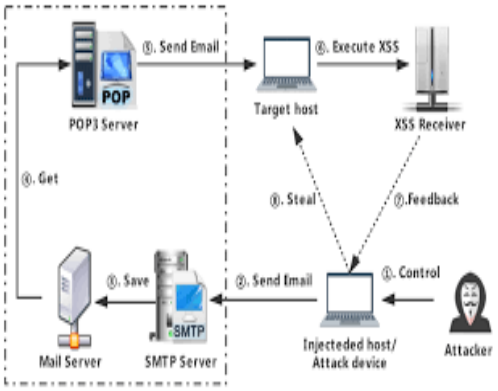

Figure 21: Cross-site scripting (XSS) Attack

- **Eavesdropping Attack:** Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. To minimize the risk, Eavesdropping attacks can be prevented by using a personal firewall, keeping antivirus software updated, and using a virtual private network (VPN)

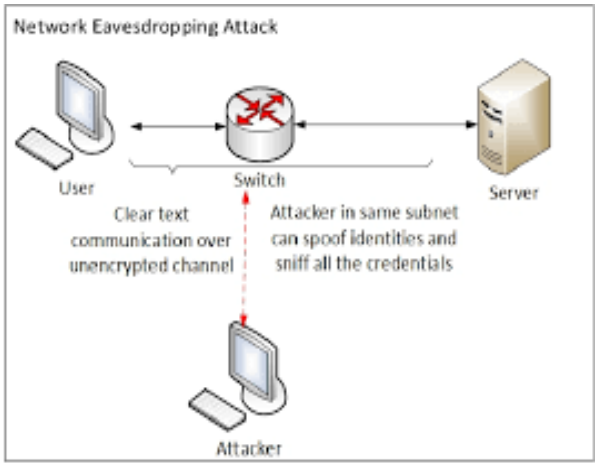

Figure 22: Eavesdropping Attack

- **Birthday Attack:** Birthday attacks are made against hash algorithms that are used to verify the integrity of a message

software or digital signature. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. To minimize the risk, the output length of the hash function used for a signature scheme can be chosen large enough so that the birthday attack becomes computationally infeasible, i.e. about twice as many bits as are needed to prevent an ordinary brute-force attack.

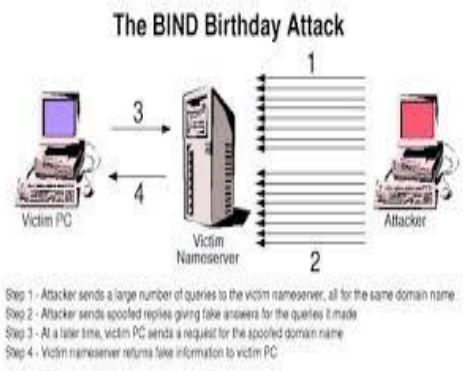

Figure 23: Birthday Attack

- **Malware Attack**- malicious software can be described as unwanted software that is installed your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the internet. Examples are, macro viruses, file infectors, system or boot record infectors, polymorphic viruses, stealth viruses, Trojans, logic bombs, worms, droppers, ransomware, adware, spyware. To minimize the risk, Malware attacks can be prevented by using a personal firewall and keeping antivirus software updated.

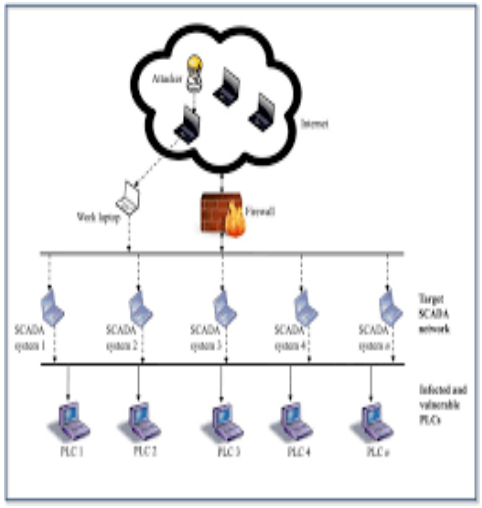

Figure 24: Malware Attack

A. Security measures in place: industry security initiatives for the cyber space:

Firewalls, Antivirus, Anti-Malware, Pass-Wording, Encryption, Biometric Authentication Systems, Intrusion Detection and prevention Systems, etc.

B. Some Tested Palliative solutions in place

If correctly installed, the following technologies can help to block attacks: (These will be explained further in the following pages).

- **Firewalls:** Firewalls are hardware or software devices that block certain network traffic according to their security policy.
- **Software solutions:** It exist to identify and remove malware and to help manage spam email. Many must be paid for but free versions are also available.
- **Authentication:** It involves determining that a particular user is authorized to use a particular computer. This can include simple mechanisms such as passwords, to more complex methods using biometric technology.
- **Hardware cryptography:** It uses computer chips with cryptographic capabilities intended to protect against arrange of security threats.
- **Patches:** They are programs designed by software manufacturers to fix software security flaws. Patching is often installed automatically. This reduces end-user participation and increases ease of use

VI. CONCLUSION

Cyber crime is real! The internet is the nervous centre of world economy. Cybercrime is conducted remotely and anonymously to take advantage of flaws in software code. Cyber crime has created major problems and has continued to increase at institutions of higher learning. The academia is emerging as a particularly vulnerable for internet crime. Organizations and individuals have suffered losses at the hands of cyber- criminals with only nine percent of such incidents reported to the security operatives. There is need for consistent training of the Nigerian Police in Cyber Crime Prevention and Forensic science for cyber crime policy and control. There is urgent need to develop a single national database to gather and compile cybercrime data. The National Assembly should consider enacting a legislation that encourages incident reporting while reducing the risks associated with reporting and provide policies that provide stronger sentences for those found guilty of committing a cybercrime.

REFERENCES

[1] Akpan, A. G., Mmeah S. and Baah Barida (2018). Cybercrime and Cyber security: A painted scenario of a new type of war. *Journal of Scientific and Engineering Research*, 5(10):185-197.

[2] Internet security Threats Report. Symantec, http://symantec.com/threatreprot/,last accessed: August, 2020. http://www.maawg.org/ last accessed: August, 2020.

[3] Goodman, S. E. and Lin, h. S. (2007). Toward a safer and more secure Cyberspace. The National AcademicsPress. Anti-phishing group tech report, http://www.antiphlishing.org/phishreports Acrhive.html, last accessed: September, 2020.

[4] Tatum, Malcolm (2010). "What Is a Cyber-attack?" Available on-line from: http://www.wisegeek.com/what-isa-cyberattack.htm (Accessed 29th September, 2020).

[5] Alhaji Idi Babate, Maryam Abdullahi Musa, Aliyu Musa Kida, Musa Kalla Saidu (2015). State of Cyber Security: Emerging Threats Landscape. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, Vol. 3, Issue 1, pp. 113 – 119.

[6] Julian jang – Jaccard and Surya Nepal (2014). A survey of emerging threats in Cyber security. *Journal of Computer and System Sciences*. Volume 80, Issue 5, pp. 973 – 993.

[7] Whitney, S. (2004). Trend turns more purchase coverage for cybercrime. Best's review, 105(8): 90. Oldwick, NJ: AM. Best Co. Inc.

[8] Kosutic, D 2007, what is Cyber security and how can ISO 271001 help? Blog. Accessed 5 September, 2020 < http://blog. iso27001standard.com/2011/10/25/what-is- cyber security and - how-can-iso-27001- help/#

[9] Williams, P. (2002). Organized crime and cyber crime: implications for business. Retrieved on September, 2020.

[10] Canty, D. (2012). Digital Danger Zone: tackling cyber security. Arabian Oil and Gas, http://www.arabianoilandgas.com/article-9868-digitaldanger-zone-tackling-cyber security/ last accessed September, 2020.

[11] Justin, M. Rao (2011). The economics of spam email metric MAAWG report Microsoft research. Available at: http://www.maawg.org/system/ les/news/ MAAWG 2013

[12] Ponemon, (2012) Cost of Cyber Crime Study: United Kingdom benchmark Study of UK Organizations, Ponemon Institute Research Report October.

[13] Australian Parliament the report of the inquiry into Cyber Crime http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

[14] DHSS and T Roadmap for cyber security research, Jan. 2009 http://www.cyber.st.dhs.gov/docs/DHS - Cybersecurity-Roadmap.pdf **(**Accessed: September, 2020**).**

[15] ChiChao Li, Wen Yuan Jen & Weiping Chang, Shihchieh Chou (2006*), Journal*

of Computers, Vol. 1, No. 6, Sept. 2006, Academicy Publisher, USA.

[16] Osuagwu O.E., Anyanwu E. (2003) Management of Information Technology at Periods of Technological Discontinuity, OIPH, Owerri, Nigeria, p. 23.

[17] Top 20 Countries found to have the most Cybercrime: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ (Accessed September 10th, 2020)

[18] List of countries with lowest malware infection rates in computers: https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/ (Accessed September 16th, 2020)

[19] Denise Marcia Chatam (2007). The Study on Cybercrime's Impact in the Workplace, Campus Technology, USA.

[20] McConnel, B. W. (2001). Hearing on Cybercrime, Committee on legal affairs and Human nights, parliamentary assembly of the Council of Europe, Paris, France: McConnel International.

[21] E.E. Schultz (2006). Where have the worms and viruses gone? New trends in malware Computer. Fraud Secure (7) (2006), pp. 4- 8

[22] Anti-phishing group tech reports: http://www.antiphishing.org/phishReports Archive.html (Accessed August 13th, 2013)

[23] Cluley, G. (2010), Sizing up the malware threat-key malware trends for 2010**.** Netw. Secur. (2010), 10.1016/S1353-4858(10)70045-3