International Digital Organization for Scientific Research
IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES 7(1):1-8, 2022. ISSN: 2579-0803

Evolving Cybercrimes and How to Contain them

Nwosu, John Nwachukwu
Department of Computer Science Federal Polytechnic, Oko, Anambra State, Nigeria
drnwachukwunwosu@gmail.com

ABSTRACT

This study examined the different modern types of cybercrimes and determines how they can be curbed. The study made use of secondary data that were collected from Federal Bureau of investigation (FBI), International telecommunication Unit (ITU), Sophos Inc., Forbes, and Cybint. Sophos Inc is a cyber security company that is based in the UK. It commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries on form of cyber attacks and cyber security. 100 respondents were selected from Nigeria different companies. Data were also collected from reports of SonicWall Network Security Provider, World Economic Forum, Federal Bureau of Investigation, International Telecommunication Unit, cyberpedia, and Kaspersky for the period 2020 – 2021. The study identified common cyber crimes that are evolving as cloud cyber attacks and cryptojacking. It also observed that ransomeware and other malware attacks are on the increase from 3013 till mow. It concludes that more awareness is needed among users of computers especially those that work in cyber security prone attack departments on social engineering prevention techniques. Users should use strong passwords and use anti-virus which should be updated regularly. There should be authentication and trail mechanism which will handle malicious insider attack.

Keywords: Cybercrimes, malware, cyberpedia, cryptojacking, passwords and anti-virus

INTRODUCTION

Cybercrime continue to be a growing threat despite effort by companies and government to curb it. Companies and organization lose money that run into billions of naira to cyber attacks every year [1,2,3]. The concern on the using threats has made the government and many organizations to channel energy and resources that equally run into billions of naira on research and technologies that will curb the menace of cyber crime, but despite the efforts, cybercrime remain on the increase. Report from Federal Bureau of Investigation (FBI) internet Crime Complaint Centre shows that there are millions of cyber threat reports in 2020 [4,5,6,7]. The increase in online business as a result of the COVID-19 pandemic is one of the factors that resulted to the increase in cybercrime. To curb the menace of cybercrime, the United nations, through one of its arms, the international Telecommunication Unit (ITU), undertake regular assessment of how different countries manage their cyber security and publish their report which comes as Global Cybersecurity Index [8,9,10].Regional organizations such as African unions and Economic Community of West African States (ECOWAS),have departments that deals with issues on cybersecurity. Also, countries and business enterprises are in the forefront of developing strategies that aim at curbing the menace of cybercrimes. Cybercriminals are adopting different strategies to launch their attack and are equally succeeding in the attacks despite huge amount of money that business owners, individuals and government are investing to curb the menace of cybercrime [11,12,13,14]. The effect of COVID-19 which forced many businesseswork remotely, emerging technologies such as Internet of Things (IOTs) – which aims at linking every device to the internet, cloud computing and new research in Artificial Intelligence and machine learning are some of the activities that have opened vulnerabilities for cyber attacks [15,16]. However, despite these efforts, cybercrime is still on the increase. With new technologies, not only that there is an increase in cyber attacks, the pattern

of attacks has drastically changed [17,18,19].

Purpose of study

The purpose of the study is to examine the modern types of cybercrimes and determine how they can be curbed.

Methodology

The study made use of secondary data that were collected from Federal Bureau of investigation (FBI), International telecommunication Unit (ITU), Sophos Inc., Forbes, and Cybint. Sophos Inc is a cyber security company that is based in the UK. It commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries on form of cyber attacks and cyber security. 100 respondents were selected from Nigeria different companies. Data were also collected from reports of SonicWall Network Security Provider, World Economic Forum, Federal Bureau of Investigation, International Telecommunication Unit, cyberpedia, and Kaspersky for the period 2020 – 2021.

Findings

The findings from some organizations on cyber attacks and their methods of operation are shown under the three major sub-headings of social engineering attacks, malware attacks and cloud cyber attacks. Social engineering include all the activities that involves luring cyber users to take actions that will reveal their private information, malware involves the codes that actually cause most of the harms that are prevalent in cyber space, while cloud computing involves the application of the two types of attacks on the cloud storage facilities

A. Social Engineering

Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. In this aspect, scammers pose as friends, customers, customer service representatives, law enforcement officials, and even family members to gain access to a victim's account. They can equally pose as a victim's family member to prompt money transfer to fraudulent accounts [9]. Some of the social engineering attacks include data leak/breach, identity theft, business email compromise, phishing hacking.

i. Data leak

Data breach exposes data to cybercriminals. In 2021, the number of data breach recorded by is 51, 829 [8].

ii. identity theft

In 2021, the number of identity thief recorded 51, 629 [8].

iii. Business Email Compromise (BEC)

Google report revealed that around 18million COVID-19 related phishing and malware emails threats are observed every day with 240 million spam messages. According to [4] Google Gmail blocks more than 100 million phishing emails. [4] reported that there was 200% increase in BEC attacks in 2020 as against the recorded attacks in 2019. The targets are companies that transact their business online and do online payment. Hackers pose as vendors, suppliers or customers and high money exchanges and redirect the victims to their accounts where they will make the deposit.

iv. Phishing

Phishing is a cybercrime that involve the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Phishing/vshing/smshing recorded the highest number of cyber attacks in 2021 with a total number of 323,927 attacks [8]. Elderly people in UK received emails and calls that promised them Covid-19 vaccinations as long as they provide data the email sender or caller asked for [12]. Another form of phishing is email recipients being asked to click link on health issues and retirements. Some of

these links leads to download of malware.

v. Hacking

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system [3]. Cybercriminals make people to believe that they are logging in to real platform but they are logging to fake platforms. [5] reported that hacking attacks occurs every 39 seconds on the internet. [9], reported that hacking attacks target small and medium scale industries. It reported that that out of 43% cyber attacks that target small business, 60% of the victims are out of business within six months.

B. Malware

Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the objectives: provide remote control for an attacker to use an infected machine, send spam from the infected machine to unsuspecting targets, investigate the infected user's local network and steal sensitive data [9]. Some of the current common malware are Trojan, adware, hacktool, riskware tool, backdoor, spyware, worm, rogue, ransomeware, highjacker, mobile malware and cryptojacking.

Top 10 business malware categories 2020 compared to 2019

	Threats	2019	2020	% Change
1	Trojan	11,140,084	6,135,219	-45%
2	Adware	4,586,057	3,997,158	-13%
3	HackTool	937,941	2,562,196	173%
4	RiskwareTool	1,715,806	1,763,072	3%
5	Backdoor	1,235,067	490,201	-60%
6	Spyware	291,525	440,368	51%
7	Worm	414,349	391,854	-5%
8	Rogue	94,210	243,208	158%
9	Ransom	704,991	199,838	-72%
10	Hijacker	248,877	167,252	-33%

Source: Malwarebytes Cyber Threat Report 2021

[10], reported that Nigeria experienced 16.7 million malware cyber attacks in 2021. They equally reported that Nigeria experienced 23% increase in cyber attacks in post Covid-19 period. World Economic Forum reported that in 2020, malware increased by 358%.

i. Ransomeware

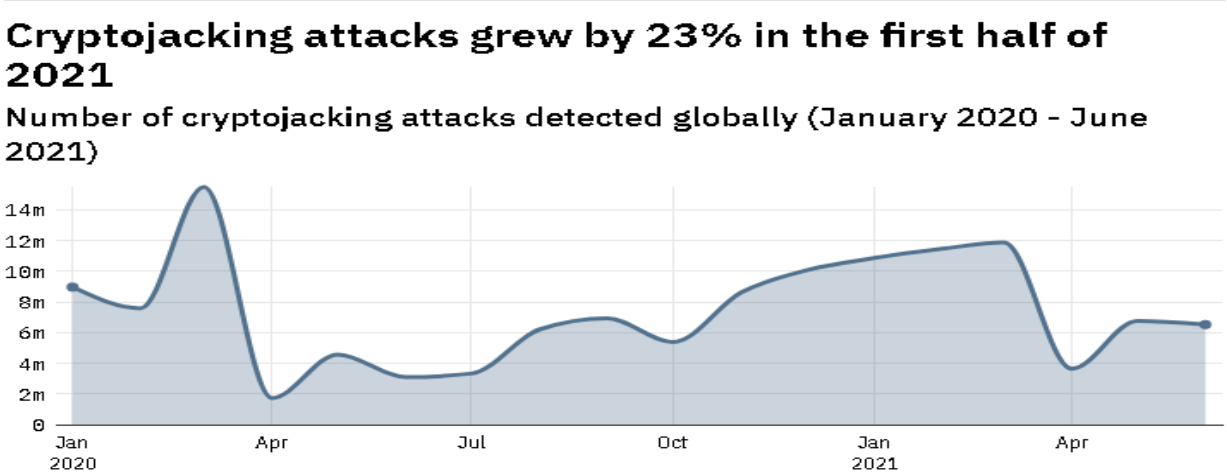
These include all cyber attacks which is perpetuated by cybercriminals with the mindset of their victim(s) paying ransome in order to get back their data. In 2020, 51% of organizations were hit by ransomeware attacks, 26% paid ransome to get their data back, but 1% of those that paid did not have their data released to them [11]. World Economic Forum reported that in 2020, ransomeware increased by 435%.

ii. Mobile Malware

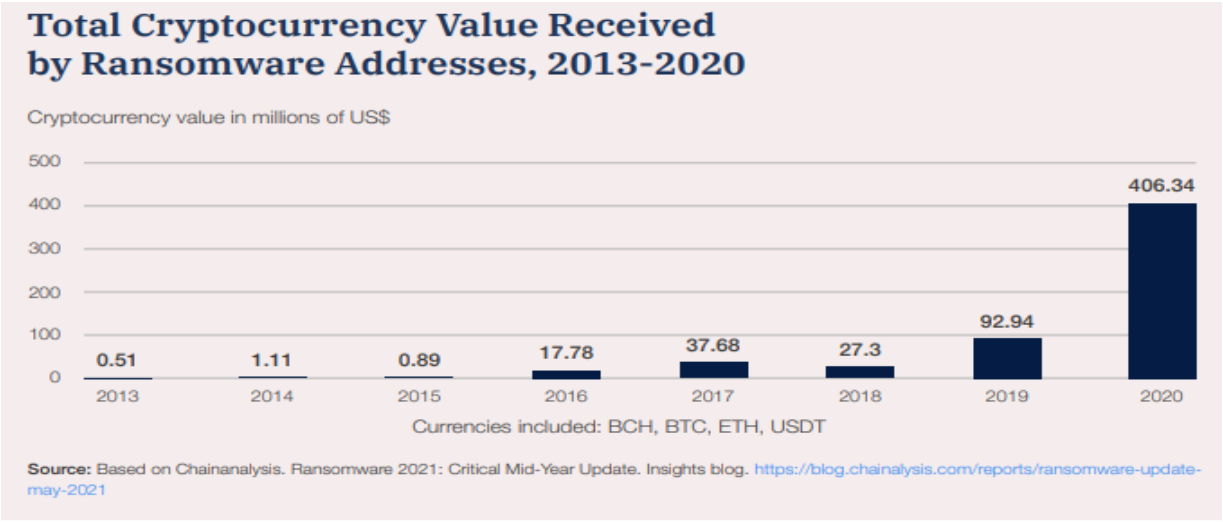
Mobile malware is common among mobile devices such as android based phones. For instance, Android phone that were attacked were disabled and the individuals had to pay ransomeware to get it back [13]. A report from [14] shows that Nigeria suffered 13.31% mobile attack in 2020.

iii. Cryptojacking

They are malware that were developed to infest systems to mine for cryptocurrency. The malware is designed to stay completely hidden from the victim and it takes the form of token or coins. Cryptojackers hack into devices to install cryptojacking software which work on the background to steal cryptocurrency wallets. They practice involve either getting a victim to click on a malicious link in an email that loads cryptomining code on the computer or infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser [5]. There was an increase in cryptojacking attacks in 2021. Million SonicWall detected 51.1million attacks in the first half of 2021, a 23% increase compared to the same period in 2020 [9].



Source: SonicWall Cyber Threat Report 2021 mid-year update.The report from World Economic Forum shows that cryptocurrency attacks rose from 0.51million in 2013 to 406.34 million in 2020.



Source: World Economic Forum

C. Cloud Cyber attacks

Cloud computing is the on-demand availability of computer system resources, especially cloud storage and computing power without direct active management by the user [9]. The popularity of cloud computing increased

with big companies like Amazon, Google and Microsoft which provide cloud computing platforms. The technology which began as a backup storage option has now become an all-inclusive platforms that has fundamentally altered the way organizations use, store and share information [12]. [9] reported that cloud cyber attacks accounted for 20% of all cyber attacks in 2020. Some of the biggest cloud cyber attacks include an attack on CAM4-an adult live streaming website in which 10.8billion sensitive entries were leaked. The leaked database includes location details, email addresses, IP addresses, payment logs and user name. Also, Advanced Info Service (AIS), witnessed data breach, which was observed by Justine Paine. The leaked database includes 8.3billion network flow logs and DNS query logs of ANN customers. Keepnet labs 2020 witnessed data leaks of 15billion entries [11].

Discussion

From the findings, the volume of activities on the internet has continued to be on the increase. The major factors that contribute to the increase include increase in population and the effect of COVID-19 pandemic. The current world population is 7.9 billion as of May 2022 [6]. The increase in population increased the number of users on the internet thereby increasing activities on the cyber space. As good cyber user increase, so cyber criminals also increase. Also, the effects of Covid-19 pandemic made many companies to resort to online transactions enabling people to work remotely from the confines of their homes. These increase in online businesses posed a lot of challenges in the cyber ecosystem as it involved volumes of files being transferred from one point to another on the cyber space. Cyber criminals always look for vulnerabilities to attack unsuspecting victims.

Current high Risk cyber attacks

From the findings, cloud cyber attacks, ransomeware and cryptojacking are the most current high risk cyber attacks.The vulnerabilities in cloud cyber attacks are caused by lapses in Cloud Service Providers (CSPs) and end users. Some of the vulnerabilities include misconfiguration, compromised user account, Application Program Interface (API) vulnerability and malicious insider activity.

Misconfiguration

CSPs have different platform for different organizations. Such platforms include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Unfortunately, some of the organizations do not have enough cloud cyber security potentials to appropriately deploy the platforms for theiruse.

Compromised user accounts

Many users on cloud service have weak passwords that can be exploited easily. So many spyware can keep database of passwords and with easy manipulations, cyber criminals can access a password.

API vulnerability

Many application providers produce documentation on how to perform certain activities on the application. Cybercriminals can exploit such vulnerabilities and launch attack.

Malicious insider activity

A malicious insider within an organization can commit a lot of havoc within the organization. They can steal data and expose the data to fellow cyber criminals.

Ransomeware

From the findings of Sophos and World Economic Forum, ransomeware attacks in currently on the increase. Although ransomeware attacks have been observed in previous years, the method of attacks currently differs from the previous methods. Modern technologies and cryptocurrency have increased cybercrimnals reliance on ransomeware. Many victims of cyber attacks reported that cybercriminals demand payments of ransome in cryptocurrency, the highest payment being made in bitcoin.

Cryptojacking

Cryptojacking is also another cybercrime that is on the increase as reported by SonicWall and World Economic Forum. Cryptojackers hack into devices to install cryptojacking software which work on the background to steal cryptocurrency wallets. Cryptojacking is on the increase as most businesses have started accepting payments in cryptocurrency. Cryptocurrencies have allowed cybercriminals to collect payments with an only modest risk of detection and monetary clawback [10].

Other cybercrimes

From the findings of Btdefender, FBI and Infosec, BEC attacks and phishing were relatively high in 2021. Malawarebytes also observed that the level of hacking and rogue software increased highly in 2021. Rogue software are cybercrime that use malware to trick users into revealing financial and social account details or paying for bogus products. Cybint report equally shows that hacking was on the increase in 2021. From Malwarebytes report, there were decrease in adware, Trojan, riskwaretool, worm, cracktool and virus while hacktool, spyware and rogue software witnessed an increase when compared to 2020.

How to prevent cybercrimes

Prevention of cybercrime depends on the nature of the attack. Each cybercrime has its own peculiar approach to prevent it.

Prevention of Social Engineering Attacks

Awareness remains a viable tool. Users should properly made to be aware of the various techniques cybercriminals use phishing to lure unsuspecting users into clicking their link. This awareness can be achieved by organizing workshop and seminars where cyber security professionals can properly guide the users. People should be wary of opening emails that they are not familiar with. They should be able to identify emails with unusual attachments and send to spam or quarantine. They should identify unauthorized emails trying to spoof a domain and send it to spam or quarantine. They should route emails that match phishing and malware controls to a new quarantine, and they should scan every linked image.

Prevention of malware

Malware can be prevented by the following techniques:

Firewall

This is a network system that monitors and controls incoming and outgoing packets based on established rules. It will block packets that are identified as being malicious from entering into a network or prevent it from leaving a network. Firewall programs should be installed at gateway systems.

Instruction Prevention System (IPS)

All the network system and links have to be identified and properly monitored. The system will know the nature of information that flows and whether an information can be permitted or not.

Deep Packet Inspection (DPI)

This is an advanced method of examining and managing network traffic. The program should be installed so that it will locate, identify, classify and reroute or blocks packets with specific data or code payloads so that such packets can be quarantined.Installation of Anti-virus. Some anti-virus programs can prevent some malware programs such as virus, Trojan, spyware and spam. These anti-viruses have to be updated regularly so that they can handle new malware that are discovered.

Virtual Private Networks (VPN)

This encrypts internet traffic and disguise online identity by hiding IP address and letting the network redirect it through specially configured remote server that is run by VPV host. When you surf online with a VPN, the VPN server becomes the sourse of the data thereby preventing the Internet Service Providers from seeing the websites you

visited and the data that were sent. This process guarantees identity protection.

Prevention of cloud cyber attacks

On misconfiguration, cloud users should be adequately trained by cloud owners on the security management. This will enable the cloud users to be able to recognize threats and know how to be proactive to forestalling the threats and attacks. Cloud users should also be made to realize the importance of strong passwords. They should change their passwords after sometime to avoid being victims of spyware. Documentation on the use of API are very important as they guide cloud users, but the aspects that deals with security should be separated and expose to only those in cybersecurity unit who will use the information. Inside cloud users have to be known. Their identification will involve knowing the infrastructure they use and time of usage. There should be access control and authentication that will be used to distinguished a user from another, and the log activities of each of them should be kept for easy audit trail. Also, only an authorized user will be able to use the system.

CONCLUSION

This study examined the different modern types of cybercrimes and determines how they can be curbed. It used secondary data that were obtained from various cybersecurity companies and some individual cyber security experts. The study observed that there are agreements among the companies on increase in the prevalence of some malware attacks, however the percentage of the attacks differ. This is as a result of the quantity of data that was available to the respective companies at the time of the research. The common cyber crimes that are evolving are cloud cyber attacks and cryptojacking. The impact of cryptocurrency has increased the percentage of attacks on ransomeware. Other types of cyber attacks such as malaware and other social engineering attacks remained on the increase. There is need more awareness among users of computers especially those that work in cyber security prone attack departments on social engineering prevention techniques. Users should use strong passwords and use anti-virus which should be updated regularly. There should be authentication and trail mechanism which will handle malicious insider attack.

REFERENCES

1. Cyberpedia (2020). “What is malware and how to stay protected from malware attacks”.
2. Retrieved from https://www.paloaltonetwork.com/cyberpedia/what-is-malware.html.
3. Federal Bureau of Investigation (2021). IC3 logs 6million complaint. Retrieved from https://www.fbi,com on 10 May 2022.
4. Infosec (2020). “Top 9 cybercrimetactics, technologies and trends in 2020: A recap”. Retrieved from https://www.resources.infosecinstitute.com on 15 May 2022.
5. International Telecommunication Unit (2021). Measuring digital development – facts and figures 2021. Retrieved from https://www.itu.inter.com on 12 May 2022.
6. Kaspersky (2021). Incident response analyst report 2021. Retrieved from https://www.media.kasperskycontenthub.com on 11 May 2022.
7. Kumaran, N. & Lugani, S. (2020). Protecting businesses against cyber threats during COVID-19 and beyond. Retrieved from https://www.cloud.google.com on 11 May 2022.
8. Malawarebytes (2021). Malwarebytes Cyber Threat report 2021Retrieved from https://www.go.malwarebytes.com/rs/805
9. Montazerolghaem, A., Yaghmaee, M. H. & Leon-Garcia, A. (2020). “Green cloud multimedia networking: NFV/SDN Based Energy-Efficient Resource Allocation”. *IEEE Transactions*

on Green Communications and Networking. 4(3): 873-889.

10. Morgan, N. (2021). Cloud cyber attacks: the latest cloud computing security issues. Retrieved from https://www.trislelelab,com on 10 May 2022.
11. Rosenzweig, P. (2021). "There is a better way to stop ransomeware attacks". New York Times (Guest Essay), 31 August 2021. Retrieved from https://www.nytimes.com/2021
12. Shepherd, M. (2021). 30 surprising small business cyber security statistiscs in 2021. Retrieved from https://www.fundera.com
13. Smith, Z. S. (2022). Cybercriminals stole $6.9 billion in 2021 using social engineering to break into remote workplace. Retrieved from https://www.forbes.com.
14. SonicWall (2021). Cyber Threat Report 2021 Midyear update. Retrieved from https://www.techmonitor.com/rs/805 on 15 April 2022.
15. Sophos (2021). "The state of ransomeware 2021. A sophos white paper of April 2021. Retrieved from https://www.sophos.com on 11 May 2022.
16. Sweeney, M. (2020). Cybint 2020 cybersecurity risk report for business. Retrieved from https://www.cybintsolution.com on 12 May 2022.
17. United Nations Population Division of Department of Economic and social welfare (2022). https://www.worldometer.com. Retrieved on 15 May 2022.
18. Williams, L. (2022). "What is hacking? Types of hackers/Introduction to cybercrime". Retrievedfromhttps://www.guru.com/what-is-hacking-introduction.html on 18 May 2022.
19. World Economic Forum (2020). Addressing systemtemic challenges and improving digital trust. Retrieved from https://www.weforum.com on 16 May 2022.