Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.11, No.2, 2021

A review of cyber security attack trends in Kenya

Dr. Anthony Luvanda

School of Science Technology and Engineering Alupe University

E-mail: luvanda@auc.ac.ke

Abstract

The COVID 19 pandemic led to a situation where Kenyan institutions were forced to embrace remote learning, remote working and e-commerce services. These basically led to an upsurge in financial cyber activity and with it came an upsurge in cybercrime. This paper conducted a review of available secondary data on cyber attacks in Kenya with the aim of identifying the most popular trends embraced by attackers while perpetrating cyber-attacks on financial institutions and their clients. The paper was also able to obtain a ranking of the most popular trends associated with attacks within the Kenyan cyber space.

Keywords: Cybersecurity, cyber-attacks, cybercrime, malware, phishing

DOI: 10.7176/JIEA/11-2-09

Publication date: November 30th 2021

1. Introduction

The comprehension of the term cybersecurity can only be made possible if we are able to first understanding the term from which it is coined, cyberspace. The widespread interconnectivity of digital technology is what is popularly referred to as Cyberspace. Cyberspace can be viewed to be just a hypothetical environment in which computer networks are communication enablers. The use of the term Cyberspace gained popularity in the 1990s when the use of terms such as Internet, networking, and digital communication were all growing dramatically and the term cyberspace was able to represent the many new notions and marvels that were emerging. (Lance 99)

According to Marco Mayer, Luigi Martino, Pablo Mazurier and Gergana Tzvetkova, Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and the electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share, and extract, use, eliminate information and disrupt physical resources.

With the above in mind then cybersecurity can be defined as engaging in activity that is aimed at protecting interconnected systems that consist of software, hardware and data, (Comodo 2018). Just like any other Information Systems security implementation approach, a cyber security system consists of hardware equipment, data, software, processes and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency plus recovery policies and activities.

Most Kenyans today operate in a digital environment where almost every activity and/or transaction in their lives is networked together, from internet banking to government infrastructure, where data is stored on computers and other devices. A fraction of the said data may be in the form of sensitive information irrespective of whether it is

intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative repercussions.

1.1 Cyber Security Breaches

Cyber security is a subset of information security which in turn has its own goals as far as implementing security is concerned. The goals however are universal in nature, focusing on the three objectives confidentiality; integrity; and availability, and are simply cascaded downwards and implemented at a cybersecurity level. It is on that basis that we look at the overall Information Security goals and how they apply to cybersecurity.

While considering breaches in cyber security one needs to put into consideration the following: who and where the attacker is; and what the attacker is trying to achieve, that is, what is the attack model that belongs to the threat. Different attackers will have different capabilities and also have different goals. Examples of cyber security breaches that maybe manifested during the perpetration of an attack may include but not be limited to:

(i) **XSS: Cross site scripting attacks** occurs when an attacker uses a web application to send malicious actions. It allows the attacker to take control of the victim's browser and obtain information on the user via the browser.

(ii) **SQL Injection:** makes it possible for an attacker to bypass security measures and execute malicious SQL statements, Where an attacker waits for a victim to initiate a query on the database and then modifies the SQL query to return additional results, not requested for by the victim, to the user.

(iii) **Session Hijacking:** where by an attacker steals a session id through the cookies or through a Trojan horse. During a session hijacking, a malicious hacker places himself/herself in between your computer and the website's server while you are engaged in an active session. He or she then actively monitors everything that happens on your account, and may even eject you from the session and take control of it.

(iv) **IP spoofing:** Creating a false IP address for the purpose of impersonating another network node.

(v) **Eavesdropping:** access to content while it is on transmission

(vi) **DNS spoofing:** exploiting weaknesses in the domain name server to divert traffic away from legitimate servers and direct them towards fake ones (Sitelock, 2019)

2. Methods and materials

The research relied heavily on secondary data to perform a comparative analysis of common cyber security attacks frequencies and trends in Kenya and more specifically in relation to financial transactions.

The advent of mobile money due to the ability to link mobile telephony via telcos to banks has led to a highly digitalized Kenyan economy, data from the Central bank of Kenya indicates that

mobile money transactions in Kenya jumped 52 percent to Sh3.26 trillion in the six months to June 2021. This in turn has led to an increase in cyber-attacks on players and their clients within the industry.

In its quarterly sector statistics report covering July-September 2020 the Communication Authority of Kenya reported 35.1 million cyber threats in the country, a rise of 152.9%. The report also indicated a rise in child online abuse, online abuse and online fraud with this being mainly attributed to working remote and an uptake on e-commerce thanks mainly to the COVID-19 Situation.

Despite the Kenyan government placing a huge focus on data protection up to the point of enacting the data protection act, the Ernest and Young Data Protection and Privacy Report for July 2021 shows that 41 per cent of firms still transfer their client's personal data to third party service providers. The report further states established that 53 per cent of companies do not seek the consent of their customers, thus violating the law that protects sensitive private information.

Statistics from Kaspersky further indicates that there were approximately 14 million malware attacks and 41 million potential unwanted programs in Kenya which accounted for 50% of all attacks in Africa thus ranking it with the highest cyber-attacks on the continent followed by South Africa and Nigeria. Corporate users and institutions continue to be the main targets of cyber attacks in Kenya with Kaspersky reporting that in the period between January to June 2021 29.3% of the 7 962 attacks recorded in the country targeted corporate users, which is clearly a cause for concern.

The National Kenya Computer Incident Response Team Coordination Center reported in June 2021 that cyberattack perpetrator's ability to innovate, develop and deploy ingenious and sophisticated techniques that are not easily detectable are on a steep rise. It further reveals that during the same period there were 21.56 Million Malware attacks, 3.76 million web application attacks and 2.89 million attacks on corporate software and/or networks perpetrated via Denial of Service (DDos)

3.Conclusion

Mobile banking security issues have been and continue to be a major concern within the mobile computing circles. More worrying is the fact that most perpetrates of attacks, take advantage of the users lack of awareness on security matters to perpetrate their attacks. (Luvanda et all 2014). Criminals on the Kenyan financial sector tend to take advantage of this with regards to cyber-attacks, unfortunately some of the activities are abetted by the same financial institution that are supposed to offer protection to their clients.

As already indicated 41 per cent of firms in Kenya still transfer their client's personal data to third party service providers despite existing laws prohibiting the same. The sharing of client information to third parties basically leads to unregulated/unsolicited text and email messages which in turn exposes the clients to phishing attacks and other fraudulent activities. This is basically referred to as phishing where attackers in Kenya will basically circulate messages offering freebees in the form of airtime, cash or various products and in the process the attackers end up collecting personal information from the victims with the aim of perpetrating a financial crime. Such messages can be channeled through legitimate looking text messages, social media messages, emails and counterfeit web pages that look identical to the companies' sites.

Over three quarters of successful cyber-attack actives in Kenya are in one form or another associated with malware. While we have cases where employees have been accused of sneaking malware vie a USB disk into a corporate network for purposes of initiating an attack in conjunction with individuals outside the network (a fact highlighted by the number of publicly announced staff dismissals by telcos and financial institutions) mainly as a part of a Cyber security syndicates that hack into financial institutions for purposes of embezzle money, it is worth noting that some devices are actually shipped to the African market with inbuilt malware. Take a case of mobile phones for example, there exists brands on the Kenyan market that have been proven to contain inbuilt malware. The issue in such a case is mainly two-fold in the sense that the malware has been installed in the user's handset without the

knowledge and consent of the user plus the fact that such programs may be exploited to perpetrate an attack with the most common approach being a disguise for malware download and/or execution.

Denial of service (DDoS) attacks are another source of concern in the Kenyan cyberspace environment. They are mainly aimed at disabling essential infrastructure and equipment, plus disrupting services.

Due to the technical complexities associated with ransomware, where attacks optimize

ransom payment by first exfiltrating data before encrypting it thus making it inaccessible to the legitimate users. Failure to meet the ransom demands may lead to corporate date being sold online to the highest bidder. The use of malware either in the form of a trojan horse or a pre-installed program in a portable device seems to be the most popular form of attack in Kenya for cyber criminals, this is followed closely by various forms of phishing with DDos attacks coming a distant third. Other forms of attacks like ransomware may seem to be low key at the moment but financial institutions and their clients still need to be aware and on the lookout for the same.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security, 4,* 65–88. https://doi/10.13052/jcsm2245-1439.414

Anthony Luvanda, Stephen Kimani and Michael kimwele (2014) Lack of awareness by end users on security issues affecting mobile banking: a case study of Kenyan mobile phone end users International Institute for Science, Technology and Education (IISTE) Journal of Information Engineering and Applications, ISSN (Paper)2224-5782 ISSN (Online)2225-0506.

Communication Authority of Kenya Annual Report for the year 2019/2020 https://ca.go.ke/wp-content/uploads/2021/05/Annual-Report-for-Financial-Year-2019-2020.pdf#

Communication Authority of Kenya First Quarter Sector Statistics Report for the financial year 2020/2021 (July - September 2020)

Comodo. (2018, December 24). *Computer vulnerability: Definition.* Retrieved from https://enterprise.comodo.com/blog/computer-vulnerability-definition/

Comodo. (2019, January 11). *What Is network security?* Retrieved from https://enterprise.comodo.com/blog/what-is-network-security/

Computer Security Resource Center. (n.d.). *Operations security (OPSEC).* Retrieved from https://csrc.nist.gov/glossary/term/operations-security

Ernest and Young Data Protection and Privacy Report July 22, 2021

https://kaspersky.africa-newsroom.com/press

https://kenyanwallstreet.com/cyber-attacks-edge-up-59-in-q2-2021-kaspersky/

KCB Group Sustainability Report 2020 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjtjez

r6LfzAhUxz4UKHf0VCC0QFnoECBEQAQ&url=https%3A%2F%2Fkcbgroup.com%2F2019-sustainability-report%2F&usg=AOvVaw0b2nLGsE9xAqCHKJl-zj_W

Lance, S (1999). "The varieties of cyberspace: Problems in definition and delimitation". Western Journal of Communication. 63 (3): 382–83

Lord, N. (2019, July 15). *What is cyber security? Definition, best practices & more.* Retrieved from https://digitalguardian.com/blog/what-cyber-security

Marco Mayer, Luigi Martino, Pablo Mazurier and Gergana Tzvetkova, Draft Pisa, 19 May 2014 https://www.academia.edu/7096442/How_would_you_define_Cyberspace

SiteLock. (2019, July 10). *Types of cybersecurity threats your incident response plan should include.* Retrieved from https://www.sitelock.com/blog/types-of-cybersecurity-threats/

Software Testing Help. (2019). *What is network security: Its types and management?* Retrieved from https://www.softwaretestinghelp.com/network-security/

Spencer, J. (2019). Why is cybersecurity important in 2019? Retrieved from https://securityfirstcorp.com/why-is-cyber-security-important/