Data breach challenges facing Kenyan Ecommerce

Elvine Saikwa[1], Moses Thiga [2]
[1]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: +254 719153128, Email: esaikwa@kabarak.ac.ke
[2]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: + 254 720780468, Email: mthiga@kabarak.ac.ke

Abstract

E-commerce in Kenya continues to grow in leaps and bounds mainly driven by increased affordability of smartphones, greater internet penetration and affordability and the very extensive automation of government services at the national and county government levels. The success stories and positive impacts in the form of greater convenience, efficiency, increased business revenues and improved revenue collections among others are well known. However, the practice has experienced a great number of challenges most of which have gone unreported and undocumented making it difficult for eCommerce practitioners to learn from the challenges of their counterparts. This study sought to develop a structured body of knowledge on the specific aspect of data breaches in the eCommerce practice in Kenya and examined the occurrences of these breaches, their impacts and further proposes actions for consideration by the practitioners in the sector.

Keywords: eCommerce, data breach, information security

1. Introduction

Ecommerce is sharing business information, maintaining business relationships and conducting business transactions by means of telecommunications networks (Zwass, 1998). The systems and communication networks used should be secure from potential attack vectors that can lead to data breaches. A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion (Rouse, 2017). Any organization should, therefore, take appropriate measures to protect its computer systems from attacks. In order to protect itself from attacks, an organization would have to implement the information security principles in its systems. Although taking appropriate measures does not guarantee a hundred percent security, and this has made it possible for hackers to attack and compromise systems and services.

Across the world, organizations and governments have experienced data breaches, and some of them have been reported while others have not. In Kenya, some organizations have experienced data breaches but we still do not have a body of knowledge on the breaches This study therefore sought to develop a body of knowledge so that eCommerce practitioners who have not been affected by data breaches can learn from the experiences of their counterparts and this would enable them to be better prepared to protect their systems from probable attacks.

2. Objectives

The main objective of this study is to document the nature of data breaches that organizations have experienced in Kenya.

3. Problem statement

Data breaches have been occurring in Kenya and they have been reported. Unfortunately, we still do not have a detailed body of knowledge where eCommerce practitioners can refer to so that they can learn from their counterparts. This study, therefore, sought to come up with a knowledge base of data breaches that have occurred in Kenya.

4. Literature review

Many organizations across the world, whether private or government have experienced data breaches that have led to loss of information worth billions of dollars. Besides information, organizations have also lost huge amounts of money for litigation and price hive offs when they were sold to other companies (Yahoo and Uber have been the biggest victims). Yahoo is a search engine, subject directory, and web portal (Collins, 2018) while Uber is a technology platform that uses its Uber application to connect driver-partners and riders (Uber, 2018). Clients belonging to those organizations have also had their personal information like credit card numbers and social security numbers compromised. According to (Kan, 2017), Yahoo experienced the largest ever breach in the history of the world, considering that over 3 billion user accounts were compromised. In addition, banking institutions like JP Morgan Chase, Heartland Payment Systems, Equifax, government institutions like the US Office of Personnel Management and private businesses like Adult Friend Finder Network, Sony, eBay , Uber, RSA Security have not been spared either (Armerding, 2018).After these attacks, a company like Yahoo forced password reset for all its users and introduced three-factor authentication of username, password and a verification code that is sent to users who try to login into their accounts. This indicates that no organization in the world is immune from these cyber-attacks. It is therefore not surprising that Kenya has also been a victim of data breaches.

In the recent past, the Government of Kenya, decided to automate most of its services and this is evidenced by eCitizen, iTax, National Transport and Safety Authority portal, online registration of students sitting for national examinations, among others. “The more we adopt IT and the more data we put online, the more we will see cyber-attacks targeted at the government in Kenya. The problem is, we are not secure,” Mr William Makatiani managing director of IT security firm Serianu said (Mumo, 2016). It is because of Kenya not being secure from cyber-attacks that we decided to investigate data breaches that organizations have experienced. We will look at the nature of the breaches, the loses they incurred after the violations and recommend appropriate measures to take so that an organization can protect itself from such attacks.

5. Methodology

In conducting the study, a critical evaluation of literature on data breaches in Kenya was used. The data obtained provided a basis for the study. Additionally, for ethical reasons, names of people were anonymized. For example, if a person’s name was Bob, it was changed to Anonymous person one.

6. Results

i) Kenya Revenue Authority (KRA)

The authority is charged with the responsibility of collecting revenue on behalf of the Government of Kenya. In the year 2017, they made discoveries that may have led to data breaches. The first one was when detectives discovered a hidden laptop at KRAs network chambers that was connected to using port 11 (Kamau & Cherono, 2017). The fraudster, accused person one, who was a former employee at KRA, planted the laptop which enabled him to siphon money into his account in addition to allowing access of crucial data by cybercriminals which led to the taxman losing millions of shillings (Ombati, 2017).

The other discovery was when they lost Sh3,985,663,858 through an attack that was propagated by interfering with the tax collector computer systems (Kakah, 2017; Okoth, 2017) over a period of one year between March 2016 to March 2017. The prosecution lawyer, prosecutor one, informed the court that the printout data seized from the suspect would fill a room measuring 30 by 40 feet. They also said that the analysed data indicated that the accused, accused person two had been working with suspects outside the country. According to (BBC, 2017), he is part of an international network involving expatriates from the United States and other countries that steals money from several state bodies using high tech equipment and software.

In the year 2018, the taxman sued internet giant Google over a mystery hack (Wasuna, 2018) that prompted investigations. Investigator one of KRA's DCI unit said that unauthorised email address on more than one occasion performed tasks reserved for the taxman officers and it infringed on the information security of KRA (Fayo, 2018; Muthomi, 2017)(Kakah, 2018). The mystery hacker may have probably accessed millions of data on taxpayers and he/she could have used the information to solicit for money from taxpayers who had avoided paying taxes.

ii) Safaricom PLC

Safaricom is one of the leading mobile network operators in Kenya and this is evidenced by the net profit of around Sh 55 billion in the year ending March 2018 (Kubania, 2018). Nevertheless, they have not been spared by hackers. In 2017, a mobile subscriber for Safaricom lost Sh260,000 through unauthorized sim swap (Mumo, 2017), though the money was later refunded. This was discovered after Safaricom detected suspicious activity on its network and their risk management unit caught the intrusion before it could escalate (Mumo, 2017; Kangethe, 2017). When investigations were done, the hack was associated with a Safaricom staff account

Similarly, in 2018, between the dates of 24th and 30th April, they suffered another attack. This time, an attacker by the name Attacker one, unlawfully sent 24,258,730 million queries to the Safaricom App system using a laptop and mobile phone with a Safaricom line with the intent to defraud Safaricom (Bocha, 2018; Karanja, 2018). The requests were not normal based on the historical data of the accused.

iii) Banks

Regrettably, banks have also been victims of cyber-attacks. In the year 2008, Equity bank was subjected to a social engineering attack when one of its staff was told over the phone to transfer money from an account that belonged to a company called Dyer and Blair to a fraudster (Ochieng, 2017). The client lost Sh 26,250,250.

In the year 2013, the Central Bank of Kenya website was subjected to a denial of service attack by a group called the Gaza Hacker Team (Nguta, 2013). Although, the website was restored at 11 pm, critical services like the exchange rate was severely affected during the attack.

In January 2015, the infamous hacker, accused person two and an accomplice accused person three were arraigned before a court of law and they were charged with hacking into NIC Bank database in December, 2014 (Okuttah, 2015). They later demanded to be paid 200-Bitcoins which was valued at KSh 6.2 million at that time. Failure to that would lead to them exposing confidential information (Agoya, 2015) which could have led to extortion of money from the clients whose information had been disclosed.

In January, 2018, National Bank of Kenya confirmed that they had lost Sh 29 million through a data breach. Initially, there had been reports in the social media they had lost between Sh 150 million and 340 million. National bank through its twitter handle said that unauthorized people gained access to several accounts and siphoned off money before the bank detected and froze the accounts (Alushula, 2018). The bank also assured customers that their accounts had not been affected (Macharia, 2018).

iv) Ministry of Foreign Affairs

The government of Kenya confirmed that the Ministry of Foreign Affairs had been hacked and as a result, the hackers were able to get access to some data which was classified as open (Mutambo, 2016). The Anonymous claimed responsibility for the hack and said that they acquired one terabyte of data and they would be releasing it in the dark web in phases (Waqas, 2016). The data dump contained confidential and non-confidential pdf and docx files from the ministry server including email conversations, letters of conversation related to weapon clearance in Namibia ,details about a business collaboration between Kenya and Oman, documents discussing state officials visit to Kenya, security related communication, international trade agreements and letters discussing the security situation in (South)Sudan where government forces are fighting the Sudan People's Liberation Army (SPLA). Surprisingly, it contained an alert email from an ICT administrator warning them of a phishing campaign that could compromise their staff ID and he even shared a screenshot of an email sent by the hackers (Waqas, 2016).

v) Ministry of Defence

Anonymous claimed responsibility of taking control of the ministry of defence twitter account and a senior ranked military official. This was confirmed through their twitter handle Anon_0x03. Two hours after the account had been restored, they regained control of the accounts (Mumo, 2016; Ombati, 2016; Munyori, 2016; Muraya, 2016). The Kenya Defence Forces in an interview with the Nation said that no confidential information been obtained (Mumo, 2016).

vi) National Oil

The Operation Africa banner by the anonymous that is against corruption, child labour and child abuse in March 2016 through the World Hacker Team were at it again. According to (Uzair, 2016), they were able to hijack the database of National Oil Corporation in Kenya and posted data and screen shoot online to prove legitimacy of their claim. The data contained email, usernames, email addresses and along with the user's rank. It also contained a survey by the company (Cimpanu, 2016)

vii) Communications Authority of Kenya (CA)

CA is the state agency that regulates internet resources for public and private entities. It is tasked with protecting all the governments websites from malicious attack (Sunday, 2017). In spite of this, hackers identified as AnonPlus defaced the organizations website together with the National Environment Management Authority (NEMA) website for several hours.

viii) Kenya Police Website

In January 2011, a renowned journalist called Journalist A posted on his twitter account posted that the Kenya police website had been hacked. The website normally contains information about and provided by Kenya's primary national law enforcement body. According to (Constantin, 2011), there was no information about the hacker's motives for targeting the website. The attack only affected the home page but the rest of the links indexed by Google remained accessible.

ix) Office of the President

According to (Waqas, 2015),on 11th May,2015, the official website for president of Kenya was hacked and the home page was replaced with the hacker's information. Indonesian hackers known as Gantengers Crew took responsibility for the hack. During an interview with HackRead, the hackers said that their reason for attacking the website was to show that they were powerful.

x) Office of the Attorney General

In the year 2013, the website of attorney general of Kenya was defaced by the hacker with the handle Dz Mafia of Algeria (Waqas, 2013). They left greetings for their team and curse messages for USA. However, they did not state their motivation for the attack (Waqas, 2013). The website was later restored.

xi) Google Kenya

One would really wonder why a person would even think of hacking google. Nevertheless, the hacker going by the name Tiger-M@te hacked Google.co.ke but he did not give any reason for his attack (Waqas, 2013). The website was later restored.

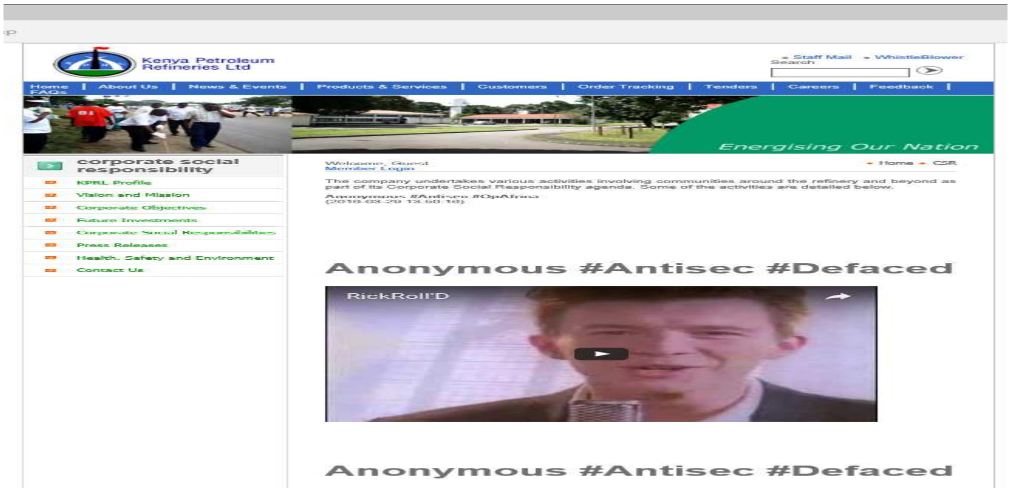
xii) Kenya Petroleum Refineries Limited

The organization was originally set up by Shell and the British Petroleum Company BP to serve the East African region in the supply of a wide variety of oil products. On 29th March, 2016, one of their website pages was defaced by Anonymous under their Operation Africa campaign (Cimpanu, 2016).The hackers did not breach the database or steal anything from the backend but they left a music video.Probably this was a stunt to show their capability.

7. Discussion

In the introduction, we mentioned that some of the data breaches are normally reported. This section discusses the identified breaches.

Among the breaches was defacement of websites. It consists of hacking into a web server and replacing a web page with a new page bearing some sort of message (Samuel, 2004). Some of the indicators of a defaced site is through notification by the hacker on the web pages or a peer. Defaced websites can lead to erosion of consumers' confidence, downtime, disruption of business activities, potential data breach and loss of time and money when restoring the website. This is the most prevalent attack in Kenya. The following images shows how the attacks were manifested.


Kenya Petroleum Refineries Ltd
» Staff Mail » WhistleBlower
Search
Home | About Us | News & Events | Products & Services | Customers | Order Tracking | Tenders | Careers | Feedback | FAQs
Energising Our Nation
corporate social responsibility
KPRL Profile
Vision and Mission
Corporate Objectives
Future Investments
Corporate Social Responsibilities
Press Releases
Health, Safety and Environment
Contact Us
Welcome, Guest
Member Login
• Home • CSR
RickRoll'D

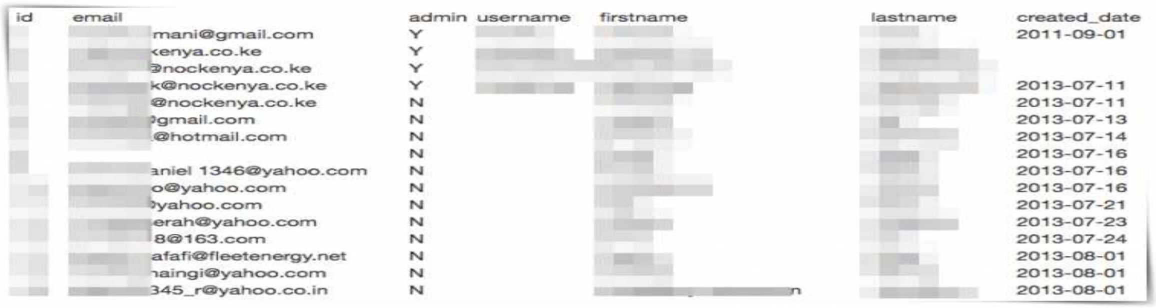
The company undertakes various activities involving communities around the refinery and beyond as part of its Corporate Social Responsibility agenda. Some of the activities are detailed below.

Anonymous #Antisec #OpAfrica
(2016-03-29 13:50:16)

Anonymous #Antisec #Defaced

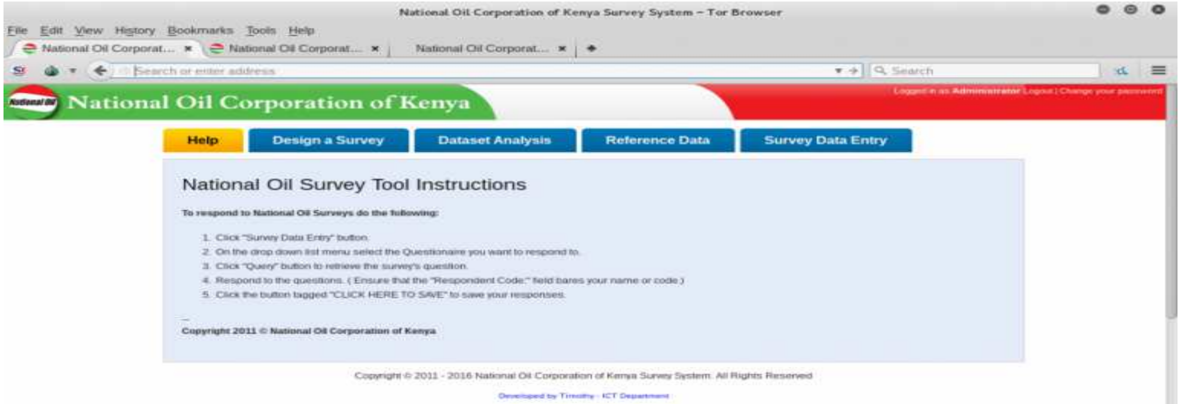
Anonymous #Antisec #Defaced

Figure 2:Kenya petroleum refineries limited defaced webpage



id	email	admin	username	firstname	lastname	created_date
[redacted]	[redacted]mani@gmail.com	Y	[redacted]	[redacted]	[redacted]	2011-09-01
[redacted]	[redacted]kenya.co.ke	Y	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]@nockenya.co.ke	Y	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]k@nockenya.co.ke	Y	[redacted]	[redacted]	[redacted]	2013-07-11
[redacted]	[redacted]@nockenya.co.ke	N		[redacted]	[redacted]	2013-07-11
[redacted]	[redacted]@gmail.com	N		[redacted]	[redacted]	2013-07-13
[redacted]	[redacted]@hotmail.com	N		[redacted]	[redacted]	2013-07-14
[redacted]		N		[redacted]	[redacted]	2013-07-16
[redacted]	[redacted]aniel 1346@yahoo.com	N		[redacted]	[redacted]	2013-07-16
[redacted]	[redacted]o@yahoo.com	N		[redacted]	[redacted]	2013-07-16
[redacted]	[redacted]@yahoo.com	N		[redacted]	[redacted]	2013-07-21
[redacted]	[redacted]erah@yahoo.com	N		[redacted]	[redacted]	2013-07-23
[redacted]	[redacted]8@163.com	N		[redacted]	[redacted]	2013-07-24
[redacted]	[redacted]afafi@fleetenergy.net	N		[redacted]	[redacted]	2013-08-01
[redacted]	[redacted]haingi@yahoo.com	N		[redacted]	[redacted]	2013-08-01
[redacted]	[redacted]345_r@yahoo.co.in	N		[redacted]n	[redacted]	2013-08-01

Figure 3: National oil Kenya hacked website


National Oil Corporation of Kenya Survey System – Tor Browser
File Edit View History Bookmarks Tools Help
National Oil Corporat... ×
National Oil Corporat... ×
National Oil Corporat... ×
Search or enter address
Search
National Oil
National Oil Corporation of Kenya
Logged in as Administrator Logout | Change your password
Help
Design a Survey
Dataset Analysis
Reference Data
Survey Data Entry

National Oil Survey Tool Instructions

To respond to National Oil Surveys do the following:

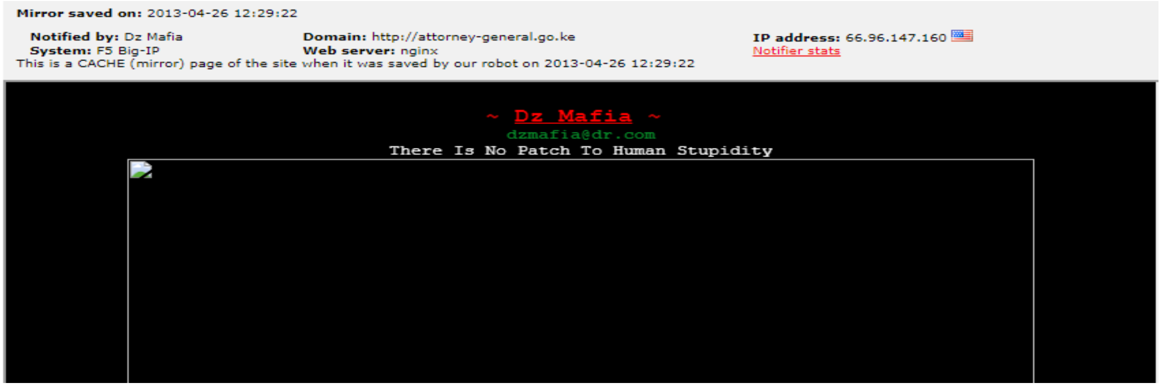
1. Click "Survey Data Entry" button.
2. On the drop down list menu select the Questionaire you want to respond to.
3. Click "Query" button to retrieve the survey's question.
4. Respond to the questions. (Ensure that the "Respondent Code:" field bares your name or code.)
5. Click the button tagged "CLICK HERE TO SAVE" to save your responses.

Copyright 2011 © National Oil Corporation of Kenya

Copyright © 2011 - 2016 National Oil Corporation of Kenya Survey System. All Rights Reserved

Developed by Timothy - ICT Department

Figure 4:National oil survey that was exposed



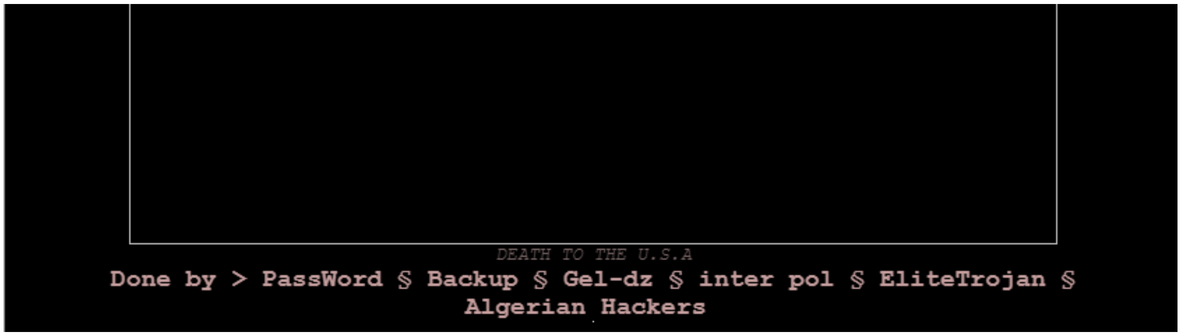
Mirror saved on: 2013-04-26 12:29:22

Notified by: Dz Mafia
System: F5 Big-IP
Domain: http://attorney-general.go.ke
Web server: nginx
IP address: 66.96.147.160
Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2013-04-26 12:29:22

~ Dz Mafia ~
dzmafia@dr.com
There Is No Patch To Human Stupidity

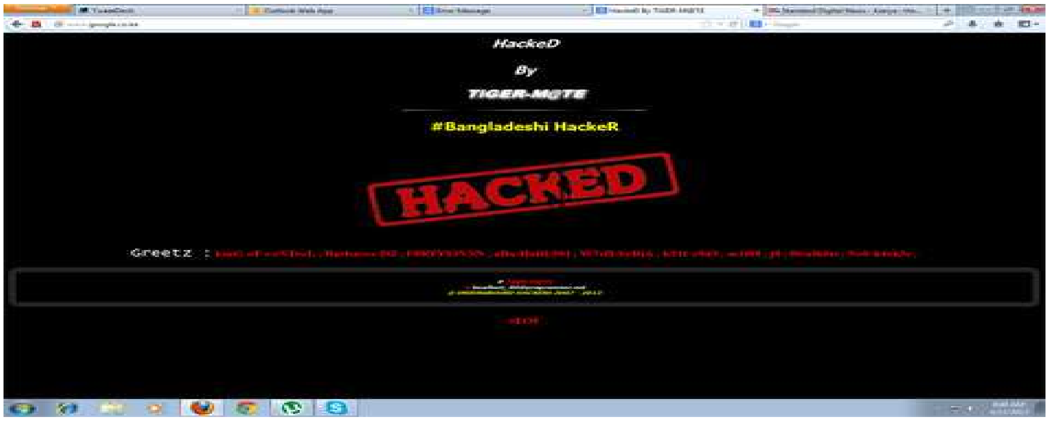
Figure 5: Ag website that was defaced



DEATH TO THE U.S.A

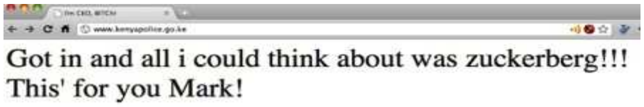
Done by > PassWord § Backup § Gel-dz § inter pol § EliteTrojan § Algerian Hackers

Figure 6: Ag website that was defaced



HackeD
By
TIGER-M@TE
#Bangladeshi HackeR
HACKED
Greetz : [illegible]

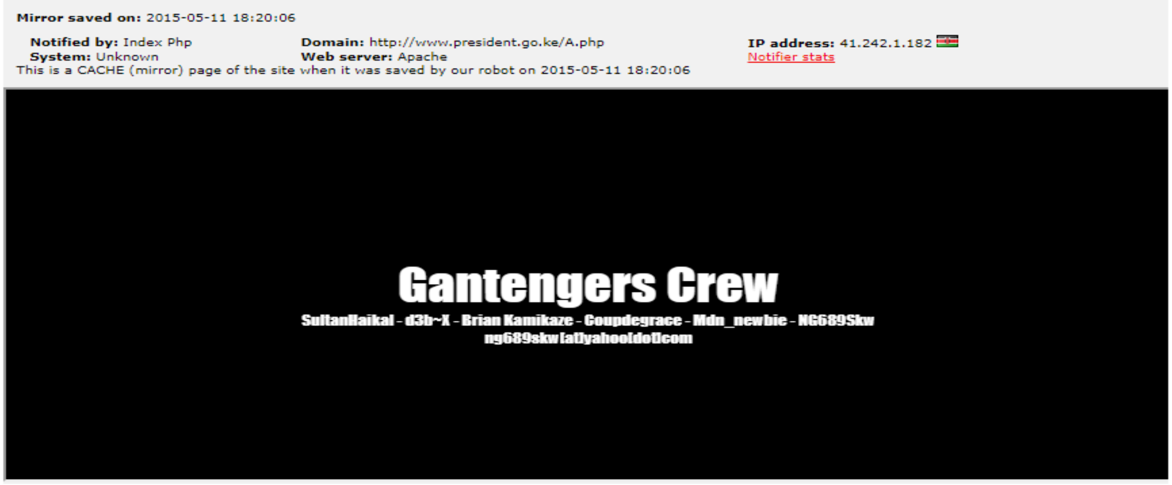
Figure 7: Google website that was defaced



www.kenyapolice.go.ke

Got in and all i could think about was zuckerberg!!!
This' for you Mark!

Figure 8:Kenya police web page that was defaced



Mirror saved on: 2015-05-11 18:20:06

Notified by: Index Php **Domain:** http://www.president.go.ke/A.php **IP address:** 41.242.1.182
System: Unknown **Web server:** Apache Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2015-05-11 18:20:06

Gantengers Crew

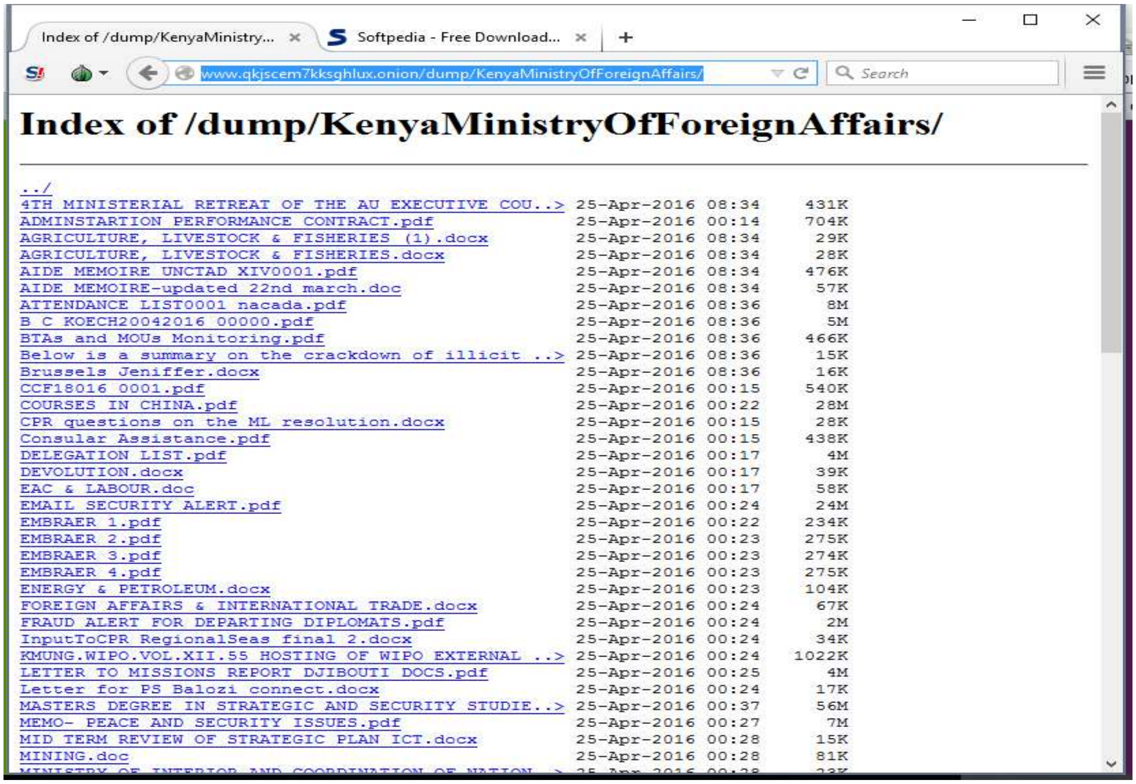
SultanHaikal - d3b~X - Brian Kamikaze - Coupdegrace - Mdn_newbie - NG689Skw
ng689skw[at]yahoo[dot]com

Figure 9: President's web page that was defaced

Insider threats was also another vector of data breaches. It normally happens when an individual working for an organization aide an intruder by allowing him to have unauthorized access to their internal systems. The access is made possible by sharing confidential information like usernames and passwords, installing backdoors in organizational computer systems or allowing remote access of the computer systems. This threat can lead to loss of revenue and personal information of people in an affected organization. Kenya Revenue Authority was a victim of this. They discovered a computer hidden in their network chamber. The computer may have been used to alter tax collection history for individuals, change log books of vehicles, falsify tax payment records, creation and deletion of user accounts, deletion of system logs and transfer of money from KRAs accounts.

Unauthorized sim swap is also another threat. According to Communications Authority of Kenya, it happens when a fraudster in collaboration with a staff at Safaricom or by himself calls you pretending to be an employee of a mobile service provider and asks for your personal identifiable information (PIN). After getting the PIN, he conducts a sim swap and the legitimate sim is switched off and rendered unusable to the owner. The fraudster gets access to all sim services like mobile money transfer, mobile and internet banking, SMS, voice calls and any other data service. Lastly, the fraudster transfers money in the phone or bank accounts. Unauthorized sim swap can mainly lead to loss of money and identity theft.

Phishing was also among the attacks. Phishing happens when an attacker possesses as a genuine entity and asks for confidential information like usernames and password. The confidential information may be obtained when legitimate users are requested to change their passwords or update their records. This happened to the staff working at the ministry of foreign affairs. Such attacks normally lead to compromises of user accounts and exposure of information. The following image shows the information that was exposed after the attack.


Index of /dump/KenyaMinistry...
Softpedia - Free Download...
www.qkjscem7kksghlux.onion/dump/KenyaMinistryOfForeignAffairs/
Search

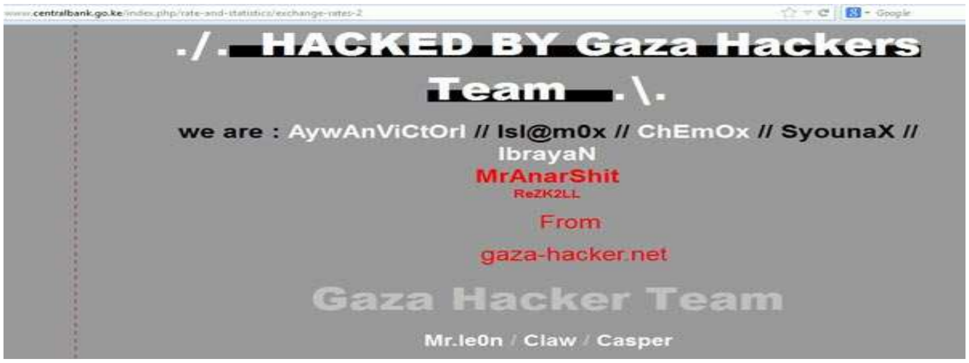
Index of /dump/KenyaMinistryOfForeignAffairs/

```
../
4TH MINISTERIAL RETREAT OF THE AU EXECUTIVE COU..> 25-Apr-2016 08:34     431K
ADMINSTARTION PERFORMANCE CONTRACT.pdf             25-Apr-2016 00:14     704K
AGRICULTURE, LIVESTOCK & FISHERIES (1).docx        25-Apr-2016 08:34      29K
AGRICULTURE, LIVESTOCK & FISHERIES.docx            25-Apr-2016 08:34      28K
AIDE MEMOIRE UNCTAD XIV0001.pdf                    25-Apr-2016 08:34     476K
AIDE MEMOIRE-updated 22nd march.doc                25-Apr-2016 08:34      57K
ATTENDANCE LIST0001 nacada.pdf                     25-Apr-2016 08:36       8M
B C KOECH20042016 00000.pdf                        25-Apr-2016 08:36       5M
BTAs and MOUs Monitoring.pdf                       25-Apr-2016 08:36     466K
Below is a summary on the crackdown of illicit ..> 25-Apr-2016 08:36      15K
Brussels Jeniffer.docx                             25-Apr-2016 08:36      16K
CCF18016 0001.pdf                                  25-Apr-2016 00:15     540K
COURSES IN CHINA.pdf                               25-Apr-2016 00:22      28M
CPR questions on the ML resolution.docx            25-Apr-2016 00:15      28K
Consular Assistance.pdf                            25-Apr-2016 00:15     438K
DELEGATION LIST.pdf                                25-Apr-2016 00:17       4M
DEVOLUTION.docx                                    25-Apr-2016 00:17      39K
EAC & LABOUR.doc                                   25-Apr-2016 00:17      58K
EMAIL SECURITY ALERT.pdf                           25-Apr-2016 00:24      24M
EMBRAER 1.pdf                                      25-Apr-2016 00:22     234K
EMBRAER 2.pdf                                      25-Apr-2016 00:23     275K
EMBRAER 3.pdf                                      25-Apr-2016 00:23     274K
EMBRAER 4.pdf                                      25-Apr-2016 00:23     275K
ENERGY & PETROLEUM.docx                            25-Apr-2016 00:23     104K
FOREIGN AFFAIRS & INTERNATIONAL TRADE.docx         25-Apr-2016 00:24      67K
FRAUD ALERT FOR DEPARTING DIPLOMATS.pdf            25-Apr-2016 00:24       2M
InputToCPR RegionalSeas final 2.docx               25-Apr-2016 00:24      34K
KMUNG.WIPO.VOL.XII.55 HOSTING OF WIPO EXTERNAL ..> 25-Apr-2016 00:24    1022K
LETTER TO MISSIONS REPORT DJIBOUTI DOCS.pdf        25-Apr-2016 00:25       4M
Letter for PS Balozi connect.docx                  25-Apr-2016 00:24      17K
MASTERS DEGREE IN STRATEGIC AND SECURITY STUDIE..> 25-Apr-2016 00:37      56M
MEMO- PEACE AND SECURITY ISSUES.pdf                25-Apr-2016 00:27       7M
MID TERM REVIEW OF STRATEGIC PLAN ICT.docx         25-Apr-2016 00:28      15K
MINING.doc                                         25-Apr-2016 00:28      81K
MINISTRY OF INTERIOR AND COORDINATION OF NATION..> 25-Apr-2016 00:28      23K
```

Figure 10: Exposed information from the ministry of foreign affairs

Information systems were also infiltrated. System infiltration happens when unauthorized users gain unauthorized access to an organizations internal system. This access can lead to loss of revenue and confidential information of users and clients of a given organization. National bank of Kenya and Safaricom detected the intrusion using their intrusion detection systems and stopped the attacks. NIC bank received threatening emails of black mail from hackers. KRA found logs of an unauthorised email account that had performed transactions on its systems.

Denial of service is also another attack. It happens when a web server is flooded with requests thereby constricting the bandwidth and making it difficult for legitimate requests to get response. Central bank of Kenya was a subject of this attack which caused a huge disruption of business activities and it resulted in loss of money because clients could not get access to the offered services. Normally, denial of service attack results from poor programming practises or programmer error. The banks main url address http://www.centralbank.go.ke gave a not found response after the attack. The following image shows the response from their website when the attack happened.



www.centralbank.go.ke/index.php/rate-and-statistics/exchange-rates-2

./. HACKED BY Gaza Hackers Team .\.

we are : AywAnViCtOrl // Isl@m0x // ChEmOx // SyounaX // IbrayaN

MrAnarShit

ReZK2LL

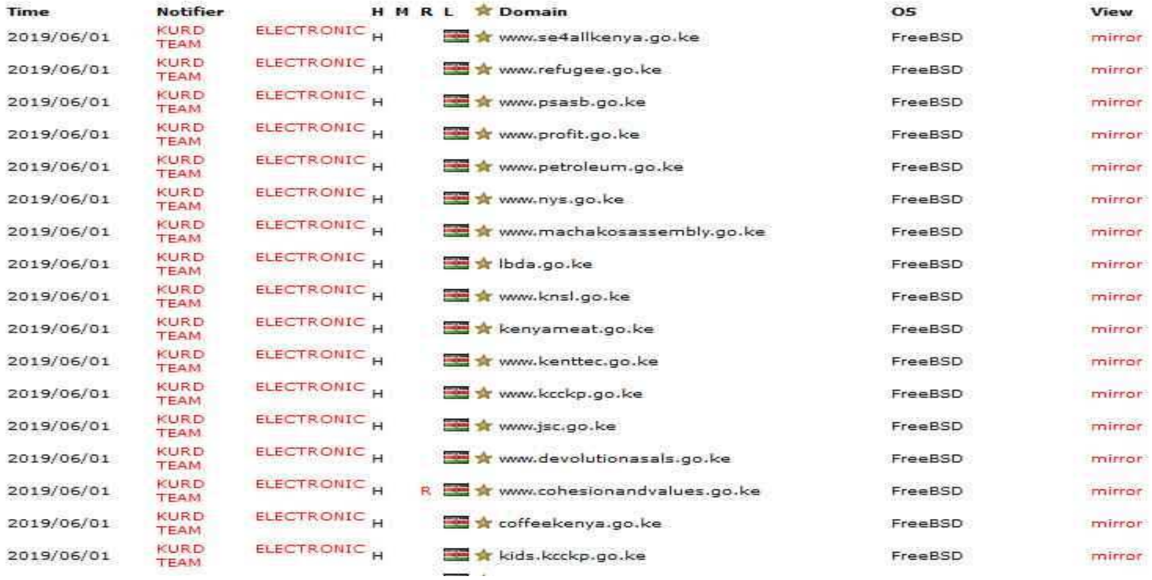
From

gaza-hacker.net

Gaza Hacker Team

Mr.le0n / Claw / Casper

Figure 11: CBK website after the attack



Time	Notifier		H	M	R	L	☆ Domain	OS	View
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.se4allkenya.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.refugee.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.psasb.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.profit.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.petroleum.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.nys.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.machakosassembly.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ lbda.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.knsl.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ kenyameat.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.kenttec.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.kcckp.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.jsc.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ www.devolutionasals.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H		R	🇰🇪	☆ www.cohesionandvalues.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ coffeekenya.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H			🇰🇪	☆ kids.kcckp.go.ke	FreeBSD	mirror

Figure 12: List of hacked websites in Kenya, 2019. (Source, Zone-H)

Password guessing was also used. It happens when an attacker tries to get access to an account by either guessing or running automated scripts to find any possible combination of password and username. Ministry of Defence in Kenya and a senior ranked military officer in Kenya twitter accounts were subjected to this attack and their account was taken over by hackers. They posted derogative tweets about the military. One of the tweets read “So much poverty in Africa while you are wasting money in guns.” This raises the question of whether the real hackers were the militia that the government of Kenya was fighting in Somalia. In addition, during the breach, the number of followers of the military’s twitter account increased. Did this mean that the followers subscribed to the ideas of the attackers after getting wind of the breach that had occurred.

Observations

We observed that, after the breaches have occurred, most of the affected organizations do not publicize the data breaches. Additionally, some of the organizations take litigation measures against those found/suspected of trying to get unauthorised access to their information systems. Furthermore, some of the organizations assure their clients that their personal information had not been interfered with. Majority of the organizations affected belong to the government of Kenya.

Lastly, some of the organizations opted to keep quiet about the breaches that they had experienced.

Recommendations

We would like to recommend that, organizations should conduct penetration testing on their systems so that potential vulnerabilities can be identified and patched in order avoid data breaches.

We would also recommend that the government of Kenya should implement proper security policies which would help its institutions to mitigate against data breaches

Conclusion

Data breaches will continue to occur to organizations if they do not take their information security with great concern. Given that most of the affected organizations belong to the government, it is imperative that the government of Kenya takes appropriate measures to secure its systems from any potential attacks.

This study has been able identify organizations that have experienced data breaches and documented how they happened. ECommerce practitioners should take lessons from the discussed data breaches so that they can be able to equip themselves with the necessary knowledge, tools and techniques to deal with data breaches before and after they happen.

References

Agoya, V. (2015, 4 10). Meet the man police link to Safaricom, NIC Bank frauds. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/The-man-police-have-linked-to-Safaricom-NIC-Bank-fraud/539550-2681054-46or3ez/index.html

Alushula, P. (2018, 1 20). National Bank reassures customers after Sh29m fraud. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2001266542/national-bank-reassures-customers-after-sh29m-fraud

Armerding, T. (2018, 1 26). The 17 biggest data breaches of the 21st century. *CSO*. Retrieved from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

BBC. (2017, 3 22). Kenya Revenue Authority 'lost $39m to hacker'. *BBC News*. Retrieved from https://www.bbc.com/news/world-africa-39351172

Bocha, G. (2018, 5 15). Man in court for trying to hack Safaricom app. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Man-charged-for-trying-to-hack-Safaricom-app/4003102-4563176-132uduw/index.html

Cimpanu, C. (2016, 5 30). Anonymous Leaks Employee Details from National Oil of Kenya. *Softpedia News*. Retrieved from https://news.softpedia.com/news/anonymous-leaks-employee-details-from-national-oil-corporation-of-kenya-504671.shtml

Cimpanu, C. (2016, 3 29). Anonymous Rickrolls Kenyan Petrol Refinery as Part of Its Anti-Corporations Op. *Softpedia News*. Retrieved from https://news.softpedia.com/news/anonymous-rickrolls-kenyan-petrol-refinery-as-part-of-its-anti-corporations-op-502325.shtml

Collins, J. (2018, 5 26). What is Yahoo? Yahoo 101. *Lifewire*. Retrieved from https://www.lifewire.com/what-is-yahoo-3483209

Constantin, L. (2011, 1 4). Hacker Defaces Kenyan Police Website in Mark Zuckerberg's Honor. *Softpedia News*. Retrieved from https://news.softpedia.com/news/Hacker-Defaces-Kenyan-Police-Website-in-Mark-Zuckerberg-s-Honor-176141.shtml

Fayo, G. (2018, 6 19). KRA duel with Google in Gmail account hack probe. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/KRA-duel-with-Google-in-Gmail-account-hack-probe/4003102-4621152-eb47ls/index.html

Kakah, M. (2017, 3 28). Court detains computer geek in Sh4bn KRA case for 40 days. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Alex-Mutungi-Mutuku-KRA-cybercrime-kenya/1056-3867562-10bq6hvz/index.html

Kakah, M. (2018, 1 31). Google wins order against email search in battle with KRA. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Google-wins-order-against-email-search-in-battle-with-KRA/4003102-4286500-egyx30z/index.html

Kamau, J., & Cherono, S. (2017, 3 9). Police bust ring of hackers in multi-million shilling KRA, bank thefts. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Police-bust-ring-of-hackers/1056-3842558-11h7q5xz/index.html

Kan, M. (2017, 3 2). Yahoo execs botched its response to 2014 breach, investigation finds. *CSO*. Retrieved from https://www.csoonline.com/article/3176181/security/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html

Kangethe, K. (2017, 4 6). Safaricom foils elaborate attempt to hack company systems. *CapitalBusiness*. Retrieved from https://www.capitalfm.co.ke/BUSINESS/2017/04/SAFARICOM-FOILS-ELABORATE-ATTEMPT-HACK-COMPANY-SYSTEMS/

Karanja, F. (2018, 5 16). Man charged with unlawful access to Safaricom systems. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/article/2001280627/man-charged-with-unlawful-access-to-safaricom-systems

Kubania, J. (2018, 5 9). Safaricom full-year profit hits Sh55.3bn, Bob makes comeback. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Safaricom-full-year-profit-Sh55-3bn-Bob-makes-comeback/4003102-4552246-14m8rsoz/index.html

Macharia, K. (2018, 1 19). Fraudsters steal Sh29Mn from National Bank of Kenya. Retrieved from https://www.capitalfm.co.ke/business/2018/01/fraudsters-steal-sh29mn-national-bank-kenya/

Mumo, M. (2016, 7 22). Cyber security in the spotlight as hackers infiltrate defence account. *Daily Nation*. Retrieved from https://www.nation.co.ke/business/Cyber-Security-Hacking-KDF-Emmanuel-Chirchir/996-2393516-10j3pduz/index.html

Mumo, M. (2017, 4 6). Two men charged with hacking into Safaricom system. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/Two-men-charged-with-hacking-Safaricom-system/539550-3880240-140vv0az/index.html

Munyori, W. (2016, 7 21). Group hacks defence forces Twitter account. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Group-hacks-defence-forces-Twitter-account/1056-2392622-format-xhtml-r58cnaz/index.html

Muraya, J. (2016, 7 22). Kenya military Twitter accounts ‘captured’ again. *CapitalNews*. Retrieved from https://www.capitalfm.co.ke/news/2014/07/kenya-military-twitter-accounts-captured-again/

Mutambo, A. (2016, 4 28). Govt admits hackers stole data from Foreign Affairs ministry. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Govt-admits-hackers-stole-data-at-Foreign-Affairs-ministry/1056-3180962-90t2wyz/index.html

Muthomi, K. (2017, 2 1). Google Kenya battle State in digital privacy suit. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2001268029/google-battle-state-in-digital-privacy-suit

Nguta, J. (2013, 7 22). Central Bank of Kenya website hacked. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2000089020/central-bank-website-hacked

Ochieng, A. (2017, 12 23). Banks vulnerable to theft by staff, not just tunnel diggers. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Banks-vulnerable-to-thefts-by-staff/1056-4239424-13tjigjz/index.html

Okoth, B. (2017, 3 22). This man Mutuku: Inside opulent lifestyle of man, 28, charged with loss of KRA's Ksh4 billion. *Citizen Digital*. Retrieved from https://citizentv.co.ke/news/this-man-mutuku-inside-opulent-lifestyle-of-man-28-charged-with-loss-of-kras-ksh4-billion-161518/

Okuttah, M. (2015, 4 10). Meet the man police link to Safaricom, NIC Bank frauds. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/The-man-police-have-linked-to-Safaricom-NIC-Bank-fraud/539550-2681054-46or3ez/index.html

Ombati, C. (2016, 7 23). KDF Twitter account hacked yet again. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/article/2000129139/kdf-twitter-account-hacked-yet-again

Ombati, C. (2017, 3 11). How Kenyan banks lost Sh30 billion in two years to tech savvy criminals. *The Standard*. Retrieved from https://www.standardmedia.co.ke/business/article/2001232241/how-kenyan-banks-lost-sh30-billion-in-two-years-to-tech-savvy-criminals

Rouse, M. (2017, 12). Data breach. *TechTarget*. Retrieved from https://searchsecurity.techtarget.com/definition/data-breach

Samuel, A. W. (2004). *Hacktivism and the Future of Political Participation (Doctoral dissertation).* Cambridge, Massachusetts: Harvard University .

Sunday, F. (2017, 1 7). Shame as Kenya's Internet regulator website hacked. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2000228978/shame-as-kenya-s-internet-regulator-website-hacked

Uber. (2018, 1 1). What is Uber? *Uber Help*. Retrieved from https://help.uber.com/h/eac2e43e-af42-4521-a042-2982c18664af

Uzair, A. (2016, 6 1). Anonymous Linked Team Hacks Kenyan Oil Firm Against Police Brutality. *HackRead*. Retrieved from https://www.hackread.com/anonymous-hacks-kenyan-oil-firm-against-police-brutality/

Waqas, A. (2013, 4 30). Attorney General of Kenya Website Hacked by Dz Mafia Algerian Hacker. *HackRead*. Retrieved from https://www.hackread.com/attorney-general-of-kenya-website-hacked-by-dz-mafia/

Waqas, A. (2013, 4 15). Google Kenya Hacked and Defaced by Tiger-M@te Hacker. *HackRead*. Retrieved from https://www.hackread.com/google-kenya-hacked-and-defaced-by-tiger-mte-hacker/

Waqas, A. (2015, 5 13). President of Kenya Website Hacked by Indonesian hackers. *HackRead*. Retrieved from https://www.hackread.com/kenya-president-website-hacked-indonesia-crew/

Waqas, A. (2016, 4 28). Anonymous Leaks 1TB of Data from Kenya' Ministry of Foreign Affairs. *HackRead*. Retrieved from https://www.hackread.com/anonymous-hacks-kenya-ministry-foreign-affairs/

Waqas, A. (2016, 4 28). Anonymous Leaks 1TB of Data from Kenya' Ministry of Foreign Affairs. *HackRead*. Retrieved from https://www.hackread.com/anonymous-hacks-kenya-ministry-foreign-affairs/

Wasuna, B. (2018, 2 1). Taxman, Google Kenya in court battle over mystery KRA hack. *The Star*. Retrieved from https://www.the-star.co.ke/news/2018/02/01/taxman-google-kenya-in-court-battle-over-mystery-kra-hack_c1706694

Zwass, V. (1998). *Structure and Macro-level Impacts of Electronic Commerce: From Technological Infrastructure to Electronic Marketplaces.* McGraw-Hil