KENYA CYBER SECURITY REPORT 2012

Getting Back to Security Basics

EDITION ONE

SERIANU

CYBER INTELLIGENCE TEAM

KENYA CYBER SECURITY REPORT 2012

Getting Back to Security Basics

EDITION ONE

Contents

SERIANU

Introduction

Welcome to the first edition of the Serianu Kenya Cyber Security Report2012: Getting back to security basics. This report is prepared by the Serianu Cyber Intelligence Team (CIT). At Serianu we strongly believe that as a country we cannot adequately stop information security threats unless we fully understand them. Therefore, we have established a very qualified and experienced team dedicated to thoroughly researching, analysing and understanding the motives and methods of information security threats in Kenya. The team also provides cyber security assessment, detection and mitigation services.

Executive Summary

Over the past couple of years, internet usage in Kenya has grown rapidly due to high demand and increase in mobile device usage. According to the most recent internet usage report from the Communications Commission of Kenya (CCK) there were an estimated 17.38 million internet users in Kenya as at December 2011. This represents a 95.63% increase from 8.8 million internet users reported in December 2010. As internet usage continues to grow in the country so does the number of internet security incidents reported. The increased use of and dependence on information technology has exposed Kenyan organisations to premeditated security threats with possibly disastrous effects. Most of these organisations are prime targets for insider attacks as well as cyber-criminal acts.

While information security trends globally indicate an increase in sophisticated and targeted attacks, the trends locally are not only shocking but also embarrassing. Most of the issues identified in this report are not new, they've been around for a long time and they all point to: poorly trained technical staff, misconfigured systems, lack of company security strategies and unpatched and vulnerable systems.

Kenyan organisations are ill-equipped and unprepared to respond to information security threats and they need to get back to security basics. Getting back to security basics means, identifying the most critical information assets, confirming what controls are implemented on each asset, and continuously assessing these controls to ensure compliance with set policies.

Although there are different initiatives in place set out to address information security issues in Kenya, these initiatives cannot adequately address our current security issues. Public and private organisations need to rethink their whole approach to information security and establish security practices needed to protect critical IT infrastructure. They also need to train and grow security experts needed to secure this infrastructure.It is imperative that local organisations take action before the situation worsens and the cost of inaction becomes even greater.

Report Highlights

Local Cyber Threat Trends

ISPs in Kenya: spamming, phishing and poor reputation scores

- Majority of internet-connected computers in Kenya are infected with malicious programs that expose users to risks such as loss of personal data, as well as increased susceptibility to online fraud.
- Most ISPs in Kenya have poor reputation scores, which lead to email or web traffic from Kenyan Internet users being filtered or blocked

Malware Threat: viruses, trojans, botnets and worms

- Presence of botnet activity in Kenya presents the greatest cyber threat to the country’s critical infrastructure and corporate networks and requires immediate action from key stakeholders.
- Kenya has a considerably higher percentage of com puters infected with malicious software compared with the global average
- The most common malware and potentially unwant ed software family in Kenya is Win32/Autorun
- Poorly designed and insecure web applications expose local financial institutions to possible compromise and defacement by cyber criminals

Security Incident Reports: insider threats and credit card fraud

- Automated attacks targeting organizations in Kenya are going undetected due to poor detection and prevention methods
- Cyber criminals are selling stolen credit cards issued by Kenyan banks online for $10 US dollars
- The Data Protection Bill, 2012, will have huge impact on how businesses and government agencies imple ment cyber security measures

Global Vulnerabilities and Threats

- TCP Ports 445 (Microsoft Directory Services) and 1433 (Microsoft SQL) are the most targeted ports in 2012
- Oracle and Google reported the highest number of distinct vulnerabilities between January – April 2012
- Cisco IOS (Operating system) and MySQL (Application) had the highest number of reported vulnerabilities for enterprise software products be tween January and April 2012
- Macs Are No Longer Safe from attacks as research ers predict an increase in security threats
- Millions of computers in hundreds of countries are infected with DNS Changer Malware

ISPs in Kenya: spamming, phishing and poor reputation scores

Thousands of computers in Kenya are infected with malicious programs that send spam emails infected with viruses and worms

Every machine on the internet has a unique identifier. Just as you would address a letter to send in the mail, computers use a unique identifier to send data or to communicate using the internet protocol to specific computers on a network. This unique identifier is the internet protocol address (IP address). IP addresses are assigned to organisations by their Internet Service Provider (ISP) out of a range of addresses that have been assigned to the ISP. The organisations in turn give addresses to their hosts. If the hosts are involved in botnets or have malware and are sending out spam, they not only affect the confidentiality, integrity and availability of their network resources, but they also give their ISPs poor spamming reputation scores and lead to the ISP being blacklisted by other ISPs.

Spamming refers to the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. Spamming is a huge issue for internet users in Kenya and globally, in fact some research companies estimate that email spam accounts for 68.0 percent of global email traffic. Whereas most email spam contain harmless advertising messages there is a new breed of spam that is spreading viruses, worms and Trojans into end user computers. Spam increases bandwidth charges for ISPs as a result of increased network traffic and also causes problems for internet users because of increased fraud, wasted time, and various other scams. Globally many countries have launched initiatives to detect and prevent spammers. Such initiatives have focused on identifying sources of spam and working with ISPs in an attempt to block such computers from sending out spam.

To better understand the extent of the spamming problem in Kenya, Serianu collected data from The Project Honey Pot, a web based honeypot network which tracks abuse, fraud, spamming and other cyber threats. We analyzed a sample of 150 spamming IP addresses that are assigned to Internet Service Providers (ISPs) located in Kenya. The analysis revealed the following statistics for the period starting January through April 2012: distribution of spam sending IP addresses in Kenya by ISP, distribution of detected spam events originating from Kenya by ISP, distribution of comment spammers by ISP and distribution of the top 20 spammers of all time from Kenya by ISP.

Data based on the analysis of 150 spam sending IP addresses that are owned by ISPs located in Kenya - between January and April 2012

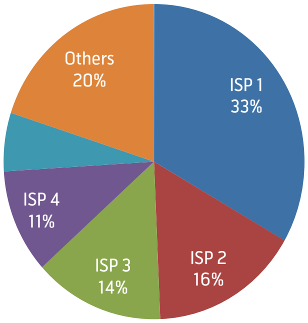
Name of ISP	# of IP addresses identified in our analysis	# of total spam events detected	# of comment post spam	# of IP address in the top 20 all time spammers
ISP 1	50	66,321	5,410	8
ISP 2	24	34,210	1	1
ISP 3	21	14,594	806	2
ISP 4	16	10,517	0	1
ISP 5	9	6,723	405	0
ISP 6	6	5,527	0	0
ISP 7	7	4,877	200	1
ISP 8	5	4,779	0	0
ISP 9	5	3,987	0	4
ISP 10	2	1,090	0	0
ISP 11	2	477	0	1
ISP 12	1	371	0	1
ISP 13	1	282	0	0
ISP 14	1	68	0	0
Total	150	153,823	6,822	19

Table 1.1

See definition in Appendix 1

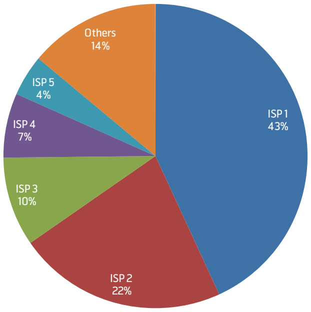
Distribution of detected spam sending IP addresses by ISP

As can be seen in Table 1.1, 33% (50) of the 150 IP addresses identified are owned by ISP 1. ISP 2 owns 16% (24 IP addresses), ISP 3 owns 14% (21 IP addresses), ISP 4 owns 11% (16) and ISP 5 owns 9 IP addresses.



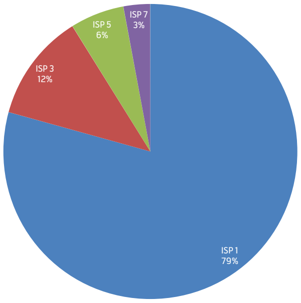
Distribution of detected spam events by ISP- percentage

During the period under review, a total of 153,823 spamming events were sent from the 150 IP addresses analysed. Of these events, 66,321 events (43%) originated from ISP 1, followed by 34,210 events from ISP 2 IP space (22%), ISP 3 came in third with 14,594 events (9%) and ISP 4 was fourth with 10,517 events (7%).



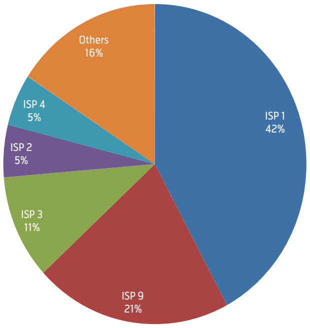
Distribution of detected comment spam events

During this period, there were a total of 6822 comment post spam events resolving to IP addresses owned by Kenyan ISPs. Of the 6822 comment spam events detected, 5410 events were originating from IP address owned by ISP 1, followed by ISP 3 with 806 events, ISP 5 had 405 events and ISP 7 originated 200 comment spamming events.



Distribution of top 20 spammers of all time by ISP

As per the table, we selected the top twenty spammers of all time from the sample of 150 IP addresses analyzed. Based on this list 8 IP addresses on the top twenty list of spammer were resolving to ISP 1, followed by ISP 9 with 4 IP addresses, ISP 3 came in third with 2 IP addresses and the rest had 1 IP address each in the top twenty spammers of all time.



Majority of ISPs in Kenya have poor reputation scores, which lead to email or web traffic from Kenya to be filtered or blocked

Many ISPs and Businesses use different ways of identifying and preventing spam from reaching the end user's mailbox. The most popular way of filtering email or web traffic is the use of reputation scores of the senders IP address. This reputation score is determined using different factors including; if the IP address is listed on a reliable public blacklist or open proxies, if the IP address is in a hijacked IP space, the number of messages sent to invalid spam trap accounts from an IP address and number of end-user complaints associated with an IP address. Reputation scores can be categorized as either Good - Email or Web traffic is not likely to be filtered or blocked; or Poor - Email or Web traffic is likely to be filtered or blocked.

To better understand the reputation scores of ISPs in Kenya, we analyzed data from the SenderBase Network, the world's largest email and Web traffic monitoring network that utilizes carefully researched public data sources to establish a sender's reputation. We collected data on ISPs in Kenya and determined the reputation scores of IP addresses that were used to send email in the period under review.

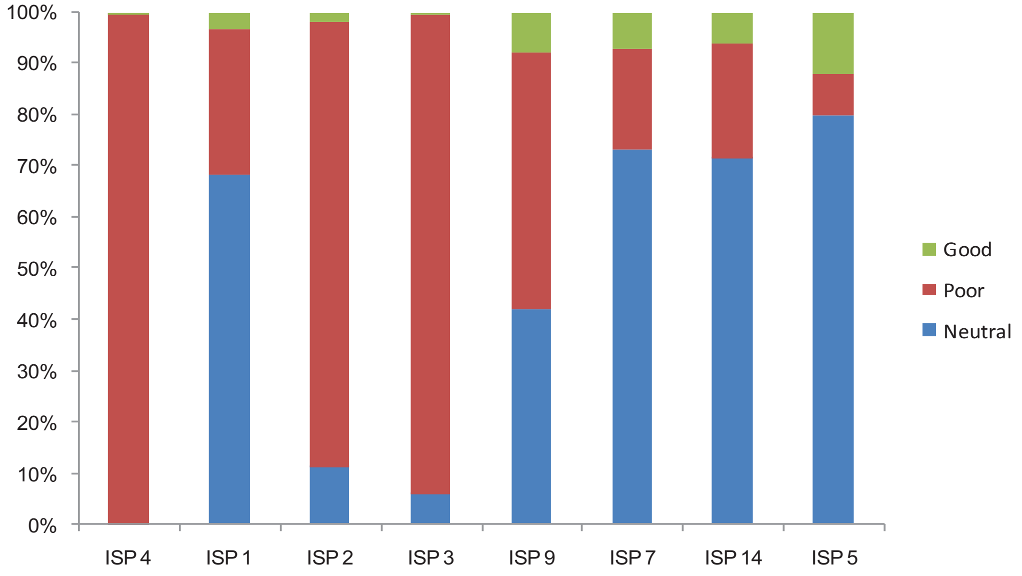
The table below shows the Email and Web reputation of IP addresses originating from Kenya. The total number of IPs used in the analysis represents the number of IP addresses that the SenderBase email reputation service identified as having sent email during the period under review. The information provided here was extracted from the SenderBase Network as at May 01, 2012.

Reputation scores of Kenyan Internet Service Providers (ISPs)

The SenderBase Network Reputation Score				
Name of ISP	Total # IP addresses	Good	Neutral	Poor
ISP 4	8149	0.02%	0.13%	99.84%
ISP 1	2191	3.33%	68.37%	28.30%
ISP 2	934	1.82%	11.24%	86.94%
ISP 3	792	0.51%	6.06%	93.43%
ISP 9	624	7.69%	42.15%	50.16%
ISP 7	241	7.05%	73.44%	19.50%
ISP 14	205	5.85%	71.71%	22.44%
ISP 5	135	11.85%	80.00%	8.15%
Total Sampled	13271	1.42%	17.76%	80.82%

Table 1.2

Based on this data, majority of IP addresses used to send email from Kenya have poor reputation scores. A total of 13271 IP addresses were analysed and 80% of these addresses had a poor reputation, 18% had a neutral reputation while 1% had a good reputation. This means that a problematic level of threat activity was observed from the Kenyan IP address space or network. This results in email traffic originating from Kenya being filtered or blocked.



Graph 1.1

In terms of ranking, 99.84% of IP addresses on the ISP 4 network had a poor reputation score ranking as the highest number of IP addresses with a poor reputation score in Kenya, followed by ISP 3 with 93.43%, ISP 2 with 86.94%, ISP 9 with 50.16%, ISP 1 with 28.30%, ISP 14 with 22.44%, ISP 7 with 19.50% and ISP 5 with 8.15%. Overall these statistics are alarming and they should give any internet user pause. The poor reputation score means that foreign ISPs and Email service providers that use the SenderBase network to assess their email traffic are more than likely to filter or block emails received from internet users in Kenya.

Mitigating against spamming and poor ISP reputation
• Ensuring hosts within the ISPs filter incoming emails to prevent spam which would lead to infection and further spamming of others • Block automatic downloads of contents contained in inbound mails • Limit places where you post your email addresses or if you have to, put the @ in brackets so as to prevent email harvesting • Create awareness among the hosts to regularly check their networks and informing those who are infected to clean their systems so as to avoid bad reputations for the ISP

Table 1.3

Malware Threats: viruses, trojans, botnets and worms

Presence of botnet activity in Kenya presents the greatest cyber threat to critical infrastructure and corporate networks requiring immediate action from key stakeholders

A botnet is a network of compromised computers that are controlled remotely by cybercriminals. In most cases, malicious bots are deployed without the permission or conscious understanding of the internet user. Botnets expose internet user's to risks such as loss of personal data and increased susceptibility to online fraud. Such computers can also become inadvertent participants in or components of an online crime network, spam network, and/or phishing network as well as be used as a part of a distributed denial-of-service attack.

During our analysis of the 150 Spam sending IP addresses that are located in Kenya, we identified a number of IP addresses that were participating in botnets. Some of the botnet families detected are listed in the table below.

Detected botnet families in Kenya

Botnet	Description	Characteristics
Torpig	Also known as Sinowal or Mebroot Troj/Torpig-A is a Trojan for the Windows platform. The Trojan logs keypresses and open window titles to text files and periodically sends the collected information to a remote user via HTTP.	Torpig is particularly dangerous because it captures sensitive information, such as credit card data, passwords, and login locations from the victim's browsing activity.
Grum	Also known as Tedroo Grum is a pesky spam botnet as it has a tendency to infect files referenced by autorun registries. Due to its kernel-based rootkit characteristics, it is capable of hiding component files as well as legitimate windows system files, hence the difficulty of its detection and removal.	Grum usually concentrates on sending out pharmaceutical spam.
Waledac	W32.Waledac is a worm that spreads by sending emails that contain links to copies of itself. It also sends spam, downloads other threats, and operates as part of a botnet.	Waledac is a worm that is capable of harvesting and forwarding password information.
Lethic	Lethic is a proxy type bot which relays spam from a control server to its destination. Win32/Lethic connects to remote servers, which leads to unauthorized access to an affected system.	Lethic mainly sends out pharmaceutical and replica spam
Cutwail	Win32/Cutwail is a Trojan which downloads and executes arbitrary files. Downloaded files may be executed from disk or injected directly into other processes. Whilst the functionality of the files that are downloaded is variable, Cutwail usually downloads a Trojan which is able to send spam.	Cutwail is mostly involved in DDoS attacks and sending spam e-mails.
Bobax	Bobax is a trojan proxy that uses the MS04-011 (LSASS.EXE) vulnerability to propagate. When instructed to do so it scans random IP addresses for vulnerable computers. When Bobax infects a host, the exploit uses HTTP to download the executable from a webserver which listens on a random port on the attacker host. The data is downloaded into a dropper file called 'svc.exe'.	Bobax uses infected systems as a spam e-mail relay

Table 2.1

Kenya has a considerably higher percentage of computers infected with malicious software compared with the global average

Malware refers to malicious software that includes viruses, worms, and Trojan horses. Malware normally utilize popular electronic communication methods to spread, including worms sent through email, text messages and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware also seek to exploit existing vulnerabilities on systems making their entry quiet and easy. To better understand the spread of malware in Kenya, Serianu reviewed the latest Microsoft Security Intelligence Report (SIR). Microsoft produces this report twice a year to keep the Security industry informed on the changing landscape and provide actionable guidance for customers in an effort to create safer more trusted computing experiences for everyone. The latest report, volume 12, provides insight into online threat data with new information for analysis of data from more than 100 countries and regions around the world.

Percentage of computers infected with malicious software in Kenya

	Prevalence of different categories of malware and potentially unwanted software in Kenya vs. worldwide average (percentage of all computers reporting detections)	
Malware Type	Kenya (%)	Worldwide Average (%)
Worms	36.1	11
Misc. Trojans	29.6	20
Misc. Potentially Unwanted Software	29.6	21
Viruses	25	6.7
Adware	15	17
Trojan Downloaders and Droppers	10	11
Exploits	8	10
Backdoors	6	4
Password Stealers and monitoring tools	4	6.3
Spyware	0.3	0.3

Table 2.2

Table 2.2 shows the relative prevalence of different categories of malware and potentially unwanted software in Kenya in comparison with worldwide averages. The most common category in Kenya for the period under review is Worms. Worms affected 36.1 percent of all computers cleaned, compared to the worldwide average of 11 percent. The second most common category in Kenya was Miscellaneous Trojans. It affected 29.6 percent of all computers cleaned in Kenya, compared to 20 percent worldwide average. The third most common category in Kenya was Miscellaneous Potentially Unwanted Software, which affected 29.6 percent of all computers cleaned compared to 21 percent worldwide average. On average the percentage of computers reporting malware and potentially unwanted software is higher than worldwide averages.

The most common malware and potentially unwanted software family in Kenya is Win32/Autorun

Table 2.3 lists the top 10 malware and potentially unwanted software families that were detected on computers in Kenya by Microsoft.

	Family	Most significant category	% of cleaned computers	Description
1	Win32/Autorun	Worms	19.90%	Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer
2	Win32/Sality	Viruses	19.40%	Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .Wexe.
3	Win32/Rimecud	Worms	11.70%	Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging.
4	Win32/Vobfus	Worms	9.00%	Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files.
5	Win32/Keygen	Misc. Potentially Unwanted Software	7.80%	Keygen is a generic detection for tools that generate keys for illegally obtained versions of various software products.
6	Win32/CplLnk	Exploits	5.90%	CplLnk is a generic detection of specially-crafted, malicious shortcut files which run when a user browses a folder that contains the malicious shortcut using an application that displays shortcut icons.
7	Win32/Dorkbot	Worms	5.80%	Dorkbot is an IRC-based botnet family with rootkit capability and password stealing functionality.
8	Win32/Conficker	Worms	5.50%	A worm that spreads by exploiting vulnerability in Microsoft systems. Conficker disables several important system services and security products, and downloads arbitrary files.
9	Win32/Hotbar	Adware	5.30%	Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.
10	Win32/Virut	Viruses	5.10%	Virut is a family of file infecting viruses that target and infect .EXE and .SCR files accessed on infected systems

Table 2.3 – See appendix <IV> for source and other evidence

Win32/Autorun, a family of worms that spread by copying itself to the mapped drives of an infected computer is the most common threat family in Kenya. Autorun was detected on 19.9 percent of all computers cleaned by Microsoft. The second most common threat is Win32/Sality with 19.4%, followed by Win32/Rimecud (11.7%), Win32/Vobfocus (9.0 %), and Win32/Keygen (7.8%).

Mitigating against malware threats

- Setting up firewalls for Access Control on inbound (Internet to Internal network) and outbound (Internal Network to Internet) communications
- Put up Intrusion Detection Systems (IDS) that identify network traffic and detect port scans, malware and other abnormal communications
- Using only authorized local network devices on the network and ensuring they are provided by the organization
- Hardening Opertaing systems to improve the ability to withstand attacks
- Routine Vulnerability scanning mimicing the malicious network activity that networked hosts may encounter

Table2.4

Incident Reports: Insider threat, web applications' compromise and credit card fraud

Businesses in Kenya are experiencing cases of insider threat including data leakage and insider fraud

When organizations hire employees or contractors, the employee is expected to act in the best interest of their employer. This expectation is a general duty that an employee takes on when they contractually accept employment. While employees in most organizations are honest and trustworthy, there are cases where some employees will act malicious to undermine their employer. The U.S Computer Emergency Response Team (CERT), a U.S based research and development centre that conducts research on insider threats defines a malicious insider as a current or former employee or contractor who intentionally exceeds or misuses an authorized level of data access in a manner that affects the security of the organizations' data, systems, or daily business operations.

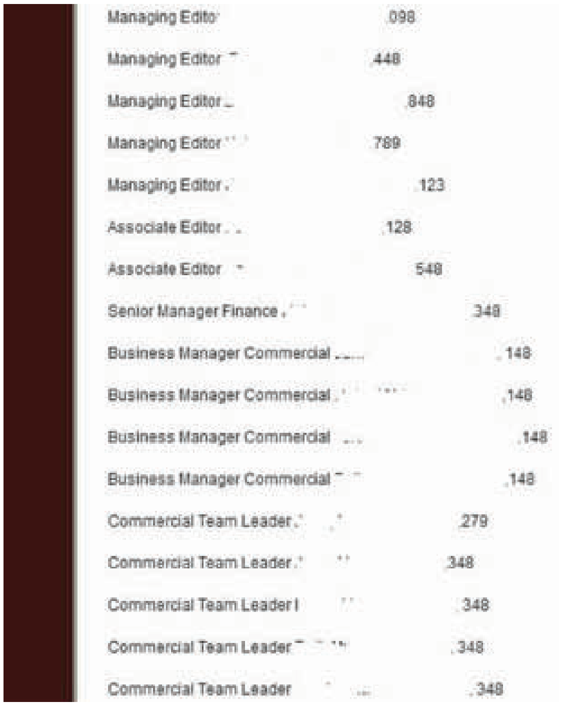
What kinds of Insider attacks did we see in Kenya and what are their consequences?

There are few statistics on insider attacks because they are rarely reported. Unlike in the western world where any loss of personal data is required to be reported, in Kenya, there are no uniform reporting requirements for computer-related crimes, and most such crimes go unreported because management feels that the harm from reporting outweighs the benefit of public prosecution of the perpetrators. As a result of lack of statistics, the examples we are providing are only from the general media and other public sources.

A leading media house payroll information published online

In February 2012, a leading media house's payroll information for April 2011 was published online. The information published disclosed employee names, titles and monthly salaries. The information published was sensitive and could only have been accessed by a current employee, a contractor or a former employee. Not only was this information embarrassing but it also raises questions on what controls local organisations put in place to ensure the security of sensitive company information like salary data. Figure 3.1 above, shows an excerpt of the payroll that was published on the internet.

The names are erased to avoid further exposure.



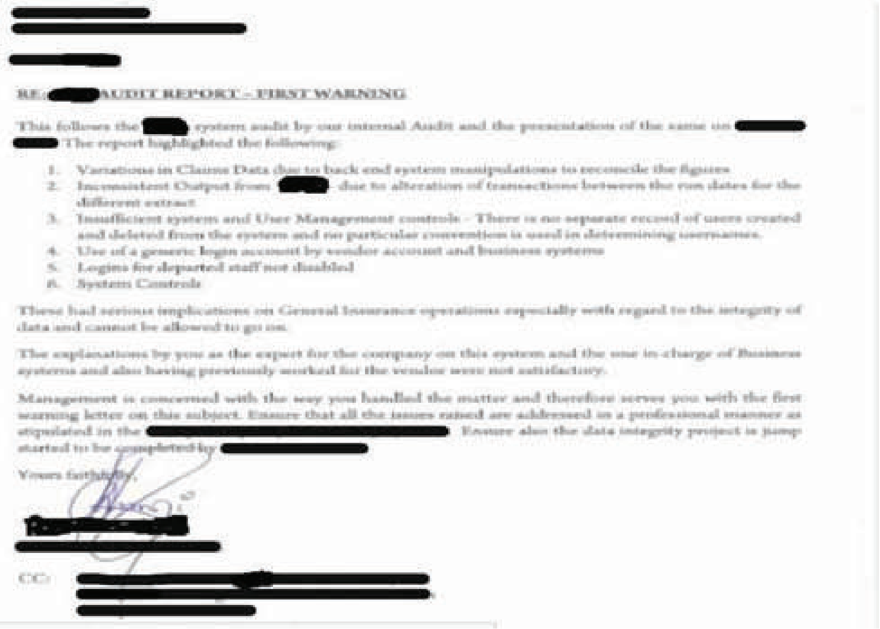
Managing Edito	098
Managing Editor	448
Managing Editor	848
Managing Editor	789
Managing Editor	123
Associate Editor	128
Associate Editor	548
Senior Manager Finance	348
Business Manager Commercial	148
Business Manager Commercial	148
Business Manager Commercial	148
Business Manager Commercial	148
Commercial Team Leader	279
Commercial Team Leader	348
Commercial Team Leader I	348
Commercial Team Leader	348
Commercial Team Leader	348

Fig 3.1 above, shows an excerpt of the payroll that was published on the internet.

Sensitive information from a leading NSE listed company published online

We came across a shocking case of an insider attack against a leading company in Kenya. We identified an internet website that has published a wide range of internal and sensitive documents. The website which has been in operation since May 2011 includes sensitive documents such as; internal management memos, internal audit reports, internal email messages to employees and HR documents. As a publicly owned company this organisation holds sensitive information that their customers, business partners, regulators, shareholders and the Board expect them to protect. The impact of negative publicity and public perception generated by this website should prompt the company to take immediate measures to understand the confidential information they hold, how it is controlled and how to prevent it from being leaked. Due to the content of the documents published on the website, we strongly believe the website owner is a current employee, contractor or a former employee of the company.

Figure 3.2 on the next page shows a warning letter sent after an audit. This is one of the documents that is published on the website.



[redacted]

[redacted]

RE: [redacted] AUDIT REPORT – FIRST WARNING

This follows the [redacted] system audit by our internal Audit and the presentation of the same on [redacted] The report highlighted the following:

1. Variations in Claims Data due to back end system manipulations to reconcile the figures
2. Inconsistent Output from [redacted] due to alteration of transactions between the run dates for the different extract
3. Insufficient system and User Management controls – There is no separate record of users created and deleted from the system and no particular convention is used in determining usernames.
4. Use of a generic login account by vendor account and business systems
5. Logins for departed staff not disabled
6. System Controls

These had serious implications on General Insurance operations especially with regard to the integrity of data and cannot be allowed to go on.

The explanations by you as the expert for the company on this system and the one in-charge of Business systems and also having previously worked for the vendor were not satisfactory.

Management is concerned with the way you handled the matter and therefore serves you with the first warning letter on this subject. Ensure that all the issues raised are addressed in a professional manner as stipulated in the [redacted] Ensure also the data integrity project is jump started to be completed by [redacted]

Yours faithfully,

[redacted]

CC: [redacted]

Fig 3.2

Mitigating against insider threats

- Implement background checks and drug testing for all employees on a pre-employment basis and Implementing random checks for all existing employees
- Retain a signed Acceptable Network Use Policy agreement for each employee
- Adhere to the Principal of "Least Privilege": ordinary company users should not have administrative access to their workstations
- Enforce strict Separation of Duties: all network Administrator roles and duties should be separated, without exception
- Company security policies must be comprehensive and contain specific procedural details. This prevents ambiguity and "wiggle room"
- All employees should be periodically trained and re-trained on the company security policies

Table 3.1

Poorly designed and insecure web applications expose local financial institutions to possible compromise and defacement by cyber criminals

Most web applications are vulnerable to threats which cannot be detected or prevented by traditional network security devices. Programming errors and weaknesses in the application leave sensitive data open to unauthorized disclosure and internal business systems open to compromise. Security breaches in vulnerable web applications lead to negative publicity, lost business, direct financial loss, breach of customer confidentiality and legal liabilities.

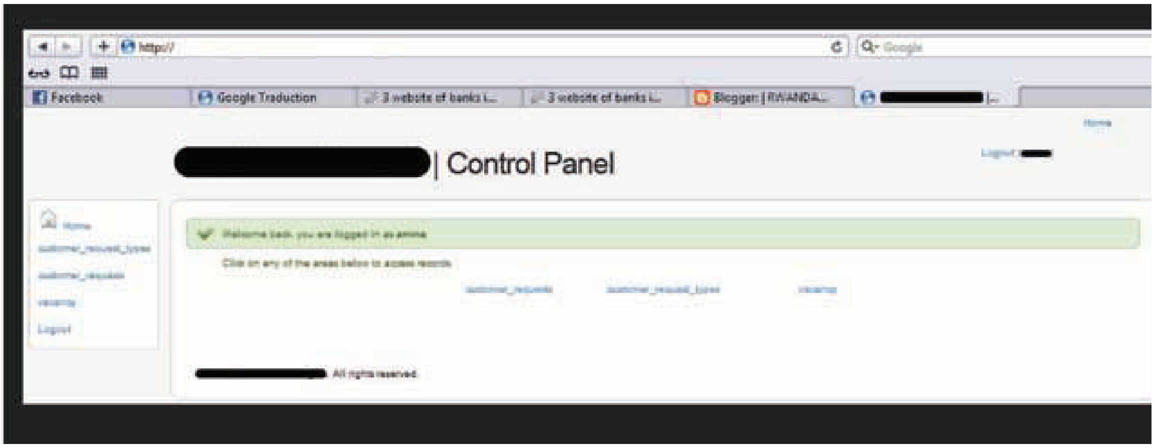
Between January and April 2012, a number of Kenyan websites were compromised by cyber criminals. Most of the compromised websites employed some application functionality, allowing customers to access sensitive account information upload documents or perform transaction. The functionality delivered by most of the compromised websites required connectivity between public web servers, back-end application and database servers. In all the cases identified, attacks against the web applications used standard web services that are usually allowed through firewalls. As a result, the web sites themselves formed part of the perimeter defences of the organisation. Weaknesses in these web sites left the sensitive data hosted on these websites exposed to the world.

Affected Organisation	Description	Evidence
Government of Kenya	103 Government of Kenya owned websites were compromised by a hacker known as Direxer. The hacker defaced the websites, leaving them inaccessible to the general public.	Appendix IV/Fig3.3
A Leading Media House	In the period under review, the company's website was compromised by a group of hackers known as Rwandan hackers. The compromise exposed personal user information including usernames, passwords and emails.	Appendix IV/Fig 3.4
Bank A	The Bank website was compromised by a group of hackers known as Rwandan hackers. The compromise exposed the banks e-portal content with full access to the back-end database supporting the e-portal website. The hackers were also able to access the bank website's control panel, which means they were able to change/edit any content published on the website	Appendix IV/Fig3.5
Bank B	The Bank website was compromised twice. First by a hacker known as Sepo, who discovered vulnerabilities that could be exploited to gain access to back-end databases supporting the website and later on, the Rwandan Hackers compromised the website and they were able to access confidential information - back-end database with sensitive information supporting the bank's website.	Appendix IV/Fig3.6
Bank C	The Bank website as compromised by a group of hackers known as Rwandan hackers. The compromise exposed the banks e-portal content with full access to the back-end database supporting the e-portal website.	Appendix IV/Fig3.7
Bank D	The Bank's mobile website was compromised by a group of hackers known as Rwandan hackers. The compromise exposed the banks mobile website granting the hackers full access to the back-end database supporting the mobile portal website.	Appendix IV/Fig3.8

Table 3.2

Most web applications in Kenya are developed or customised in-house or by short term consultant programmers, in implementation projects where security is not the primary consideration. These factors combine to make development and maintenance of web application in Kenya an inherently risky business.

Below is a figure of the Bank's control panel after their website was compromised giving the hackers access to the bank's database and control panel. This was then published on www.pastebin.com.



[redacted] | Control Panel

Welcome back, you are logged in as amina

Click on any of the areas below to access records

[redacted] All rights reserved.

Fig 3.5

Developing secure web applications

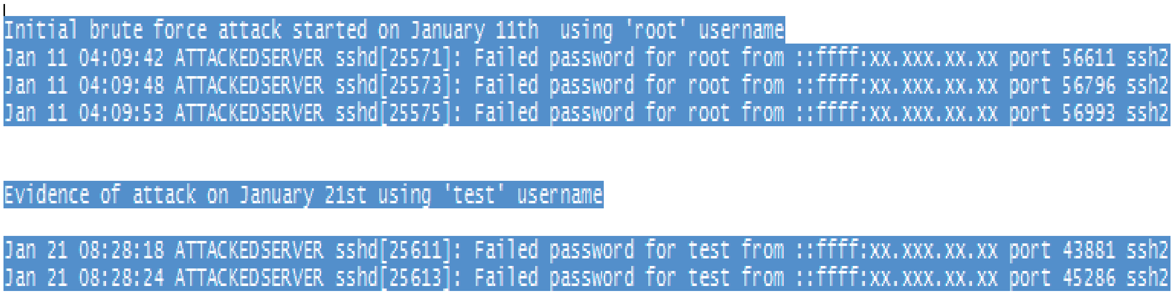
- Validate all user input and output to ensure that the result is both expected and acceptable
- Implement security mechanisms that are in such a way that when they fail, they fail closed rejecting any sub sequent security requests
- Implement simple but effective security to avoid complexity that would lead the users to look for a way to bypass the security
- Layer the defense mechanisms such that if one component fails to catch a security event, a second one should catch it

Table 3.3

Automated and brute force attacks targeting organisations in Kenya are going undetected due to poor detection and prevention methods

In the first four months of 2012, we came across cases of brute force attacks especially targeting SSH (Secure Shell). The brute force attacks observed were using pre-compiled lists of usernames and passwords in an attempt to access an internet facing server. In all the cases observed, the most common username used for the attacks was the 'root' followed very closely by 'test', 'admin' and 'guest'.

For purposes of this report, we will discuss one particular case where the attack was successful. In this case, there was unlimited number of login attempts from botnets that were trying to log onto the server via port 22.



```
Initial brute force attack started on January 11th  using 'root' username
Jan 11 04:09:42 ATTACKEDSERVER sshd[25571]: Failed password for root from ::ffff:xx.xxx.xx.xx port 56611 ssh2
Jan 11 04:09:48 ATTACKEDSERVER sshd[25573]: Failed password for root from ::ffff:xx.xxx.xx.xx port 56796 ssh2
Jan 11 04:09:53 ATTACKEDSERVER sshd[25575]: Failed password for root from ::ffff:xx.xxx.xx.xx port 56993 ssh2


Evidence of attack on January 21st using 'test' username

Jan 21 08:28:18 ATTACKEDSERVER sshd[25611]: Failed password for test from ::ffff:xx.xxx.xx.xx port 43881 ssh2
Jan 21 08:28:24 ATTACKEDSERVER sshd[25613]: Failed password for test from ::ffff:xx.xxx.xx.xx port 45286 ssh2
```

Fig 3.9

As per the evidence collected, the SSH attacks began on January 11, 2012 and continued through January 31, 2012, we observed a total of 21 separate attack sessions on the server originating from different IP addresses. The number of logins attempted during each session varied somewhat, but the number of logins attempted during a single session never exceeded twenty. The total number of login attempts over the twenty days was 1200, most of which targeted the root and test accounts.

Attackers IP address	Resolving ISP/Country
109.100.126.73	Romtelecom/Romania
109.99.35.39	Romtelecom/Romania
213.177.105.34	NGTS OJSC VolgaTelecom/Russia
61.133.99.99	WFCT-COM/China

Table 3.4

Once the attackers were able to access the server using the 'root' account, they modified a number of binaries. Some of the binary files modified were infected with Linux.RST.B. This is a Linux virus that implements several backdoor facilities, allowing an attacker to take control of the system infected with it in case the virus has been executed on account with root privileges'. The virus infects all the Linux binary executables in the current directory and the /bin directory, and listens to the first network card 'eth0' as well as the first PPP (Point-to-Point Protocol) connection interface, and 'ppp0' for special packets sent in the EGP (Exterior Gateway Protocol) communication protocol. Whenever such a special package arrives, the virus allows the attacker to take control of the system with a root shell.

In this case, the virus implemented backdoor facilities that allowed the remote user to attack other vulnerable systems. The hackers used the backdoor facilities to install IRC based malware and used IRC channels to control other compromised computers – which were attacking other vulnerable servers. Since this was an application server, the server's performance was negatively impacted leaving the application unavailable to customers.

Defending against automated and brute force attacks

- Lock out an account after a defined number of incorrect attempts and require the administrator to unlock them
- Inject random pauses when checking the passwords as the success of a brute force attack is dependent on time
- Lock down all ssh connections onto your server apart from one so that all the other boxes can only be sshed into from the open gateway boxes
- Move SSH to a non standard port
- Sensitizing users about choosing strong passwords for their accounts

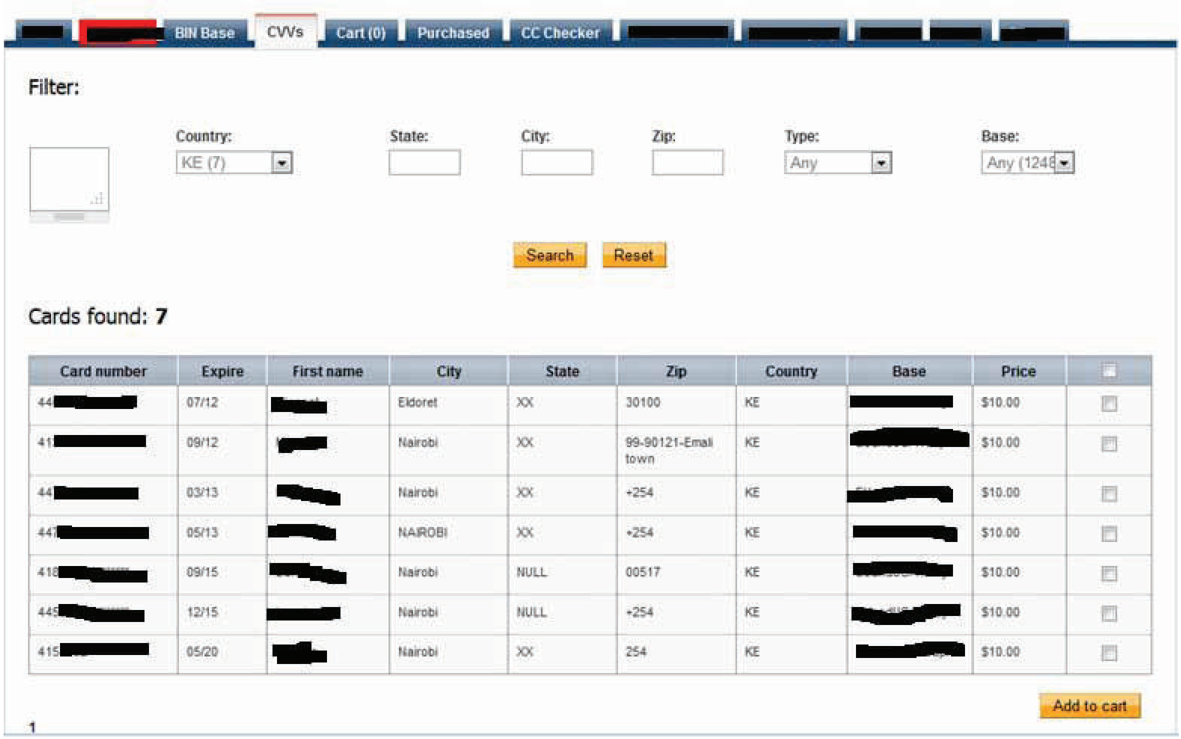
Table 3.5

Cyber criminals are selling stolen credit cards issued by Kenyan banks for $10 US dollars

For many years, cyber criminals have been stealing compromised financial information (bank account, credit and debit card details) and selling them online.

During our research on credit card fraud we came across a credit card shop that was selling credit card data issued by banks located in Kenya. The shop was selling the credit card data for $10 and had the option for the buyer to check if the card was valid after they purchase it, if not - the store would offer a refund.

On the next page is a snapshot of the available credit cards from this shop. Most of the information is hidden to avoid further exposure of these personal details.



[redacted] [redacted] BIN Base | CVVs | Cart (0) | Purchased | CC Checker | [redacted]

Filter:

Country: KE (7) State: City: Zip: Type: Any Base: Any (1248

Search Reset

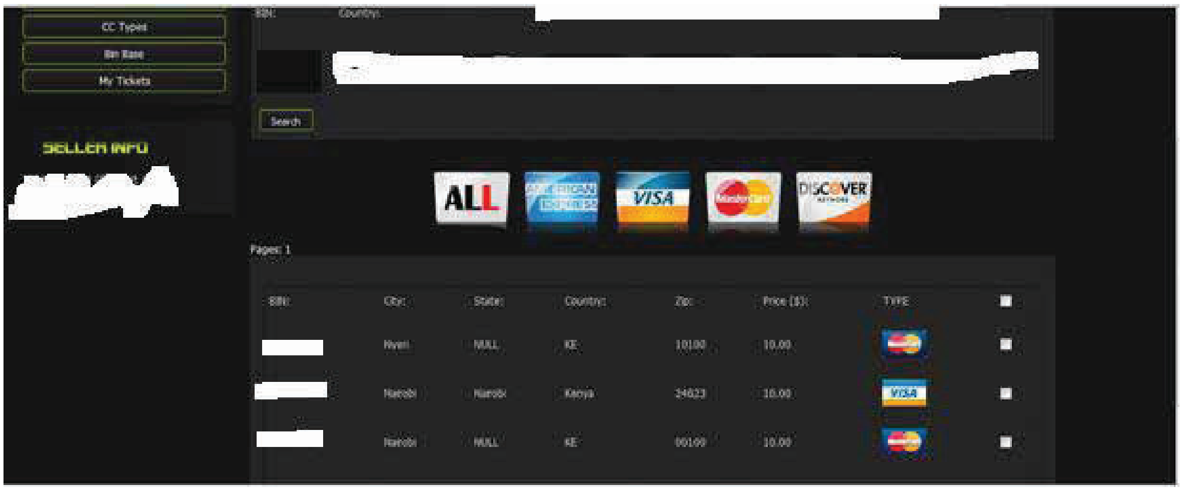
Cards found: 7

Card number	Expire	First name	City	State	Zip	Country	Base	Price	□
44[redacted]	07/12	[redacted]	Eldoret	XX	30100	KE	[redacted]	$10.00	□
41[redacted]	09/12	[redacted]	Nairobi	XX	99-90121-Emali town	KE	[redacted]	$10.00	□
44[redacted]	03/13	[redacted]	Nairobi	XX	+254	KE	[redacted]	$10.00	□
447[redacted]	05/13	[redacted]	NAIROBI	XX	+254	KE	[redacted]	$10.00	□
418[redacted]	09/15	[redacted]	Nairobi	NULL	00517	KE	[redacted]	$10.00	□
449[redacted]	12/15	[redacted]	Nairobi	NULL	+254	KE	[redacted]	$10.00	□
415[redacted]	05/20	[redacted]	Nairobi	XX	254	KE	[redacted]	$10.00	□

1

Add to cart

Fig 3.10



BIN: Country: [redacted]

SELLER INFO [redacted]

Pages: 1

BIN:	City:	State:	Country:	Zip:	Price ($):	TYPE	□
[redacted]	Nyeri	NULL	KE	10100	10.00	MasterCard	□
[redacted]	Nairobi	Nairobi	Kenya	24623	10.00	VISA	□
[redacted]	Nairobi	NULL	KE	00100	10.00	MasterCard	□

Fig 3.11

Most cyber criminals obtain credit card information by paying someone who works in a shop, someone that has physical access to customer's credit cards. Another way for thieves to get credit card number is by hacking into computer networks that store credit card information - online store or any other stores that accept credit cards.

Protecting against Credit Card Fraud

- Keep an eye on your card during the transaction, and get it back as quickly as possible.
- Void incorrect receipts.
- Destroy carbons.
- Save receipts to compare with billing statements.
- Open bills promptly and reconcile accounts monthly, just as you would your checking account.
- Report any questionable charges promptly and in writing to the card issuer.

Table 3.6

The Data Protection Bill, 2012 will have huge impact on how businesses and government agencies implement cyber security measures

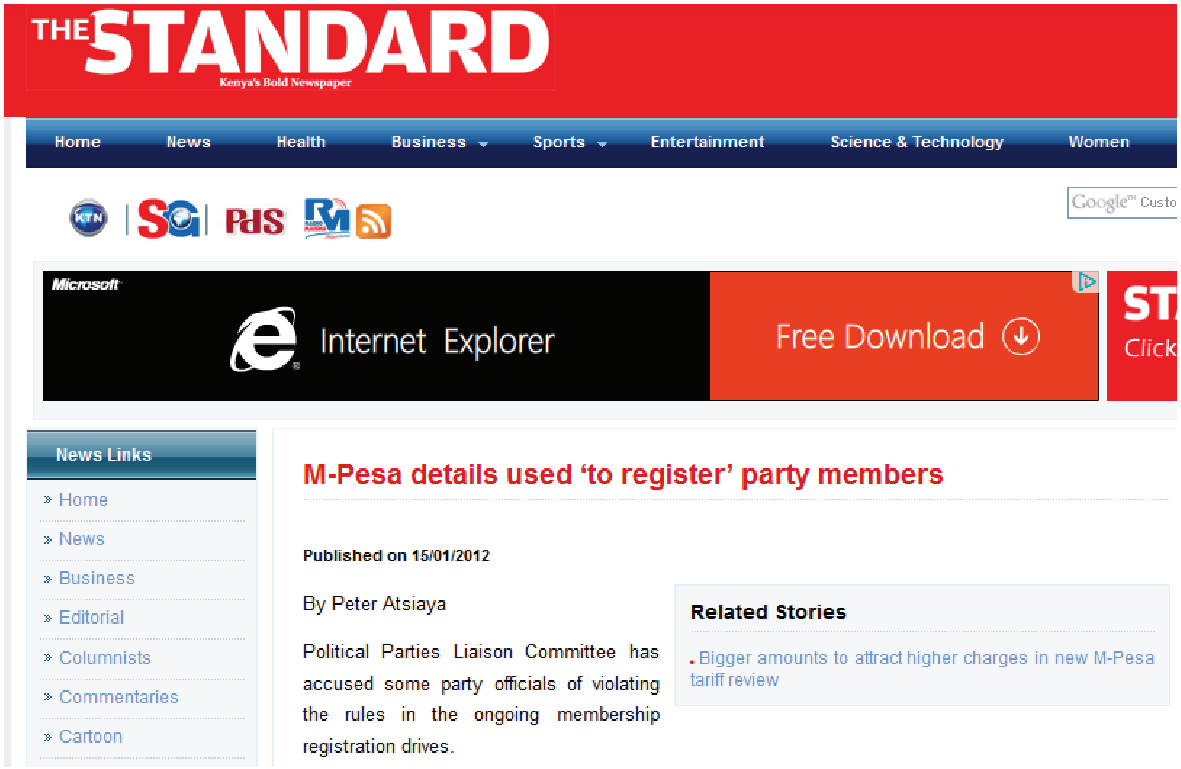
The Ministry of Information and Communication has proposed a bill that aims to govern the collection, processing and distribution of personal information. The bill applies whenever personal information related to individuals is processed through automated or manual means. Processing covers anything done to personal information (PI), which includes the entire lifecycle from the time the information is collected until the information is destroyed. While the bill is specifically geared towards instilling confidence amongst internet and e-commerce users in Kenya that their personal information is adequately protected, the government is also making sure that businesses and public organisations are maintaining the security and confidentiality of personal data.

With the continued use of the internet, many users in Kenya now have a lot of their information available on the internet. Such information could include financial information, travel information, email data and other types of sensitive information. Now that all of this information is available online, criminals are now targeting internet users and stealing their identities, hacking into their accounts, tricking them into revealing the information, or infecting their devices with malware. The Data Protection Bill, 2012 addresses these concerns by ensuring that anyone collecting or storing confidential information is putting in place security safeguards to limit access to this information. There is no doubt, that if this bill is well implemented, it will improve the standard of cyber-security in Kenya because it will force businesses to implement security controls and limit the exposure of personal information.

Political Parties are using M-PESA Agents' lists to register Party members

Recently, the local media reported a case that highlighted the need for regulations on how businesses use confidential information . According to the Political Parties Liason committee, some political parties were colluding with M-Pesa agents to access confidential customer information and using this information to register M-Pesa customers as members of their parties without their consent. The Data Protection bill addresses such cases by requiring the M-Pesa agents to put in place controls that will protect customer information and require customer consent before sharing information with third parties.

The figure below shows the story as it was published on the Standard Media.



M-Pesa details used 'to register' party members

Published on 15/01/2012

By Peter Atsiaya

Political Parties Liaison Committee has accused some party officials of violating the rules in the ongoing membership registration drives.

Related Stories

. Bigger amounts to attract higher charges in new M-Pesa tariff review

Fig 3.12

Preparing for the Data Protection Bill

- Read and understand the Data Protection Bill, 2012
- Review internal processes (automated and manual) to determine when, how and why Personal Information is collected
- Perform a risk assessment to determine the level of effort required to protect Personal information in the organisation
- Establish an organisation-wide committee that will oversee the development of a data protection strategy

Table 3.7

Central Bank of Kenya Guidelines

The Central Bank of Kenya Turns the Spotlight on Information Security Risk – requiring financial institutions to implement stricter security controls.

The Central Bank of Kenya has released revised draft Prudential Guidelines and Risk Management Guidelines for institutions licensed under the Banking Act. In the guidelines, CBK identifies information security within the banking sector as emerging service areas that should be included in their risk management program.

The purpose of these new guidelines is to assist institutions to establish an effective mechanism that can identify, measure, monitor, and control the information security risks inherent in institutions' infrastructure to ensure data integrity, availability, confidentiality and consistency and provide the relevant early warning mechanism.

The guidelines require Board of Directors to ensure that financial institutions have sufficient technical support to maintain the integrity of the operating systems and security, technology risks regarding information and data security in wireless networks are properly identified and mitigated, their institutions at all times monitor the safety, security and efficiency of the equipment being used to prevent any tampering or manipulation by any person.

- Financial institutions will need to put in place systems that specifically address physical and logical security of infrastructure, availability of services, data confidentiality and integrity, encryption of Personal Identification Numbers and electronic transactions, error messaging and exception handling.
- Access to customer information by the bank employees should be limited to those areas where the information is required in order to perform specific functions.

The institution should immediately notify CBK in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the institution would be liable to its customers for any damage. CBK may from time to time as part of its on-site examination mandate, require to inspect institutions' ICT information and communication technology infrastructure and the ICT risk management program. All institutions will be expected to fully co-operate with the CBK regulators during such on-site examinations.

Preparing for the new CBK Prudential Guidelines and Risk Management Guidelines

- Read and understand the CBK Prudential Guidelines and Risk Management Guidelines, 2012
- Perform a risk assessment to determine the level of effort required to implement these new guidelines in the organisation
- Establish an organisation-wide committee that will oversee the implementation of the guidelines

Table 3.8

Global Vulnerability Report: Network ports, vendors, products and macs

TCP Ports 445 (Microsoft Directory Services) and 1433 (Microsoft SQL) are the most targeted ports in 2012

In computer networking a port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. Different ports are used for different purposes on a host, as such it is important to ensure only certain ports are open. Cyber criminals scan ports to discover services they can break into. By identifying which ports are available on the host, the cybercriminal finds potential weaknesses that can be exploited.

This section provides insight into port-level attack traffic, as observed and measured by three leading security research firms. The data used only reflects rejected or denied connection attempts; therefore, legitimate port activity is not represented in the data. This information identifies the top ports targeted by attackers. (Ports are network-level protocol identifiers.)

Port	Port Use	Description or vulnerability
445	TCP Microsoft Directory Services	Microsoft-DS Service is used for resource sharing on Windows systems, and other samba based connections.
1433	TCP Microsoft SQL	Microsoft SQL Server port used typically for remote connections to the database.
80	TCP - HTTP	This port is commonly used by the server to listens to or expects to receive from a Web client, assuming that the default was taken when the server was configured or set up.
23	TCP Telnet protocol	Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection
3389	TCP/UDP Microsoft Terminal Server (RDP)	Remote Desktop Protocol (RDP) allows a user to connect to a computer running Microsoft Terminal Services (also known as Remote Desktop Services). This is a mode of thin-client computing, where Windows applications or an entire desktop are made accessible to a remote client machine.
22	TCP Secure Shell (SSH)	This port is used for secure logins, file transfers (scp, sftp) and port forwarding
443	TCP HTTP secured	This port is used for secure web browser communication.
8080	TCP HTTP Alternative	Commonly used for Web proxy and caching server, or for running a Web server as a non-root user
135	TCP Microsoft Remote Procedure Call (RPC) service.	TCP port 135 is used by RPC (Remote Procedure Calls) and provides location services for dynamically assigned ports, to be used for RPC calls under Windows.
5060	TCP/UDP Session Initiation Protocol (SIP) - VoIP	This port is used by SIP for VoIP traffic. Port 5060 is unencrypted while Port 5061/ tcp is used for VoIP running over Transport Layer Security (TLS).
9415	PPLive Open Proxy (TCP/UDP)	PPLive is a peer-to-peer streaming video network created in Huazhong University of Science and Technology, People's Republic of China. It is part of a new generation of P2P applications that combine P2P and Internet TV, called P2PTV.

Table 4.1

Based on our research TCP port 445 is the most targeted port. Port 445 is usually well controlled but worms and other malicious code targeting vulnerabilities over this port are able to bypass the network perimeter through secured connections.

TCP Port 1433 came in second, this port is used for remote connections to Microsoft SQL server. TCP Port 80 came in third. This port is commonly used to received communications from web clients. Other ports in the top ten include; TCP Port 23 - Telnet protocol, TCP Port 443 - Secured HTTP, TCP Port 8080 - HTTP alternative or Web proxy port, TCP port 135 - Microsoft RPC service, TCP-UDP Port 5060 - Used for Session Initiation Protocol and finally Port 9415 - used by PPLive Open Proxy a peer-to-peer streaming video network.

Based on the research reports it appears that Port 8080 is associated with vulnerabilities in the Cisco Unified Communications Manager and Cisco Unified Contact Center Express1 products, as well as in unpatched or unsecured JBoss Application Servers and variant products. Port 9415 which is associated with the Chinese PPLive video streaming software has a flaw in the software that allows it to be used as an open proxy on Port 9415 therefore the increase in observed attacks targeting that port may be malware searching for open proxies on this port that can be used to hide its tracks.

An analysis of top vulnerabilities by vendors and products for the period under review

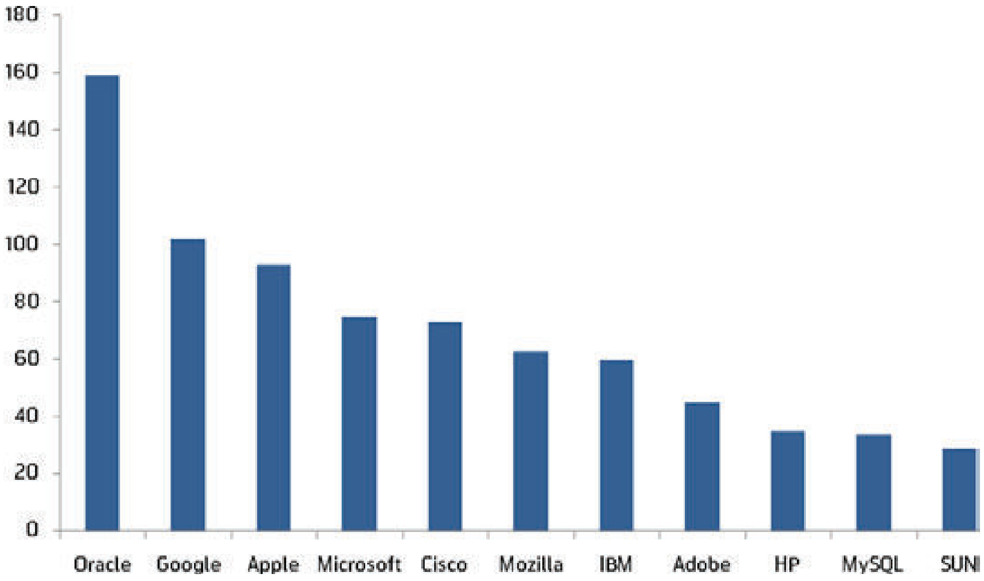
Vulnerabilities are flaws that can be exploited, enabling unauthorized access to IT systems or enabling users to have access to greater privileges than authorized. At the current rate of vulnerability reporting, even small organizations with a single server can expect to spend considerable time reviewing and applying critical patches. Organizations must be aware of and use available security patches. Since not all vulnerabilities have related patches, however, it is essential to apply other security controls that are selected through an analysis of the vulnerabilities and the risks to systems.

New vulnerabilities are discovered each day, and organisations are constantly threatened by new attacks. There are a number of websites that publish Common Vulnerabilities and Exposures data. Users can get access to vendors, products and versions and view CVE entries and vulnerabilities related to them. Users can also view statistics about vendors, products and versions of products. Below you will find statistics on the most vulnerable products and vendors that reported the highest number of vulnerabilities in period under review.

Oracle and Google reported the highest number of distinct vulnerabilities between January – April 2012

Based on the figure below, Oracle reported the highest number of vulnerabilities in the period under review, with a total of 159 vulnerabilities. Of the 159 vulnerabilities - 33 were related to MySQL vulnerabilities, PeopleSoft had 21 vulnerabilities, financial services software had 17, and Database Server had 17 and others. Google reported a total of 102 vulnerabilities; most of these were related to their Chrome web browser. Apple reported a total of 93 vulnerabilities - most of these were related to iPhone operating system -66, ITunes 59 and Mac OS 27 vulnerabilities. Microsoft reported 75 vulnerabilities. Most of these were related to Microsoft Windows 2008 - 25, Windows 7 - 20, Windows Visa 20 and Windows XP 17. Cisco reported a total of 73 vulnerabilities. Cisco IOS accounted for 27 of these vulnerabilities are related to Cisco WebEx and Cisco Unified Communications Manager amongst other products.

Top 10 Vendors by Total Number of “Distinct” Vulnerabilities between January and April 2012



Graph 4.1

Cisco IOS (Operating System) and MySQL (Application) had the highest number of reported vulnerabilities for enterprise software products between January and April 2012

Top 13 Enterprise Products by Total Number of "Distinct" Vulnerabilities between January and April 2012.

Ranking	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	MySQL	MySQL	Application	34
2	IOS	Cisco	OS	27
3	Windows Server 2008	Microsoft	OS	25
4	PeopleSoft Products	Oracle	Application	21
5	Windows 7	Microsoft	OS	20
6	Fusion Middleware	Oracle	Application	20
7	Windows XP	Microsoft	OS	17
8	Windows Server 2003	Microsoft	OS	16
9	Mac Os X Server	Apple	OS	14
10	Database Server	Oracle	Application	14
11	OpenSSL	OpenSSL	Application	13
12	JRE	SUN	Application	12
13	Linux Kernel	Linux	OS	12

Table 4.3

Cyber criminals look for vulnerable systems that they can exploit for malicious purposes. Systems that display known commercial vulnerabilities are soft targets. Unpatched devices and software leave businesses vulnerable to attacks. Most cyber criminals have access to the same vulnerability information and testing systems that businesses have. Therefore, not having patch management processes leave Kenyan businesses open to potential data breaches. A robust, programmatic approach to patch and update is required to keep up with the vulnerabilities and keep organisations information assets safe and secure. Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software.

Macs are no longer safe from attacks as researchers predict an increase in security threats

Mac systems have always been considered safe and secure as compared to other systems Not anymore according to a recent study by security firm Sophos, one fifth of all Macs are harbouring some kind of malware, further damaging the reputation of Apple computers. The study by Sophos revealed a disturbingly high level of malware on Mac computers - with both Windows and Mac threats being discovered. A 100,000 strong snapshot of the millions of Mac computers which have recently downloaded Sophos's free Mac anti-virus software, revealed that 20% of Mac computers were carrying one or more instances of Windows malware.

Threats targeting mobile phone users a growing concern

The continued growth of Mobile Money has had a huge impact on the Kenyan economy but also increased the number of scams and fraud targeting local Mobile phone users.

According to Symantec, Mobile vulnerabilities increased by 93 percent in 2011. At the same time, there was a rise in threats targeting the Android operating system. With the number of vulnerabilities in the mobile space rising and malware authors not only reinventing existing malware for mobile devices, but creating mobile-specific malware geared to the unique mobile opportunities, 2011 was the first year that mobile malware presented a tangible threat to businesses and consumers. These threats are designed for activities including data collection, sending of content and user tracking.

Key steps to ensure effective Patch and Vulnerability management

- Identify all critical Information assets in your organisation: IP devices connected to the network; Software, applications and services, and; individual configurations, latest software release, patches, etc.
- Categorise and prioritise assets by potential impact on business availability and establish interrelations between systems and services
- Scan assets against comprehensive and industry standard database of vulnerabilities, this increases accuracy of scanning and minimizes false positives
- Create manual or automated reports and distribute to the respective stakeholders and proof compliance with regulations
- Apply patches, updates and fixes or install workarounds to mitigate the risk. Pre-test all patches, etc. in your organization's test environment before deployment
- Re-scan to verify applied patches and confirm compliance and Update the remediation workflow and the assets baseline

Millions of computers in hundreds of countries infected with DNS changer malware

DNS (Domain Name System) is an Internet service that converts user-friendly domain names into the numerical Internet protocol (IP) addresses that computers use to talk to each other. When a user enters a domain name such as www.fbi.gov in their web browser address bar, their computer contacts DNS servers to determine the IP address for the website. Their computer then uses this IP address to locate and connect to the website. DNS servers are operated by their Internet service provider (ISP) and are included in their computer's network configuration. DNS and DNS Servers are a critical component of your computer's operating environment—without them, users would not be able to access websites, send e-mail, or use any other Internet services.

Criminals have learned that if they can control a user's DNS servers, they can control what sites the user connects to on the Internet. By controlling DNS, a criminal can get an unsuspecting user to connect to a fraudulent website or to interfere with that user's online web browsing. One way criminals do this is by infecting computers with a class of malicious software (malware) called DNSChanger. In this scenario, the criminal uses the malware to change the user's DNS server settings to replace the ISP's good DNS servers with bad DNS servers operated by the criminal. A bad DNS server operated by a criminal is referred to as a rogue DNS server.

DNSChanger malware causes a computer to use rogue DNS servers in one of two ways. First, it changes the computer's DNS server settings to replace the ISP's good DNS servers with rogue DNS servers operated by the criminal. Second, it attempts to access devices on the victim's small office/home office (SOHO) network that run a dynamic host configuration protocol (DHCP) server (e.g. a router or home gateway). The malware attempts to access these devices using common default usernames and passwords and, if successful, changes the DNS servers these devices use from the ISP's good DNS servers to rogue DNS servers operated by the criminals. This is a change that will impact all computers on the SOHO network, even if those computers are not infected with the malware.

Mitigating and Preventing DNSChanger Malware in your Organisation

- Restrict the DNS resolvers that computers in your organisation can use
- Keep anti-virus software current on all computers, and track or check the updates
- Look for internal addresses that are accessing the addresses of the formerly rogue DNS servers primarily on port 53/udp. The address blocks of these formerly rogue DNS servers are:
  - 85.255.112.0 through 85.255.127.255
  - 67.210.0.0 through 67.210.15.255
  - 93.188.160.0 through 93.188.167.255
  - 77.67.83.0 through 77.67.83.255
  - 213.109.64.0 through 213.109.79.255
  - 64.28.176.0 through 64.28.191.255

Addressing Cyber Threats – The ADRC threat management approach

Rapidly changing Cyber Security Environment

The cyber threat environment is changing rapidly, as are the approaches, applications and technologies businesses used to engage customers and partners — and threat and vulnerability management strategies must change with them. Many organisations are in the process of developing defences and processes to deal with known threats — for example, viruses and malware — but targeted attacks are now having a far greater impact on the business. Attacks now are often either targeting applications such as the Web browser or installing rootkits or corrupting drivers. This threat shift is driving a need for improved data protection and activity monitoring capabilities, as well as more-effective approaches to eliminating infrastructure and application security weaknesses.

Kenyan businesses must focus most of their resources on implementing new approaches that will keep their IT environments secure as threats and business processes change. To enable them, Serianu has developed a methodology that guides local organisations through the whole process.

Serianu ADRC Threat Management Approach

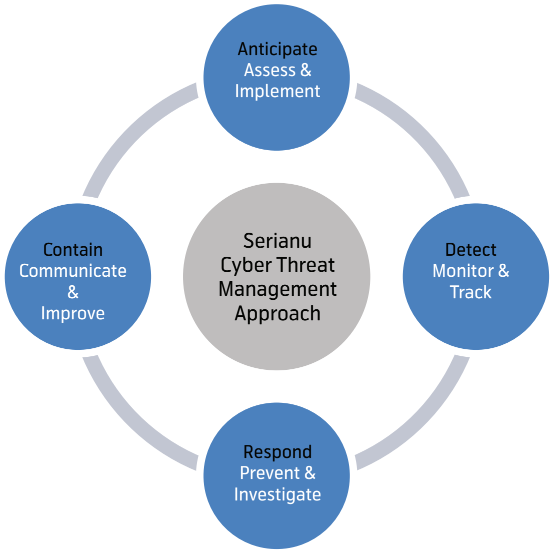


Fig 5.1

Serianu's ADRC (Anticipate, Detect, Respond, and Contain) methodology applies a lifecycle approach to Cyber Threat Management. This lifecycle is designed to be portable to the unique legal, regulatory, security and business needs of any organization. It enables an organisation to anticipate, detect, respond to and contain threats.

Anticipate - assess and implement

Kenyan organisations should anticipate threats by assessing their current IT environments and implementing appropriate security controls. An organisation is able to anticipate threats once they have built processes and capabilities that enable them to consistently and methodically:

- Perform an inventory of all their critical information assets and risk assessments
- Analyze their organisation's Internet-facing in frastructure to determine what cyber criminals may already know about their organization's technology weaknesses
- Anticipate the techniques that are presently being used to penetrate organizations.
- Understand the internal use of technology and pos sible insider threats
- Implement technical and process controls to reme diate any identified weaknesses

Detect - monitor and track threats

Once an Organisation has built the capabilities to anticipate threats; - which involve monitoring and tracking threats. Organizations should monitor their environments to watch for malicious or unauthorized activity by either outsiders or insiders. Organizations should include detection capabilities in their Cyber threat management programs. This includes deploying specialized technologies, such as content-aware data loss prevention (for data-oriented monitoring) and host or network intrusion prevention (for application monitoring) in order to gain domain-specific monitoring capabilities. Building monitoring capabilities enables an organisation to be more effective in the early discovery and tracking of threats.

An organisation is able to detect threats once they have built processes and capabilities that enable them to consistently and methodically:

- Define incidents and establish parameters and definitions
- Tie incident management to threat management and prioritize definitions and responses to incidents
- Implement security event management technolo

gies for the real-time monitoring and correlation of network and security events

- Implement user Activity, file integrity, server activity monitoring and log management
- Implement a sustainable and repeatable threat detection program

Respond - prevent and investigate

An organisation should be able to respond to any detected threats. The Respond phase enables a company to prevent and investigate incidents which threaten the company's information assets.

In this phase a set of controls around the organisation's reaction to cyber threats should be established. These controls will assist an organisation's legal, human resources, public relations, and risk management groups in their efforts to resolve the portions of the threats directly related to their areas of responsibility. The key to a successful threat response is control, low-profile, and speedy resumption of normal business processes with minimal risk to the overall business.

An organisation is able to respond to threats once they have built processes and capabilities that enable them to consistently and methodically:

- Establish a process to determine if the event is actu ally a threat (incident).
- Explore all events to determine source (account ability), destination (assets effected), security weakness, probability of these weaknesses being exploited.
- Inform and involve support teams and effected parties during the different phases of the Response process.
- Implement the correct counter-measures to mini mize the threat to the organisation's business assets.

Contain - communicate and improve

The final and critical component of the cyber threat management process is containment. Once an organisation has responded to threats, they need to communicate with key stakeholders (employees, customers and legal authorities), conduct a post-mortem analysis, manage media communication and update internal threat management processes and policies.

An organisation is able to contain threats once they have built processes and capabilities that enable them to consistently and methodically:

- Acquire, preserve, secure, and document evidence
- Identify and mitigate all vulnerabilities that were exploited
- Remove malicious code, inappropriate materials, and other components
- Return effected systems to an operationally ready state
- Confirm that the affected systems are functioning normally
- Implement additional monitoring to look for future related activity
- Develop a strategy to communicate with sharehold ers, employees and customers
- Develop a strategy to communicate with third par ties - media and legal authorities
- Conduct post-mortem analysis to evaluate dam ages, difficulties, and successes

About Serianu

Serianu is an IT services and business consulting firm that enables organisations to extract value from their information assets. We help our customers collect, protect, and analyze critical business information.

Our Mission:

At Serianu, we strive to enable our clients to use their information assets to save money, reduce risk and to discover and realize new opportunities for their business through deeper insights of customers, markets and performance.

Our Vision:

To encourage and increase the adoption of information enablement in African organisations

Serianu Cyber Security Services

The Serianu security offering is built around the ADRC approach, which ensures an organisation is able to Anticipate, Detect, Respond and Contain threats. Our Information Security service includes the following offerings:

We assist our clients plan not only for threats that exist now, but also for those that may emerge in as much as three years' time. These planning efforts require advanced threat intelligence that most organisations are not capable of developing cost-effectively in-house.

We also assist our clients in developing comprehensive threat-mitigation strategies that enable them to be proactive in understanding their opponents. The Serianu Cyber-intelligence service provides continuous threat monitoring, proactive alerts, and criminalactivity intelligence on the greater Internet and internal networks.

Serianu provide the following offerings under the Enterprise Threat Management Service

1. Malware Threats Monitoring:

- Spam, botnets, phishing
- Viruses, worms and Trojans
- Hackers, crime ware, spyware

2. Vulnerability Management:

- Log management
- Vulnerability assessment and exploitation
- Patch management

3. Internal Continuous Monitoring:

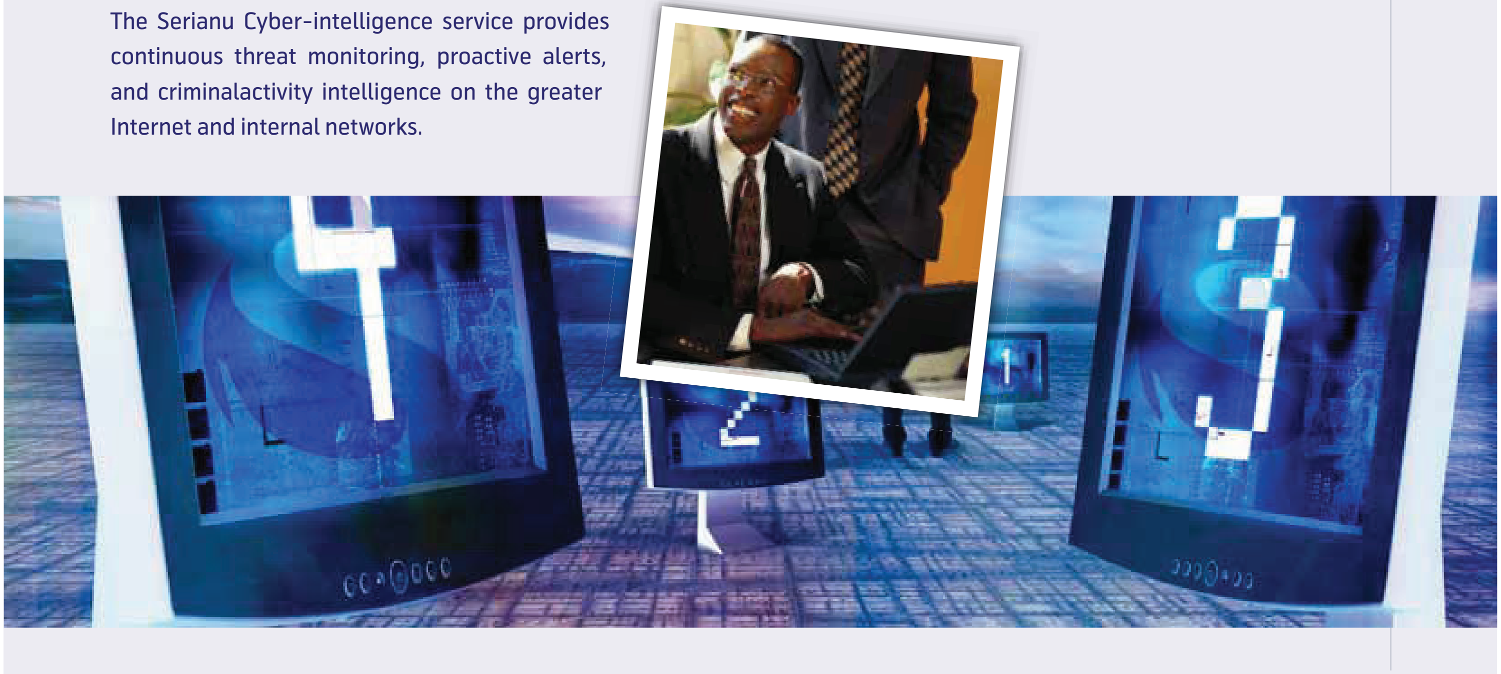
- Critical systems security
- Data at rest - file servers and shares
- Data in motion - Email, IM, FTP, IRC and Web traffic
- End user devices - USB, , Wireless devices
- User activity monitoring - internet traffic, down loads, web logs

4. Internal Compliance Audits:

- Access to critical systems, apps and networks
- User management - employees, partners and third parties
- Change management - applications and critical systems
- Segregation of duties - critical systems
- Business continuity - backups and testing

5. Serianu Cyber Intelligence Service

- Local and Global Research reports
- Active Fraud monitoring
- Cyber Threat reports
- Vendor vulnerability reports



Appendix I

Data sources and research material

Data used to come up with this report comes from publicly available databases, which includes a daily summary of spammers and spambots identified by honey pots set up and executed by Project Honey Pot members on their global network infrastructures. The spam data used in this report focuses on spam detected in the first four months of 2012.

References:

Akamai State of the Security Report Q12012 - http://www.akamai.com/

Microsoft Security Intelligence Report – www.microsoft.com/security/sir

Symantec Internet Security Threat Report - http://www.symantec.com/

Microsoft Security Blog - http://blogs.technet.com/b/security/

Project Honey Pot - http://www.projecthoneypot.org/

SenderBase – http://www.senderbase.org/

Composite Blocking List (CBL) - http://cbl.abuseat.org/

CVE website - http://cve.mitre.org/

UCE Protect Network - http://www.uceprotect.net/Watch Guard Reputation Authority - http://www.reputationauthority.org/

Pastebin - http://pastebin.com

Sophos - www.sophos.com

https://www.owasp.org

http://wiki.clug.org.za

http://www.ftc.gov

http://www.commandfive.com

http://www.standardmedia.co.ke

Appendix II

Definitions related to the spamming observation

Definitions (Source Project Honey Pot)

As used in this report, Email Spammers consolidates dictionary attackers, spam servers and harvesters as defined by the Project Honey Pot website

Spam servers:

A spam server is the computer used by a spammer in order to send messages. A substantial percentage of these computers do not belong to the spammers themselves, but instead are "zombies" compromised by viruses or other malware. Project Honey Pot publishes the list of the top IP addresses used by spam servers.

Harvesters:

A harvester is a computer program that surfs the internet looking for email addresses. Harvesting email addresses from the Internet is the primary way spammers build their lists. Harvesters must connect to the Internet through an IP address. Project Honey Pot publishes the list of the top IP addresses used by harvesters.

Dictionary attackers:

A dictionary attack involves making up a number of email addresses, sending mail to them, and seeing what is delivered. Dictionary attackers typically send to common usernames. A username is the part of the email address before the @ sign.

Comment Spammers:

Comment spammers do not send email spam. Instead, comment spammers post to blogs and forums. These posts typically include links to sites being promoted by the comment spammer. The purpose of these links is both to drive traffic from humans clicking on the links, as well as to increase search engine rankings which are sometimes based on the number of links to a page.

Appendix III

Reputation score definitions

SenderBase Network:

SenderBase® — is the world's largest email and Web traffic monitoring network. SenderBase can be used like a "credit reporting service" for email, providing comprehensive data that ISPs and companies can use to differentiate legitimate senders from spammers and other attackers and giving email administrators visibility into who is sending them email.

Reputation Score:

By tracking a broad set of attributes for email and web, SenderBase supports very accurate conclusions about a given host. Sophisticated security modelling leverages the breadth of SenderBase data to generate a granular reputation. Granular reputation score is grouped into Good, Neutral and Poor.

Good:

Little or no threat activity has been observed from an IP address or domain. Email or Web traffic is not likely to be filtered or blocked*.

Neutral:

IP address or domain is within acceptable parameters. However, Email or Web traffic may still be filtered or blocked*.

Poor:

A problematic level of threat activity has been observed from an IP address or domain. Email or Web traffic is likely to be filtered or blocked*.

Appendix IV: Hacking Evidence

Figure 3.3 below, shows some of the 103 Government of Kenya websites that were compromised and exposed to hackers.

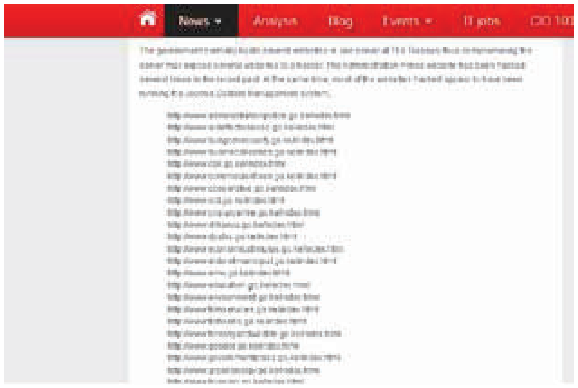
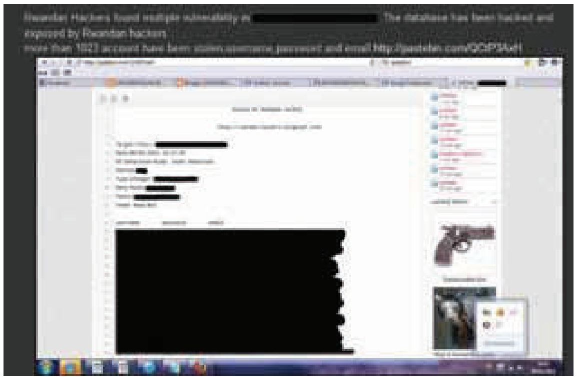


Fig 3.3

The figure below shows the Website exposure which led to theft of usernames and exposure of passwords. This was posted on www.pastebin.com.

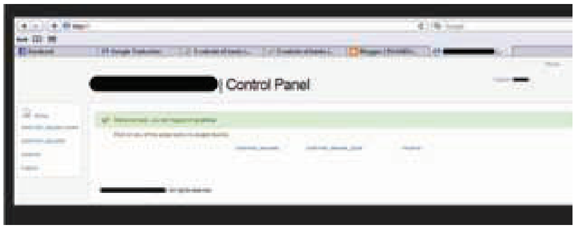


Rwandan Hackers found multiple vulnerability in [redacted] The database has been hacked and exposed by Rwandan hackers
more than 1023 account have been stolen.username,password and email http://pastebin.com/QCtP3Axt

[redacted]

Fig 3.4

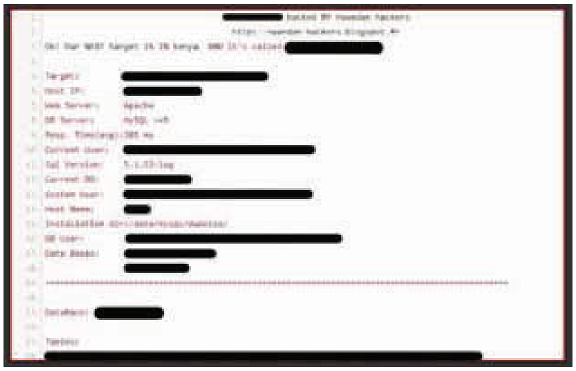
Below is evidence that the Rwandan hackers posted on their website showing the access they had gained into the control panel of Bank A. This allowed them to change whatever they pleased.



[redacted] Control Panel

Fig 3.5

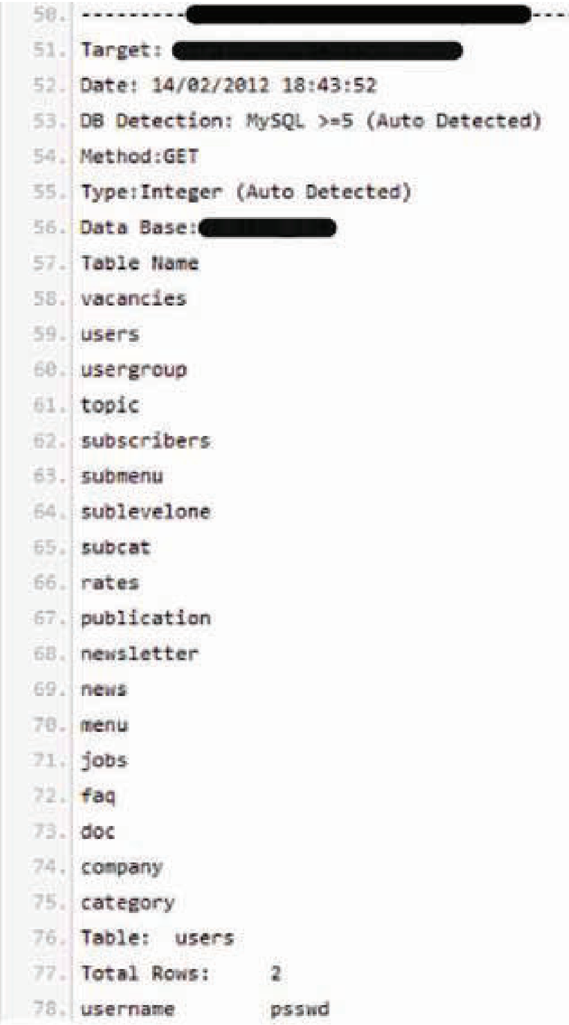
Figure 3.6 below, shows a sample of Bank B's database that was exposed by the Rwandan hackers on www.pastebin.com.



```
[redacted] hacked BY rwandan hackers
           http://rwandan-hackers.blogspot.#/
Ok! Our NEXT Target IS IN kenya. AND It's called [redacted]

Target:           [redacted]
Host IP:          [redacted]
Web Server:       Apache
DB Server:        MySQL >=5
Resp. Time(avg):  385 ms
Current User:     [redacted]
Sql Version:      5.1.53-log
Current DB:       [redacted]
System User:      [redacted]
Host Name:        [redacted]
Installation dir: [illegible]
DB User:          [redacted]
Data Bases:       [redacted]

--------------------------------------------------------------------

Database: [redacted]

Tables:
[redacted]
```

Fig 3.6

The figure below shows Bank C's database which was also hacked and exposed by the Rwandan hackers.

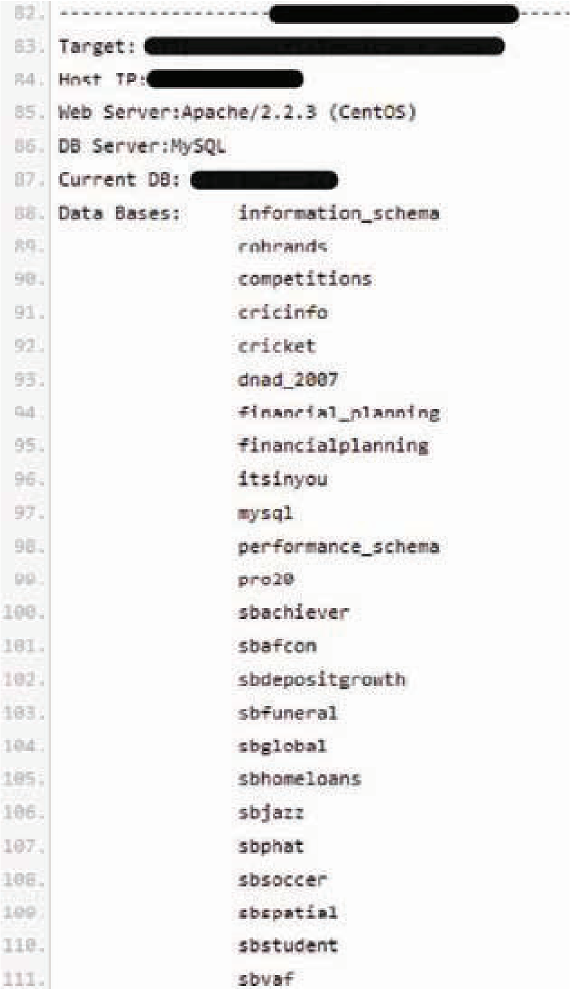


```
---------[redacted]---
Target: [redacted]
Date: 14/02/2012 18:43:52
DB Detection: MySQL >=5 (Auto Detected)
Method:GET
Type:Integer (Auto Detected)
Data Base:[redacted]
Table Name
vacancies
users
usergroup
topic
subscribers
submenu
sublevelone
subcat
rates
publication
newsletter
news
menu
jobs
faq
doc
company
category
Table:  users
Total Rows:     2
username        psswd
```

Fig 3.7

Below is an excerpt of some of Bank D's databases that were published on on www.pastebin.com after their DB server was hacked into by the Rwandan hackers.

Fig 3.8



```
------------------[redacted]----
Target: [redacted]
Host IP:[redacted]
Web Server:Apache/2.2.3 (CentOS)
DB Server:MySQL
Current DB: [redacted]
Data Bases:     information_schema
                cobrands
                competitions
                cricinfo
                cricket
                dnad_2007
                financial_planning
                financialplanning
                itsinyou
                mysql
                performance_schema
                pro20
                sbachiever
                sbafcon
                sbdepositgrowth
                sbfuneral
                sbglobal
                sbhomeloans
                sbjazz
                sbphat
                sbsoccer
                sbspatial
                sbstudent
                sbvaf
```

SERIANU

SERIANU (K) LTD
14 Chalbi Drive, Lavington
P. O. Box 56966 - 00200 Nairobi, Kenya
Email: info@serianu.com
Tel: +254 702 847 570

www.serianu.com