CYBER CRIME & CYBER SECURITY TRENDS IN AFRICA

Published November, 2016

Symantec

CONTENTS

CHARTS & TABLES

INTRODUCTION

This report provides an overview of cyber security and cyber crime related developments in Africa. It assesses the major trends around the world and on the Continent. It also takes stock of the many advances made by government authorities as well as identifies some of the challenges in a rapidly connected and ICT-dependent world.

The research for and writing of this report was carried out jointly by the African Union Commission (AUC) and Symantec, as part of the Global Forum for Cyber Expertise (GFCE) Initiative, with additional support from the U.S. Department of State and the Council of Europe. The AUC leveraged their network of official contacts with governments throughout Africa, and in particular those national agencies or institutions leading cyber security or cyber crime related efforts.[1] Symantec gathered information through its global network, which is made up of more than 63.8 million attack sensors and records thousands of events per second. Spam, Phishing, and Malware data provided by Symantec is captured through a variety of sources including a system of more than five million decoy accounts, and a threat detection network processing over nine billion email messages each month and more than 1.8 billion web requests filtered each day across 13 data centers. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 52 million consumers and 175 million endpoints. Other partners contributed with information according to their areas of expertise. The information reported by government authorities and collected by Symantec and others yielded useful insights in terms of the trends observed on the Continent, the steps being taken to address them, and those areas where significant gaps or deficiencies remain.

[1] Government authorities provided information voluntarily through a detailed country survey.

FOREWORD

November 2016

Africa is growing quickly in terms of population, the economy, and global influence. Today, Africa is home to 1.21 billion people (up from just 800 million in 2000), with a median age of just 19.5 years, the youngest population in the world.[1] With this prominence of youth comes a diverse population that is looking for productive employment, social engagement, free expression, and increased global connectivity. Technology adoption continues to rise in Africa, with mobile smart device ownership growing exponentially, social media use increasing, and the Internet of Things (IoT) becoming a reality. Even the most conservative metrics show that Africa is poised to make great gains and help fuel global growth into the future. With this growing prosperity and digitization however comes new risks and vulnerabilities that could undermine progress. In order for Africa to realize its full potential and to reap the full dividend from the development of the digital economy, the most important driver today for innovation, competiveness and growth, policymakers will need to implement effective policies and awareness initiatives to stem the rising tide of cyber threats. These same policymakers, technicians, and other experts have long noted the lack of detailed and reliable threat information regarding cyber crime threats in the region. Such information is invaluable in assessing and managing cyber risks by providing governments a more complete and nuanced understanding of how criminals and other actors are targeting and exploiting cyber-related vulnerabilities in African Countries.

As such, the African Union Commission (AUC) , and Symantec are pleased to partner together in developing this report, *Cyber Crime & Cyber Security Trends in Africa* to help provide insight into the African cyber eco-system as well as provide specific cyber threat information. This opportunity for the AUC and Symantec to partner came about through the extraordinary efforts of the Global Forum for Cyber Expertise (GFCE), a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from NGOs, the tech community and academia, GFCE members develop practical initiatives to build cyber capacity.

In addition to the AUC and Symantec this report represents a multi-stakeholder effort, with support from the United States Department of State and contributions from the Organization of American States and the Council of Europe. The report also provides a truly comprehensive landscape of cyber security in Africa with information submitted by 32 countries in Africa. Together, the information provides one of the clearest pictures to date of where the African continent stands with regard to cyber security. We acknowledge that this is only a snapshot in time and that the cyber security landscape is evolving quickly.

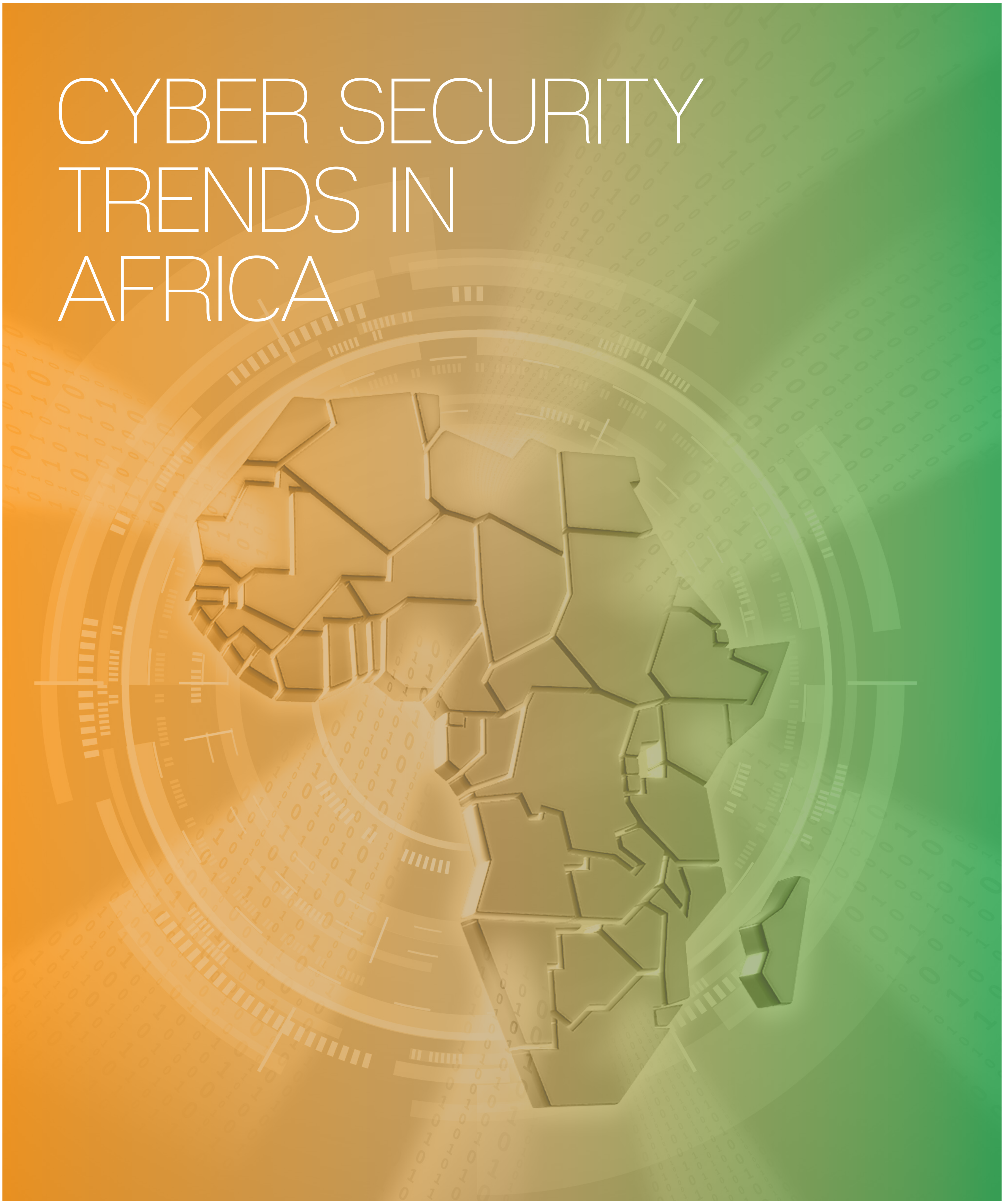
Our hope is that this report will serve as a baseline for which to identify areas in need of improvement and also to recognize many of the great strides African governments have made on cyber security in recent years. Above all, we hope that this information will be of assistance in guiding and strengthening all of our efforts going forward, particularly as we pursue future multi-stakeholder engagements to help build a safe, secure and stable digital world.

Sincerely,
Moctar Yedaly
Head of Information Society Division
African Union Commission

Sincerely,
Bill Wright
Director, Government Affairs
Symantec

[1] http://www.worldometers.info/world-population/africa-population/

CYBER SECURITY TRENDS IN AFRICA



THE MOST IMPORTANT TRENDS

Africa is a continent on the rise. It is growing quickly in terms of population, the economy, and global influence. Today, Africa is home to 1.21 billion people (up from just 800 million in 2000), with a median age of just 19.5 years, the youngest population in the world.[1] With this prominence of youth comes a diverse population that is looking for productive employment, social engagement, free expression, and increased global connectivity. While the downturn in world commodity prices has hit African economies hard, nearly every African nation is poised to grow over the coming years. Some will continue on a trajectory putting them among the fastest growing economies in the world. Technology adoption continues to rise as well, with mobile device ownership growing exponentially, social media use increasing, and the Internet of Things (IoT) quickly becoming a reality. Even the most conservative metrics show that Africa is poised to make great gains and help fuel global growth into the future. Along with this rapid economic growth, comes a burgeoning e-commerce industry that is poised to expand to an estimated $75 billion USD by the year 2025.[2]

With this growing prosperity and digitization however comes new risks and vulnerabilities that could undermine progress. Chief among these is the global rise of cyber crime. As the African Continent's economy moves online, citizens, their computer systems, and the Continent's information technology (IT) infrastructure become enticing targets for an increasingly professional cadre of cyber criminals. The growth of cyber crime is by no means just an African problem. In fact, in 2013, the total global direct cost of cyber crime reached an estimated $113 billion USD. In South Africa alone, 67% of adults reported experiencing cyber crime in the last year, which is estimated to have cost the South African economy $242 million USD. On average, cyber crime cost each cyber crime victim in South Africa US $274 per year.[3]

In order for Africa to realize its full potential, policymakers will need to implement effective policies and awareness initiatives to stem the rising tide of cyber threats. Unfortunately, these same policymakers, technicians, and other experts have long noted the lack of detailed and reliable threat information regarding cyber crime threats in the region. Such information is invaluable in assessing and managing cyber risks by providing governments a more complete and nuanced understanding of how criminals and other actors are targeting and exploiting cyber-related vulnerabilities.

Symantec discovered more than 430 million new unique pieces of malware globally in 2015, up 36 percent from the year before. Perhaps what is most remarkable is that these numbers no longer surprise us. As real life and online become indistinguishable from each other, cyber crime has become a part of our daily lives. Attacks against businesses and nations hit the headlines with such regularity that we've become numb to the sheer volume and acceleration of cyber threats.

8.8 million South Africans were victims of online crime in the past year. Globally, there were 602 million cyber crime victims over the last 12 months.

Norton Cyber Security Insights Report 2016

Due to the borderless nature of cyber crime, many of the cyber security trends we see globally also are affecting Africa, including the explosion of ransomware, social media scams, and the proliferation of new malware and website vulnerabilities. However, because of how the IT infrastructure evolved in Africa, several of these cyber crime trends will become especially acute and pose a significant danger.

Smartphones and The Internet of Things

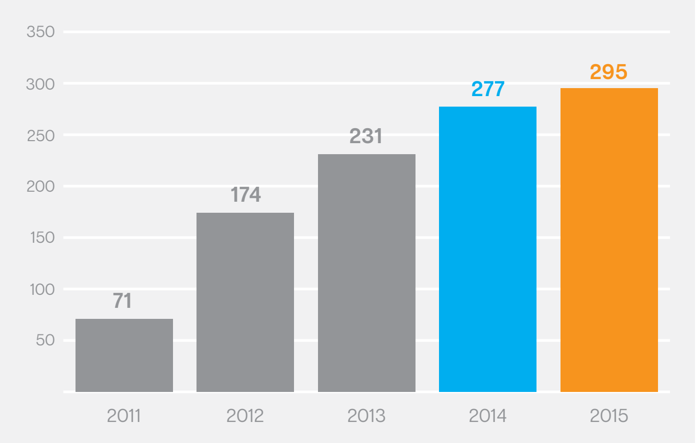
The world bought more than 1.4 billion smartphones in 2015, up 10 percent from the 1.3 billion units sold in the previous year, according to IDC's Worldwide Quarterly Mobile Phone Tracker (January 27, 2016). Five out of six new phones were running Android and one in seven running Apple's iOS operating system.[4] One mobile manufacturer, Ericsson, predicts there could be as many as 6.4 billion smartphone subscriptions globally by the end of 2020 – almost one per person.[5] Globally, the number of new vulnerabilities identified in mobile software grew a staggering 214% in 2014.[6] Globally, smartphones are an increasingly attractive target for cyber criminals who are investing in more sophisticated attacks that are effective at stealing personal data or extorting money from victims. In South Africa, 47% of spartphone users have experienced mobile cyber crime in 2013.[7] Mobile malware, is an especially concerning problem in Africa today and will continue to be a major threat into the future.

[1] http://www.worldometers.info/world-population/africa-population/
[2] http://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa
[3] https://us.norton.com/cyber-security-insights-2016
[4] http://www.idc.com/prodserv/smartphone-os-market-share.jsp
[5] https://www.ericsson.com/mobility-report
[6] Symantec Internet Security Threat Report, Volume 21
[7] https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Over the past decade, mobile phone networks have transformed communications in Africa. The ubiquity of mobile phones has allowed African communications networks to leapfrog the entire landline generation of development and go directly to the digital age.[8] However, the steady rise of mobile malware that mainly targets Android systems is concerning given that 89% of the smartphone market share in Africa runs on that platform.[9] For example, according to Symantec data, more than one out of every seven mobile devices in Nigeria is currently infected with mobile malware.

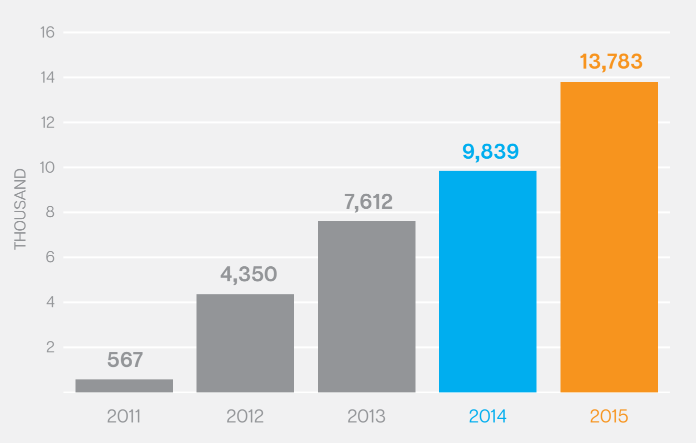
Cumulative Global Android Mobile Malware Families

▶ *The number of Android malware families added in 2015 grew by 6 percent, compared with the 20 percent growth in 2014.*



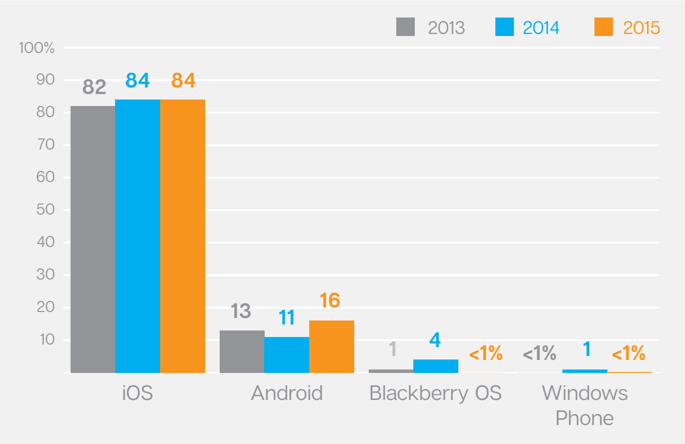
Cumulative Global Android Mobile Malware Variants

▶ *The volume of Android variants increased by 40 percent in 2015, compared with 29 percent growth in the previous year.*



Mobile Vulnerabilities by Operating System, Global

▶ *Vulnerabilities on the iOS platform have accounted for the greatest number of mobile vulnerabilities in recent years, with research often fueled by the interest to jail-break devices or gain unauthorized access to install malware.*



Africa also leads the world in money transfers using mobile phones, with 14% of all Africans receiving money through mobile transfers.[10] And with some of the world's largest mobile money transfer services, such as Kenya's Mpesa, cyber criminals will continue to heavily target mobile devices in Africa.

And while it may seem like a far away concept, the Internet of Things (IoT) also holds great potential and promise for Africa. Because the Continent is leap-frogging infrastructure-reliant communications, it will be able to adopt IoT solutions far more easily. For instance, in South Africa smart meters are already being installed to measure energy usage. And in Rwanda, they are connecting SIM cards to Point-of-Sale terminals to isolated areas to accommodate the use of credit cards payments.[11] The applications for IoT technology in Africa are only limited by ones own imagination. One innovative use of IoT technology is being used to protect the endangered Black Rhinoceroses in eastern and central Africa from poachers. The technology includes an RFID chip embedded into the Rhino's horn and an ankle monitor which pinpoints the animals location as well as an alert if the horn is ever removed from the animal. This IoT technology can also be used to monitor the Rhino's vitals. However, as the main component of IoT involves content sharing among relevant platforms, data security, privacy, and risks of hacking will be of paramount concern.[12] Symantec saw many proof-of-concept and real-world attacks globally last year, identifying serious vulnerabilities in cars, medical devices, and more. Manufacturers need to prioritize security to reduce the risk of serious personal, economic, and social consequences.

[8] http://www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline/

[9] https://www.idc.com/getdoc.jsp?containerId=prAE25737515

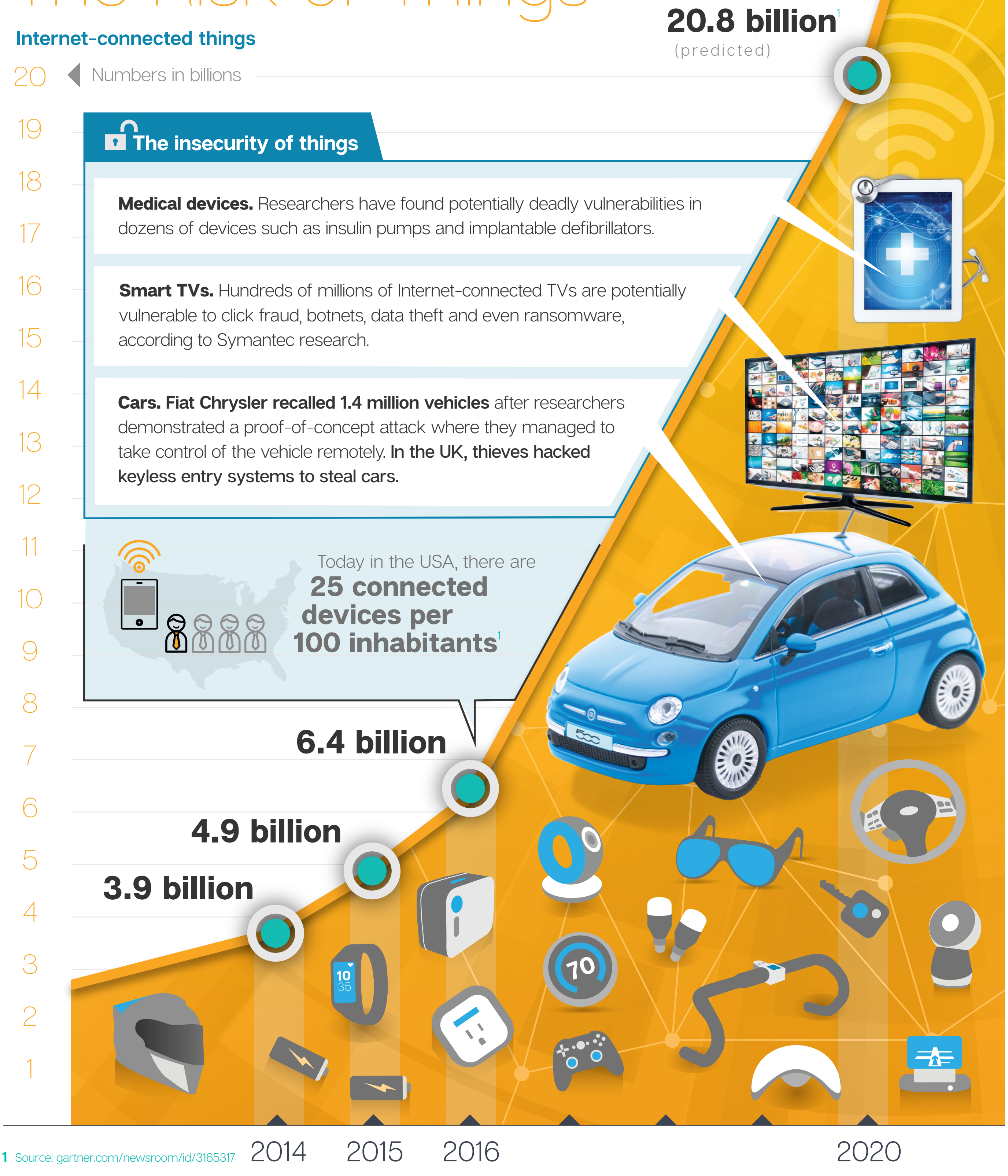
[10] UNCTAD Information Economy Report 2015

[11] http://africanbusinessmagazine.com/sectors/infrastructure/will-africa-take-lead-internet-things/

[12] http://motherboard.vice.com/blog/iot-technology-may-be-the-key-to-protecting-our-wildlife

Peek into the Future: The Risk of Things

Internet-connected things



The insecurity of things

Medical devices. Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators.

Smart TVs. Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft and even ransomware, according to Symantec research.

Cars. Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. **In the UK, thieves hacked keyless entry systems to steal cars.**

Today in the USA, there are **25 connected devices per 100 inhabitants**[1]

[1] Source: gartner.com/newsroom/id/3165317

Cyber Crime: Ransomware Increased 35 Percent in 2015

Cyber criminals are using encryption as a weapon to hold companies', governments and individuals' critical data hostage

The underground economy is booming and cyber crime is growing fast across the globe and Africa is no exception. Africa could be viewed as a permissive environment for cyber criminals due to a lack of security capabilities, absence of relevant legislation and general lack of awareness of cyber security measures.

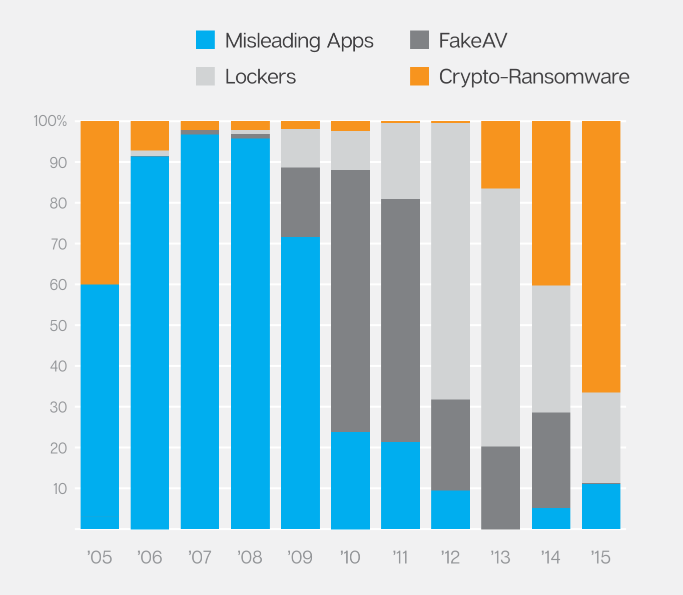
Cyber criminals are more professional and are much bolder, not only in the targets they choose to go after, but also the sums of money they seek. These criminal enterprises are for all intents and purposes, look like fully-functioning businesses, covering a multitude of areas, each with their own speciality. Just as legitimate businesses have partners, associates, resellers, and vendors, so do those enterprises operating in the shadows. While blackmarket prices for email addresses have dropped in recent years, credit card prices have remained relatively low but stable.[13] However, if they come with 'luxury' data – verification that the seller's accounts are still active or that a credit card has not yet been blocked – they now fetch a premium price. At the other end of the market, a drive-by download toolkit, which includes updates and 24x7 support, can be rented for between US$100 and US$700 per week, while distributed denial-of-service (DDoS) attacks can be ordered from US$10 to US$1,000 per day. At the top of the market, a zero-day vulnerability can sell for hundreds of thousands of dollars. And while there have been a number of high-profile cyber crime arrests made by law enforcement over the last year, cyber criminals continue to evolve and diversify their arsenal.

Ransomware has become increasingly dominant in recent times and continues to evolve. Last year, we saw Crypto-ransomware (encrypting files) push the less damaging locker-style ransomware (locking the computer screen) out of the picture. Crypto-style ransomware grew 35 percent last year. An extremely profitable type of attack, ransomware will continue to ensnare PC users and expand to any network-connected device that can be held hostage for a profit. In 2015, ransomware found new targets and moved beyond its focus on PCs to smart phones, Mac, and Linux systems. Symantec even demonstrated proof-of-concept attacks against smart watches and televisions in 2015.[14]

Never before have people across the world been subjected to extortion on such a massive scale as they are today. But why are criminals favoring ransomware, especially crypto-ransomware? With the glut of stolen information on the black market and the introduction of the more secure EMV standard (chip-and-pin) payment cards for card payments, the potential profit criminals can gain by exploiting stolen credit card details has reduced. Moreover, credit card fraud involves several people to conduct, and consumer legislation ensures the victim's financial loss is minimized. In contrast, an attacker can obtain a ransomware tool-kit from an underground source, and target their intended victims, who may have few alternatives but to pay-up. There are no middlemen for the criminal to pay and nothing to mitigate the losses to the victim, thus maximizing the profits.

Growing Dominance of Crypto-Ransomware, Global

▶ *Percentage of new families of misleading apps, fake security software (Fake AV), locker ransomware and crypto ransomware identified between 2005 and 2015.*



Overall, 67% of South Africans have experienced some form of online crime – compared to 48% globally.

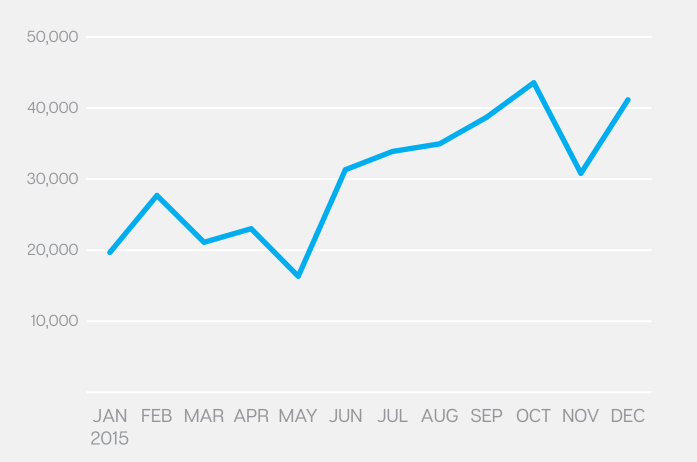
Norton Cyber Security Insights Report 2016

[13] https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

[14] https://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it

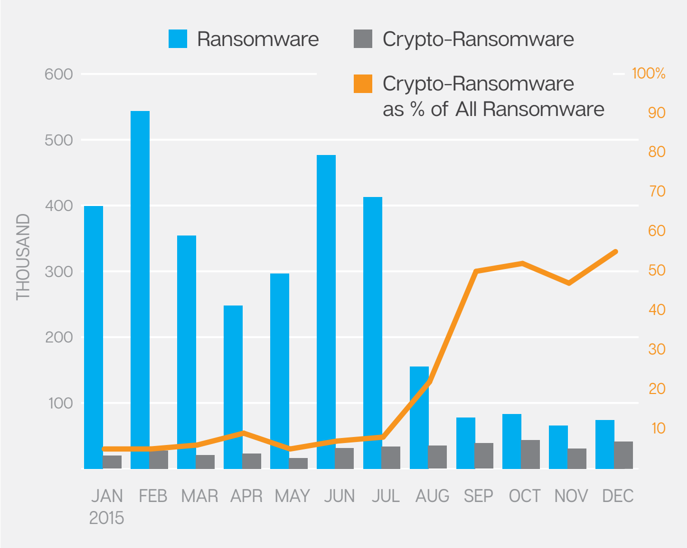
Crypto-Ransomware Over Time, Global

- *While more traditional locker-style ransomware is showing a rapid decline, crypto-ransomware continues to grow. Crypto-ransomware employs very strong, ostensibly unbreakable key-based cryptography to hold a victim's personal files to ransom by encrypting them with a key that only the criminals have access to.*

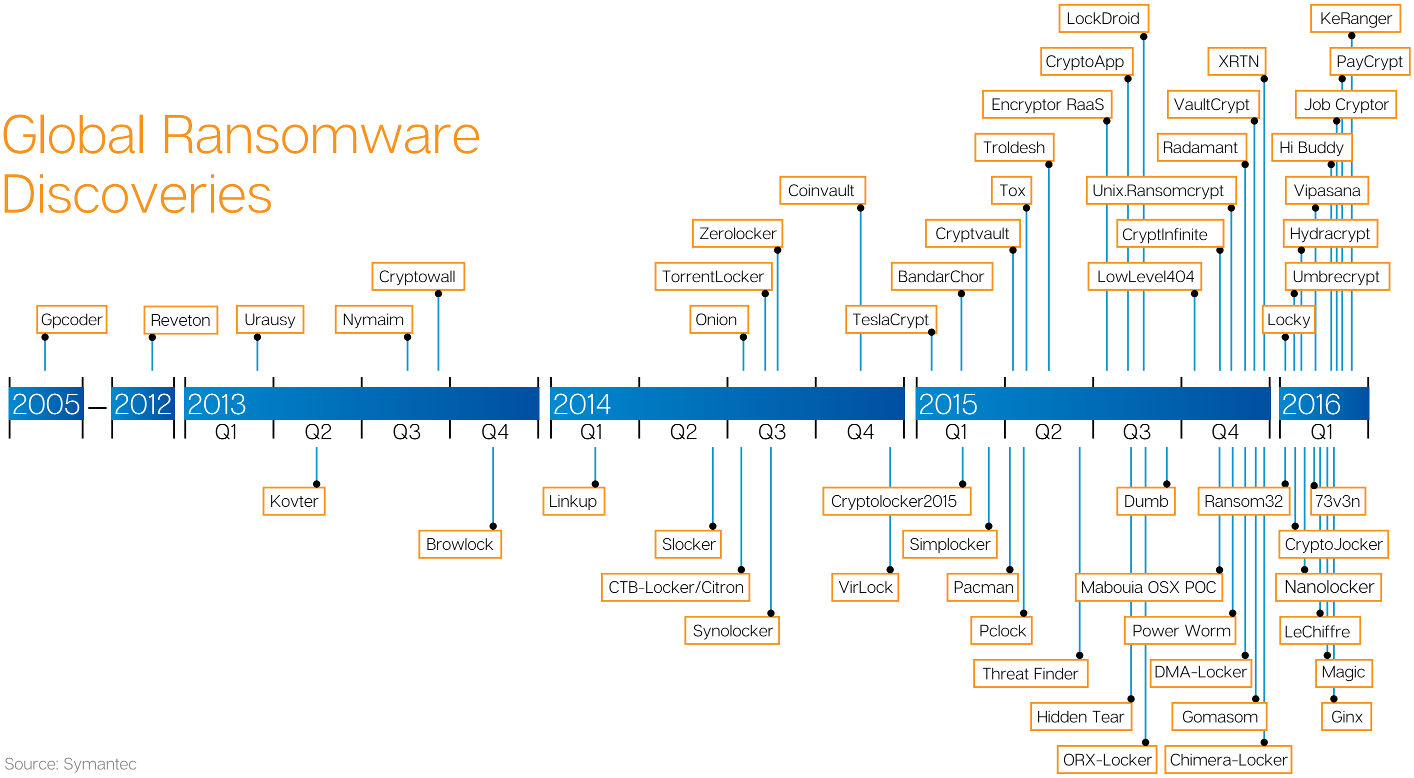


Crypto-Ransomware as Percentage of All Ransomware, Global

- *Although the chart indicates a steady decline in traditional ransomware in 2015, crypto-ransomware now accounts for the majority of all ransomware.*



Global Ransomware Discoveries



Source: Symantec

Social Media, Scams, & Email Threats

Cyber crime on the continent of Africa has moved far beyond the notorious 419 Nigerian email scams, coined after the code of legislation aimed to suppress such scams.[15],[16] The sophistication of some attacks and tactics used by cyber criminals demonstrates how vulnerable individuals are online and has chipped away at public confidence in online security and commerce. Data breaches, government surveillance, and good old-fashioned scams came together to further encroach on personal privacy, whether it is personal photos, login credentials or medical histories.

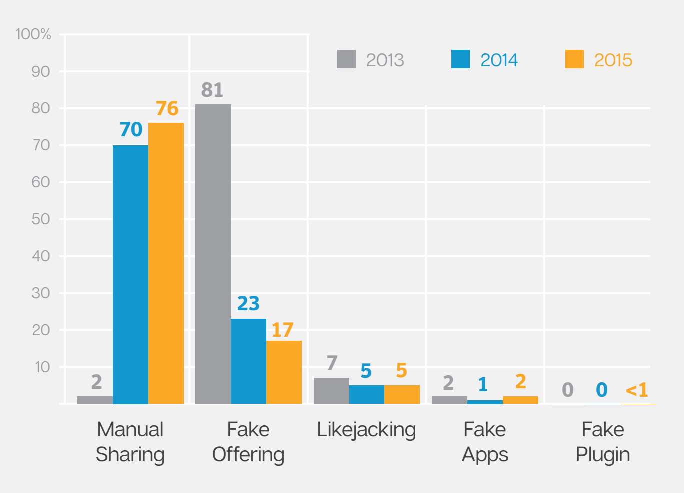
In 2015, Symantec saw plenty of traditional scams and malware attacks intended to gather personal information. For example, one scam promised large numbers of followers for free on Instagram, while seeking to fool people into revealing their passwords. Some attacks impersonated tax officials in an attempt to trick people into downloading malicious email attachments.

In their simplest form, many scams still rely on the poor security habits of the general public to succeed. However, we have also seen how poor website security can expose customer data. In the latter example, it doesn't matter how strong a password may be if the website is vulnerable to a data breach.

More concerning are attacks in 2015 that made use of sophisticated social engineering to bypass the two-factor authentication systems designed to safeguard users. By going through a legitimate password-reset process and posing as Google via SMS, however, one scam was able exploit the public's trust in a reputable brand to gain access to email accounts without raising the victims' suspicions.

Social media remains a favored target of scammers, as criminals seek to leverage the trust people have in their own social circles to spread scams, fake links, and phishing. To succeed, the social engineering involved must be convincing, so we have seen more ingenious tactics being used to dupe potential victims. Social media is quickly becoming a daily part of life across Africa. Around 9% of the population uses social media and that number is growing each year, with South Africans among the world's leaders in time spent on social networks at 3.2 hours per day.[17]In 2015, 120 million people were using Facebook across Africa, over 80% via their mobile device.[18]

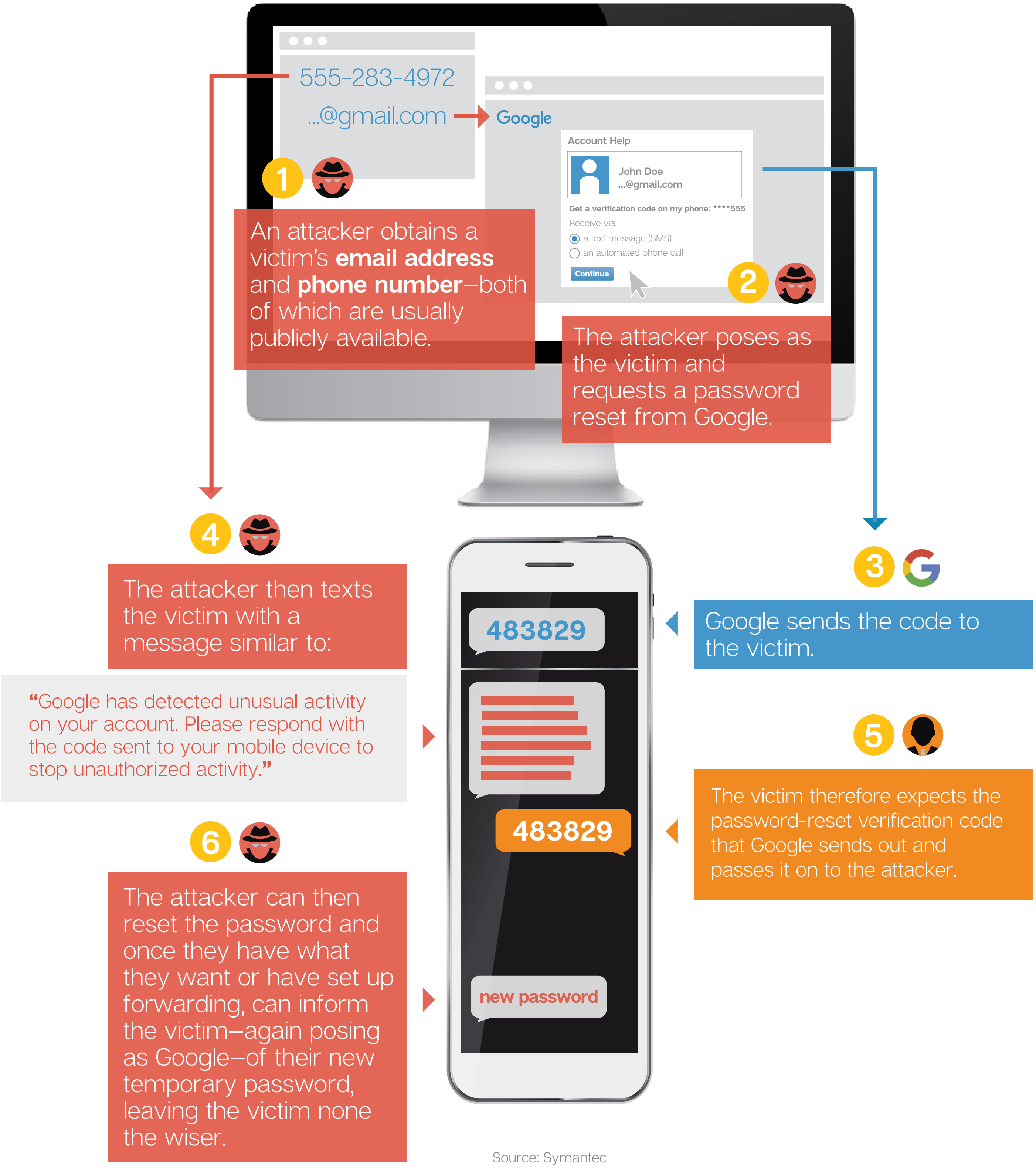
Global Social Media



- **Manual Sharing** – *These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers, or messages that they share with their friends.*
- **Fake Offering** – *These scams invite social network users to join a fake event or group with incentives, such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.*
- **Likejacking** – *Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.*
- **Fake Apps** – *Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described, and may be used to steal credentials or harvest other personal data.*
- **Fake Plugin** – *Users are invited to install a plugin to view a video, but the plugin is malicious and may spread by re-posting the fake video message to a victim's profile page without permission. Examples include installing a fake YouTube premium browser extension to view the video, or noticing that a DivX plugin is required, and the fake plugin masquerades as such. For more information visit: http://www.symantec.com/connect/blogs/fake-browser-plug-new-vehicle-scammers*

[15] http://www.bbc.com/news/business-32079748
[16] http://foreignpolicy.com/2010/03/24/africas-cyber-wmd/
[17] https://www.facebook.com/business/news/connecting-100-million-people-in-africa
[18] http://www.cnn.com/2016/01/13/africa/africa-social-media-consumption/

How the Gmail Scam Works



1 An attacker obtains a victim's **email address** and **phone number**—both of which are usually publicly available.

2 The attacker poses as the victim and requests a password reset from Google.

3 Google sends the code to the victim.

4 The attacker then texts the victim with a message similar to:

"Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity."

5 The victim therefore expects the password-reset verification code that Google sends out and passes it on to the attacker.

6 The attacker can then reset the password and once they have what they want or have set up forwarding, can inform the victim—again posing as Google—of their new temporary password, leaving the victim none the wiser.

Source: Symantec

Safeguarding Against Social Engineering

Cyber crime costs the global economy up to US$575 billion annually according to Bank of America and Merrill Lynch, whose report goes on to say that in a potential worst-case 2020 'Cybergeddon' scenario, cyber crime could extract up to a fifth of the value created by the Internet. It is everyone's responsibility to do all they can to prevent that from happening. For consumers, it's time kick bad habits. Many people know the basics of good cyber security, yet people continue to share their passwords. In fact more than a third of people who share passwords in the United States have shared the password to their online banking account. People need to start taking more responsibility for shoring up their online security. For example, in South Africa alone, 20% of social network users share their passwords with others, while 21% connect with people they do not know.[19]

Users should be more wary of who they follow on social media. Bots can appear more and more like a real person, and are sometimes difficult to spot. When choosing who to trust on social media, consider the following advice:

- **Be skeptical of new followers.** If a random person follows you, do not automatically follow them back. Look at their tweets. Are they retweeting content that looks like spam? If they are, they are most likely a bot.
- **Numbers can lie.** Even if these random followers have tens of thousands of followers, those numbers can easily be faked. Do not base your decision to follow them back based on how many people follow them.
- **Look for the "verified" badge.** Twitter users should always check to see if a well-known brand or famous celebrity has been verified by Twitter before following. The blue verified badge denotes that Twitter has authenticated the true owner of an account.

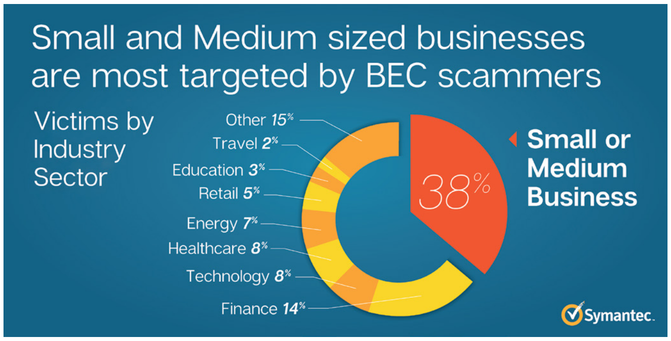
Conclusions

With a young population that is rapidly adopting new technologies, Africa is on the verge of an internet boom. To keep pace, Africa needs to urgently address efforts to combat cyber crime and improve its cyber security posture. The current cyber threat landscape in Africa shows that users are being impacted both by threats that are trending globally as well as some that more specific to the region. It will take a concerted effort from international governments, industry, and civil society to fight cyber crime and improve cyber security so that Africa can reach its full potential and stay on track to be a major driver of the global economy. ■

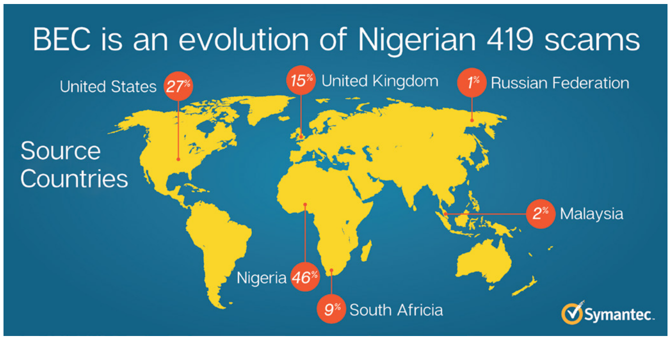
[19] https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

CASE STUDY: BUSINESS EMAIL COMPROMISE (BEC) SCAMS

One particularly successful scam is the Business E-mail Compromise (BEC). More than 400 companies worldwide are targeted with BEC scams every day. BEC scams are low-tech financial fraud in which spoofed emails from CEOs are sent to financial staff to request large money transfers. While they require little expertise and skill, the financial rewards for the fraudsters can be high. Almost 40 percent of identified victims are small to medium sized businesses. The next largest category of victim is the financial sector, at 14 percent.

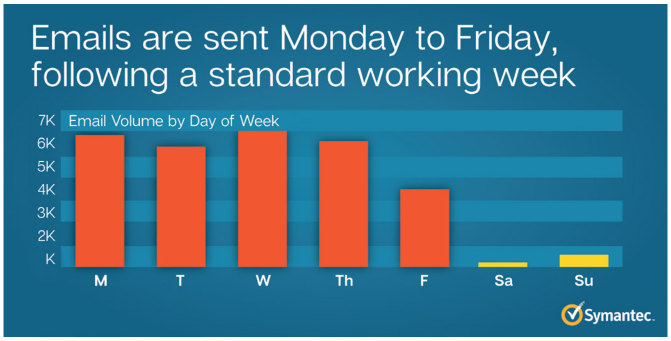


At least $3 billion have been lost to BEC scams in the past three years, with over 22,000 victims globally.[1] The BEC scam evolved from the infamous is Nigerian 419 scams, where individuals were sent emails promising victims riches in return for a small donation to help a fictional Nigerian prince. These scammers have now moved onto targeting businesses and are using less elaborate ruses to trick victims into transferring money. Symantec examined a large number of email addresses used by the scammers and found that 46 percent have Nigerian IP addresses. The rest are operating from the United States, the United Kingdom, South Africa, Malaysia, and Russia.



[1] https://www.ic3.gov/media/2016/160614.aspx#ref1

It should come as no surprise that the majority of BEC emails are sent on weekdays. The scammers know that this is when most businesses would expect emails. And more importantly, most financial transactions can only be cleared during weekdays. BEC scammers are also most active during a typical working day. They will generally begin sending emails from 0700 GMT, take break from 1100 until 1400 GMT and then resume sending until 1800 GMT.



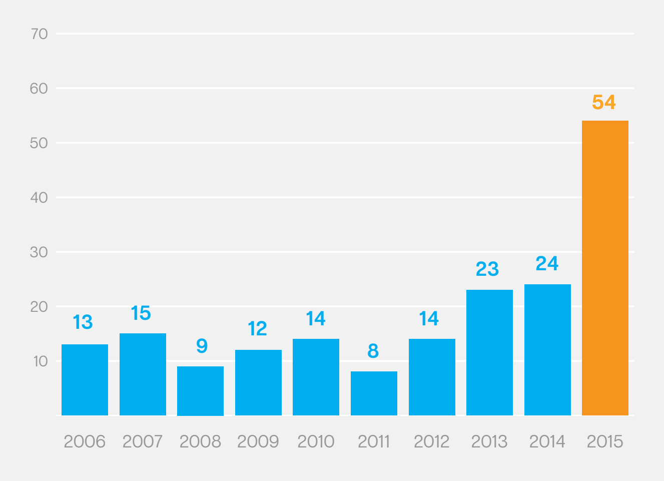
BEC scammers keep things simple with most emails containing a single-word subject line. Subjects always contain one or more of the following words: request, payment, urgent, transfer, enquiry. Simple, innocuous subject lines are less likely to arouse suspicion and are also harder to filter.[2]

Professionalization of Cyber Criminals, Zero Days Explode

In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125 percent increase from the year before. In 2013, the number of zero-day vulnerabilities (23) doubled from the year before. In 2014, the number held relatively steady at 24, leading us to conclude that we had reached a plateau. That theory was short-lived. The 2015 explosion in zero-day discoveries reaffirms the critical role they play in lucrative targeted attacks.

Global Zero-Day Vulnerabilities, Annual Total

▶ *The highest number of zero-day vulnerabilities was disclosed in 2015, evidence of the maturing market for research in this area.*



Given the value of these vulnerabilities, it's not surprising that a market has evolved to meet demand. In fact, at the rate that zero-day vulnerabilities are being discovered, they may become a commodity product. Targeted attack groups exploit the vulnerabilities until they are publicly exposed, then toss them aside for newly discovered vulnerabilities. When The Hacking Team was exposed in 2015 as having at least six zero days in its portfolio, it confirmed our characterization of the hunt for zero days as being professionalized.[3]

Vulnerabilities can appear in almost any type of software, but the most attractive to targeted attackers is software that is widely used. Again and again, the majority of these vulnerabilities are discovered in software such as Internet Explorer and Adobe Flash, which are used on a daily basis by a vast number of consumers and professionals in Africa and across the globe. Four of the five most exploited zero-day vulnerabilities in 2015 were Adobe Flash. Once discovered, the zero days are quickly added to cyber criminal toolkits and exploited. At this point, millions will be attacked and hundreds of thousands infected if a patch is not available, if people have not moved quickly enough to apply the patch, or if people are left unaware of an update.

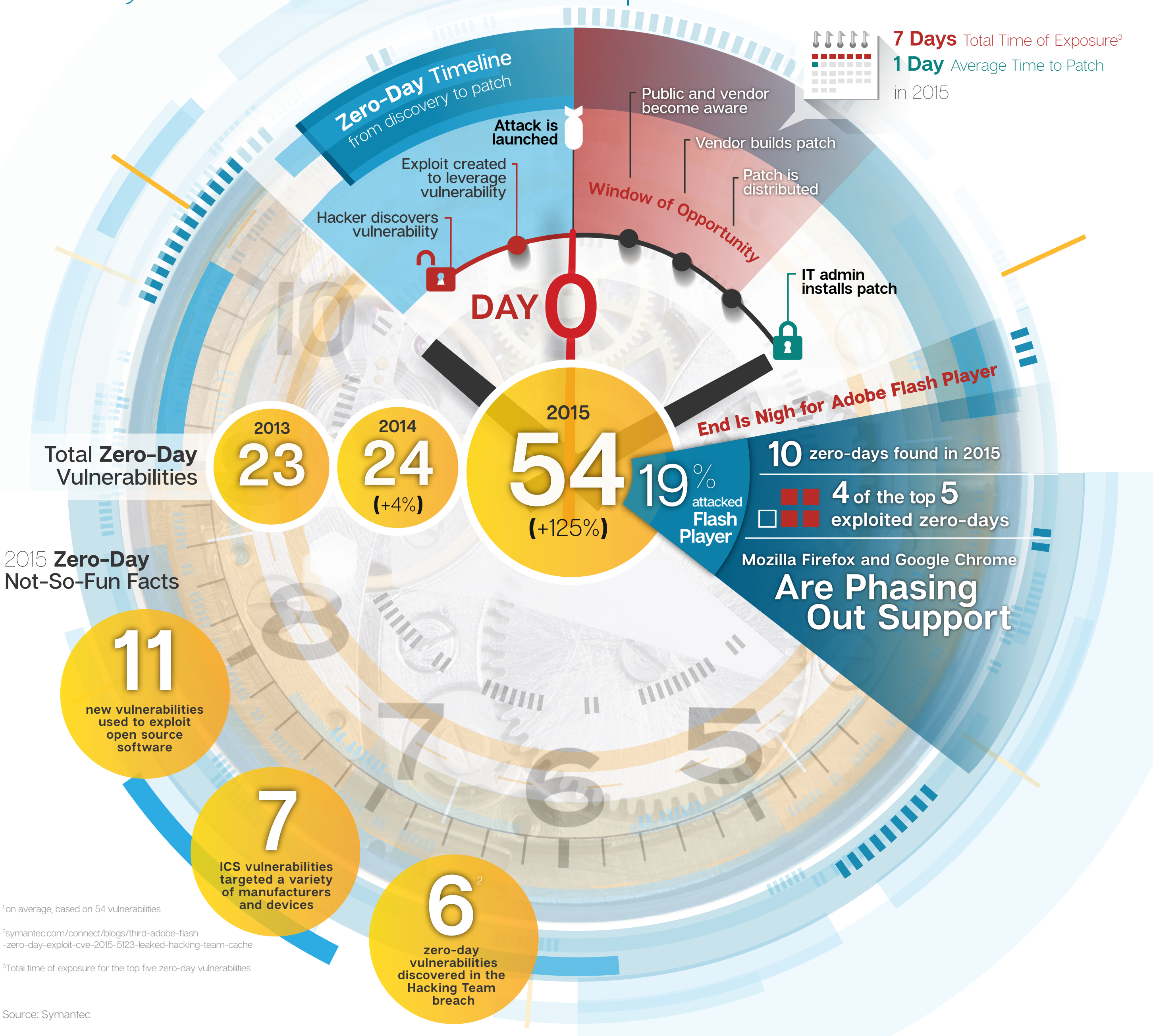
[2] https://www.symantec.com/connect/blogs/billion-dollar-scams-numbers-behind-bec-fraud

[3] https://www.symantec.com/connect/blogs/leaked-hacking-team-windows-vulnerability-could-facilitate-remote-attacks

A New Zero-Day Vulnerability Discovered Every Week in 2015[1]

Advanced attack groups continue to profit from previously undiscovered flaws in browsers and website plugins.

In 2015, 54 zero-day vulnerabilities were discovered.



7 Days Total Time of Exposure[3]
1 Day Average Time to Patch
in 2015

Zero-Day Timeline
from discovery to patch

Hacker discovers vulnerability

Exploit created to leverage vulnerability

Attack is launched

DAY 0

Window of Opportunity

Public and vendor become aware

Vendor builds patch

Patch is distributed

IT admin installs patch

Total **Zero-Day** Vulnerabilities

2013	2014	2015
23	24 (+4%)	54 (+125%)

End Is Nigh for Adobe Flash Player

19% attacked **Flash Player**

10 zero-days found in 2015

4 of the top **5** exploited zero-days

Mozilla Firefox and Google Chrome
Are Phasing Out Support

2015 **Zero-Day** Not-So-Fun Facts

11 new vulnerabilities used to exploit open source software

7 ICS vulnerabilities targeted a variety of manufacturers and devices

6[2] zero-day vulnerabilities discovered in the Hacking Team breach

[1] on average, based on 54 vulnerabilities

[2] symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache

[3] Total time of exposure for the top five zero-day vulnerabilities

Source: Symantec

Compounding the problem is the fact that many Africans are still using outdated, or in many cases unlicensed, software. In fact, one of the drivers behind the increasing rates of cyber crime in Africa could be the widespread use of outdated or unlicensed software programs. According to the Business Software Alliance's annual Global Software Survey reports that approximately 57% of software used in Africa and the Middle East is unlicensed.[4] Nearly one quarter of users in Africa are currently using the operating system, Microsoft Windows XP which was first released in 2001, and for which software patches were discontinued in 2014.[5]

Major Security Vulnerabilities in Three Quarters of Websites Globally

Web administrators still struggle to stay current on patches

There were over one million web attacks globally against people each and every day in 2015. Many people believe that keeping to well-known, legitimate websites will keep them safe from online crime. This is not true. Cyber criminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. More than 75 percent of all legitimate websites have unpatched vulnerabilities. Fifteen percent of legitimate websites have vulnerabilities deemed 'critical,' which means it takes trivial effort for cyber criminals to gain access and manipulate these sites for their own purposes. It's time for website administrators to step up and address the risks more aggressively.

Scanned Websites with Vulnerabilities

▶ *A critical vulnerability is one which, if exploited, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.*

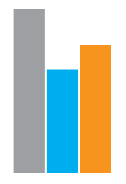
2013	2014	2015
77%	76% -1% pts	78% +2% pts

Percentage of Vulnerabilities Which Were Critical

2013	2014	2015
16%	20% +4% pts	15% -5% pts

[4] http://globalstudy.bsa.org/2016/index.html
[5] http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

BIG NUMBERS
(GLOBAL)



Total Identities Exposed

2013	2014	2015
552M	348M	429M
–	-37%	+23%

BREACHES

Total Breaches

2013	2014	2015
253	312	318
–	+23%	+2%

Breaches With More Than 10 Million Identities Exposed

2013	2014	2015
8	4	9
–	-50%	+125%

Average Identities Exposed per Breach

2013	2014	2015
2.2M	1.1M	1.3M
–	-49%	+21%

Median Identities Exposed per Breach

2013	2014	2015
6,777	7,000	4,885
–	+3%	-30%

EMAIL THREATS, MALWARE AND BOTS

Overall Email Spam Rate

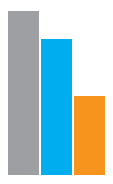
2013	2014	2015
66%	60%	53%
–	-6%pts	-7%pts

Email Phishing Rate (Not Spear Phishing)

2013	2014	2015
1 in 392	1 in 965	1 in 1,846

Email Malware Rate (Overall)

2013	2014	2015
1 in 196	1 in 244	1 in 220



Number of Bots

2013	2014	2015
2.3M	1.9M	1.1M
–	-18%	-42%

New Malware Variants (Added in Each Year)

2014	2015
317M	431M
–	+36%

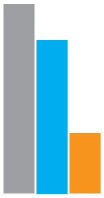
Crypto-Ransomware Total

2014	2015
269K	362K
–	+35%
Average Per Day 737	Average Per Day 992

MOBILE

New Mobile Vulnerabilities		
2013	2014	2015
127	168	528
–	+32%	+214%

New Android Mobile Malware Families		
2013	2014	2015
57	46	18
–	-19%	-61%



New Android Mobile Malware Variants		
2013	2014	2015
3,262	2,227	3,944
–	-32%	+77%

VULNERABILITIES

New Vulnerabilities		
2013	2014	2015
6,787	6,549	5,585
–	-4%	-15%

Zero-day Vulnerabilities		
2013	2014	2015
23	24	54
–	+4%	+125%

WEB

Web Attacks Blocked per Day		
2013	2014	2015
569K	493K	1.1M
–	-13%	+117%

Scanned Websites with Vulnerabilities …		
2013	2014	2015
77%	76%	78%
–	-1% pts	+2% pts

… Percentage of Which Were Critical		
2013	2014	2015
16%	20%	15%
–	+4% pts	-5% pts

Websites Found with Malware		
2013	2014	2015
1 in 566	1 in 1,126	1 in 3,172

SPEAR-PHISHING (EMAIL TARGETED ATTACKS)

Spear-Phishing Emails per Day		
2013	2014	2015
83	73	46
–	-12%	-37%

MALICIOUS ACTIVITIES REPORT

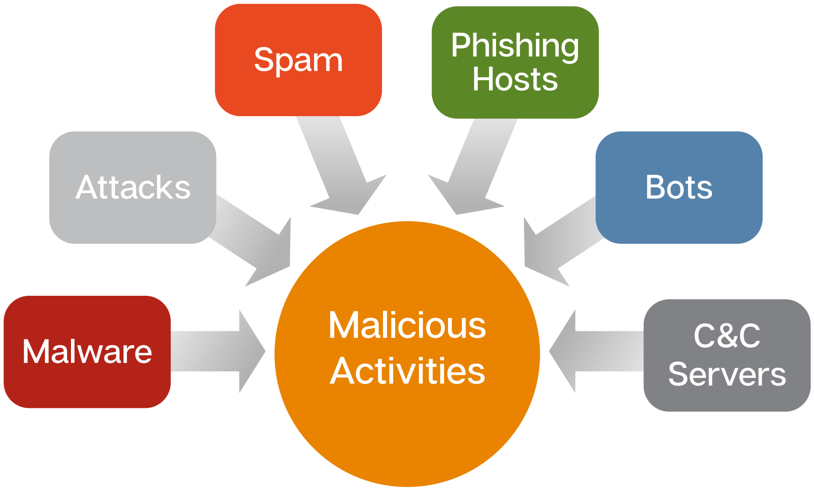
HIGHLIGHTS

METRIC	DESCRIPTION / PERCENTAGE
ATTACK	
Global percentage of attacks originating from Africa	0.6%
Top attack originating from Africa	Anonymous open proxy activity detected (38%)
Top attack targeting Africa	Microsoft Windows .lnk file code execution (13%)
MALWARE	
Global percentage of malware originating from Africa	1.5%
Top malware originating from Africa	W32.SillyFDC.BDP Attack (47%)
Top malware targeting Africa	Downloader.Dromedan Activity (15%)
SPAM	
Global percentage of spam originating from Africa	3.5%
PHISHING HOSTS	
Global percentage of phishing hosts originating from Africa	0.8%
BOT	
Global percentage of bots originating from Africa	11.4%
Top named botnet family for bots originating from Africa	Virut (40%)
C&C SERVERS	
Global percentage of C&C servers originating from Africa	2.9%

OVERALL MALICIOUS ACTIVITY—AFRICA

The Overall Malicious Activity metric looks at malicious activity originating from Africa across several different categories during the reporting period. To determine this, Symantec has compiled geographical threat data on malware, attacks, spam, phishing hosts, bots, and C&C servers (see Figure 1). See Appendix A: Methodology for descriptions of these activities.

Figure 1: Malicious Activity Types



Symantec has observed that malicious activities are often related and detection of any one of these malicious activities may indicate the presence of others. For example, C&C servers communicate with bots to relay commands, bots are often used to distribute spam and phishing campaigns, spam can often have malicious attachments that contain malware, and once infected with malware, a website can be leveraged to perform attacks on visitors. Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically more stable connections.

Spam incidents originating from Africa accounted for the greatest number of incidents of the six malicious behaviors during the reporting period (see Figure 2 and Table 1). During the reporting period, there were 1.1 billion spam events observed by Symantec that originated from Africa, representing 3.5% of the global total. It is not surprising that spam is the top malicious activity since Symantec has observed that monthly global spam rates in September 2016 were at 53%[1]. This means that half of all email messages sent are spam emails. Spam is a financially profitable business that requires very little infrastructure investment, especially if the actors involved use spam bots to send out the emails. A few hundred spam bots can send out tens of thousands of spam messages per day. Even if the click-through rate on these spam campaigns is very small, scammers can still make a large profit on millions of spam emails.

During the reporting period, bot activity ranked second with 14 million distinct IP addresses accounting for 11.4% of the global total, while malware activity ranked third with 8.5 million incidents representing 1.5% of the global total. Globally, Africa was not a significant source of malicious activity, accounting for less than 3% of the worldwide activity total.

[1] https://www.symantec.com/security_response/publications/monthlythreatreport.jsp#Spam

Figure 2. Malicious Activity Originating from Africa–2016

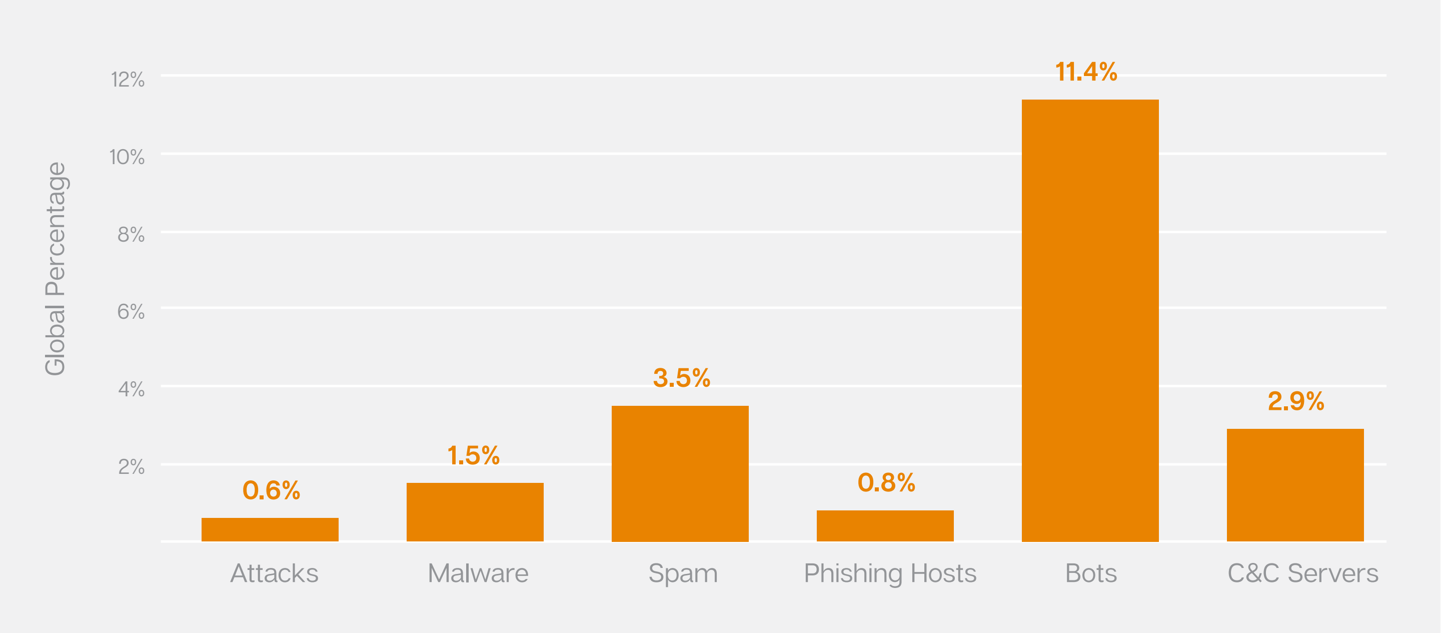


Table 1. Overall Malicious Activity Originating from Africa–2016

MALICIOUS ACTIVITY	INCIDENT COUNT		GLOBAL PERCENTAGE
	GLOBAL	AFRICA	
Attacks	201,283,309	1,249,575	0.6%
Malware	559,789,928	8,501,677	1.5%
Spam	32,298,641,930	1,122,760,857	3.5%

MALICIOUS ACTIVITY	INCIDENT COUNT		GLOBAL PERCENTAGE
	GLOBAL	AFRICA	
Phishing Hosts	785,770	6,210	0.8%
Bots	122,605,684	14,006,143	11.4%
C&C Servers	69,872	2,017	2.9%

MALICIOUS ACTIVITY DATA TABLES

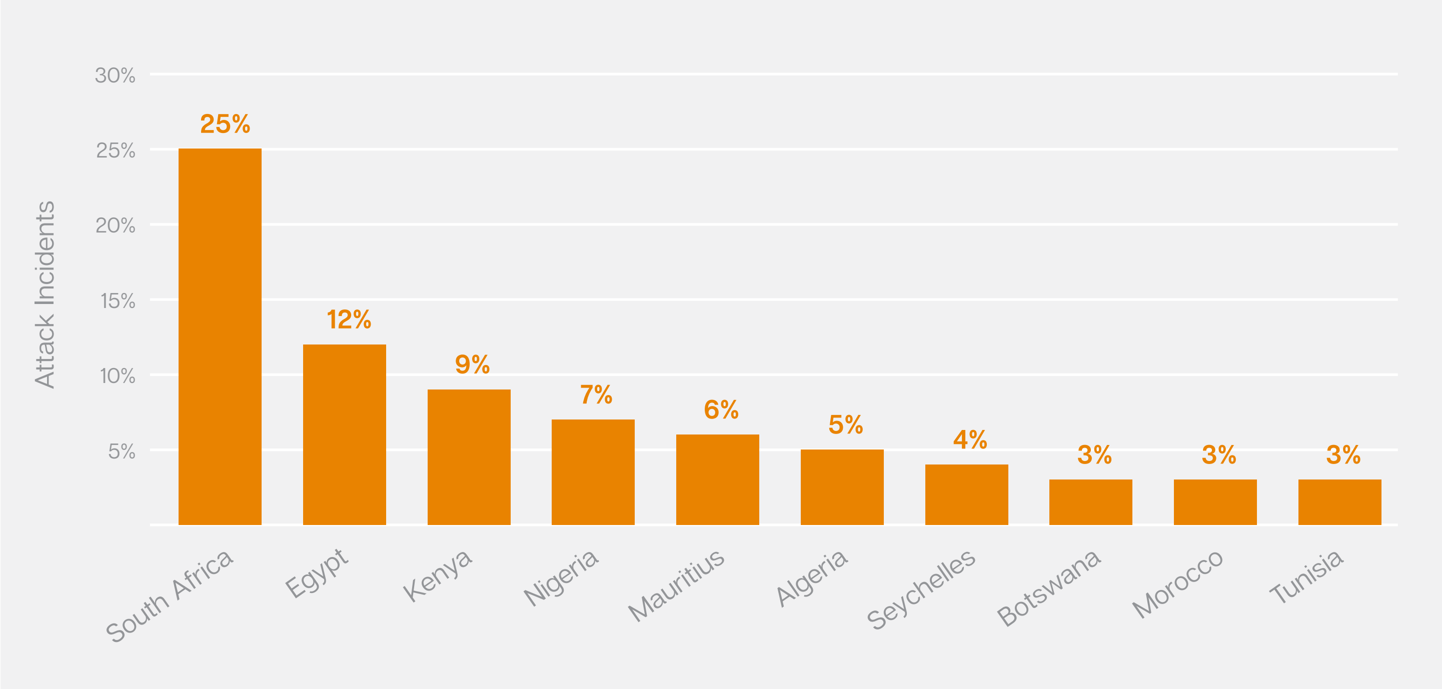
The data in this section lists the top 10 source African countries for each malicious behavior and their percentage within the continent. For attacks, malware, and spam, the incident counts, also known as event counts, are shown. For phishing hosts, bots, and C&C servers, the numbers of distinct IP addresses are given.

1. Attacks

Table 2. Top 10 Source African Countries for Attacks–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	25%	314,880
Egypt	2	12%	149,685
Kenya	3	9%	106,265
Nigeria	4	7%	89,100
Mauritius	5	6%	73,134
Algeria	6	5%	60,381
Seychelles	7	4%	45,661
Botswana	8	3%	37,880
Morocco	9	3%	34,464
Tunisia	10	3%	32,187

Figure 3. Top 10 Source African Countries for Attacks–2016

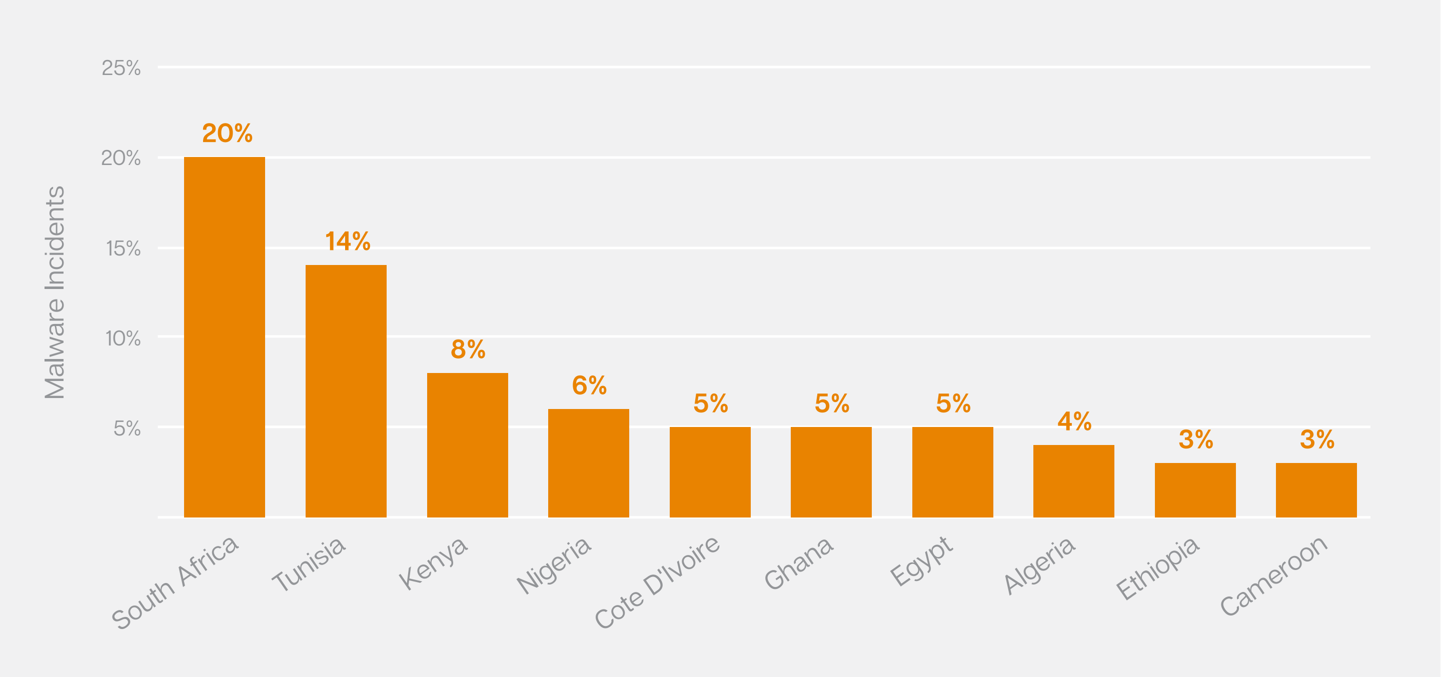


2. Malware

Table 3. Top 10 Source African Countries for Malware–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	20%	1,716,308
Tunisia	2	14%	1,166,774
Kenya	3	8%	668,194
Nigeria	4	6%	469,018
Cote D'Ivoire	5	5%	407,112
Ghana	6	5%	405,805
Egypt	7	5%	400,679
Algeria	8	4%	304,114
Ethiopia	9	3%	245,172
Cameroon	10	3%	224,546

Figure 4. Top 10 Source African Countries for Malware–2016

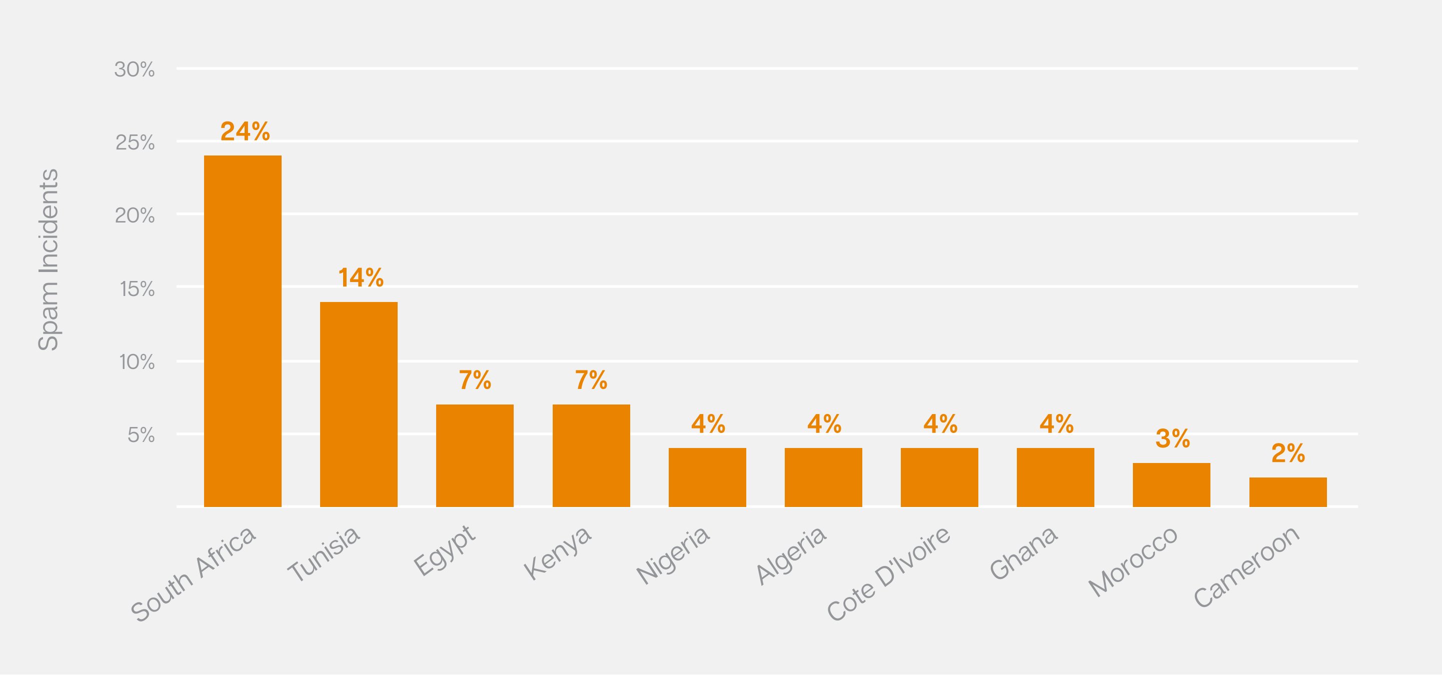


3. Spam

Table 4. Top 10 Source African Countries for Spam—2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	24%	271,700,021
Tunisia	2	14%	160,301,789
Egypt	3	7%	78,429,009
Kenya	4	7%	78,410,109
Nigeria	5	4%	50,491,804
Algeria	6	4%	50,253,534
Cote D'Ivoire	7	4%	47,632,285
Ghana	8	4%	43,938,441
Morocco	9	3%	32,197,294
Cameroon	10	2%	25,478,566

Figure 5. Top 10 Source African Countries for Spam—2016

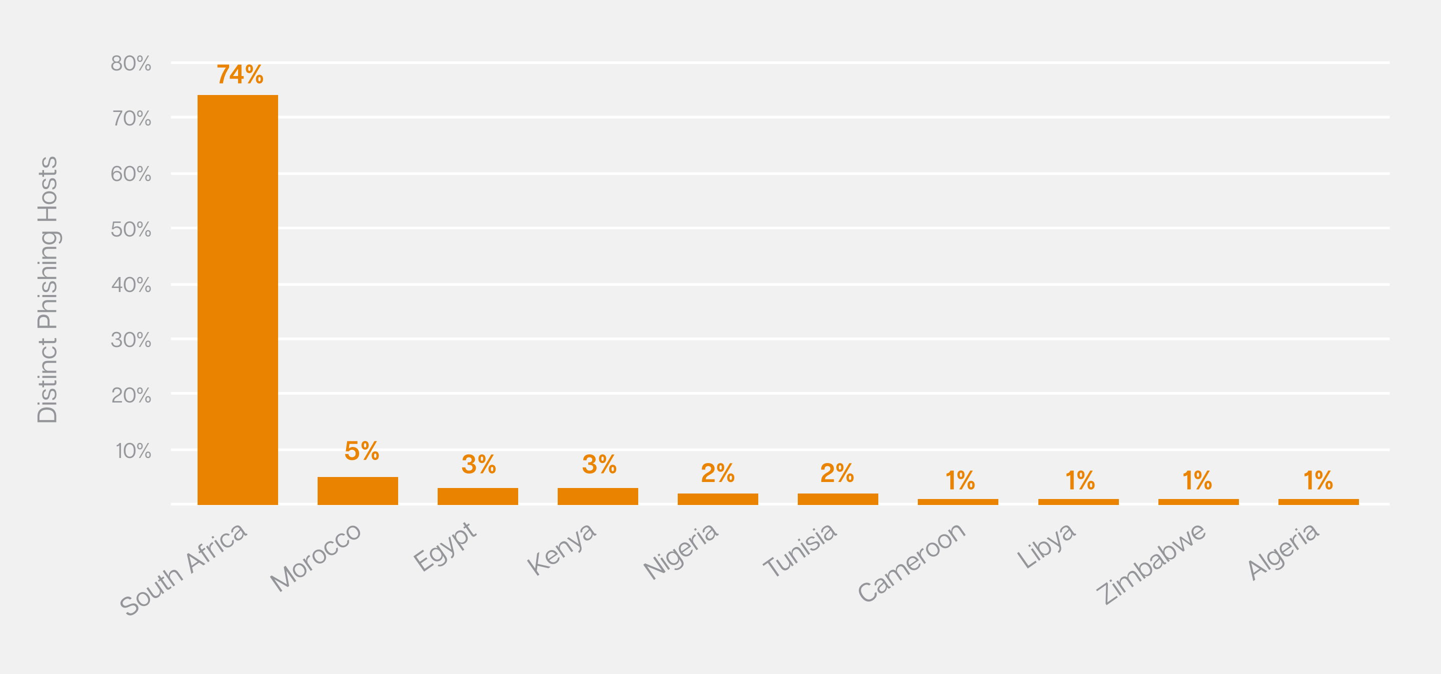


4. Phishing hosts

Table 5. Top 10 Source African Countries for Phishing Hosts–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	74%	4,621
Morocco	2	5%	319
Egypt	3	3%	184
Kenya	4	3%	160
Nigeria	5	2%	136
Tunisia	6	2%	112
Cameroon	7	1%	57
Libya	8	1%	53
Zimbabwe	9	1%	51
Algeria	9	1%	48

Figure 6. Top 10 Source African Countries for Phishing Hosts–2016

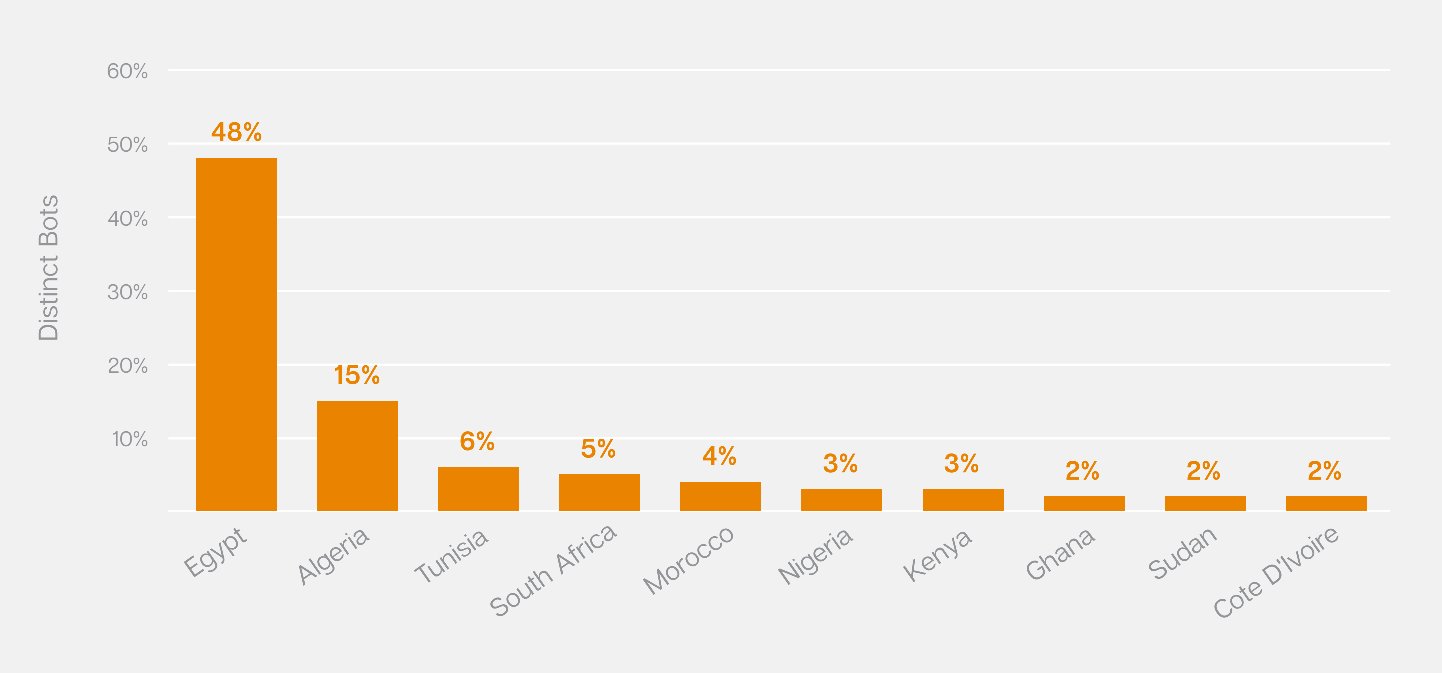


5. Bots

Table 6. Top 10 Source African Countries for Bots–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
Egypt	1	48%	6,778,893
Algeria	2	15%	2,117,402
Tunisia	3	6%	798,121
South Africa	4	5%	768,800
Morocco	5	4%	601,180
Nigeria	6	3%	488,416
Kenya	7	3%	435,032
Ghana	8	2%	282,776
Sudan	9	2%	258,914
Cote D'Ivoire	10	2%	247,672

Figure 7. Top 10 Source African Countries for Bots–2016

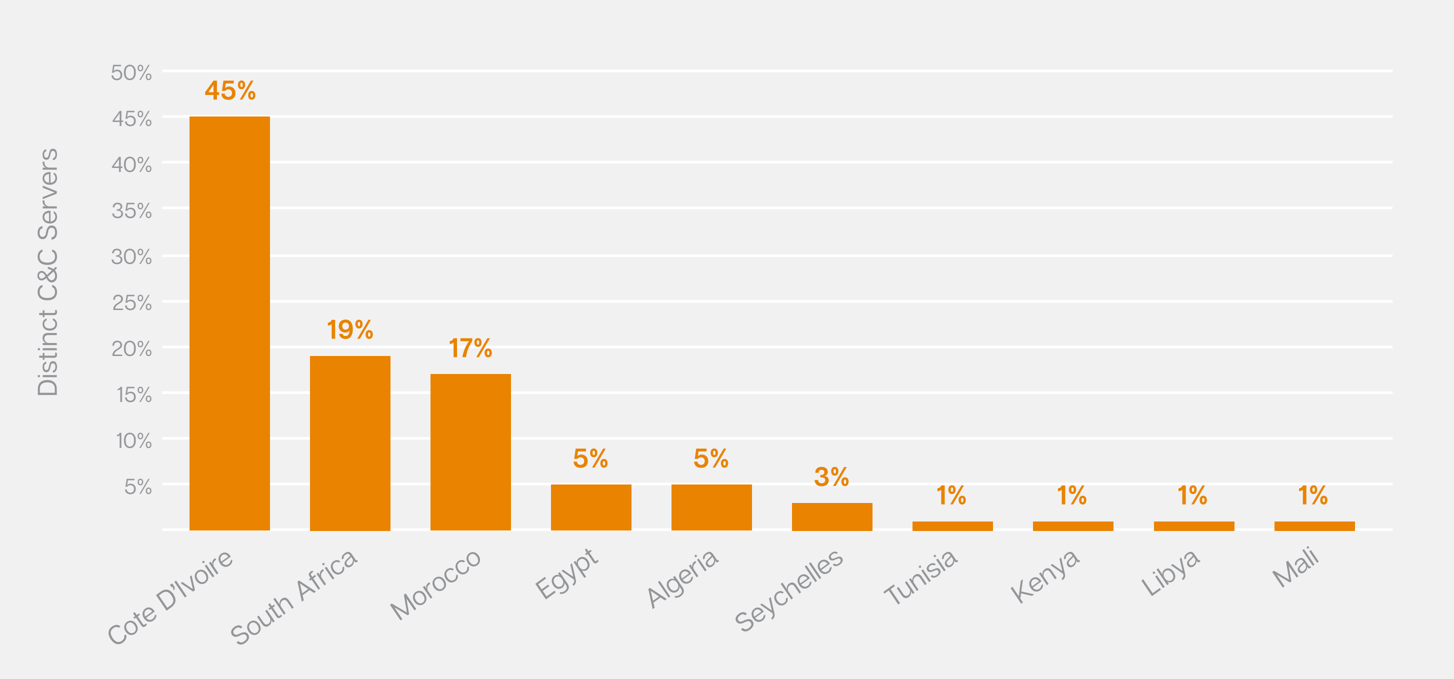


6. C&C Servers

Table 7. Top 10 Source African Countries for C&C Servers–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
Cote D'Ivoire	1	45%	910
South Africa	2	19%	391
Morocco	3	17%	345
Egypt	4	5%	99
Algeria	5	5%	98
Seychelles	6	3%	61
Tunisia	7	1%	29
Kenya	8	1%	21
Libya	9	1%	19
Mali	10	1%	15

Figure 8. Top 10 Source African Countries for C&C Servers–2016



ATTACK ANALYSIS

Attackers use various exploits to gain unauthorized access to a computer or an organization's network. Motivations for these attacks can range from gaining financial profit, stealing sensitive information, disabling a network, establishing a C&C server, or using the system as a launching point for future attacks. Attacks can be active such as a brute-force attack that determines a user's password, or passive such as a web-based attack that waits for a user to visit a malicious webpage in an attempt to infect the user's computer with malicious code.

Top Attacks Originating from Africa

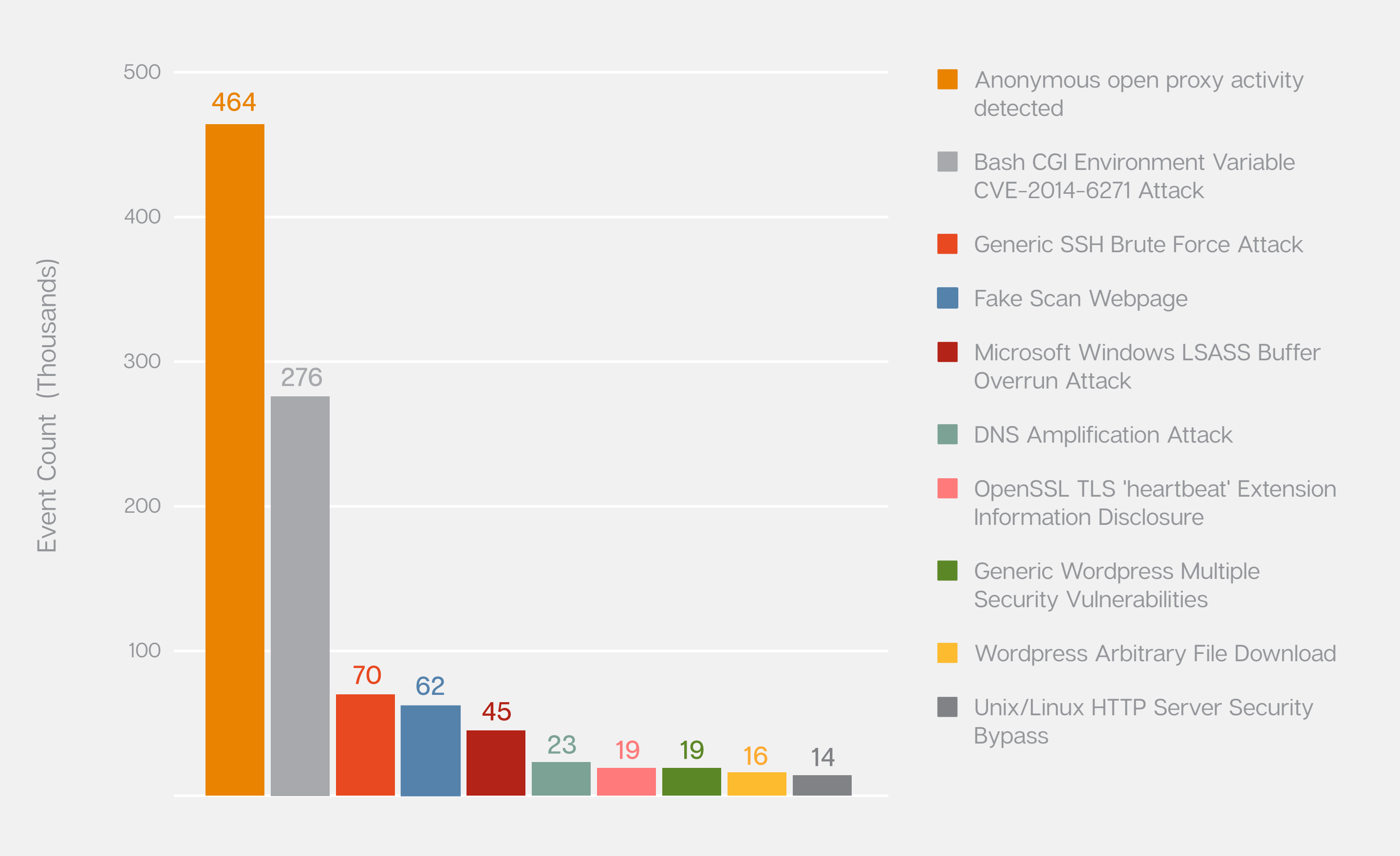
During the reporting period, there were 1,230,038 attack incidents over 363 different attack signatures originating from Africa. This accounted for less than 1% of the global attacks and as such, Africa was not a significant source of attacks globally. During the reporting period, the top attack originating in Africa was the Anonymous open proxy activity detected event with 463,762 incidents, accounting for 38% of the total Africa attacks (see Table 8 and Figure 9).

The Anonymous open proxy activity detected event indicates access to an open proxy has been detected. This may allow a user to bypass firewall rules which block access to certain internet content which has been deemed to violate corporate policy. Open proxies are also widely used in repressed countries which the government restricts internet content to its citizens.

Table 8. Top 10 Attacks Originating from Africa–2016

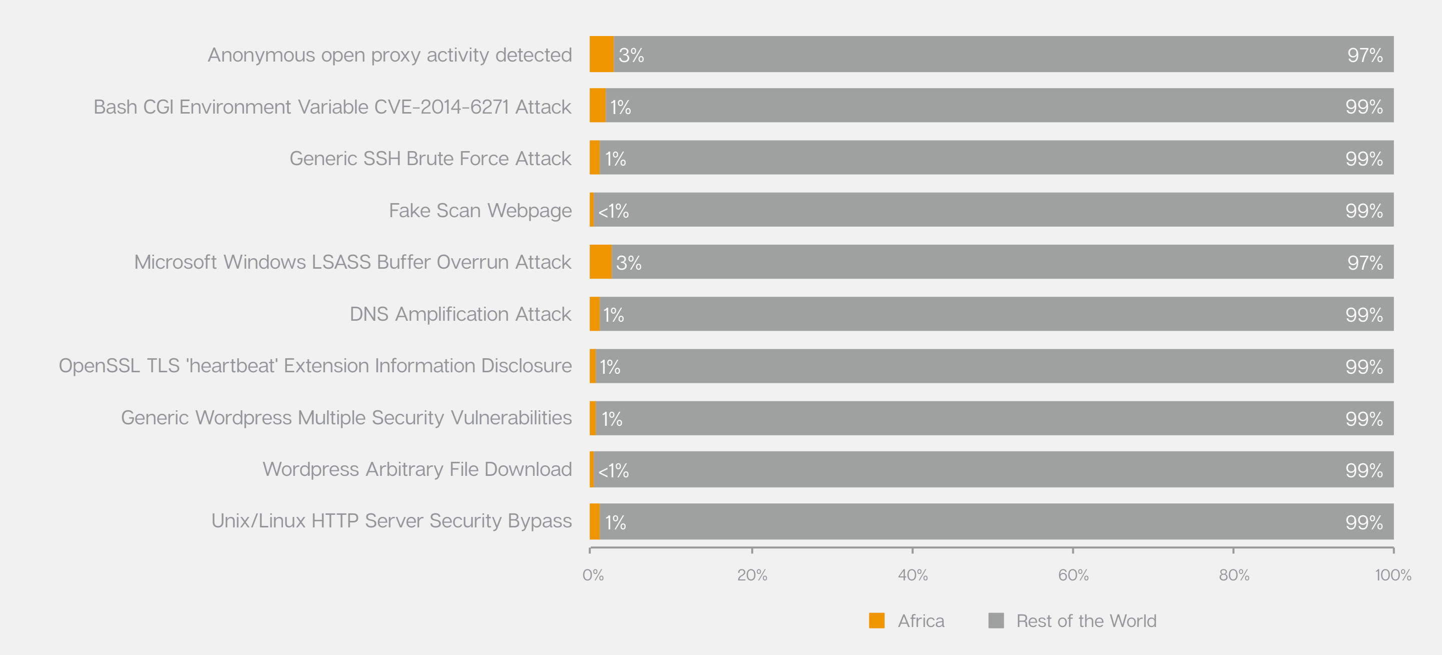
ATTACK	RANK	PERCENTAGE WITHIN AFRICA	GLOBAL RANK	GLOBAL PERCENTAGE
Anonymous open proxy activity detected	1	38%	13	6%
Bash CGI Environment Variable CVE-2014-6271 Attack	2	22%	13	6%
Generic SSH Brute Force Attack	3	6%	17	2%
Fake Scan Webpage	4	5%	12	5%
Microsoft Windows LSASS Buffer Overrun Attack	5	4%	34	1%
DNS Amplification Attack	6	2%	30	1%
OpenSSL TLS 'heartbeat' Extension Information Disclosure	7	2%	23	1%
Generic Wordpress Multiple Security Vulnerabilities	8	2%	23	1%
Wordpress Arbitrary File Download	9	1%	13	2%
Unix/Linux HTTP Server Security Bypass	10	1%	33	1%

Figure 9. Top 10 Attacks Originating from Africa–2016



Globally, there were nearly 16 million Anonymous open proxy activity detected events during the reporting period, which accounted for 6.0% of all global attacks (see Table 8). For the top 10 African attacks, Symantec compared the number of attack incidents against the total global number of incidents to determine whether Africa was a large source of those attacks globally. Symantec observed that 3% of all Anonymous open proxy activity originated from Africa during the reporting period (see Figure 10). Globally, Africa was not a significant source for the top 10 attacks.

Figure 10. Percentage of Attacks Originating from Africa with Global Comparison—2016



Top Attacks Targeting Africa

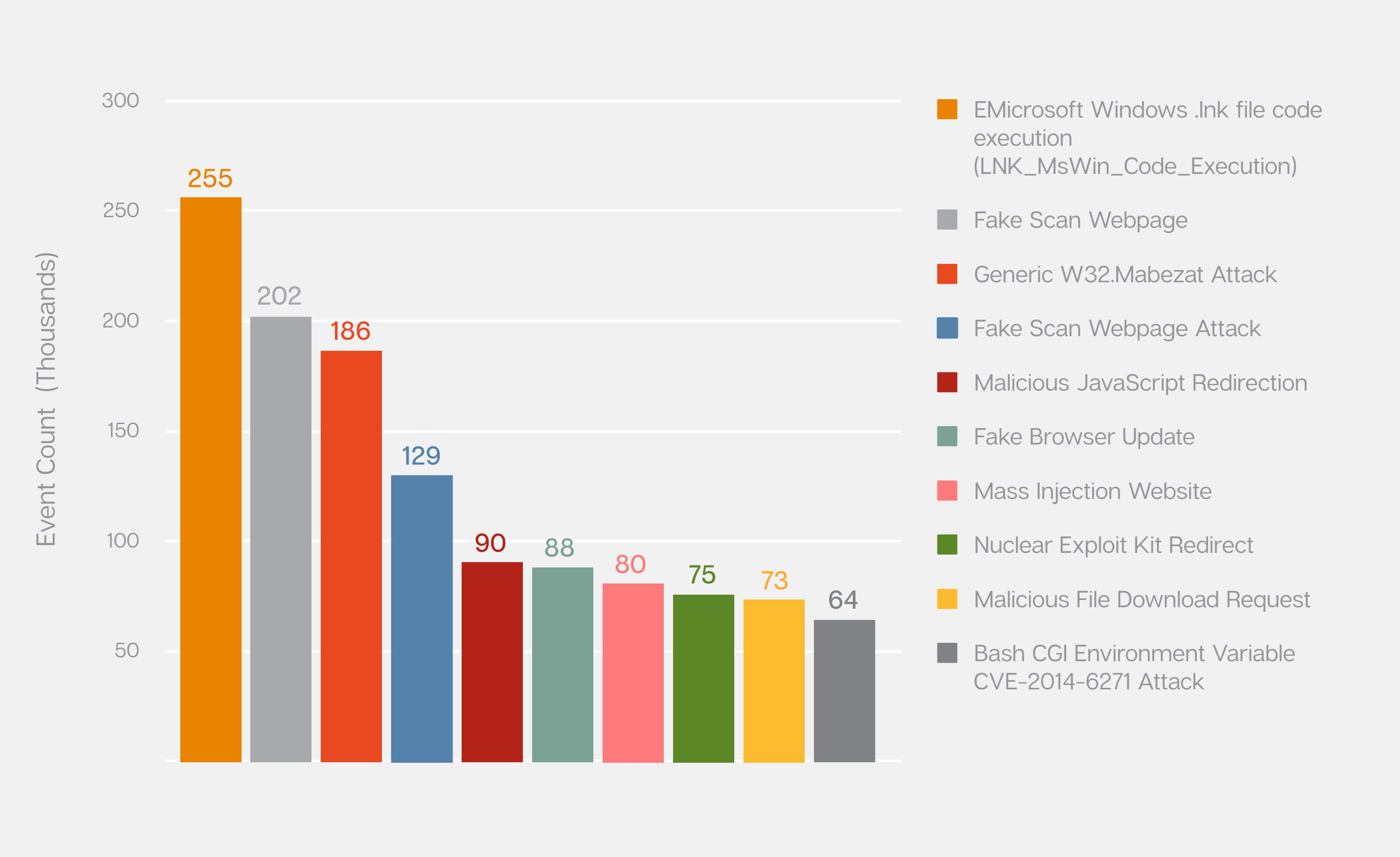
During the reporting period, there were 1.9 million attack incidents over 378 different attack signatures targeting Africa. This accounted for 1% of the global attacks. The top attack targeting Africa during the reporting period was the Microsoft Windows .lnk file code execution attack with 255,408 incidents, accounting for 13% of the total (see Table 9 and Figure 11).

The Microsoft Windows .lnk file code execution attack signature detects attacker's attempts to exploit a known vulnerability in Microsoft Windows when handling LNK or PIF files. Successful exploits could allow an attacker to completely compromise the affected computer.

Table 9. Top 10 Attacks Targeting Africa—2016

ATTACK	RANK	PERCENTAGE WITHIN AFRICA	GLOBAL RANK	GLOBAL PERCENTAGE
Microsoft Windows .lnk file code execution	1	13%	16	1%
Fake Scan Webpage	2	10%	5	5%
Generic W32.Mabezat Attack	3	10%	53	<1%
Fake Scan Webpage Attack	4	7%	1	21%
Malicious JavaScript Redirection	5	5%	8	2%
Fake Browser Update	6	4%	10	2%
Mass Injection Website	7	4%	13	2%
Nuclear Exploit Kit Redirect	8	4%	14	1%
Malicious File Download Request	9	4%	6	4%
Bash CGI Environment Variable CVE-2014-6271 Attack	10	3%	4	6%

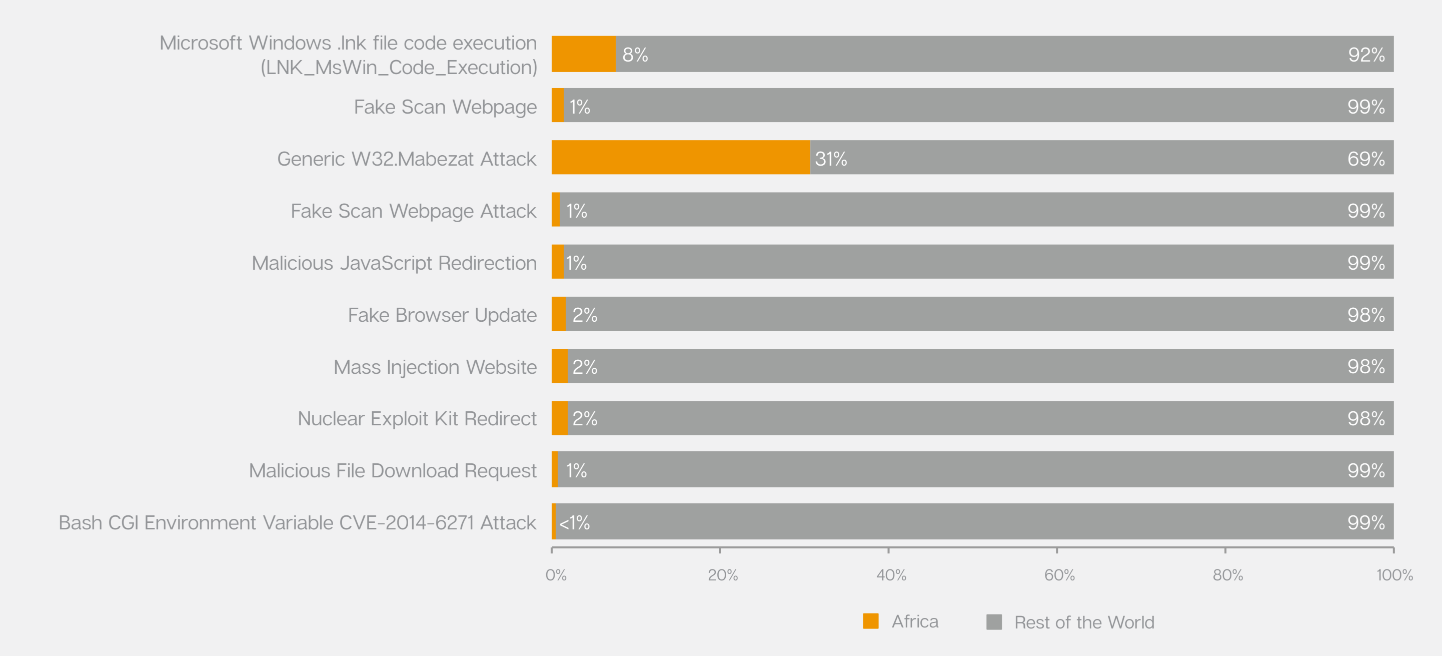
Figure 11. Top 10 Attacks Targeting Africa–2016



Of note during the reporting period, Symantec observed that nearly one in three global Generic W32. Mabezat Attacks targeted Africa (see Figure 12). This event indicates detection of activity from one of the W32.Mabezat families of worms. W32.Mabezat[2] is a worm that spreads through email, removable drives, and network shares that are protected by weak usernames and passwords. It can also infect executable files and encrypts data files, such as PDF, TXT, and Microsoft Office files, on the infected system. The Mabezat worm spreads by using spam emails with malicious attachments.

[2] http://www.symantec.com/security_response/writeup.jsp?docid=2007-120113-2635-99

Figure 12. Percentage of Attacks Targeting Africa with Global Comparison–2016



MALWARE ANALYSIS

Malware is software that attackers use to steal confidential information, destroy data, disrupt computer operations, or gain access to the network from the compromised system. Types of malware include viruses, worms, Trojans, and ransomware, and they spread through the use of a variety of tools such as email, drive-by downloads, and infected files. They can also exploit existing vulnerabilities to infect systems.

Top Malware Originating from Africa

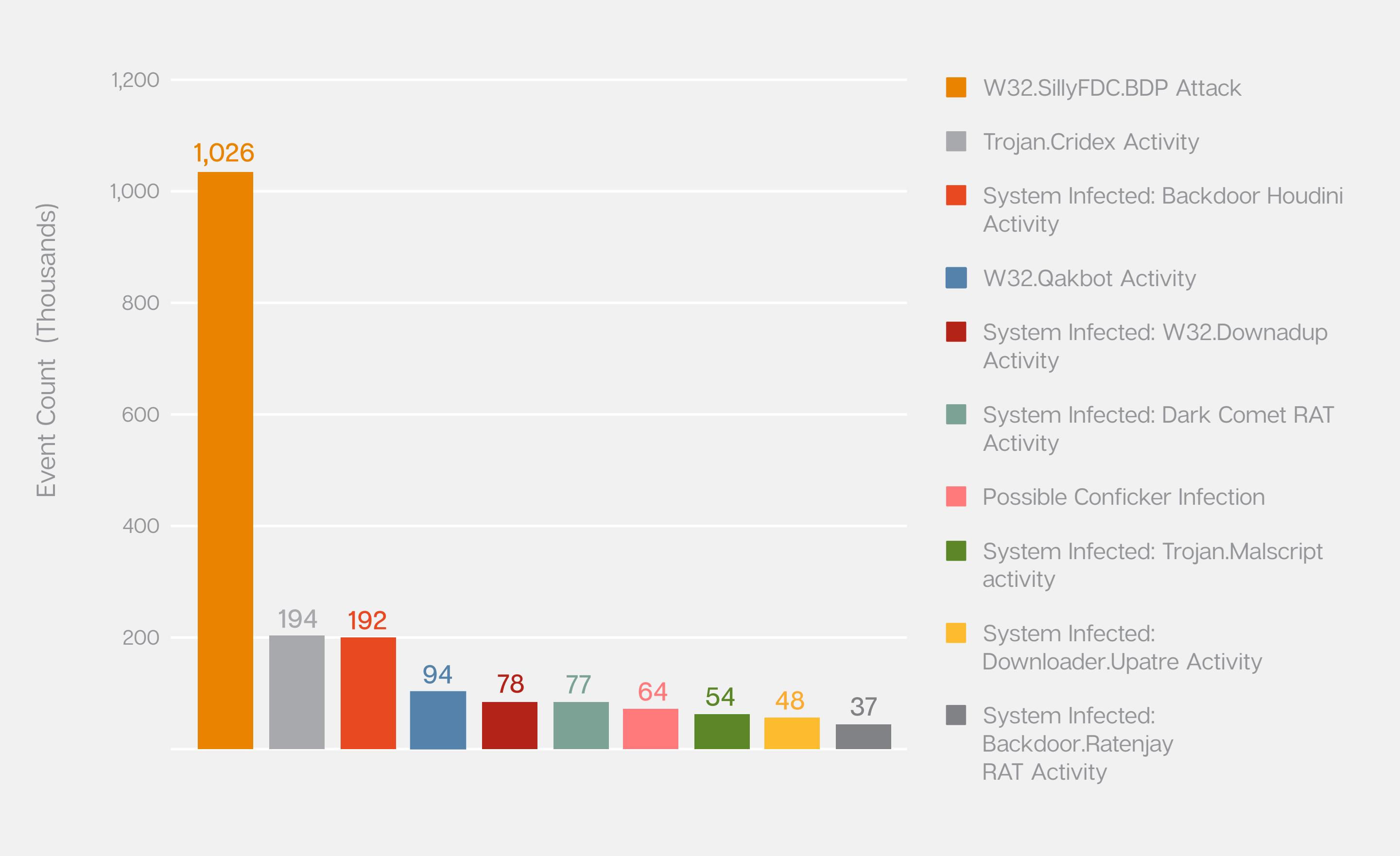
During the reporting period, there were nearly 2.2 million malware incidents over 213 different malware signatures originating from Africa, all accounting for 1.5% of global malware. During the reporting period, the top malware originating from Africa was W32.SillyFDC.BDP Attack with 1,025,563 incidents, accounting for 47% of the total (see Table 10 and Figure 13). W32.SillyFDC.BDP[3] is a worm that spreads through network shares and removable media by exploiting two vulnerabilities in Microsoft Windows[4,5]. The worm downloads other malicious files on the compromised computer to further spread by posing as a DHCP server for the network.

[3] https://www.symantec.com/security_response/writeup.jsp?docid=2011-031106-4835-99
[4] http://www.securityfocus.com/bid/41732
[5] http://www.securityfocus.com/bid/31874

Table 10. Top 10 Malware Originating from Africa–2016

MALWARE	RANK	PERCENTAGE WITHIN AFRICA	GLOBAL RANK	GLOBAL PERCENTAGE
W32.SillyFDC.BDP Attack	1	47%	77	<1%
Trojan.Cridex Activity	2	9%	72	<1%
System Infected: Backdoor Houdini Activity	3	9%	27	1%
W32.Qakbot Activity	4	4%	66	<1%
System Infected: W32.Downadup Activity	5	4%	54	<1%
System Infected: Dark Comet RAT Activity	6	4%	216	<1%
Possible Conficker Infection	7	3%	6	2%
System Infected: Trojan.Malscript activity	8	3%	104	<1%
System Infected: Downloader.Upatre Activity	9	2%	12	1%
System Infected: Backdoor.Ratenjay RAT Activity	10	2%	109	<1%

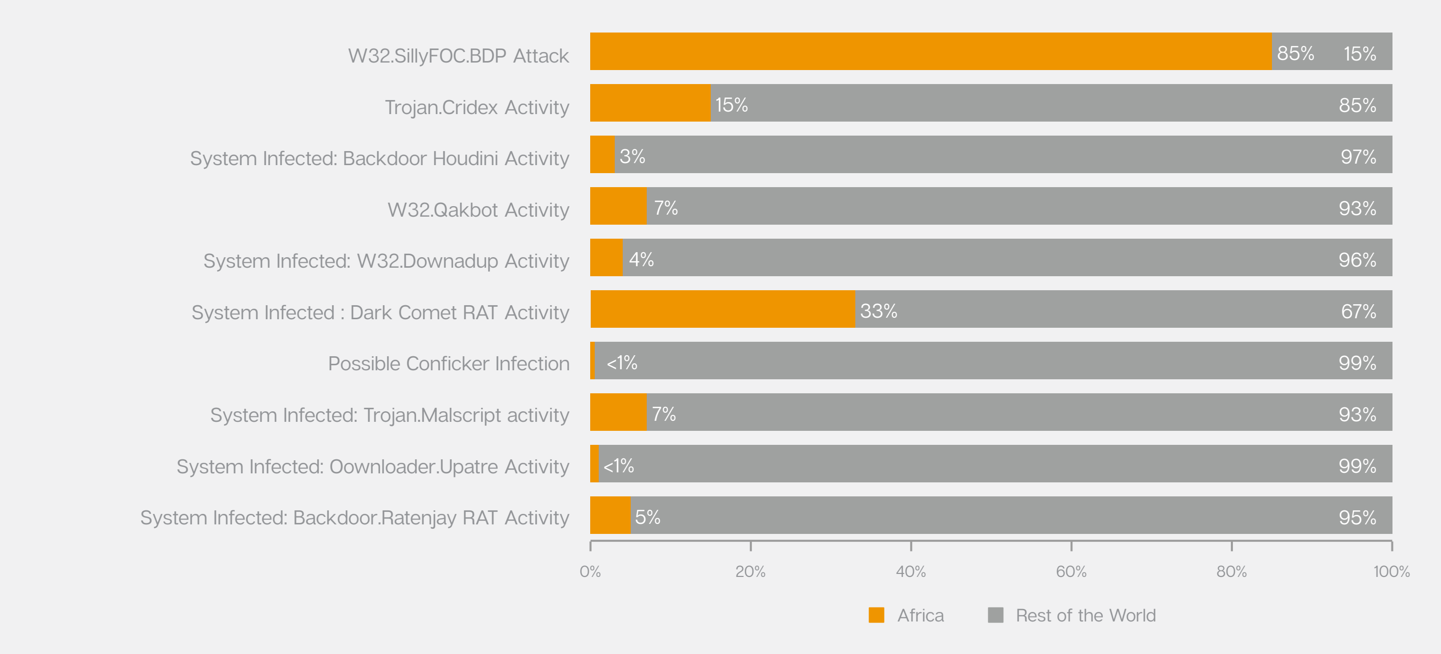
Figure 13. Top 10 Malware Originating from Africa–2016



During the reporting period, Africa was a large source of the W32.SillyFDC.BDP Attack, System Infected: Dark Comet RAT Activity, and Trojan.Cridex Activity (see Figure 14). The following is a summary of the findings:

- Eighty-five percent of the W32.SillyFDC.BDP Attack events were from Africa. As mentioned, W32. SillyFDC.BDP is a worm that spreads through removable media and can download other files onto the compromised computer.[6]
- Africa was the source of 33% of the global System Infected: Dark Comet RAT Activity attack incidents. Dark Comet RAT is a remote access tool that has been tied to a number of global incidents.[7,8]
- Africa was the source of 15% of the global Trojan.Cridex[9] activity. Trojan.Cridex is a widespread banking Trojan that may infect the targeted computer with a bot program.

Figure 14. Percentage of Malware Originating from Africa with Global Comparison—2016



Top Malware Targeting Africa

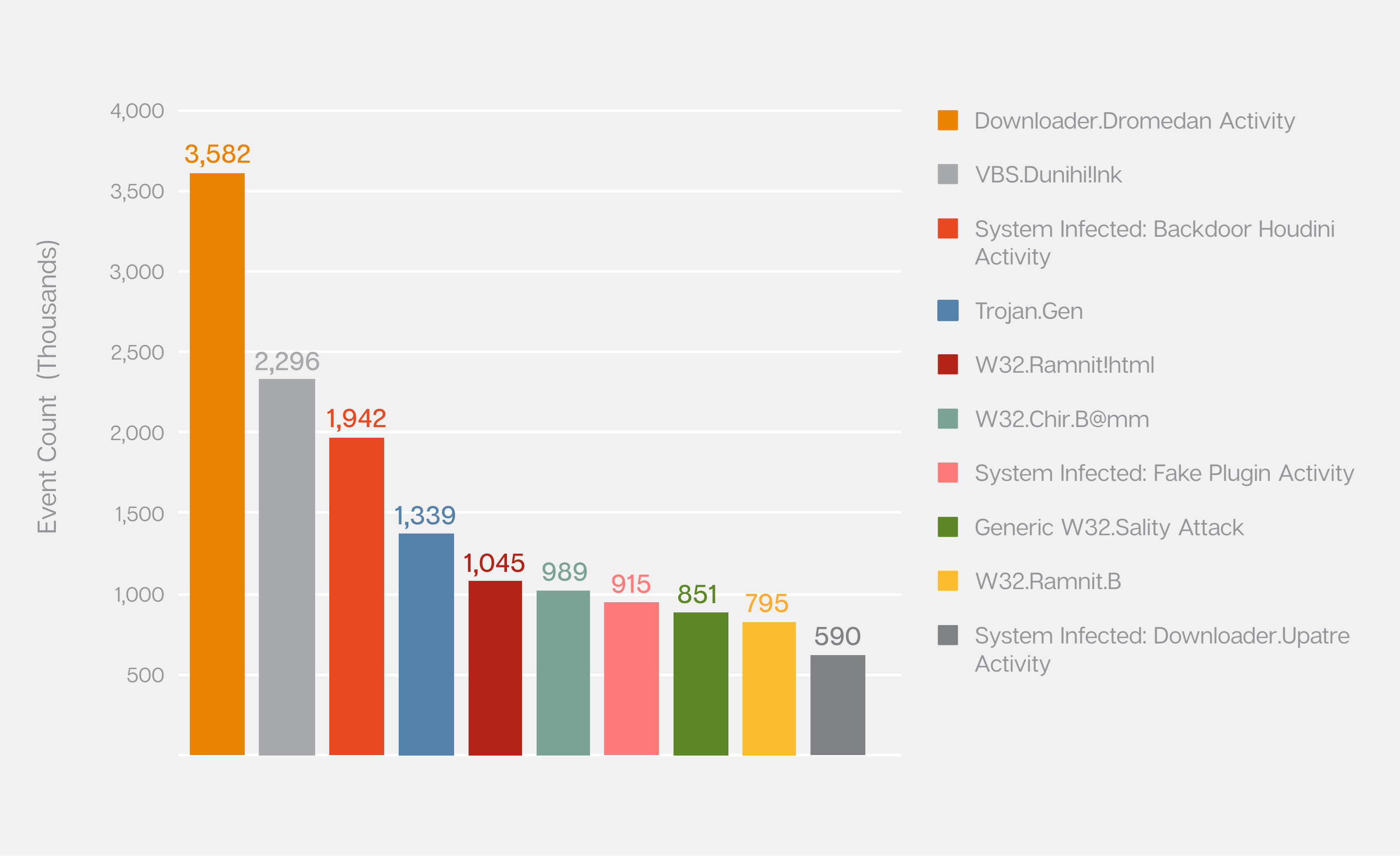
During the reporting period, Symantec observed 24 million malware incidents targeting Africa with 3,490 different malware signatures. This accounted for 2.5% of the global malware total. The top malware targeting Africa was Downloader.Dromedan Activity, accounting for 15% of the targeted total (see Table 11 and Figure 15). Downloader.Dromedan Activity[10], indicates the presence of a malicious Trojan on the affected computer. This Trojan downloads additional files to further compromise the affected computer.

[6] http://www.symantec.com/security_response/writeup.jsp?docid=2011-031106-4835-99
[7] https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=26653
[8] http://www.symantec.com/connect/blogs/darkcomet-rat-it-end
[9] https://www.symantec.com/security_response/writeup.jsp?docid=2015-012314-0117-99
[10] https://www.symantec.com/security_response/writeup.jsp?docid=2011-101915-4058-99

Table 11. Top 10 Malware Targeting Africa–2016

MALWARE	RANK	PERCENTAGE WITHIN AFRICA	GLOBAL RANK	GLOBAL PERCENTAGE
Downloader.Dromedan Activity	1	15%	5	4%
VBS.Dunihi!lnk	2	9%	20	1%
System Infected: Backdoor Houdini Activity	3	8%	27	1%
Trojan.Gen	4	6%	4	5%
W32.Ramnit!html	5	4%	16	1%
W32.Chir.B@mm	6	4%	33	<1%
System Infected: Fake Plugin Activity	7	4%	9	2%
Generic W32.Sality Attack	8	4%	19	1%
W32.Ramnit.B	9	3%	32	<1%
System Infected: Downloader.Upatre Activity	10	2%	12	1%

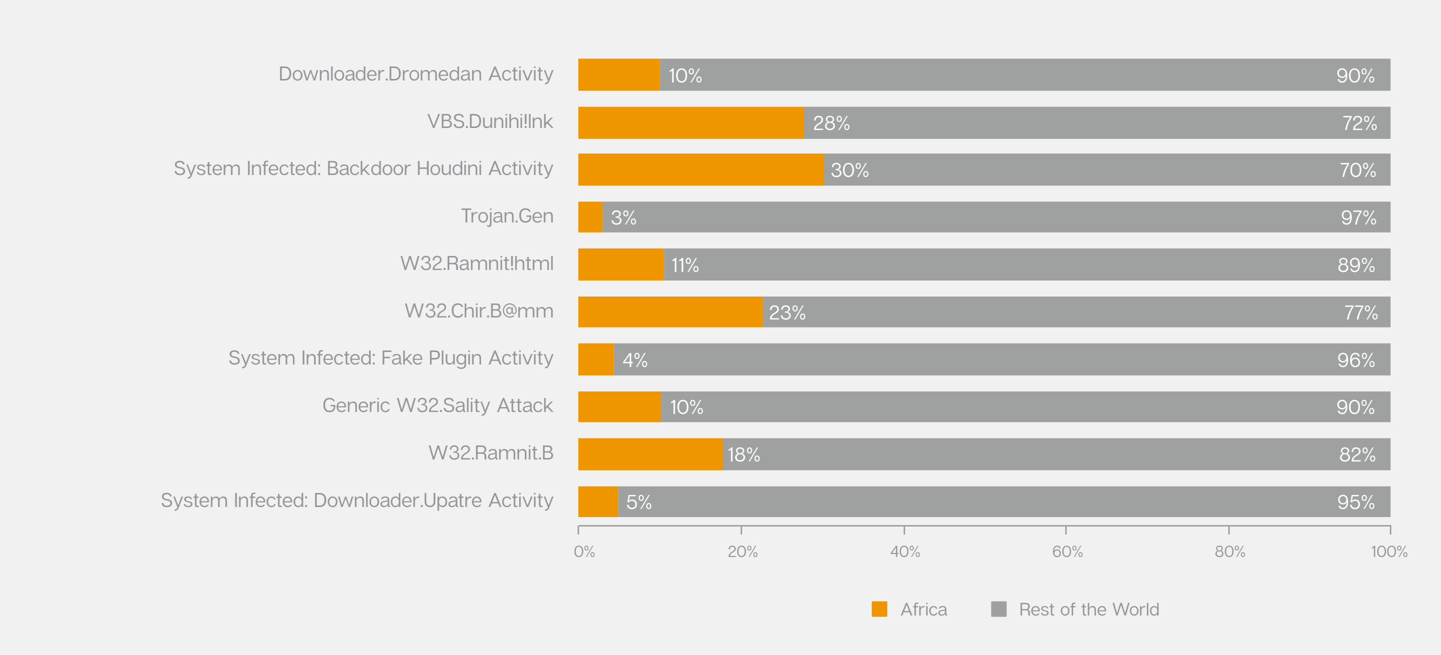
Figure 15. Top 10 Malware Targeting Africa–2016



Symantec observed that Africa was a large target of System Infected: Backdoor Houdini Activity, VBS. Dunihi!lnk, and W32.Chir.B@mm global malware incidents during the reporting period (see Figure 16). The summary details are as follows:

- Thirty percent of global System Infected: Backdoor Houdini Activity events targeted Africa. Backdoor Houdini is a Trojan that opens a backdoor on the compromised computer. The malicious software may then download other programs.
- Africa was the target of 28% of the global VBS.Dunihi!lnk malware incidents. This signature detects .lnk files created by the VBS.Dunihi worm.[11] Microsoft Windows uses the .lnk file extension for shortcuts to local files and executable files. The VBS.Dunihi worm spreads by copying itself onto removable drives. It creates .lnk files to replace all the files in the removable drive and once executed, it copies itself onto a computer.
- Twenty-three percent of the global W32.Chir.B activity targeted Africa during the reporting period. W32.Chir.B W32 is a mass-mailing worm that spreads by sending emails to address book contacts on the compromised computer.[12]

Figure 16. Percentage of Malware Targeting Africa with Global Comparison—2016



[11] http://www.symantec.com/security_response/writeup.jsp?docid=2013-091222-3652-99
[12] https://www.symantec.com/security_response/writeup.jsp?docid=2002-072920-3942-99

BOT ANALYSIS

Bots are programs that are covertly installed on a user's machine to allow an attacker to remotely control the targeted system through a communication channel, such as internet relay chat (IRC), peer-to-peer (P2P), or HTTP. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service (DoS) attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft, all of which can have serious financial and legal consequences.

Top Named Botnet Families for Bots Originating from Africa

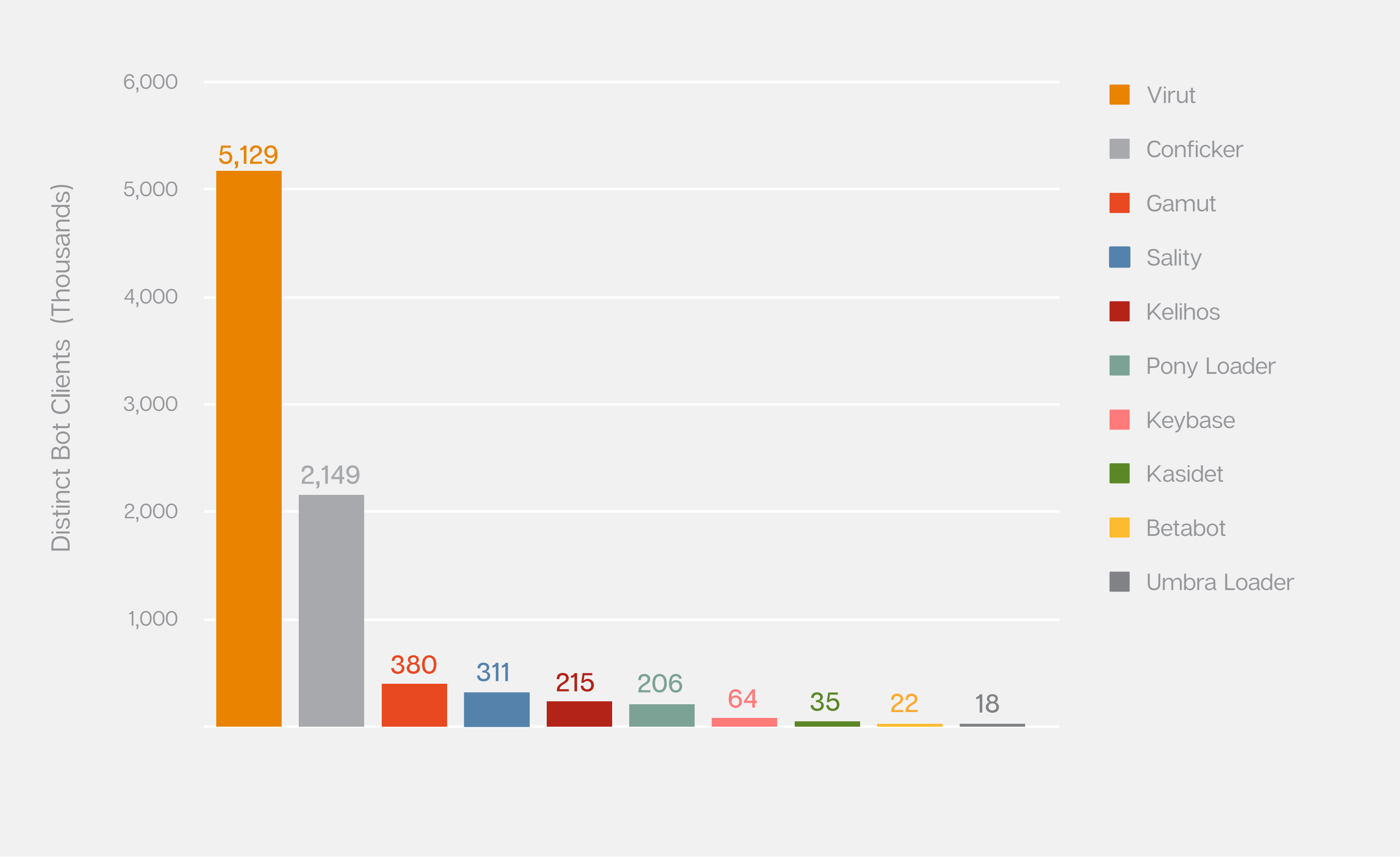
During the reporting period, Symantec observed that Virut was the top named botnet family for bots originating from Africa with 5,128,775 distinct bots. This accounted for 40% of the total distinct named bots from Africa (see Table 12 and Figure 17). Globally, Virut was the second ranked named botnet family for bots with 24.8 million distinct bots.

Virut is a bot that performs various attacks including spreading spam emails, fraud, data theft, and performing DDoS attacks. It was first reported active in 2006.

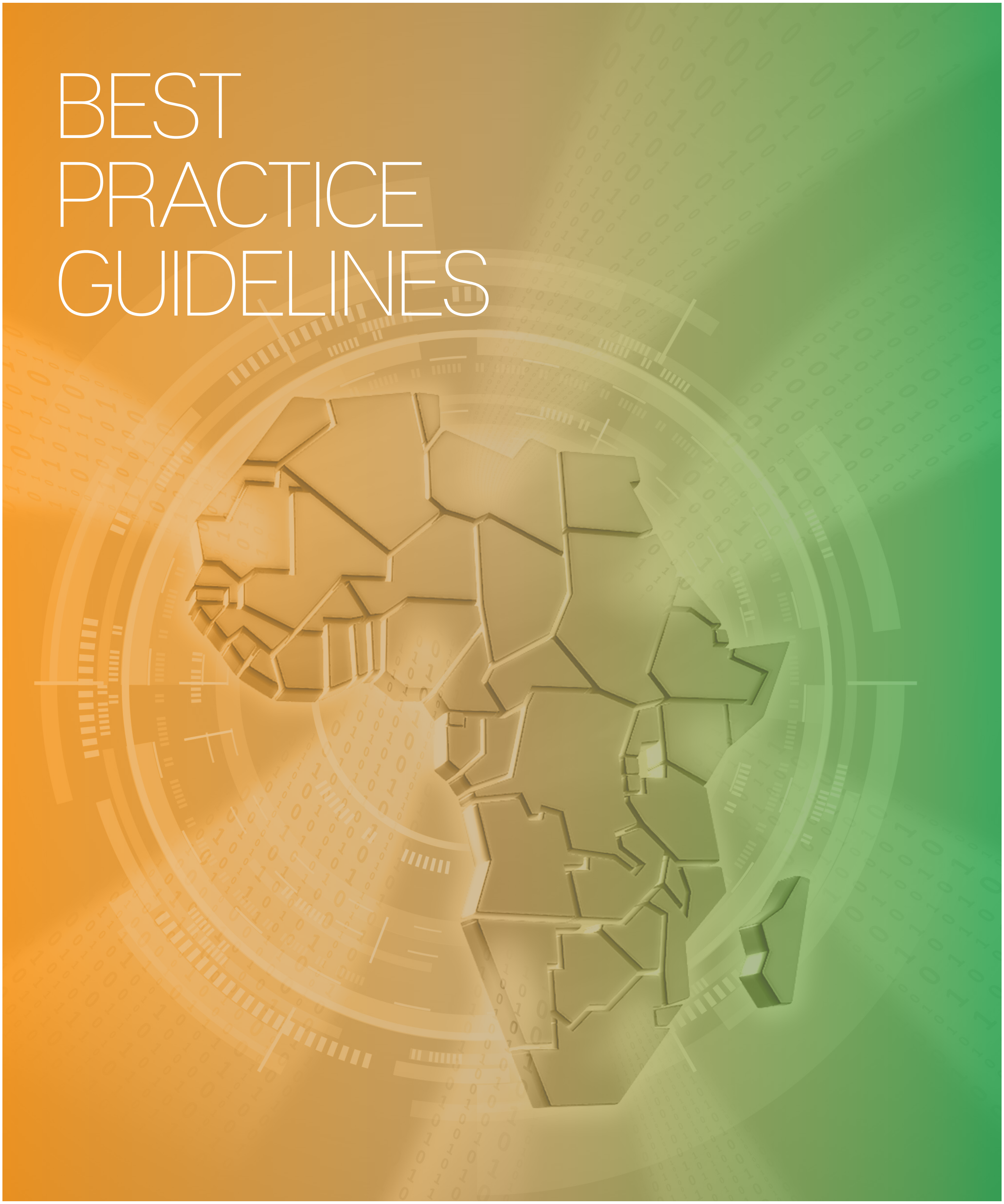
Table 12. Top 10 Named Botnet Families for Bots Originating from Africa—2016

BOTNET FAMILY	RANK	PERCENTAGE WITHIN AFRICA	GLOBAL RANK	GLOBAL PERCENTAGE
Virut	1	40%	2	30%
Conficker	2	17%	1	36%
Gamut	3	3%	4	5%
Sality	4	2%	9	1%
Kelihos	5	2%	5	4%
Pony Loader	6	2%	3	9%
Keybase	7	<1%	7	2%
Kasidet	8	<1%	6	3%
Betabot	9	<1%	23	<1%
Umbra Loader	10	<1%	18	<1%

Figure 17. Top 10 Named Botnet Families for Bots Originating from Africa–2016



BEST PRACTICE GUIDELINES



BEST PRACTICE GUIDELINES FOR BUSINESSES

Employ Defense-in-Depth Strategies

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

Monitor for Network Incursion Attempts, Vulnerabilities, and Brand Abuse

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

Antivirus on Endpoints Is Not Enough

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection, including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints.
- Browser protection for avoiding obfuscated web-based attacks.
- File and web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware.
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware.
- Application control settings that can prevent applications and browser plugins from downloading unauthorized malicious content.
- Device control settings that prevent and limit the types of USB devices to be used.

Secure Websites Against Attacks and Malware Infection

Avoid compromising your trusted relationship with customers by regularly assessing your website for vulnerabilities and malware. Additionally, consider:

- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users.
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

Protect Private Keys

Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures.
- Secure keys in secure, tamper-proof, cryptographic hardware devices.
- Implement physical security to protect your assets from theft.

Use Encryption and DLP to Protect Sensitive Data

Implement and enforce a security policy whereby any sensitive data is encrypted. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution that can help prevent data breaches and minimize their impact.

- Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss.
- Monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.
- DLP should be configured to identify and block suspicious copying or downloading of sensitive data.
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.

BEST PRACTICE GUIDELINES FOR BUSINESSES

Ensure All Devices Allowed on Company Networks Have Adequate Security Protections

If a bring-your-own-device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

Implement a Removable Media Policy

Where practical, restrict unauthorized devices, such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Be Aggressive in Updating and Patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plugins. This also applies to operating systems, not just across computers, but mobile, ICS, and IoT devices as well. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic updates.

Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

Enforce an Effective Password Policy

Ensure passwords are strong. Passwords should be at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

Ensure Regular Backups Are Available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

Restrict Email Attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

Ensure Infection and Incident Response Procedures Are in Place

- Keep your security vendor contact information handy; know who you will call, and what steps you will take if you have one or more infected systems.
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems.
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media.
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

Educate Employees

As ever, basic common sense and the introduction of good security habits can go a long way to keeping sites and servers safe this year.

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless from a trusted source or the download has been scanned for malware.
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends.
- Deploy web browser URL reputation plugin solutions that display the reputation of websites from searches.
- Restrict software to corporate-approved applications, if possible, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites.

BEST PRACTICE GUIDELINES FOR BUSINESSES

- Educate users on safe social media conduct. Offers that look too good usually are, and hot topics are prime bait for scams. Not all links lead to real login pages.
- Encourage them to adopt two-step authentication on any website or app that offers it.
- Ensure they have different passwords for every email account, applications and login—especially for work-related sites and services.
- Remind then to use common sense. Having antivirus and security software doesn't mean it is ok to visit malicious or questionable websites.
- Encourage employees to raise the alarm if they see anything suspicious. For example, if Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (indicative of fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or to use the task manager, and then notify the helpdesk.

Protect Mobile Devices

We recommend that people and employers treat mobile devices like the small, powerful computers that they are and protect them accordingly using:

- Access control, including biometrics where possible.
- Data loss prevention, such as on-device encryption.
- Automated device backup.
- Remote find and wipe.
- Regular updating. For example, the latest version of Android, codenamed 'Honeycomb', includes a number of features designed specifically to thwart attackers.
- Common sense. Don't jailbreak devices and only use trusted app markets.
- Training, particularly around paying attention to permissions requested by an app.
- Security solutions such as Symantec Mobility or Norton Mobile Security

We have seen the number of mobile vulnerabilities increase every year over the past three years—although this is perhaps an indicator of progress rather than a cause for despair. It is an indication that security researchers, operating system developers and app writers are, in fact, paying more attention to mobile security by identifying and fixing more problems.

Although we expect mobile devices to come under growing attack over the next year, there is also hope that with the right preventative measures and continuing investment in security, users can achieve a high level of protection against them.

Building Security into Devices

The diverse nature of ICS and IoT platforms make host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), with customizable rulesets and policies that are unique to a platform and application, suitable solutions.

However, manufacturers of ICS and IoT devices are largely responsible for ensuring that security is built into the devices before shipping.

Building security directly into the software and applications that run on the ICS and IoT devices should prevent many attacks that manage to side-step defenses at the upper layers. Manufacturers should adopt and integrate such principles into their software development processes.

Business users and consumers need to be assured that suppliers are fundamentally building security into the IoT devices that they are buying, rather than it being considered as a bolt-on option.

It's a Team Effort

Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. But it only takes one bad experience of stolen data or a drive-by download to tarnish the reputation of every website in the consumer's mind.

As we said at the start of the report, there is a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks websites potentially pose to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt Complete Website Security in 2016, and together with Symantec, make it a good year for cyber security and a very bad one for cyber criminals. ■

BEST PRACTICE GUIDELINES FOR WEBSITE OWNERS

For website security to be effective, it has to be implemented with care and attention and it has to be monitored and maintained continually.

While there are tools to help you keep your website ecosystem secure, it all starts with education. You've read about the risks—now find out what you can do about them.

Get in line with industry standards

- **Implement always-on SSL.** Implement SSL/TLS on every page of your website so that every interaction a visitor has with your site is encrypted. Switching to 'HTTPS everywhere', as it's also called, with OV or EV SSL/TLS certificates demonstrates your credibility and can also improve your search rankings and paves the way for an upgrade to HTTP/2, delivering better performance.
- **Migrate to SHA-2.** As discussed in the report, certificate authorities should have stopped issuing SHA-1 certificates as of 1 January 2016, but you need to ensure any legacy certificates are also upgraded and that any devices and applications that may not currently recognize SHA-2 are upgraded too.
- **Consider adopting ECC.** Symantec also offers the use of the ECC encryption algorithm. All major browsers, even mobile, support ECC certificates on all the latest platforms, and compared to an industry-standard 2048-bit RSA key, 256-bit ECC keys are 64,000 times harder to crack.

Use SSL/TLS Correctly

SSL/TLS is only as good as its implementation and maintenance. So be sure to:

- **Keep protocol libraries up to date.** SSL/TLS implementation is an on-going task and it's vital that any patches or updates to the software you use are implemented as soon as possible.
- **Don't let your certificates expire.** Keep track of what certificates you have, from which certificate authority, and when they are due to expire. Symantec offers a range of automation tools to help you do this, giving you more time for proactive security tasks.
- **Display recognized trust marks.** Display trust marks (such as the Norton Secured Seal) in highly visible locations on your website to show customers your commitment to their security.

Manage your SSL/TLS keys properly. Limit the number of people with access to them; have separate administrators for managing the passwords for the server where they're kept and for managing the systems they're actually stored in; and use automated certificate and key management systems to reduce human involvement.

Any breach affecting SSL keys should be notified to the CA quickly, so that corresponding certificates can be revoked.

Adopt Comprehensive Website Security

- **Scan regularly.** Keep an eye on your web servers and watch for vulnerabilities or malware. Automation tools can help with this.
- **Use antivirus.** Antivirus software isn't just for PCs and smartphones—it's for servers too and could help prevent a serious malware attack against your entire website infrastructure.
- **Be picky about your plugins.** The software you use to manage your website comes with vulnerabilities too. The more third-party software you use, the greater your attack surface; so only deploy what's absolutely necessary.
- **Consider the whole ecosystem.** Have you deployed a Web Application Firewall to defend against injection attacks? Is your code signing secure for your web apps? Do you have automated tools to detect and defend against the increasingly common problem of DDoS attacks?

Symantec offers a range of tools that makes maintaining complete website security a straightforward and efficient task.

Avoid Compromising Trusted Relationships with Customers by:

- Regularly assessing your website for any vulnerabilities.
- Scanning your website daily for malware.
- Setting the secure flag for all session cookies.
- Securing your websites against man-in-the-middle (MITM) attacks and malware infection.
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users.
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

There Is No 'I' in Team

Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. It only takes one bad experience to tarnish the reputation of every single one in the consumer's mind.

As we said in the report, there exists a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks your website potentially poses to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt comprehensive website security in 2016 and, together with Symantec, make it a good year for cyber security and a very bad one for cyber criminals.

BEST PRACTICE GUIDELINES FOR CONSUMERS

Protect Yourself

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file- and heuristic-based) and behavioral malware prevention can prevent unknown malicious threats from executing.
- Bi-directional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer.
- Browser protection will protect against obfuscated web-based attacks.
- Use reputation-based tools that check the reputation and trust of a file and website before downloading, and that check URL reputations and provide safety ratings for websites found through search engines.
- Consider options for implementing cross-platform parental controls, such as Norton Online Family.

Update Regularly

Keep your system, program, and virus definitions up-to-date; always accept updates requested by the vendor.

Running out-of-date versions can put you at risk from being exploited by web-based attacks. Only download updates from vendor sites directly. Select automatic updates wherever possible.

Be Wary of Scareware Tactics

Versions of software that claim to be free, cracked, or pirated can expose you to malware or social engineering attacks that attempt to trick you into thinking your computer is infected and getting you to pay money to have it removed.

Use an Effective Password Policy

Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or websites.

Use complex passwords (upper/lowercase and punctuation). Passphrases and password management apps can help too.

Think Before You Click

Never view, open, or copy email attachments to your desktop or execute any email attachment unless you expect it and trust the sender. Even when receiving email attachments from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails or social media communications, even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using a preview tool or plugin.
- Use a web browser plugin or URL reputation site that shows the reputation and safety rating of websites before visiting.
- Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop up asking you to install media players, document viewers, and security updates. Only download software directly from the vendor's website.
- Be aware of files you make available for sharing on public sites, including gaming, BitTorrent, and any other peer-to-peer (P2P) exchanges. Keep Dropbox, Evernote, and other usages to a minimum for pertinent information only, and only use when approved for corporate use.

Safeguard Your Personal Data

Limit the amount of personal information you make publicly available on the Internet (in particular via social networks). This includes personal and financial information, such as bank logins or birth dates. Additionally:

- Regularly review your bank, credit card, and credit information frequently for irregular activity.
- Avoid banking or shopping online from public computers (such as libraries, Internet cafes, and similar establishments) or from unencrypted.

Wi-Fi Connections

When using public wireless hotspots consider the following:

- Use HTTPS when connecting via Wi-Fi networks to your email, social media, and sharing websites. Check the settings and preferences of the applications and websites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

COUNCIL OF EUROPE OVERVIEW OF CYBER CRIME LEGISLATION IN AFRICA

THE STATE OF CYBER CRIME LEGISLATION IN AFRICA – AN OVERVIEW

Council of Europe/Project Cybercrime@Octopus[1]

1. Introduction: Why Should Countries of Africa Adopt Legislation on Cyber Crime and Electronic Evidence?

Cyber crime is not only a question of attacks against the confidentiality, integrity and availability of computer data and systems but against the core values and the human development potential of societies increasingly relying on information technology.

In the light of this, governments cannot remain passive; they have the obligation to protect society and individuals against crime.

In practice, however, governments face serious challenges:

- while millions of attacks against computers and data are recorded each day worldwide, only a small fraction of cyber crime[2] – that is, offences against and by means of computers – is actually prosecuted and adjudicated;
- moreover, evidence in relation to any crime is increasingly available in electronic form on computer systems or storage devices and needs to be secured for criminal proceedings.[3] Criminal investigations not relying on electronic evidence seem to become the exception.

An effective criminal justice response is needed. This involves the investigation, prosecution and adjudication of offences against and by means of computer systems and data as well as the securing of electronic evidence in relation to any crime. It also requires efficient international cooperation given the transnational nature of cyber crime and in particular of volatile electronic evidence.

2. A Legal Framework on Cyber Crime and Electronic Evidence: What Is Required?

Governments are not only obliged to take effective measures for the prevention and control of cyber crime and other offences involving electronic evidence, but they must also respect human rights and rule of law requirements when doing so. Criminal law is a means to achieve this.

Comprehensive legislation covering both substantive law (conduct to be defined as a criminal offence) and procedural law (investigative powers for law enforcement) is the foundation of a criminal justice response.

Legislation on cyber crime and electronic evidence needs to meet a number of requirements:

- It must be sufficiently (technology) neutral to cater for the constant evolution of technology and crime as it otherwise risks becoming obsolete already by the time it enters into force.
- Law enforcement powers must be subject to safeguards to ensure that rule of law and human rights requirements are met.
- It must be sufficiently harmonised or at least compatible with the laws of other countries to permit international cooperation, for example, to meet the dual criminality condition.

African States preparing legislation on cyber crime may draw on a number of documents to seek guidance. These include in particular the African Union Convention on Cyber Security and Personal Data Protection

[1] The views expressed in this technical report do not necessarily reflect the official position of the Council of Europe or of the Parties to the Budapest Convention on Cyber Crime. Contact: alexander.seger@coe.int

[2] Defined here as offences against and by means of computer data and systems in the sense of Articles 2 to 11 of the Budapest Convention on Cyber crime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[3] For example, the recent disputes over the encryption of iPhones were not related to cyber crime but to cases of terrorism and drug trafficking. http://recode.net/2016/04/08/apple-fbi-encryption-battle-shifts-to-new-york/

adopted in Malabo in June 2014.[4] That treaty reflects a strong commitment by Member States of the African Union to establish a secure and trusted foundation for the information society. It covers a broad range of measures ranging from electronic transactions, to the protection of personal data, cyber security and also cyber crime.

Given that this treaty is rather new and is yet to be tested in practice, and given its broad scope, the present report uses the Budapest Convention on Cyber Crime[5] as reference. This Convention is more specifically focusing on cyber crime and electronic evidence, including international cooperation, and is increasingly being used in Africa.

The Convention on Cyber Crime was opened for signature in Budapest, Hungary, in 2001. Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA it is open for accession by any State prepared to implement it and to engage in international cooperation. By April 2016 it had 49 Parties and a further 17 States that had been invited to accede or have signed it.

The Budapest Convention is backed up by the Cyber Crime Convention Committee representing the Parties to this treaty and capacity building programmes.[6]

It would seem that the African Union Convention on Cyber Security and Personal Data Protection and the Budapest Convention on Cyber Crime complement each other.

Concepts and Definitions

In terms of concepts and definitions, States should define "computer system" in a broad sense to encompass also devices such as smart phones, tablets or others while remaining technology neutral. Article 1.a of the Budapest Convention offers an example.[7] Similarly, for criminal law purposes, "service providers" should comprise all types of service providers as proposed in Article 1.c Budapest Convention. While a general definition of "computer data" will be required (see Article 1.b), a specific definition of "traffic data" should be foreseen (see Article 1.d).

In criminal investigations, the data most often needed is "subscriber information". This type of information is less privacy-sensitive than traffic or content data. It will, therefore, be useful to define "subscriber information" separately so that a lighter regime for access to and sharing of subscriber information can be established while traffic and in particular content data require stricter safeguards. Article 18.3 Budapest Convention offers a definition of "subscriber information".

Substantive Criminal Law: Conduct to Be Defined as a Criminal Offence

In terms of substantive law States should criminalise illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography and offences related to infringements of copyright and related rights.

Substantive criminal law under the Budapest Convention on Cyber Crime	
Article 2	Illegal access to a computer system
Article 3	Illegal interception of non-public transmissions to, from or within a computer system
Article 4	Data interference
Article 5	System interference
Article 6	Misuse of devices

[4] https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf
[5] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG
[6] In 2014, a dedicated Cyber Crime Programme Office of the Council of Europe became operational in Bucharest, Romania, and is responsible for capacity building programmes on cyber crime and electronic evidence worldwide.
[7] See also the Guidance Note on the notion of "computer system" http://www.coe.int/en/web/cybercrime/guidance-notes

Article 7	Computer-related forgery
Article 8	Computer-related fraud
Article 9	Offences related to child pornography
Article 10	Offences related to infringement of copyright and related rights
Article 11	Attempt, aiding or abetting
Article 12	Corporate liability

It is noteworthy that these provisions alone or in combination still cover most of what constitutes cyber crime even now, fifteen years after adoption of the Convention, because they have been formulated in a technology-neutral manner. Guidance Notes adopted by the Cyber Crime Convention Committee show how different provisions can be applied to address botnets, distributed denial of service attacks and other phenomena.[8]

Of course, an international agreement always represents a minimum common denominator, and a State is free to decide to go beyond. However, many States, including in Africa, often face opposition when attempting to criminalise additional types of conduct. This is particularly true for often vaguely defined provisions that criminalise contents, speech or anything "contrary to morality".

Procedural Law: Law Enforcement Powers to Secure Electronic Evidence

The Budapest Convention comprises a range of specific procedural law powers such as orders for the search, seizure and production of data or the interception of communications as well as the power to order the expedited preservation of data.

The procedural powers are:

Procedural powers in the Budapest Convention on Cyber Crime	
Article 16	Expedited preservation of any type of data
Article 17	Expedited preservation and partial disclosure of traffic data
Article 18	Production orders
Article 19	Search and seizure of stored computer data
Article 20	Real-time collection of traffic data
Article 21	Interception of content data

Importantly, these apply to:

- Specific criminal investigations where specified data is needed. They don't apply to national security measures or the bulk collection of data;
- Electronic evidence in relation to any type of crime and not only in relation to offences against and by means of computers.

[8] http://www.coe.int/en/web/cybercrime/guidance-notes

Rule of Law Safeguards

Law enforcement powers – such as the search of computer systems, the interception of communications and others – interfere with the right to private life and other fundamental rights of individuals. Such an interference is only allowed if certain rule of law conditions are met. In particular, these powers must be prescribed by law, pursue legitimate aims, be necessary and proportionate, allow for effective remedies and be subject to guarantees against abuse.

In the Budapest Convention, these safeguards are reflected in Article 15:

Article 15 – Conditions and Safeguards

- Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
- Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
- To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

International Cooperation

Finally, this treaty is to ensure effective international cooperation on cyber crime and electronic evidence by combining "traditional" mutual legal assistance with expedited means to preserve data in another country, the later with the support of a network of 24/7 points of contact. Again, cooperation is not limited to cyber crime but is extended to cooperation on electronic evidence found on a computer system in relation to any crime.

In 2014, the Cyber Crime Convention Committee established a Cloud Evidence Working Group to propose solutions allowing for effective access data stored on servers "somewhere in the cloud", that is, in foreign, multiple, unknown or changing jurisdictions. Options under consideration include an additional Protocol to the Budapest Convention.

The Budapest Convention as a Guideline

The Budapest Convention may thus serve as a checklist for the development of domestic substantive and procedural law on cyber crime and electronic evidence. It seems that more than 130 States around the world have used it as a guideline in one way or the other. However, the Convention as a whole is a mature, balanced and coherent document and is best considered as a whole.[9]

For States becoming Parties, the treaty serves as a legal framework for international cooperation. The Budapest is open for accession to any State prepared to implement its provisions.[10] And indeed, an increasing number of States in Africa are deciding to follow this path.

[9] The Budapest Convention is supplemented by an Additional Protocol on Xenophobia and Racism committed via computer systems (ETS 189). http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 Furthermore, the Cyber Crime Convention Committee – representing the Committee of the Parties – is adopting Guidance Notes to facilitate the use of the Budapest Convention for addressing new phenomena. http://www.coe.int/en/web/cybercrime/guidance-notes

[10] States that participated in the negotiation of the Convention (member States of the Council of Europe, Canada, Japan, South Africa and the USA) may sign and ratify it. Any other State may become a Party through accession. The result is the same.

3. The Situation In Africa

The Current State of Cyber Crime Legislation

A cursory overview of the 54 countries of Africa in terms of specific criminal law provisions on cyber crime and electronic evidence suggests that by April 2016:

- 11 States seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) although implementing regulations may still be missing in one or the other country.[11]
- A further 12 States seemed to have substantive and procedural law provisions partially in place (Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe).
- The majority of African States (30) did not have specific legal provisions on cyber crime and electronic evidence in force.
- Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe).[12] In some instances, bills had been presented to national parliaments, in others the fate of draft laws is uncertain.

Country	Indicative status of specific criminal law provisions on cyber crime and electronic evidence (as of April 2016, based on information available)	
Algeria	Partial	• Partial legislation in force • Criminal Code of 2004 for substantive law • Law n° 09- 04 on specific rules on the prevention and the fight against offences related to information and communication technologies of 2010.
Angola	No	• No specific legislation in force • Amendments to criminal code including substantive criminal law provisions under discussion for several years
Benin	Partial	• Substantive criminal provisions on cyber crime in Law 2011-20 on corruption and related offences (12 October 2011) • No specific procedural law provisions
Botswana	Yes	• Cyber Crime and Computer-related Crimes Act 2007 • Electronic (Evidence) Records Act 2014 for admissibility of electronic evidence
Burkina Faso	No	• No specific legislation in force • Draft law on cyber crime (substantive law)
Burundi	No	• Partial substantive law provisions in Penal Code 2009
Cabo Verde	No	• No specific legislation in force • Draft law on cyber crime following Budapest Convention (2016)
Cameroon	Yes	• Law 2010/012 (21 December 2010) relating to Cyber security and Cyber criminality
Central African Republic	No	• No specific legislation in force

[11] In addition, Chad reportedly adopted a law on cyber crime in July 2014 but the text was not accessible when the present report was finalised.

[12] Reform efforts may also be underway in additional States but may have been ignored for lack of accessible information.

Country	Indicative status of specific criminal law provisions on cyber crime and electronic evidence (as of April 2016, based on information available)	
Chad	TBC Text of the Law Not Available	• Loi relatifs à la cyber sécurité et la lutte contre la cybercriminalité (July 2014)
Comoros	No	• No specific legislation in force
Congo, Democratic Republic of the	No	• No specific legislation in force
Congo, Republic of the	No	• No specific legislation in force
Côte d'Ivoire	Yes	• Law 2013-451 (19 June 2013)
Djibouti	No	• No specific legislation in force • Draft law on cyber crime
Egypt	No	• No specific legislation in force
Equatorial Guinea	No	• No specific legislation in force
Eritrea	No	• No specific legislation in force
Ethiopia	No	• No specific legislation in force • Draft law submitted to Parliament in April 2016
Gabon	No	• No specific legislation in force
Gambia	Partial	• Information and Communications Act 2009 with substantive criminal law provisions
Ghana	Yes	• Electronic Transactions Act, 2008 (ETA) for substantive and procedural law • Mutual Legal Assistance Act, 2010 (MLAA) with specific provisions on international cooperation on cyber crime and electronic evidence • Accession to Budapest Convention underway
Guinea	No	• No specific legislation in force • Draft law (projet de loi relative à la cybercriminalité) adopted by the Government in April 2016
Guinea-Bissau	No	• No specific legislation in force
Kenya	Partial	• Legislation partially in force (Kenya Information and Communication Act 2009) • Draft law on cyber crime in preparation (April 2016)
Lesotho	No	• No specific legislation in force • Bill on computer crime and cyber crime 2013
Liberia	No	• No specific legislation in force
Libya	No	• No specific legislation in force
Madagascar	Partial	• Loi 2014-006 sur la lutte contre la cybercriminalité (19 juin 2014)
Malawi	No	• No specific legislation in force
Mali	No	• No specific legislation in force • Draft law on cyber crime available
Mauritania	Yes	• Loi 2016-007 relative à la cybercriminalité (20 January 2016) • Note: Implementing regulations pending
Mauritius	Yes	• Computer Misuse and Cyber Crimes Act 2003

Country	Indicative status of specific criminal law provisions on cyber crime and electronic evidence (as of April 2016, based on information available)	
Morocco	Partial	• Partial legislation in force • Amendments to criminal and criminal procedure codes underway with specific provisions on cyber crime and electronic evidence
Mozambique	Partial	• Partial substantive law provisions in amended Penal Code of 2015
Namibia	No	• No specific legislation in force • Draft law with substantive provisions (Electronic Transactions and Cyber Crime Bill 2013)
Niger	No	• No specific legislation in force • Draft law following Budapest Convention
Nigeria	Yes	• Cyber Crimes (Prohibition, Prevention, etc.) Act 2015 • Evidence Act as amended in 2011 for admissibility of electronic evidence
Rwanda	Partial	• Partial substantive law provisions in Penal Code (section 5)
Sao Tome and Principe	No	• No specific legislation in force (amendments to the Penal Code (Law 6/2012) cover illegal interception, computer-related fraud and child pornography)
Senegal	Yes	• Law 2008-11 (25 January 2008) following Budapest Convention • Accession to Budapest Convention underway
Seychelles	No	• No specific legislation in force
Sierra Leone	No	• No specific legislation in force
Somalia	No	• No specific legislation in force
South Africa	Partial	• Partial legislation in force • Draft law (Cyber Crimes and Cyber Security Bill) in National Assembly following public consultations in December 2015. Following Budapest Convention
South Sudan	No	• No specific legislation in force
Sudan	Partial	• Cyber Crime Act 2007
Swaziland	No	• No specific legislation in force • Draft Computer Crime and Cyber Crime Bill
Tanzania	Yes	• Cyber Crimes Act 2015 (20 February 2015)
Togo	No	• No specific legislation in force • Draft law on cyber crime
Tunisia	Partial	• Few provisions in Penal Code. • Draft law on cyber crime and accession to Budapest Convention under consideration
Uganda	Yes	• Computer Misuse Act 2011 (14 February 2011)
Zambia	Yes	• Computer Misuse and Crimes Act 2004 • Electronic Communication and Transactions Act (ECT Act) no 21 (31 August 2009)
Zimbabwe	Partial	• Chapter VIII Criminal Law (Codification and Reform) Act 2004 with substantive law provisions • Computer Crime and Cyber Crime Bill in preparation

Observations

- As only about 20% of States have the basic legal framework in place, the situation in Africa regarding legislation on cyber crime and electronic evidence is not satisfactory. On the positive side, it is encouraging that reforms are under underway in many States, even though in some cases, draft laws have been under discussion for several years with little progress.
- A number of (draft) laws contain provisions that create risks to the freedom of expression and other fundamental rights, in particular where offences are vaguely defined and conditions and safeguards are weak or missing. Examples are the criminalisation of the "creation of sites with a view to disseminating ideas and programmes contrary to public order or morality", "broadcasting information to mislead security forces", "publication of false information" and similar. This not only affects the rights of individuals and restricts media freedoms but also undermines trust and hinders international and public/private cooperation.[13]
- Procedural law powers are not always precisely defined and safeguards may be lacking. For example, a law allows for orders to compel the production of content data without court order, or a police officer can carry out searches or seizures of computers without court order. This may be contrary to rule of law requirements, namely, that investigative powers that interfere with the rights of individuals must be prescribed precisely, be subject to guarantees against abuse, be necessary and proportionate and must allow for effective remedies.
- On the other hand, data protection regulations are increasingly being adopted in African States, often in conjunction with laws on cyber crime. This creates additional safeguards to the rights of individuals. Mauritius, Morocco and Senegal are not only Parties or have been invited to accede to the Budapest Convention on Cyber Crime, but have also requested accession to the Data Protection Convention 108 of the Council of Europe.[14] The African Union Convention on Cyber Security and Personal Data Protection of 2014 also contains an important chapter on the protection of personal data.
- Joining an international treaty such as the Budapest Convention on Cyber Crime not only provides a legal framework for international cooperation but instills confidence and trust that such cooperation has a solid foundation in domestic law. This also applies to cooperation between criminal justice authorities and private sector service providers. Mauritius was one of the first countries of Africa to adopt comprehensive legislation on cyber crime in 2003, and in 2014 was the first African State to become a Party to the Budapest Convention on Cyber Crime. South Africa signed this treaty in 2001 and the additional Protocol on Xenophobia and Racism in 2008 but has not yet ratified these instruments. Morocco and Senegal have been invited to accede and it is expected that both will become Parties in the course of 2016. These countries participate in the Cyber Crime Convention Committee[15] and are priority countries for capacity building. Several other African countries have expressed their political commitment to join and implement this Convention.
- Limited capacities of law enforcement, prosecutors and the judiciary is the main impediment to an effective criminal justice response to cyber crime and other offences involving electronic evidence not only in Africa but in most countries around the world.[16] The adoption of legislation by African States needs to be accompanied by capacity building programmes. The Council of Europe – often jointly with the European Union – is providing support to those African countries that have requested accession to the Budapest Convention, including in the training of criminal justice authorities.[17]

[13] For analysis of the state of the protection of freedom of expression on the Internet in European countries see page 47 ff of http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680646af8

[14] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[15] http://www.coe.int/en/web/cybercrime/tcy

[16] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6

[17] See the GLACY and GLACY+ projects on Global Action on Cyber Crime. http://www.coe.int/en/web/cybercrime/capacity-building-programmes

4. Conclusions

The current state of legislation on cyber crime and electronic evidence in Africa is not satisfactory. By April 2016, only 20% of countries seemed to have the minimum legislation in place.

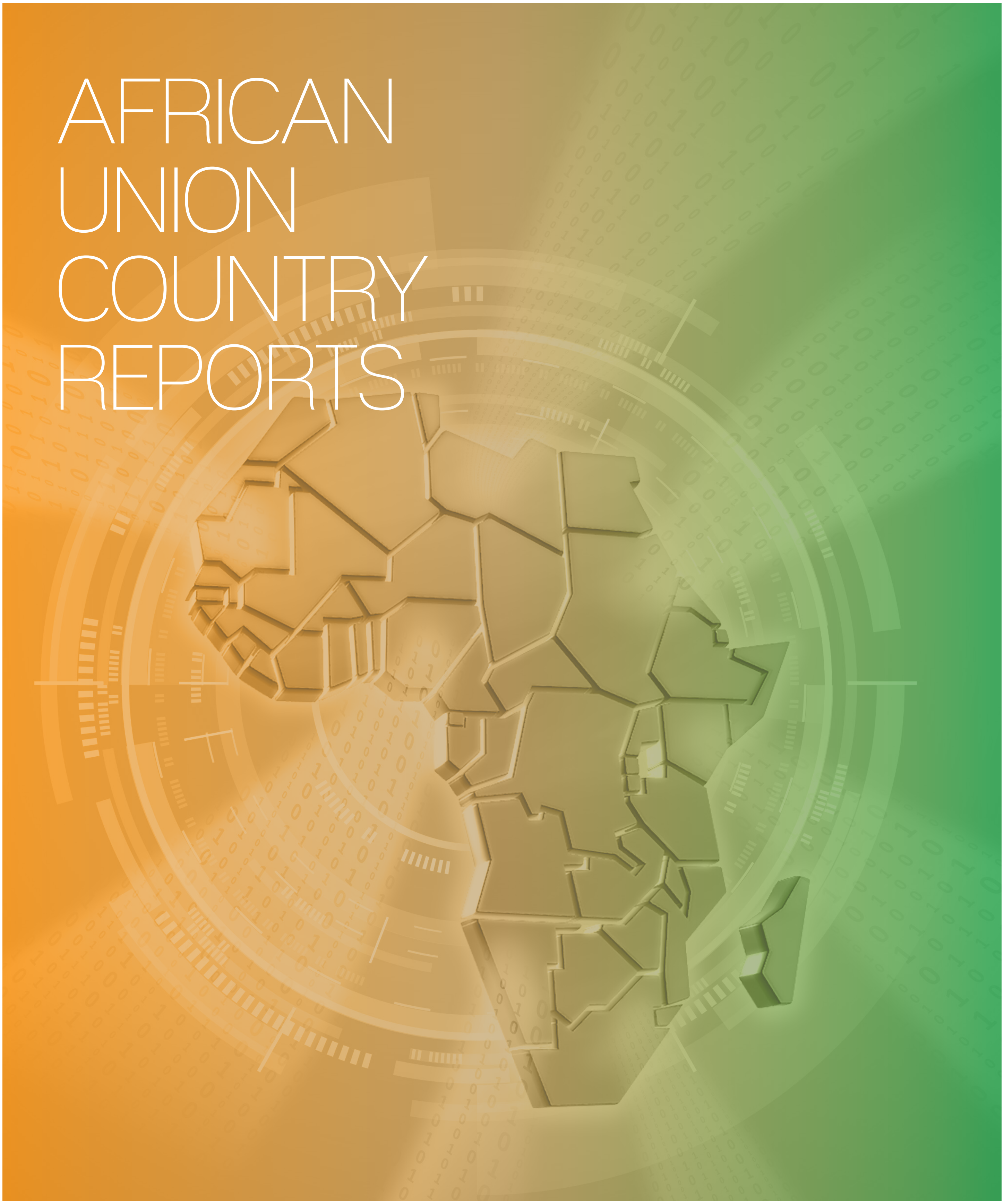
On the positive side, some African countries represent examples of good practice, the African Union Convention on Cyber Security and Personal Data Protection of 2014 should help create a political momentum for stronger legislation and the Budapest Convention on Cyber Crime may serve as a guideline for comprehensive legislation that reconciles the need for an effective criminal justice response with the need to meet human rights and rule of law requirements. Accession to this treaty will facilitate cooperation between African countries and criminal justice authorities of countries in other regions of the world.

Efforts currently underway in a number of African countries to reform domestic legislation should be supported and carried through. Over-criminalisation – in particular with regard to content and speech – should be avoided, and conditions and safeguards limiting law enforcement powers should be established. The enactment of data protection legislation should be encouraged.

The adoption of legislation should go hand in hand with the improvement of criminal justice capacities, ranging from the establishment of specialised units for cyber crime investigations and computer forensics, to the strengthening law enforcement and judicial training, interagency cooperation, financial investigations, child protection, public/private cooperation and international cooperation.

The challenge may seem immense, but as indicated at the outset: governments cannot remain passive; they have the obligation to protect society and the right of individuals and to create the conditions for realising the human development potential of information technology.

AFRICAN UNION COUNTRY REPORTS



Benin

★ Porto-Novo

Population: 11,166,658 [1]

Internet Penetration: 11.95% [2]

The Government of Benin has not yet assigned a specific government institution with oversight of cyber security related issues. However, they have developed a strategy paper regarding the establishment of a Computer Emergency Response Team (CERT), to be officially established in the near future. While there are not established laws regarding electronic communications they are currently in the process of being validated by experts. The Government of Benin has taken substantial steps in the development and execution of their Cyber Strategy. This strategy aims to establish trust in Benin's digital infrastructure and has two primary objectives: 1). To reduce cyber crime nationally, and 2). To ensure effective cyber security for national ICT infrastructure including the nation's critical infrastructure.

In a national effort to raise cyber security awareness across the country, the Government of Benin launched a cyber security campaign focused on the country's youth. The campaign is held annually and is called the Internet of Sensitization to Youth. This awareness campaign will be codified in their national cyber security strategy document once a formal framework has been established.

The Government of Benin works with multiple Non-Governmental Organizations (NGOs) and civil society organizations in order to increase overall cyber security awareness. They are also beginning to work with the private sector through informal partnerships, and recognize that cyber security requires both national and international cooperation. Benin's national cyber security strategy also includes the development of curricula leading to a formal cyber security degree program in schools. The Government of Benin also takes part in a number of Confidence Building Measures (CBM) through international meetings and cooperates in international cyber security measures through exchanges with other countries, such as the recent meetings on West African Cyber security held in Dakar, Senegal.

Going forward, the success of current efforts to improve Benin's national cyber security posture will in large part hinge on several key factors, including: the implementation of their national strategy and the establishment of their national CERT.

Burkina Faso

★ Ouagadougou

Population: 18,633,725

Internet Penetration: 9.26%

The lead agency for cyber security in Burkina Faso is the National Agency for Information Systems Security (DCSSI). Other major stakeholders include Board Members from the Prime Ministry, the National Defense and Veterans Affairs Ministry, the Ministry of Territorial Administration and Security, the Ministry of Electronic Communications, the Ministry of Justice and others. The investigation of cyber crimes and related activities is primarily carried out by the Central Directorate of Fighting Cyber

[1] Source: www.worldmeters.info/population/countries-in-africa-by-population/
the elaboration data by UN, Dept. of Economic and Social Affairs, Population Division.

[2] The Internet penetration rate has been updated accordingly from internetworldstats.com.

Crime, which reports directly to the Ministry of Territorial Administration and Internal Security (MATSI). The country has established numerous informal mechanisms for responding to cyber incidents but has not yet established into law formal procedures and policies to do so.

The Government of Burkina Faso has established and operated a national-level CIRT (BF-CIRT) for several years. The primary role of Burkina Faso's CIRT is to coordinate and assist government agencies in implementing services and technical guidance to lower the risk of computer security incidents as well as respond to mitigate such incidents when they occur. Another primary role for CIRT-BF is to develop and conduct awareness campaigns to help educate the local population about the dangers of cyber threats and cyber crime. Lastly, CIRT-BF disseminates timely cyber threat advisories to all national constituents. In addition, BF-CIRT is planning to evolve into an Agency level organization named the Security Agency of Information. Once established, this Agency will have additional tasks assigned to them including to ensure the effective implementation of national policy and to establish specific national standards for information security.

Burkina Faso developed their national cyber security strategy called the National Plan for Cyber Security in 2010 at the request of the Electric Communications Regulatory Authority with the support of the International Telecommunications Union (ITU). The primary objective of the national strategy is to "engage and authorize each Burkinabe government agency to secure the portion of cyberspace that controls and manages or with which it interacts." In addition, the national plan seeks to provide a strategy to reduce vulnerabilities in cyberspace, conduct effective incident management, and to strengthen the overall culture of cyber security through awareness initiatives.

Two notable actions stemming from the Cyber Security National Plan was the creation of a National Security Agency Information Systems (ANSSI) in 2013, and the National Incident Response Centre (BF-CIRT). Government agencies have not been actively promoting cyber resilience or cyber security awareness or carried out activities involved in cyber resilience.

Several challenges have been identified by the government in effectively implementing the National Cyber Security Policy. The primary challenges faced by the government in implementing a national cyber security policy are the establishment of standards for action, budgetary constraints, and lack of local cyber expertise. The government of Burkina Faso has not yet begun to work with NGOs to educate and raise awareness of cyber risks. Nor has the government established cyber security education and training centers due to a number of obstacles including budgetary constraints and lack of local expertise.

Over the last few years, Burkina Faso has experienced an increase in the number and severity of cyber incidents. In particular, there has been a dramatic increase in the number of attacks against websites. Unfortunately, there is a lack of reporting of incidents by victims and therefore estimates remain artificially low. But already in the first half of the year, the number of recorded attacks exceeded the total number of attacks in the previous year. Some public sources exist that provide limited data on attacks against websites in Burkina Faso, such as www.zone-h.org. The most serious cyber security incident occurred in April of 2015 when 56 government websites were defaced. While the perpetrators have not been identified, most indicators, such as indicators of compromise and IP addresses, suggest that the criminals came from outside of Burkina.

While no formal working framework has been established to partner with the private sector, a number of private entities have been identified as primary stakeholders in Burkina Faso's national CIRT, BF-CIRT. The actions that can be taken in order to effectively partner with the private sector should be clearly established in the national strategy and policy documents and agreements that are non-existent at the moment. At this time, Burkina Faso has no formal partnership arrangements signed with other countries. However, they do have several technical information exchanges established with organizations including the US-CERT, France's ANSSI, Tunisia's ANSI, and the Ivory Coast CERT

In principle, based on the public channels established by the various national agencies responsible for the management of cyber security incidents, Burkina Faso is able to exchange cyber threat information.

They have taken a number of steps to establish structures that have enabled them to process tasks and share cyber threat information. These entities include the National Security Agency Information

Systems (ANSSI), the National Incident Response Centre (BF-CIRT) and the Commission on Information and Liberties (CIL). However, there is not an overall framework or policy that guides implementation. This constitutes a major obstacle, which hinders the country's preparation and the actual operationalization of these structures. The ANSSI example is created from 2013 and suffers from lack of budgetary resources. Our hope is that this study will lead to support for cyber policy development and cyber security strategies.

The Burkina Faso "NATIONAL PLAN FOR CYBER SECURITY" is available at:
http://www.cirt.bf/documents/plan_national_FINAL.pdf

Cameroon

★ Yaoundé

Population: 23,924,407

Internet Penetration: 17.38%

In Cameroon, a 287.5 million FCFA project was launched in July 2015 to fight cyber crimes in the country. The National Cyber Expertise Centre, based at the Buea Posts and Telecommunications School, will carry out research and train experts - 25 per class - to develop cyber security protection measures, fight cyber criminality, and thwart cyber terrorist threats.

Cameroon has adopted over the last few years a number of specific laws focused on cyber crime. In addition, Cameroon has established a national Computer Emergency Response Team (www.cirt.antic.cm) to handle incidents related to cyber threats. Cameroon has a state agency known as the ANTIC - National Agency of Information and Communication Technologies, which coordinates with Information Communication Technology (ICT) security. One of ANTIC's primary functions is to help raise cyber threat awareness and strengthen the overall technical capacity to deter cyber crime and enhance cyber security. There are several challenges that the Government of Cameroon is facing, including enhancing international, national, and intra-agency cooperation as well as public private partnerships. While Cameroon does not currently have a government agency certified to international cyber security standards, efforts in this area continue.

Cameroon maintains a division, which is specially tasked to investigate cyber crimes within the Ministry of Posts and Telecommunications. Authorities have established mechanisms, procedures, and policies for responding to cyber incidents and the government assigns their CERT with national-level responsibilities. Cameroon is still developing a national cyber strategy to help guide and coordinate budget resources and cyber security efforts. The main pillars of the national strategy will be cyber security awareness, security auditing, and the maintaining of electronic certificates. The national strategy will also be very helpful in improving cyber resilience and help drive awareness initiatives. While Cameroon does not currently have personal data protection laws on the books, they are currently considering legislation.

Some of the main challenges that the Government of Cameroon has faced in the process of implementing their cyber security strategy are budgetary constraints and the coordination of multinational actors (including experts, civil society, and the private sector). Cameroon has a national cyber security awareness campaign and it is referred to as the National Target Awareness Seminar. This campaign is aimed at the general public to help raise overall cyber security awareness.

Today, the Government of Cameroon works with civil society organizations and NGOs in order to education the population and raise awareness in an effort to mitigate cyber risks. Universities and academic institutions in Cameroon maintain several cyber security degree programs that the government has established. One of the biggest challenges for Cameroon's cyber security advancement is the existence of pirated software and budgetary constraints that limit their ability to hire properly trained personnel.

The current implementation of Domain Name System Security Extensions (DNSSEC) will allow, among other things, the strengthening of the security of ".cm", by guaranteeing the authenticity and integrity of the transactions related to the resolution of domain names in ".cm" and prevent spoofing of domain names in ".cm". These vulnerability scans can detect security holes that can be exploited by cyber criminals and propose remedies to the identified vulnerabilities. Security bulletins will include alerts on the latest vulnerabilities pertaining to hosting platforms and developing websites, assorted remedies.

The development of a repository containing good safety practices to be followed for the implementation and deployment of a secure website, monitoring of websites ".cm" which aims to detect websites engaged in illegal activity and block. There has been a drop in illicit cyber activities since the new policies have been implemented.

The most significant cyber incidents, which took place over the past year, include credit card fraud from a bank. The perpetrators of the incident were quickly identified. According to electronic evidence, the actors who perpetrated the attack were located both within and outside of Cameroon.

The Government of Cameroon works with a number of private sector partners on cyber security related issues and has been able to establish fruitful working relationships with other countries when managing and responding to cyber threats. This has been the case particularly with Czech Republic, INTERPOL, and Nigeria in the context of digital investigations following a scam, which has been the victim of a pharma sales company online. Today Cameroon authorities promote several confidence building measures (CBM) and international cooperation agreements in cyberspace by exchanging information on cyber incidents and best practices for cyber security.

Cape Verde

★ Praia

Population: 526,993

Internet Penetration: 38.56%

Cyber security and cyber crime-related efforts by the Government of Cape Verde are primarily guided by the Agencia Nacional des Comunicacoes (Agency for National Communication). However, numerous other stakeholders also share in the responsibilityincluding: National Security Advisor, Ministry of Defense, and the Ministry of Justice. Cape Verde also maintains a division which is specially tasked to investigate cyber crimes within the Judiciary Police and is part of the Ministry of Justice.

While Cape Verde has not yet established formal mechanisms for responding to cyber incidents, the government has plans to establish a Computer Emergency Response Team (CERT-CV) by the end of 2016. The CERT-CV will have national-level responsibilities and will perform traditional CERT activities, including coordinating with local CERT teams, and exchanging threat information with other national CERT teams.

Efforts to develop a national cyber security policy strategy are ongoing and nearing completion. There is one approved by Resolution 18/2016 of the Council of Ministers of 7th of March. Authorities cite four primary strategy objectives over the next for years: (1) to create a national-level Cyber Security Center to host the nascent CERT-CV and and to coordinate all national; (2) to ensure cyber security of critical national infrastructure; (3) shore up cyber security in terms of national defense, and (4) guarantee the security of Cape Verde citizens in cyberspace.

With regard to date protection laws, Cape Verde authorities have passed personal data protection legislation stemming from work done by the National Commission of Data Protection. With respect to cyber security policy, it is the Cape Verde authorities view that the role of Government is to boost and integrate all efforts on cyber security. To do so, the strategy created a Cyber Security Task Force that is responsible for the implementation of the strategy.

One of the primary challenges to implementing the national cyber strategy according to authorities was the lack of properly trained personnel in this area. Currently, Cape Verde does not have a national cyber security awareness raising campaign. However, an awareness raising campaign is envisaged in the national strategy and authorities expect it will be approved and implemented in the coming years.

However, the Government of Cape Verde does work with a number of NGOs to educate people and raise awareness in order to mitigate cyber risks. Authorities reported that Cape Verde universities do not offer many cyber security related degree programs as the demand for such programs may suggest. To augment this demand the government has established several cyber security education training centers.

Going forward, one of the biggest impediments that authorities identified in advancing cyber security readiness is changing of mindsets. They reported that all national stakeholders and citizens must work together in order to change the mindset to be more proactive and less reactive on all matters of cyber security. Authorities reported that the most important evolution that could affect Cape Verde's cyber security posture is the implementation of its national cyber security strategy. Cape Verde officials believe that the national strategy will be an excellent starting point and give authorities something to build from.

While specific figures do not currently exist, authorities have reported an increase in the number of overall cyber incidents. In particular, DDoS attacks aimed at government sites, phishing, and man-in-the-middle attacks have all seen increases. They reported that there are currently no technology tools to monitor these threat statistic and trends but the Cape Verde E-Gov infrastructure is able to monitor and categorize attacks to its own infrastructure. Many of these illicit cyber activities that are affecting Cape Verde have been met with new policies and laws but they are still being completed. The national strategy addresses these initiatives in an integrated fashion. Authorities said that the most significant cyber incident that took place in Cape Verde occurred in 2015. This incident was a series of attacks to the eGov infrastructure. Fortunately, there were no major impacts as a result. Law enforcement authorities have not yet been able to find out who perpetrated the attacks on eGov infrastructure but evidence strongly suggests that that the perpetrators were located outside of the country. Global events have not significantly affected the country's cyber security posture or development of cyber security capacities.

The Government of Cape Verde works with and partners with numerous private sector entities on cyber security issues. In fact, the private sector plays a major role in the nation's cyber security posture, especially the critical infrastructure operators. These private sector operators are invited to participate in the government-led cyber security task forces. Authorities reported that they are still working on establishing more fruitful working relationships with other countries when managing and responding to cyber threats. However, authorities reported that they see great potential in establishing cyber security relationships with European Union countries, the United States, and the Economic Community of West Africa (ECOWAS). Cape Verde officials have not begun to engage in confidence-building measures (CBM) as of yet due to a lack of budget resources and tools. However, national authorities stated that they are willing to do their part for global cyber security.

Going forward, the Government of Cape Verde will emphasize tackling illicit cyber activity by pushing for the passage of their National Cyber Security Strategy. All indications are that this strategy will be adopted by the Government very soon and then authorities will begin the implementation phase.

Central African Republic

★ Bangui

Population: 4,998,493

Internet Penetration: 3.72%

The government ministry responsible for cyber security and cyber crime efforts in the Central African Republic is the Ministry of Posts and New Technologies. The other major stakeholders involved are mostly technical designers.

At this time, the Government of the Central African Republic has not yet established a specific division within law enforcement to investigate cyber crimes. Cyber crimes are generally investigated by regular police forces. While the government does not have a national cyber security strategy in place and has not yet created a CERT with national level responsibilities, authorities are in the process of considering such plans in the future.

The Government stated that they have not yet established their legal arsenal (law, decree, decisions, and other legal instruments) and the national fight against cyber crime policy are not yet fully developed. The Government has not yet developed their cyber security infrastructure including the establishment of a national-level CERT. However, the authorities have adopted a national cyber security awareness campaign highlighting the dangers of cyber crime. While the government is not currently working with any NGOs to help with cyber security awareness, this is something that they are currently considering. Due to other national priorities, conditions are not adequate for the specialized and comprehensive cyber security training and are not offered in the university system.

According to government authorities, some of the primary impediments to cyber security advancement is the overall lack of resources to train competent security professionals. Partially due to this lack of trained professionals, the Central African Republic has seen an increase in cyber security incidents and attacks over the last year. Unfortunately, authorities have stated that there are no accurate tools in place to monitor these trends.

With regard to new policies, a team from the International Telecommunications Union (ITU) visited the Central African Republic in December of 2015, to help train various officials to fight cyber crime. In most cases, it remains very difficult to identify the perpetrators of cyber crimes in the Central African Republic. Attribution is difficult because the technical identification process is still growing and being led by the Telecommunications Regulatory Agency. However, technical and non-technical evidence suggests that the perpetrators for the most significant cyber incidents were located inside the country.

In addition, authorities note that global events significantly affect the country's cyber security posture and the development of their cyber security activities. The government does not yet work with the private sector and this is due to a lack of cyber crime structures within the country. With regard to other aspects, the country does not yet promote confidence building measures (CBM) and a national strategy is still not in place.

In the future, government efforts in the Central African Republic will center around securing resources, establishing a national cyber security strategy and promoting cyber security awareness throughout the country.

Chad

★ N'Djamena

Population: 14,496,739

Internet Penetration: 4.03%

Chadian authorities stated that cyber security development in their country is very much in its early stages. The government institution with oversight of cyber security issues is called the National Agency on IT Security and Electronic Certification. In addition, Chad maintains a division within their law enforcement apparatus, which is specially tasked to investigate cyber crimes known as the National Agency for Computer Security and Digital Certification (ANSICE).

In early 2015, the Government of Chad enacted four laws regarding Cyber Security and Cyber Criminality. These laws are:[3]

- Law No. 06 / PR / 2015 of 10 February 2015, establishing the National Agency for Computer Security and Digital Certification (ANSICE)
- Law No. 07 / PR / 2015 of 10 February 2015 on the protection of personal data
- Law No. 08 / PR / 2015 of 10 February 2015 concerning electronic transactions
- Act No. 09 / PR / 2015 of 10 February 2015, on cyber security and cyber crime

There is no officially recognized nationwide cyber security strategy in existence today. As such, Chad has not established formal mechanisms for responding to cyber incidents and the Chadian government does not operate a CERT with national-level responsibilities.

Republic of Congo

★ Brazzaville

Population: 4,740,992

Internet Penetration: 8.01%

The Republic of the Congo has made several notable advances on the cyber security front over the last year. While there is no specific legislation related to cyber crime in force there is draft legislation being considered. The draft law is called the "Law on the Fight Against Cyber Crime." The primary objective of the legislation is to govern electronic transaction, protect personal data, and copyright rights. While the Republic of the Congo does not have an official CIRT in place today, this is an area they are exploring and hope to make progress on in the future.

The institution within the Republic of the Congo with oversight over cyber security issues is the Ministry of the Interior. Other major stakeholders include a special branch within the National Police that investigates cyber crimes and enforces crime laws. The Republic of the Congo maintains a unit within the National Police, which is tasked with investigating cyber crimes. While the Republic of the Congo does not yet have an established procedure for responding to cyber incidents, this is an area they are interested in making progress. While the government has not yet established a CERT with national level responsibilities, a national cyber security strategy, which coordinates all national cyber security efforts are underway and the government plans to adopt a strategy, after they have properly implemented the aforementioned cyber security law.

[3] http://www.state.gov/e/eb/rls/othr/ics/2016/af/254181.htm

With regard to cyber incidents, the government states that they have experienced SIM box fraud, where criminals install SIM boxes with multiple low-cost prepaid SIM cards. The fraudster then can terminate international calls through local phone numbers in the respective country to make it appear as if the call is a local call. The government also noted that they experienced the hacking of individual electronic addresses for criminal purposes. It is difficult for the authorities to quantify such incidents as crimes often go unreported. The ARPTC, the Congolese national telecommunication regulator, has equipment for monitoring but with limited applications. The most significant cyber incidences, which took place in the country in the last year was the series of SIM box frauds. The Congolese government works with the private sector on cyber security issues as all the internet providers are private.

The government identified several major challenges to the advancement of their cyber security posture, including the lack of established legal instruments, a lack of appropriate equipment and trained cyber security personnel. While the Republic of the Congo does not yet have a national cyber security awareness program the government views it as imperative. Although the government is not currently working with NGOs to promote cyber awareness, several universities maintain cyber security classes.

Going forward, government efforts will be focused on the establishment of a CERT and on raising general awareness of the dangers surrounding cyber crime and the importance of cyber security. To do this, authorities recognize that they will need both regional and international support.

Democratic Republic of Congo

★ Kinshasa

Population: 79,722,624

Internet Penetration: 3.72%

To the degree that it is officially designated, the Ministry of Telecommunications and New Technologies (PT-NTIC) has responsibility for cyber security and cyber crime-related efforts within the government. Other cyber security-related stakeholders include the mobile network operators and internet providers. The DRC does not maintain a division specially tasked to investigate cyber crimes in an official capacity but there are a number of initiatives spread across multiple organizations. With regard to established mechanisms for responding to cyber incidents, the Democratic Republic of the Congo does not have an established CERT or other national-level cyber security infrastructure in place. However, there are several new laws being considered in parliament that would integrate multiple aspects of cyber security.

To date, the Government of the Democratic Republic of Congo (DRC) has not been significantly involved in working with the private sector on cyber security issues. However, in some cases the government has worked closely with internet providers when they are involved in government security services. The cyber security officials noted that given that cyber crimes were borderless and represented a global phenomenon, the developed countries must bring their expertise to countries which still lag behind on these issues. The authorities also warned that cyber criminals worldwide, were taking stock of local laws and adapting their criminal behavior to avoid discovery and prosecution. They also lauded a workshop organized in August of 2015 in in Kinshasa that helped them raise awareness of the cyber crime phenomenon and they hoped that these initiatives would continue.

While the DRC does not yet have an established national cyber security strategy that coordinates cyber security efforts, a new law which must incorporate the legislation on the protection of personal data is being discussed in parliament. According to cyber security authorities, the role of government should be to put in place legal and technical tools to enable them to cope with rising cyber crime attacks and cyber security challenges. The main cyber security challenges facing the government is the lack of trained cyber security professionals and the need to raise awareness about the potential risks of cyber crime.

One of the biggest obstacles facing cyber security advancement in the DRC is that training remains a major obstacle. In addition, the authorities noted, computers and an internet connection are not accessible to most of the population in the first place.

National authorities report that the hacking of electronic mailboxes and the dissemination of false information on social networks was atop the list of cyber incidents last year. The officials also pointed out that it was difficult to know whether the perpetrators of the incidents were located within or outside of the country.

Egypt

★ Cairo

Population: 93,383,574

Internet Penetration: 40.02%

The Government of Egypt has made great strides in cyber security over the last several years. Chief among these is the national cyber security strategy that they developed in 2014. The main pillars of this strategy is to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals, through a comprehensive framework for enhancing security of and trust in the ICT infrastructure, applications and services, while protecting the privacy of the constituencies. A key priority focus of the strategy was to boost the comprehensive awareness of cyber security and CIIP as a National Priority. The Government of Egypt views the implementation of this strategy essential to being an attractive business destination in the information age and to being an active participant in the Global Digital Economy. Another key priority of the strategy was to establish a high-level Cyber Security Council and to develop it as an executive arm. The last key priority was to empower the private Cyber Security industry and to help develop and train skilled cyber security professionals.

To date, the strategy has been helpful in improving cyber resilience and awareness in Egypt, according to cyber security authorities. A Supreme Council for Cyber Security (SCC) was established in 2015. Since then, the technical committee of the SCC has been actively engaged with various sectors to further develop cyber security awareness and capabilities. The government is in the process of adopting personal data protection legislation, where it was recently forwarded to the legislative body for full review and consideration. The SCC at the Cabinet of Ministers includes members from the national security agencies and key sectors. The authorities are continuing to develop the national cyber security strategy, as well as pursuing sector-specific initiatives and activities. The main challenges faced by the government in the process of implementation of a national cyber security strategy is the mobilization of resources and developing critical cyber security skills.

Today, Egypt has established a national cyber security awareness raising campaign, which consists of sector-specific awareness raising efforts (conferences, seminars, workshops, etc.) as well as a national initiative for child online protection (COP). Target audience for the sector-specific activities include multiple decision makers and professionals. While target audience for the COP initiative is the general public with special focus on educators, parents, children and youth.

The primary institution within Egypt with oversight and responsibility for cyber security-related issues is the Supreme Council for Cyber Security (SCC), which is affiliated with the Cabinet of Ministers. Other major stakeholders are the ICT Minister (Chairs the SCC), SCC members, Egypt's national security agencies, critical sectors (Government services, Banking, Energy, Health) and the Ministry of Interior.

Egypt maintains a division which is specially tasked to investigate cyber crimes. Located within the Ministry of Interior, the Cyber Crime Division was established more than 10 years ago. In 2009, a national CSIRT was established at the National Telecom Regulator, EG-CERT, (http://www.egcert.eg/). The EG-CERT has national-level responsibilities and responds to cyber incidents nationwide Government authorities actively works with ICT professional, NGOs (CIT Chamber and EITESAL), private sector companies, as well as the National COP Committee members. Today, a number of Egyptian universities offer cyber security degree programs and the government has supported cyber security professional training programs in academia and in professional ICT training institutions. The biggest impediments to the country's cyber security advancement this year is the lack of solid legal and regulatory frameworks for cyber security and cyber crime. In addition, authorities cited that general shortage of cyber security professionals.

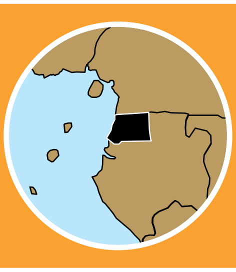
The Government of Egypt has noted an increase in the number of cyber incidents and cyber crimes over the last year. Authorities use the EG-CERT to monitor these trends and statistics through the receipt of national and international data threat feeds. Egyptian authorities state that they work closely with private sector entities on cyber security issues. Authorities note that the private sector owns and operates ICT infrastructure as well as ICT enabled infrastructure in various key sectors, therefore, they are a necessary partner in securing networks and fighting cyber crime. In addition, they note that there are many private companies developing and deploying cyber security solutions throughout the country as well as providing consultation and other cyber security related value added services. Egypt has been able to establish a number of productive working relationships with other countries and work closely with them to manage and respond to cyber security threats. In fact, the Government of Egypt has several Memorandum of Understandings (MOUs) as well as less formal partnerships with several countries in the region, including Uganda, Tanzania and Tunisia.

Equatorial Guinea

★ Malabo

Population: 869,587

Internet Penetration: 27.36%



According to the government of Equatorial Guinea, their cyber security infrastructure is very much at its infancy. At this time, the government has not established formal technical or legal mechanisms for responding to cyber incidents nor have they established a CERT with national-level responsibilities. However, ORTEL (Telecommunications Regulatory Authority) acts as an autonomous entity that in some instances provides oversight on cyber security matters. The ORTEL, aims primarily to advise on the legislative and regulatory consistency on Telecommunications issues, ensure compliance on these matters and propose institutional reforms that promote competition in Telecommunications and acts according to the principles of legality, objectivity, transparency and due diligence. Other major stakeholders in cyber security include the Ministry of ICT, which has broad powers over sybersecurity. They do not currently maintain a specific division within law enforcement, which has been specifically tasked with investigating cyber crimes.

The main national cyber security challenges right now is to develop a national strategy that can address the array of cyber security issues now facing the country as well as create specific cyber security policies and to establish a national CIRT, that can help train cyber professionals. Currently, Guinea does not yet have a national cyber security awareness raising plan, but it is considering developing one in the future. However, authorities note that they do works with NGOs to educate people and raise awareness to mitigate cyber risks. However, universities or academic institutions in Guinea do not currently offer any cyber security related degree programs or training centers.

With regard to the largest impediments to cyber security advancement in 2015, it is the development of an inclusive cyber security strategy. Officials also stated that because the development of their cyber security strategy is at such an early stage, not enough effort is being put into advancing cyber security. Because there is no comprehensive cyber security strategy in place, officials note that the government has not yet been able to consider personal data protection legislation. However, the Ministry of ICT has plans for it in the near future.

Gabon

★ Libreville

Population: 1,763,142

Internet Penetration: 39.04%

Gabon has a national cyber security framework for implementing internationally recognized cyber security standards. However, Gabon is still working on draft laws in both the areas of cyber crime and cyber security. Gabon is in the process of establishing an officially recognized national CIRT.

Two agencies serve as the primary leads for cyber crime and cyber security in Gabon, the Ministry of Economy and the Ministry of Digital Post. The major stakeholders are the National Agency of Infrastructure and Digital Frequencies (operator of the state on the implementation issues and implementation of digital projects) ARCEP Regulation and Electronic Communications & Postal Authority (Sector Regulator).

Authorities noted that Gabon does not currently maintain a division specially tasked to investigate cyber crimes and does not operate a national-level CERT. Moreover, Gabon has not yet fully developed a national cyber security strategy to coordinate existing efforts. However, laws pertaining to personal data protection have been on the books since 2001 and have so far proven to be very effective.

One of the main challenges facing the Government of Gabon in the process of developing a national cyber security strategy has been the slow process of setting up a national committee for the eventual implementation of the national strategy. Authorities note that once the strategy has been developed, Gabon will initiate a national cyber security awareness raising campaign. To date, Gabon does not work with civil society organizations or NGOs to help them educate and raise awareness throughout the country. Notably, several universities offer programs for cyber security degrees. Government authorities note that the biggest impediment to the country's cyber security advancement this year has been the lack of a national strategy.

Over the last year, Gabon has experienced an increase in the number of cyber incidents including privacy issues such as the hacking of individual email accounts and the broadcast of personal photographs. Currently the government does not possess the tools to categorize and monitor these activities. According to officials, the most serious incident experienced is the hacking of email accounts. The technical and non-technical evidence suggests that the perpetrators of these crimes were located outside the country. However, the criminals have not yet been identified. Authorities also noted that the government of Gabon works with and partners with the private sector on cyber security issues in order to set up a common response strategy to cyber crime and cyber security. Gabon has established a number of fruitful relationships with other African countries as part of workshops that have been organized at the regional and sub-regional level.

Gambia

★ Banjul

Population: **2,054,936**

Internet Penetration: **19.01%**

The Government of Gambia has made great progress over the last year in improving their cyber security and they are currently working hard to reinvigorate and expand these efforts. Gambia has one of the highest mobile phone concentrations in Africa but only 1.2 percent of the population has access to mobile broadband. Fixed-line subscriptions are prohibitively expensive for most Gambians and Internet access in Gambia is still mostly from dial-up Internet cafes.

Cyber Security efforts in Gambia are led by the Ministry of Information and Communications Infrastructure. Other major stakeholders include the Gambia Public Utilities Regulatory Authority (PURA), a multi-sector regulator with purview over broadcasting, electricity and telecommunications. The Gambia Telecommunications Services Company (GAMTEL) a national telecommunications company and the Gambia Submarine Cable Company (GSC), which is responsible for submarine cable and national fiber connectivity are all major stakeholders in the national cyber security efforts.

While Gambia does not yet have a government agency that is specifically tasked with investigating cyber crimes, some individuals who are trained on cyber security programs serve as technical specialists who work with the judiciary to prosecute cyber related crimes. In terms of cyber crime laws, Gambia enacted the Information and Communications Act (IC Act) in 2009. The IC Act is comprehensive legislation that attempts to addresses not only the rapidly evolving nature of the communications industry, but also the convergence of technologies. The main components of the Act include protection against child pornography, penalties for reprogramming telecommunication, and personal data protection.

In the future, Gambian authorities note that greater awareness and capacity building programs will be required to facilitate cyber resilience in the future. Several impediments to cyber security advancement in Gambia were identified by government authorities, including, a lack of available funding, cyber security awareness, and an overall lack of cooperation between industry and government sectors. Currently, there are no large-scale national cyber security awareness raising campaigns in Gambia. However, once enacted, Gambia's National Cyber Security Strategy aims to address the lack of cyber security awareness. The national strategy will also lay out a plan to work with Non-Governmental Organizations (NGOs) to help raise awareness. There are currently no universities or academic institutions which maintain cyber security degree programs. However, there are currently plans to establish a series of cyber training centers across the country and incorporate a cyber security curriculum into national university education. One idea is to use the Rural Community Information Centers, which are already established throughout Gambia, as cyber security training centers. Government personnel have been sent on training including civil service personnel in order to raise their cyber security awareness and to provide them with some degree of technical training.

Government officials stated that exact statistics and data on cyber crime are not readily available today in Gambia. However, several cyber crime trends were identified including social engineering attacks, spoofing, phishing, malware, and denial of service attacks (DDoS). The vast majority of these cyber crimes occurred at a personal level and are never reported to authorities. In addition, law enforcement agencies lack the technical capacity and expertise to trace these attacks and bring perpetrators to justice. Often, the perpetrators are located outside of the country and beyond jurisdiction. However, on the occasion where an arrest is made, the evidence is normally gathered through audit logs and malware scanning systems. Siloing systems (limiting networking) is currently utilized to mitigate cyber attacks at institutions and these systems vary.

While there are currently no laws that specifically address cyber crimes, the Government of Gambia is currently considering such legislation. They collaborate with the private sector on cyber security issues and there are private sector representatives on the evaluation committee for the Consultancy project to develop Gambia's National Cyber Security Strategy.

Gambia has been represented through a ministry in Geneva, Switzerland at the United Nations Conference on Trade and Development (UNCTAD) on Cyber Law Harmonization for Enhancing e-Commerce for the Economic Community Of West African States (ECOWAS).

Ghana

★ Accra

Population: 28,033,375

Internet Penetration: 30.83%

There are several agencies within the Government of Ghana that share responsibility for cyber security including the National Communications Authority (Telecom Regulator), National Information Technology Agency (ICT Regulator), Ministry of Information and Communications Technology, and the Ghanaian National Security Agency. Other major stakeholders include the private sector and operators of critical infrastructure.

CERT-GH is the national Cyber Security Emergency Response Team of Ghana. CERT-GH coordinates all national efforts to prevent and respond to cyber attacks targeting government information systems and and infrastructure deemed critical. It also serves as the focal point for engagement with other national CERTS. Officials note that there is a relatively low incidence of cyber crime in Ghana. However, there are some lapses in network security due to the fact that Ghanaians tend to use informal methods to secure personal information. The Ghanaian Cyber Security Policy and Strategy has eight pillars: effective governance, legislative and regulatory framework, research and development towards self-reliance, cyber security emergency readiness, cyber security technology framework, culture of security and capacity building, compliance and enforcement as well as international cooperation. The policy encourages a national cyber security awareness program, and the establishment of of an emergency response team has already been established.

Cote d'Ivoire

★ Yamoussoukro

Population: 23,254,184

Internet Penetration: 21.54%

In recent years the Ivory Coast has benefited from immense economic growth. Leading the way in this growth is the telecommunication sector, which is the second largest contributor to Gross Domestic Product (GDP) in the Cote d'Ivoire, at around 7%. The introduction of 3G mobile services has changed the sector, and further changes are expected following the commercial launch of LTE services, which will see a significant increase in mobile broadband availability.

Within the Government of the Cote d'Ivoire, the institution that has oversight over cyber security and cyber crime-related issues is *Autorité de Régulation des Télécommunications de Côte d'Ivoire* (ARTCI). The role of (ARTCI) is to develop the digital economy and expand ICT in Cote d'Ivoire. Other major stakeholders include the Computer Emergency Response Team of the Cote d'Ivoire (CI-CERT), the Platform to Combat Cyber Crimes (PLCC), the Ministry of Digital Economy and Post Office, and the

Association of ICT. The PLCC has been special tasked by the government to investigate cyber crimes and is set up within the Ministry of Interior and Security.

The Cote d'Ivoire has a draft national strategy that defines a governance model which includes all key cyber security stakeholders. The national strategy has not been fully implemented, but the key objectives of the national cyber security strategy are based on 6 strategic areas:

1. Protection of cyberspace, national information systems and critical infrastructure
2. Development of digital trust and protection of online services
3. Strengthening national capacity to respond to incidents and development of coordination and information sharing
4. Capacity Building and awareness
5. Adaptation of legal framework and expanding international cooperation
6. Governance of cyber security

With regard to cyber security legislation and policy, the Cote d'Ivoire has laws developed expressly for the protection of personal data. The government plays a key role in implementation of the cyber security strategy by getting all of the resources necessary to achieve the desired objectives. The Government of Cote d'Ivoire is committed to ensuring the involvement of all stakeholders. While the national strategy has not been fully implemented yet, the officials note that the government is making every effort to do so.

Officials point to a number of cyber security-related challenges facing in Cote d'Ivoire, including:

1. Cyber Crime;
2. Ensuring good governance while the cyber security strategy is being implemented;
3. Lack of coordination between key players during major national cyber-attacks;
4. Increasing the national and international cooperation in cyber security;
5. Protecting online services and developing digital trust;
6. Lack of resources (both financial and technical);
7. Lack of capacity building programs and security awareness campaigns.

Several frameworks and initiatives have been accomplished in the last year, including:

1. National Seminar on cyber security with all national stakeholders;
2. National awareness campaign about the dangers of cyber crime;
3. Awareness campaigns on cyber security and IT security made in school;
4. National Forum on Internet governance with workshops on cyber security;
5. Annual National ICT Day (JNTIC) on good information security practices.

There is a well-established framework of close cooperation with the private sector including partnerships with several ICT associations. Together with embassies and foreign diplomatic representatives, the government and private sectors, have conducted several cyber security awareness campaigns and workshops.

Cote d'Ivoire has several training centers in cyber security and information security. The government signed a Microsoft partnership agreement for the establishment of an authorized (IT ACADEMY) which provides training to officers of the national police computer and cyber security. There is also a Certified Center of Excellence (ESACTIC) by the International Telecommunication Union (ITU) which provides computer security training and cyber security. In addition, Universities in Cote d'Ivoire offer cyber security courses. In addition, the Government has established centers for cyber security training.

According to government officials, 856 IT incidents were treated in the prior year, mainly consisting of cyber attacks, including: Malware (ZEUS), Spam, phishing, defacement website and Botnet against five thousand six hundred twenty-four (5624) computers in 2014. This increase is attributed to better collection method cyber incident by the CI-CERT. CI-CERT recorded an increase in the number of incidents including new forms of illicit activities, including: - Ransomware (rançongiciels), which is malware that encrypts personal data and asks the owner to send money in exchange for the key to decipher.

The government took a range of actions to address the incidents, including:

1. Recommendations on the treatment of different types of incidents or attacks
2. Audits of vulnerabilities on online infrastructure, notices and safety alerts on IT products
3. Technological monitoring tools to monitor these trends include probes, hoyneynets;
4. The use of collection platforms such as Shadowserver, honeynets, phishing MX-clean, malware clean-MX, stopforumspam, etc.

In July 2013, more than 26 government websites (Domain gov.ci) experienced a defacement by hack-tivist group called "error 7RB" and "HusseiN98D". After conducting an analysis of log files (log), CI-CERT has identified the type of attack and vulnerability that was used. Thus the source of the attack IP address was from outside the country. World events have not significantly affected the state of cyber security in Cote d'Ivoire. The government wants to build the capacity of professionals in the public sector in terms of IT and cyber security.

The CI-CERT is currently working with several other CERTs in Africa, Europe, America and ASIA in incident management of cyberspace and information sharing related to cyber security. CI-CERT receives daily incident notifications (botnet case, viral infection, phishing, etc.) CI-CERT partners with and ensures close coordination between all stakeholders. As a founding member of the CERTs African Community (AfricaCERT) CI-CERT exchanges their experiences and best practices on management cyber incidents with other CERTs. Also, the CERT of Cote d'Ivoire is actively involved in promoting confidence-building measures and prevention of the organization of the CERTs member of the OIC countries (OIC-CERT)

Going forward the Government of Cote d'Ivoire intends to improve their cyber security posture by adopting and implementing the national cyber security strategy. Officials say they will also seek accession into the global network of CERTs (FIRST). Lastly, authorities note that they will work on strengthening communication and awareness of cyber security and work to secure the nation's critical infrastructure.

Kenya

★ Nairobi

Population: 47,251,449

Internet Penetration: 69.07%

In Kenya, cyber security matters are primarily the responsibility of the National Cyber Security Committee. Other major stakeholders concerned with cyber security are the Ministry of ICT (Chair) and various security and technology agencies. Two different divisions have been specially tasked with investigating cyber crimes are CSIRT-Kenya, and the iCSIRT (Industry Computer Security Incident Response Team) which are both overseen by Ministry of ICT.

With regard to incidents in the field of cyber, Kenya has established mechanisms, procedures and policies for responding to cyber incidents through the use of the National CSIRT-Kenya (www.csirt.or.ke) and the iCSIRT (www.tespok.co.ke). The iCSIRT was founded in 2013 and the National CSIRT-Kenya was established in 2010. Between the two CSIRTs, their primary functions are to coordinate between stakeholders and to protect, detect and manage recovery from cyber incidents affecting their networks.

In recent years, Kenya has experienced an increase in the number of cyber incidents amounting to an estimated 40% increase in 2015. Much of this increase has been attributed to the increase in the use of malware. Several technology tools are used to monitor and categorize these threats and attacks. Illicit cyber activities have been met with new policies such as setting up a secure environment, risk assessment and application hardening activities by the security operations center for the Government.

When surveying the most significant cyber incidents which took place in Kenya in the past year, officials stated that it was a series of social-engineering phishing attacks. The perpetrators of the incident were found to be groups both within and outside of Kenya's borders.

Kenya is advancing in relation to taking adequate cyber measures and has a National Cyber Security Masterplan and Strategy that has been fully implemented. The strategy was inaugurated by the President of Kenya in June 2014, and has proven to be very helpful in improving coordination among all cyber security stakeholders. The government of Kenya has several pieces of legislation that cover personal data protection and the bills are at an advanced stage of ratification. The Ministry of ICT has the express mandate to develop the policy and oversee its implementation. A national awareness raising campaign is one of the activities that is highlighted in the national cyber security strategy, and plans are already underway to commence these awareness raising activities. National cyber security programs in Kenya work with the communications regulator, known as the Communications Authority, which has implemented a number of awareness campaigns. The universities and academic institutions in Kenya maintain cyber security degree programs and the government has established cyber security education and training centers. An important evolution in cyber security advancement was the implementation of the multi-agency National Cyber Security committee.

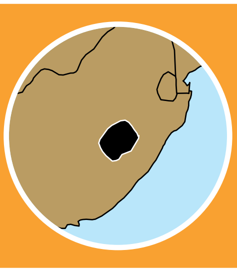
The Government of Kenya does work with the private sector on cyber security but is eager to do more. Public-private partnerships are still relatively new in Kenya and some of the traditional barriers will need to be overcome. Kenya has made contact with global private sector actors such as Google and Facebook, to help protect against with social engineering incidents. Kenya promotes confidence building measures (CBM) and international cooperation in cyberspace by exchanging information on cyber incidents and best practices for cyber security by participating actively in the UN Group of Cyber Security Experts. Critical lessons have been learned in this process about the importance of multiple actors working together harmoniously to address the problems as well as the importance of cyber diplomacy.

Lesotho

★ Maseru

Population: 2,160,309

Internet Penetration: 25.21%



In Lesotho, the Ministry of Communications leads on cyber security related issues and has overall responsibility. However, other cyber security stakeholders exist, including the Lesotho Communications Authority, various academic institutions, financial institutions and National Security forces all play a role. The cyber security strategy and policies have been developed and were submitted to Parliament for adoption earlier this year. While no national CIRT has been established yet in Lesotho, lawmakers are discussing its creation now. The mechanisms for policy and procedure related to cyber security will be in place once the national cyber security strategy has passed and implementation begins. According to the Government of Lesotho, the role of the Government will be to ensure that all citizens' rights are observed and that the perpetrators of cyber crime will be fairly charged. According to Lesotho authorities, social media is considered substantial threat vector, as people are able to get away with wrongdoings due to the unavailability of cyber laws to investigate and prosecute cyber criminals.

While there are no current cyber security awareness initiatives ongoing, authorities believe that cyber awareness campaigns will only garner support and momentum once the national strategy has been passed. There are currently no mechanisms in place to monitor cyber risks but Lesotho is vulnerable to cyber attacks and has been victimized. Academic institutions in Lesotho are part of the team which drafted the cyber security bill, therefore there are future plans to have specialized cyber security degrees to help train future cyber security professionals. Lesotho is currently working hand-in-hand with other member states in order to coordinate cyber threats and the country is very committed to confidence building measures.

Liberia

★ Monrovia

Population: 4,615,222

Internet Penetration: 9.87%

While a specific government entity responsible for cyber security has yet to be established in Liberia, it is expected that the Liberian Telecommunications Authority (LTA) will soon take on this responsibility. Other cyber security stakeholders will include, private sector service providers, the Ministry of Telecommunications, the Ministry of Justice and the Ministry of Foreign Affairs. In addition, authorities plan to engage NGOs and private organizations to help develop the conceptual framework for the establishment of a specific cyber crime unit. While there is no existing policy and procedural documents in place at the moment, the Liberian government is currently discussing the strategy going forward.

Authorities noted that most of the government's time and actions have been focused on physical security and they have not yet turned their attention to the growing problems of cyber security and cyber crime. At this time, cyber security capacity building efforts and cyber crime awareness is extremely limited. Officials pointed out that in Liberia, individuals and organizations take responsibilities for managing their own risks online. Therefore the government does not yet have mechanisms in place to monitor and quantify the various cyber crimes and cyber security risks. Authorities note that they hope they can turn their attention to cyber once a strategy is in place and they establish a responsible government entity.

While there is no formal cyber incident reporting requirement in Liberia, there have been several cyber incidents over the last year. A DDoS attack was experienced this year but nothing of such has been officially reported thus leaving the issue as a rumor. Additionally, there are no mechanisms, procedures or tools in place that can assist in the identification and location of cyber criminals. With regard to CBM, it is envisioned that CBM and international cooperation will be a cardinal principle of the entity if established.

Largest impediment for Liberia is that they do not have an established cyber security policy, strategy or entity. Most importantly, Liberia needs to begin training and national awareness. The government of Liberia has transposed into national law the ECOWAS Supplementary Act on Personal Data Protection within ECOWAS. This is part of a new Supplementary Acts on the harmonization of ICT/telecommunications regulation within ECOWAS which has been submitted to the President.

A much needed IXP was never started and completed until support and encouragement was received from the African Union Commission (AUC). In like manner, a cyber security framework for implementation is much needed in Liberia. Any strategic approach, documentation and support in this effort will be greatly appreciated.

Libya

★ Tripoli

Population: 6,330,159

Internet Penetration: 42.8%

Within Libya, the name of the institution with oversight over cyber security issues is known as the National Information Security and Safety Authority (NISSA). NISSA's primary mission is to promote and sustain secure use of ICTs as well as to prevent, detect, and respond effectively to the associated risks. The major stakeholders include Libyan citizens, the Ministry of Communication and Information, the Ministry of Interior, the Government of National Reconciliation, private sector telecommunication companies, and academia. In addition, according to cyber security officials, Libya maintains a division specially tasked to investigate cyber crimes, called the Anti-IT Crimes Administration, which falls under the administration of the Ministry of Interior.

Officials note that the government has clearly established mechanisms, procedures and policies for responding to cyber incidents. Much of this responsibility resides with Libya-CERT, which was established in February of 2013 with the support of ITU. Libya-CERT has national-level responsibilities and is charged with prevention, detection, and mitigation of cyber threats.

Authorities note that Libya is still developing a national cyber security strategy. The intent of the strategy will be to guide and coordinate all national level cyber security Once the cyber security strategy is developed, NISSA and the Ministry of Information will be responsible for implementing the policies. While Libya does not currently have laws which define and protect personal data and personal data collection, legislation is pending and could be signed into law soon. Some of the primary challenges facing the government as they work to develop and implement their national cyber security strategy is political instability, and the current national security situation. In addition, authorities cite a lack of budgetary funding as a limiting factor.

The Libyan government has an established national cyber security awareness raising campaign run by NISSA and in collaboration with a number of private ITC sector companies. Currently, the awareness campaign targets the ITC sector, but every available effort is being made to reach out to a wider audience. The Libyan government also works with NGOs to help educate and raise awareness about known cyber risks. At the moment, most of the academic institutions have mandatory classes of various information security related subjects in all IT related degrees. While the Government of Libya has not yet established cyber security education centers, NISSA is currently working with Tripoli University on introducing a new degree dedicated solely to cyber security.

Due to current political unrest and the austerity measures, that affect local government, lack of funding has hindered most of the attempts of advancing cyber security this year. The most important accomplishment this year is the evolving role played by NISSA. In order to keep up the momentum gained over the last year, officials note that they will need continued funding and show successful projects and initiatives.

While there is no reliable data available regarding whether the country has experienced an increase in the number of cyber incidents, NISSA is working hard to develop and deploy a variety of new tools. In addition, authorities will collaborate with various stakeholders to gather all cyber security-related data that is available to analyze cyber threats. Illicit cyber activities have been met with new policies, laws, initiatives and training programs. In particular, there is a new proposed Electronic Transaction Law. This new legislation will cover a wide-range of essential aspects needed for a safe cyber space. The new law covers digital signatures, electronic certification, protecting electronic transactions, online banking, personal data protection, and e-crime. According to cyber security officials, the most significant cyber incidents are those related to fraud, data exfiltration, phishing and malware infections. The government works with the private sector on cyber security issues especially with the ICT private sector. One of the goals set by the government for NISSA is to empower private sector tby encouraging them to give the InfoSec the appropriate and required level of priority.

Libyan authorities have been able to establish fruitful working relationships in managing and responding to cyber security threats. International relations and global partnerships are essential and crucial in maintaining a safe cyberspace. This is being achieved by forming a network of partnership with various regional, continental, and international entities, such as peer organizations in other countries and regional and international forums. In addition, officials are staying active and involved in much of the significant InfoSec related events held by our partners. For example, NISSA has been successful in being one of the founding members of AfricaCERT, where they were elected to be on the steering committee of OIC-CERT. NISSA is also in the process of joining FIRST. Libya promotes confidence building measures by exchanging information on cyber incidents and best practices for cyber security. This is done through working with international partners through the expanding network, such measures are being promoted nationally to ensure safer national cyberspace.

Libya has made great strides in improving their cyber security posture over the last year. Future efforts will include developing and implementing an effective national cyber security strategy and continuing to grow their international partnership model.

Malawi

★ Lilongwe

Population: 17,749,826

Internet Penetration: 6.02%

Malawi's government has stated that cyber crimes are on the rise and there is a distinct need for the establishment of a CERT to handle such issues effectively. The Government of Malawi's Minister of Information stated that the problem of cyber crime is rapidly growing as there are limited laws in place governing information and communications technology besides the the Communications Act of 1998, which was written before major technology advancements. Evidence of the mounting cyber security problem is the fact that in 2014 nearly every government website was hacked. The future plan is for the Malawi-CERT to serve as a base for national coordination in order to respond to ICT security threats in Malawi.

While the Government of Malawi has not yet established formal mechanisms for responding to cyber incidents,plans are underway to develop the national cyber security policy and implementation strategy as well as operationalizing the national Malawi-CERT, which will have national-level responsibilities.

The Malawi government has not yet adopted personal data protection legislation. However, some aspects of data protection are currently covered under the e-transactions bill which was enacted in the November 2015 Parliament sitting.

The roles and responsibilities of the government to coordinate implementation of cyber security policy and strategy will be reflected in the national strategy once developed and implemented. Similarly, Malawi does not yet maintain a division or individual specifically tasked to investigate cyber crimes. However, plans are underway to establish and operationalize the national CERT under the Department of E-Government. Malawi officials noted that under the current plan, the Department of E-Government within the Ministry of Information (tourism and civic education) is the only government agency with oversight over cyber security issues. Other major stakeholders include the University of Malawi, the Malawi Communications Regulatory Authority, the Malawi Police Service, the Malawi Defence Force, the Chamber of Commerce and the Bankers' Association of Malawi. However, according to government officials stakeholder roles and responsibilities are yet to be agreed upon.

Authorities stated that a main challenge that the government has faced is the process of developing and implementing a national cyber security strategy. To date, Malawi has had a shortage of trained cyber security professionals and inadequate cyber awareness. While Malawi has not yet developed a national cyber security strategy, the authorities are now considering it. Due to its lack of a formal cyber security strategy, the Malawi does not yet work with NGOs. The same is true for Universities or academic institutions in Malawi, where the lack of a cyber security strategy has slowed efforts to establish cyber security education training centers. The largest impediments to the country's cyber security advancements last year was their overall lack of cyber security governance and legislative framework from which to build on.

Officials noted that the Government of Malawi cannot accurately account for cyber attacks and therefore, cannot say with any certainty whether cyber incidents have increased over the last year. The hope is that once the national Malawi-CERT is operationalized, they can begin to follow these trends and track cyber threat statistics.

While the Government of Malawi does not yet work with the private sector, the hope is that once the national strategy is established these instruments will provide the platform for interaction with private sector. Malawi has not yet established fruitful working relationships with other countries managing and responding to cyber security threats as the national CERT is yet to be operationalized. While Malawi does not provide best practices for cyber security, the government of Malawi is very much committed to fighting cyber crime and is currently in the process of developing cyber security governance and the legislative framework, this process will be finalized by the end of 2016.

Mali

★ Bamako

Population: **18,134,835**

Internet Penetration: **13.18%**

The Malian authority with responsibility for cyber security is the Telecommunications/ICT Regulations and Communications Agency. Other major stakeholders include the telecommunications and ICT sector, the security forces, the Ministry of Justice, civil society groups, and private sector companies. While there currently are not any laws governing cyber security specifically, cyber crime laws can be found in Criminal Code (Article 264,271). In addition, Mali maintains a division specially tasked to investigate cyber crimes known as the Judicial Investigation Brigade. While Mali has not established formal mechanisms for responding to cyber incidents and the government does not operate a national CERT, in May 2013, the Government of Mali adopted personal data protection legislation. Officials note that while they have not developed a national cyber security strategy, they are planning to in the near future.

According to Malian officials, the main challenges faced in improving their national cyber security posture is improving overall cyber awareness. Once a cyber security strategy is established the Malawi Government plans to launch a cyber security awareness campaign using seminars and workshops. The target audience for these campaigns will be the telecommunications and ICT sectors, the national security forces, Department of Justice, civil society groups as well as private sector entities. To date, the Malian Government has not worked with NGOs to educate the public about cyber awareness. Currently, there are no Universities or other academic institutions in Mali which offer degrees or certificate programs in cyber security related areas.

Officials note that the biggest impediments to cyber security advancement is the protection of personal data and electronic transactions. Mali has experienced an increase in the number of cyber incidents over the last year. To combat this rise, authorities have used antivirus, firewall, IPS and IDS security technologies. The most significant cyber incidents which took place in Mali in the last year were financial crimes. Although the perpetrators of the incident were not found, evidence suggests that the perpetrators were located both within and outside Mali's borders. Authorities noted that global events and trends do significantly affect the country's cyber security posture and development of cyber security capacities.

The government of the country of Mali works with the private sector but the country is yet to establish fruitful working relationships with other countries when managing and responding to cyber security threats. Authorities reported that Mali does not yet participate in confidence building measures (CBM) to enhance international cooperation in cyberspace and for exchanging information on best practices.

Mauritania

★ Nouakchott

Population: **4,166,463**

Internet Penetration: **21.98%**

While the Government of Mauritania has instituted an effective ICT framework, it has not yet developed cyber crime legislation. Nor has Mauritania enacted legislation governing cyber security and personal data protection. Although Mauritania has an officially recognized national cyber security strategy, officials note that they have not designated a specific agency to be responsible for implementing the strategy, policy, and roadmap.

The Mauritania government agency which has the primary responsibility for cyber security is called the ICT Branch. Other major stakeholders include the Ministry 'Emploi, de la Formation Professionnelle et des Technologies de l'Information et de la Communication (MEFPTIC) and the Ministry of Interior and Decentrilization (MDN). The Government of Mauritania appointed a division specifically tasked with investigating cyber crimes called the Computer Security Service which is part of the Director General of Information Technology and Communications (DGITC).

The country of Mauritania has established mechanisms for responding to cyber incidents but the government does not yet operate an official CERT with national level responsibilities. However, the ITU conducted a CERT assessment with the Government of Mauritania in 20012. Today, there is an unofficial CERT but it has yet to be codified into law. The government is considering developing a national strategy guideline for cyber security and its preparation is ongoing.

Government officials recognize that one of the major issues facing the country is how to better protect their critical infrastructure. While the government has not developed a formal national cyber security awareness campaign yet, it has begun to partner with various NGOs to help mitigate cyber risks. To date, the University system has not offered any cyber security-related courses or certificate programs, nor has the government established any cyber security education and training centers. In addition to better securing their critical infrastructure, officials note that the fact that they have not established a formal CERT has hampered their progress in reaching their cyber security goals.

Mauritania has experienced cyber crime and other cyber-related incidents recently and and uses a cyber security tool called Veille to monitor these statistics and trends. The most significant illicit cyber activities over the last year have been related to attacks on both government and private sector websites. Based on the available evidence, officials are convinced that the perpetrators of the website attacks were located outside of Mauritania's borders.

The Government of Mauritania has worked with and partnered with the private sector. Officials noted that the government understands that the private sector also has critical infrastructure, which must be protected. One critical lesson that officials have learned is that that the continent of Africa must further establish the continent-level CERT that will share information and cooperate with all of the national-level CERTs African countries.

Mauritius

★ Port Louis

Population: 1,277,459

Internet Penetration: 56.47%

In order to address cyber security issues in Mauritius, a national cyber security strategy implementation (2014 - 2019) is underway. This strategy defines the main aims, guidelines, as well as action plans to respond effectively to cyber security threats. The goal is to detect and identify any disturbing activity to the vital functions of information systems and respond to them in a way, which minimizes detrimental effects.

Mauritius has a national cyber policy, which was established in 2014 to coordinate cyber security efforts. The vision and goal that has been set by the Government of Mauritius is to enhance the cyber threat preparedness through global resilience and security of its ICT assets by the year 2019. Mauritius has adopted a number of laws governing personal data protection. The primary legislation protecting personal data can be found in their Data Protection Act, which was enacted in 2004. Mauritius has also enacted several laws specifically targeting cyber crime, including the Computer Misuse and Cyber Crime Act of 2003 and the Electronic Act of 2000. The Ministry of Technology, Communication and Innovation has been charged with driving cyber security policy with the aim of improving overall cyber security preparedness.

Officials report that with regard to ICT infrastructure in Mauritius, the Computer Emergency Response Team of Mauritius (CERT-MU) has oversight of national cyber security issues. CERT-MU is within the Department of the National Computer Board, which itself is under the aegis of the Ministry of Technology, Communication and Innovation. There are several major stakeholders concerned with cyber security related issues, including the Ministry of Technology, Communication and Innovation, Law Enforcement, Regulatory Bodies, the Office of the Prime Minister, the Data Protection Office, the IT Security Unit and various critical infrastructure sectors. With regard to the investigation of cyber crimes, the Police Cyber Crime Unit and Police IT Unit are primarily tasked to investigate cyber crimes. The Computer Emergency Response Team of Mauritius (CERT-MU) 2008 (http://cert-mu.org.mu) is an established mechanism for responding to cyber incidents. The Government of Mauritius has a strong relationship with the private sector on cyber security issues. Mauritius also has longstanding relationships with CERT-IN, JP-CERT and is a member of the Forum of Incident Response Security Teams (FIRST).

In the realm of cyber security, one of the main challenges facing the Government of Mauritius is the lack of budget and other resources. Mauritius' national cyber security awareness campaign is called the Sensitization Campaign, which has been in place since 2009. In addition, Mauritius works with NGOs to help educate and raise the overall public awareness in order to mitigate cyber risks. While there are several universities in Mauritius, which offer cyber security degree programs, the government has not established cyber security education and training centers. However, officials note that the CERT-MU regularly organizes trainings around the country on cyber security-related topics. However, as stated above, the biggest impediments for cyber security advancement are general budget constraints.

Mauritius is no different to many modernizing nations and suffers from a wide range of cyber incidents. Cyber incidents, including cyber crime, experienced in Mauritius include hacked accounts, website defacements, ransomware, and faked accounts. Tools which are used to monitor these trends include internally developed incident management software. The most significant cyber incident which took place in the past year was the defacement of websites. Unfortunately, the perpetrator of this attack was not identified and prosecuted.

Mozambique

★ Maputo

Population: 28,751,362

Internet Penetration: 7.8%

According to Mozambique authorities, the laws and regulations that govern areas related to cyber security can be found in their Electronic Transaction Act. Currently, Mozambique does not have a national CERT, an official national cyber security framework to implement international cyber security standards or an officially recognized national agency, which is responsible for cyber security.

Currently, the development of a national cyber security strategy is being discussed. The government is also in discussions to adopt personal data protection legislation. The Government of Mozambique is currently working with civil society organizations and NGOs to help educate people and raise awareness of cyber related threats and the risks associated with being online. Authorities stated that the organization in the government that has primary oversight of cyber security related issues is the National Communications Institute of Mozambique (INCM). Other major stakeholders in Mozambique include other government agencies and private sector companies. Mozambique does not yet have an established mechanism for keeping track of cyber incidents.

Nigeria

★ Abuja

Population: 186,987,563

Internet Penetration: 52.02%

According to cyber security officials, Nigeria has a newly enacted national cyber security strategy, known as the National Cyber Security Policy and National Cyber Security Strategy. This strategy helps coordinate and guide national cyber security efforts and was established on May 2015.. It is intended to manage security threats in cyberspace in line with the overall national security objective. So far, the strategy has been particularly helpful in improving Nigeria's cyber resilience. The Government of Nigeria has plans to adopt personal data protection legislation in the future and for now, cyber crime laws have been recently enacted. Nigeria's National Policy Framework seeks a harmonized security strategy, which will respond to the dynamism of the national security threat landscape. One such emergent national security threat is the risk posed by coordinated cyber attacks on national infrastructure.

The primary agencies charged with protecting against cyber crime, are the Economic and Financial Crime Commission (EFCC), the Independent Corrupt Practice and other related offences Commission (ICPC), State Security Service (SSS), and the Nigerian Police all play prominent roles in the fight against the new trend of social vice. The Nigerian Cyber Crime Act was signed into law in 2015. According to officials, the Act provides a unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes in Nigeria. This act also ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

Officials state that overall national Cyber Security efforts are led by the National Security Adviser. Other major stakeholders include government institutions as well as private sector companies. The Government of Nigeria provides strategic direction in terms overall cyber security policy.

Nigeria has established policies for investigating cyber incidents including a number of cyber crime laws, a national cyber security strategy and various policies. The Nigerian government operates a CERT with national-level responsibilities, called the Nigerian Computer Emergency Response Team (ngCERT). The ngCERT's is housed in the Office of the National Security Adviser and its primary mission is to manage the risks of cyber threats in the Nigeria's cyberspace and effectively coordinate incident response and mitigation strategies to proactively prevent cyber-attacks against Nigeria.

The main challenges the government of Nigeria facing is the general lack of awareness of cyber security measures and the risks associated with cyber crime. Nigeria does not yet have a national cyber security awareness program currently, but is working on the plans for one. While Nigeria does not yet work with civil societies/NGOs to educate and raise awareness of cyber risks, officials noted that they do have a strategy on enhancing public-private partnerships. Some universities in Nigeria currently maintain cyber security degree programs, but no national cyber security training facilities have been established. The largest impediments to cyber security improvements over the last year was public awareness. An important evolution would be for institutional stakeholders to actively take part in improving Nigeria's national cyber security posture.

Nigeria has experienced a daily increase in vulnerable Internet facing systems, mostly vulnerable to User Datagram Protocol (UDP) amplification, which increased 25% on average. The daily increase in botnet drones (zombies) is 20% on average. Web defacement of government websites by hacktivists mostly has had a 3% increase on weekly average. Phishing incidents have had an increase of 4% on daily average. Tools used are the in-house developed application called Nigerian Cyberspace Intelligent Platform.

The most significant cyber incidents which took place in Nigeria in the past year were botnet attacks and command and control systems from a foreign country used infected systems (zombies) in Nigeria to attack systems in other countries. Nigeria was able to find out who perpetrated the incident by carrying out investigation in conjunction with the affected country and engaging the ISP in Nigeria with the relevant information of the date and time of the attack to get to know command and control system and the zombie involved. For this botnet incident, the command and control system was located outside Nigeria while the individual bots (zombies) resided within Nigerian borders. A global event which has significantly affected the country's cyber security posture is the proliferation of information warfare between foreign countries.

The government works with the private sector on cyber security issues in Nigeria because the economy is driven by the private sector. Nigeria has fruitful relations with International communities when managing and responding to cyber threats, and promotes confidence building measures (CBM) and international cooperation in cyberspace by exchanging information on cyber incidents and best practices for cyber security. Multi-stakeholder engagement in Nigeria, is presently underway and is viewed as a key component to successful implementation of a national cyber security strategy.

Rwanda

★ Kigali

Population: **11,882,766**

Internet Penetration: **22.28%**

The Government of Rwanda adopted a national cyber security policy in 2015 to help safeguard government information and infrastructure against a growing number of cyber-attacks. The government is planning on establishing a specific agency to help coordinate cyber security efforts. Officials note that the new policy will help to overcome inconsistencies, incompatibilities and duplicate efforts between government agencies.

The Rwanda Development Board/ Rwanda Computer Security and Incident Response Team (Rw-CSIRT) coordinates cyber security efforts. Major stakeholders concerned for Rw-CSIRT are Rwanda Development Board (RDB) which provides financial support for Rw-CSIRT activities and operations, the Ministry of Youth and ICT which develops relevant policy and strategy for national cyber security as well as public-private institutions and IT service providers which share incident reports with Rw-CSIRT.

Rwanda operates a division which is tasked with investigating cyber crime. Under Rw-CSIRT, a dedicated directorate named "Cyber Incident Analysis" is responsible for investigating and analyzing computer security incidents. Also, the Rwanda National Police have established a specialized department in charge of digital forensics and works closely with the Rw-CSIRT in case of computer security incident.

Rwanda has an established mechanism for responding to cyber incidents and it is a CSIRT or CERT with national-level responsibilities. It is known as the Rwanda National Computer Security and Incident Response Team (Rw-CSIRT). Its operationalization was launched in 2014 and it is a national CSIRT operating at the national level and mandated to establish other sector and organizational CERTs.

As cited previously, it was established in 2014 and approved by the cabinet in April 2015. Its objectives are to build cyber security capabilities for detection, prevention and response to cyber security incidents and threats; establish an institutional framework to foster cyber - security governance and coordination ; strengthen legal and regulatory frameworks, as well as promote compliance with appropriate technical and operational security standards , promote research and development in the field of cyber security ; promote Cyber Security awareness in all sectors and at levels in order to build a culture of security within country; promote National, Regional and International Cooperation in the field of cyber security. It has been helpful in improving cyber resilience and awareness.

The major role of Government is to gather together all concerned parties to discuss and define cyber security policy and strategy regarding cyber threats problems and issues they are facing. The solutions to the problems defined in cyber security policy and strategy are mostly addressed and reflected in the national ICT policy and strategy for implementation.

In Rwanda, cyber security challenges include the lack of cyber security and information security awareness, as well as the lack of enough expertise and skills in the area of cyber security. The national cyber security awareness raising campaign is through the Rw-CSIRT, the Government established a National cyber security awareness program, and the target audience are the employees in the public and private sectors at all levels (i.e. Senior managers, middle managers and officers) and the general public using ICT services. Under this program campaign every year a program called "Cyber Security awareness week" was defined and is carried out every year.

Rwanda works with NGOs to educate and mitigate cyber risks with institutions (public and private), academia and media (Televisions, Radio and newspaper companies to raise awareness and has established cyber security education and training centers.

The biggest impediments to cyber security advancement in Rwanda in 2015 was enhancing the efficiency of the existing national CSIRT (Rw- CSIRT) and the approval by the cabinet of the establishment of an agency in charge of national cyber security.

Rwanda has experienced an increase in major threats such as the defacement of Government and private websites and malware infections attacks. The Rw-CSIRT common standards possess tools (SIEMs) and Intrusion Prevention and Detection Systems to detect and identify threats targeting critical information systems. This can be achieved through building national cyber security capabilities and expertise, establishment of right policies and procedures to handle cyber security incidents, development of right tools (technologies) and build information sharing platforms.

The most significant cyber incident, which took place in the country in the past year was a malware outbreak attack. Rwanda was able to find out the perpetrator of the incident through detailed analysis and investigation of compromised computers. The perpetrators were located outside of the country. It has been stated that no global events have significantly affected the country's cyber security posture or development of cyber security capacities.

The government of Rwanda works with the private sector on cyber security issues. The Government believes that, to be successful in cyber security, the Government should collaborate with the private sector, and this is one of major policy areas in the National Cyber security policy approved recently. Rwanda has been able to been able to establish fruitful working relationships with other countries when managing and responding to cyber security threats. Through RW-CSIRT and Rwanda National Police, in case of computer incident, our country collaborates with other National CERTs and INTERPOL to locate and identify the perpetrator. The government of Rwanda has a partnership with global cyber security organization such as IMPACT and other national CERTs.

Senegal

★ Dakar

Population: 15,589,485

Internet Penetration: 55.19%

In January 2016, Senegal organized a Cyber Security Maturity Review with support from the Netherlands as well as the International Telecommunications Union (ITU) as part of the GFCE Cyber Security Awareness Initiative. Global Cyber Security Capacity Centre (GCSCC) and University of Oxford conducted the review and was based on the Centre's Cyber Security Capacity Maturity Model. The review is an effort by Senegal to reduce its vulnerabilities to cyber threats and to improve national coordination of cyber security.

Senegal aims to strengthen its cyber security capacity in order to reap benefits from a growing internet economy and IT sector. In order to achieve this, Senegal is planning to develop a National Cyber Security Strategy, establish a National Cyber Security Centre and allocate a budget for cyber security. As part of the GFCE initiative the Dutch support will focus on the National Cyber Security Strategy and ITU on the National Cyber Security Centre, while the GCSCC will provide wider recommendations across the different dimensions of cyber security.

With regard to national organizations, Senegal maintains a division to investigate cyber crimes within the Interior Ministry National Police, called Cell Investigations Cyber Crime Unit. The institution in Senegal which has oversight over cyber security issues also resides is the Ministry of Interior. Other major stakeholders concerned include the Intelligence Agency, a specialized branch within the National Police that focuses on cyber crime.

Somalia

★ Mogadishu

Population: 11,079,013

Internet Penetration: 6.24%

Somalia has experienced an increase in the number of cyber incidents at a rate of 80% and this has mostly been because of increased hacking of government emails and websites. At this time, there are no tools in place to help monitor these trends. The most significant cyber incidents over the last year has been hacking emails, destroying data, and changing passwords. The perpetrators of the incidents were never identified or prosecuted. The evidence in the case suggest that the perpetrators are located both within and outside of Somalia.

Authorities state that the Ministry of Post & Telecommunications has primary oversight over cyber security related issues. Other major stakeholder include additional Somali government agencies. At this time, the country of Somalia does not maintain a division specially tasked to investigate cyber crimes, and all cyber-related issues are handled through the Ministry of Post & Telecommunications.

Somalia does not yet have an established mechanism for responding to cyber incidents and the government has not established a CERT with national-level responsibilities. While officials note that Somalia does not have a national policy that guides and coordinates cyber security efforts yet, there are priorities and objectives in mind around cyber security. The government has not adopted personal data protection legislation but it plans to do so in the near future.

The role and responsibility of the government is to fight the national cyber crimes, and by implementing a national cyber security strategy there will be full control and command of the national strategy with only one gateway.

The main challenge that the government of Somalia has faced in the process of cyber security is the general lack of public awareness. In addition, there is no national cyber security awareness campaign in place. The government has considered launching and initiative but the plan is not yet fully implemented.

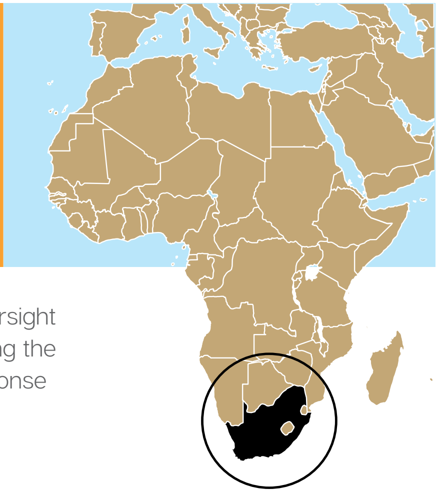
Somalia has not yet begun to partner with the private sector with regard to cyber security issues. However, the Government of Somalia has been able to establish excellent working relationships with other countries when managing and responding to specific cyber security threats.

South Africa

★ Pretoria, Cape Town, Bloemfontein

Population: 54,978,907

Internet Penetration: 53.25%



Cyber Security efforts in South Africa are led by the Cyber Response Committee, which has oversight under the State Security Agency. The Cyber Response Committee is responsible for implementing the cyber initiatives of South Africa. Other major role-players represented on the interim Cyber Response Committee are:

- **The State Security Agency**, who is responsible for the practical administration of the Cyber Response Committee and implementing the cyber security initiatives of the Republic pending promotion of comprehensive legislation dealing with various aspects of cyber security and cyber crime.
- **The Department of Telecommunications and Postal Services**, who is responsible in establishing a cyber hub which act as a nexus between government and the public sector in matters relating to cyber security. The Department also in general promotes initiatives to users of Information and Communications Technologies relating to aspects of cyber security.
- **The Department of International Relations and Cooperation**, who is responsible for the formulation, coordination, implementation and managing of South Africa's foreign policy and international relations specific to cyber security.
- **The South African Police Service**, who is responsible for dealing with aspects relating to the investigation of cyber crimes and training of law enforcement agencies to deal with cyber crime investigations.
- **The Department of Science and Technology**, who is responsible for the development and implementation of a research and development plan in order to promote the necessary skills in the Republic to deal with cyber aspects.
- **Department of Defence**, who is responsible for development and implementation of the cyber offensive and defensive capabilities of the Republic.
- **Department of Justice and Constitutional Development**, who is responsible for the drafting of legislation.

With regard to cyber crime, the Directorate for Priority Crime Investigation (DPCI) investigates organized crime, economic crime, corruption, and other serious crimes. The DPCI has their own cyber capacity to support their investigations. Other divisions in the South African Police Service, which investigate other crimes have similar support and are known as the Minister of Police.

Mechanisms, procedures, and policies for responding to cyber incidents are currently being developed as part of implementing our cyber security policy framework, named the National Cyber Security Policy Framework (NCPF). CERT is currently being developed as part of implementing our NCPF. The Cyber Hub is the first of these CERT structures to be implemented. Website: https://www.cybersecurityhub.co.za/

South Africa has a national policy to guide and coordinate cyber efforts, called the National Cyber Security Policy Framework NCPF. The NCPF was approved by the Cabinet in 2012 and is still in the process of being fully implemented. In short, the NCPF articulates the strategic priorities that will be pursued to achieve these objectives and it is expected that the NCPF will facilitate the following:

A. Centralising coordination of cyber security activities by facilitating the establishment of relevant structures, policy frameworks and strategies in support of cyber security in order to combat cyber crime, address national security imperatives and enhance the information society and knowledge-based economy.

B. The anticipation and confrontation of emerging cyber threats and coordinate responses thereto, by reducing cyber threats and vulnerabilities through technical measures, cyber crime policy and strategies, regulatory measures, general awareness and legal measures.

C. The enhancement of all substantive and procedural laws which may impact on cyber crime and cyber security.

D. The fostering of cooperation and coordination between Government, the private sector and civil society by stimulating and fostering a strong interplay between policy, legislation, societal acceptance and technology.

E. The promotion of international cooperation.

F. The development of skills, research and capacity in order to deal with cyber security.

G. The promotion of a culture of cyber security.

H. The promotion of compliance with appropriate technical and operational cyber security standards.

The NCPF is in the process of being implemented. The effect of the NCPF is that Government has become more focused on aspects relating to cyber crime and cyber security.

Comprehensive personal data protection legislation, in the form of the Protection of Personal Information Act, 2013 (Act 4 of 2013) (the POPIA), was adopted by Parliament in 2013 and is in the process of being implemented. The POPIA aims to promote the protection of personal information processed by public and private bodies; introduces conditions so as to establish minimum requirements for the processing of personal information; provides for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; provides for the issuing of codes of conduct; provides for the rights of persons regarding unsolicited electronic communications and automated decision making; regulates the flow of personal information across the borders of the Republic; and provides for matters connected therewith.

- In terms of the NCPF Government must implement the NCPF and to that extend provides for:
- The development and implementation of a Government led, coherent and integrated cyber security approach to address Cyber Security threats;
- Establishing a dedicated policy, strategy and decision making body to be known as the JCPS Cyber Security Response Committee, to identify and prioritise areas of intervention and focussed attention regarding cyber security related threats. The Cyber Security Response Committee will be chaired by the State Security Agency (SSA) and will be supported operationally by a Cyber Security Centre, situated at the SSA;
- The capability to effectively coordinate departmental resources in the achievement of common cyber security safety and security objectives (including the planning, response coordination and monitoring and evaluation);
- Fighting cyber crime effectively through the promotion of coordinated approaches and planning and the creation of required staffing and infrastructure;
- Coordination of the promotion of cyber security measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to cyber security threats, through interaction with and in conjunction with the Cyber Security Hub (to be established within the Department of Communications);
- Strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cyber crime, cyberterrorism and cyberwarfare;

- Ensuring of the protection of national critical informationinfrastructure;
- The promotion of a cyber security culture and compliance with minimum security standards;
- The establishment of public-private partnerships for national and action plans in line with the NCPF.
- A comprehensive legal framework governing cyberspace.

With regard to challenges, like most countries, South Africa does not have the necessary capacity to comprehensively implement its cyber security strategy. Capital to fund projects needs to compete with other more pressing priorities. In addition, policy decision makers in Government do not give adequate attention to this aspect.

A comprehensive cyber awareness campaign is currently being developed. The Cyber Hub has implemented certain measures to deal with awareness-raising relating to cyber security under the public. Other Departments, for instance the Films and Publications Board are also involved in awareness raising initiatives which mostly relate to child harm content over the Internet. The Department of Justice and Constitutional Development has also taken certain measures to make the public aware of electronic harassment and what remedies are available to the victims of cyber harassment. Various NGOs and electronic communications service providers are also involved in various initiatives in order to make the public aware of cyber risks and how they can protect themselves against such risks.

South Africa does not work with civil society organizations or NGOs, but a in terms of the comprehensive awareness campaign, which is being developed, this will be addressed. Universities do maintain cyber security programs. A police college provides training to the South African Police Service and has included specific training relating to cyber crime investigation in their curriculum. Justice College provides training to prosecutors and has included aspects relating to the prosecution of cyber crimes in its curriculum. The South African Judicial Training Institute, which provides training to judges and magistrates has also included specific training in it's curriculum relating to cyber crime and the evaluation of electronic evidence. External service providers are used to provide advanced training to Government.

The biggest impediments is probably the slow pace at which the NCPF is implemented and the unavailability of resources and capacity. The most important evolution is probably the Draft Cyber Crimes and Cyber security Bill which was published for comment and which will be introduced in Parliament during the course of 2016.

Information received from the financial sector indicates that cyber crimes, which has a financial aspect, has substantially increased during 2015. Incidents reported to the South African Police Service indicates that cryptolocker extortion, marketing fraud and ATM intrusion, mobile banking related crimes and card fraud showed a significant increase. Phishing attempts and denial of service attacks also showed a substantial increase. No other verifiable statistics are available to substantiate non-financial based cyber crimes such as unlawful access, interference with data, interference with a computer system etc. However, various companies which deals with cyber security indicated that there is an overall increase in the afore-mentioned crimes.

Financial cyber crime is based on complaints to financial institutions and reports to the South African Police Services. Security firms make information available in the media from time to time which is an indication of prevalent trends in cyber crime. The Cyber Hub, established in terms of the NCPF also collects statistics relating to cyber incidents.

The Cyber Crimes Bill aims to comprehensively address aspects relating to cyber crimes and cyber security in the Republic and updates the Statute Book in line with that of other countries. Various other laws, namely those dealing with Intellectual Property protection and the protection of children in cyberspace are in the process of being revised. The judiciary is in the process of being trained to deal with cyber crime cases. Prosecutors and the South African Police Service also receive additional training to deal with the investigation and prosecution of cyber crimes.

Significant Cyber Crimes:

- **Gautrain incident:** Computer-related theft/fraud committed by a group of persons. There was insider collusion with IT persons working for company. Value of potential loss was in the region of R800 Million.
- **Eskom incident:** Attempted computer-related theft/fraud committed by a group of persons. There was insider collusion with IT persons working for company. Value of potential loss was in the region Value of potential loss R3.5 Billion.
- **Telesure incident:** Relates to ransomware. Potential loss in the region of R20 Million. Perpetrated by a group of persons.

Various incidents of computer-related theft/fraud with individual values in the region of R1 Million to R3 Million.

Various incidents of phishing, DDOS attacks and crypto extortion also took place. Arrest have been made in the Gautrain, Eskom and Telesure incidents. The South African Police worked closely with the affected parties to investigate the incidents. Some of the suspects are still at large. The South African Police Service were less successful in the investigation of the less serious cases. In the Telesure incident actors from outside the country were involved and have not yet been apprehended. External perpetrators may also have been involved in the Gautrain and Eskom cases but were not yet identified.

The international impact of cyber crimes and the effect to cyber attacks on a country, directly relate to the adoption of the initiative by the Republic to deal with cyber security. The international trends to adopt cyber specific legislation played a significant role in the updating of our cyber laws. The African Union Convention on Cyber Security and Personal Data Protection also influenced the updating of our laws relating to protection of personal information and cyber crimes. The Republic participated in the Glacy initiative, which is sponsored by the Council of Europe in order to receive training for the South African Police Service, prosecutors and the judiciary.

Currently there is no extensive co-operation between Government and the private sector on cyber security issues. The private sector has the necessary capacity to deal with most cyber security issues. In terms of the NCPF cooperation between Government and the private sector need to take place. Measures will in the future be implemented to provide for closer cooperation between Government and the private sector regarding cyber security. Cyber security only came to the forefront relatively recently by the adoption of the NCPF.

Through the Mutual Legal Assistance procedure and the South African Point of Contact, cooperation is provided to other countries relating to cyber crime. In the BRICS initiative, avenues are explored to deal with co-operation on cyber-related matters. CBM is being developed as part of the implementation of the NCPF.

It is imperative when a country develop its cyber security strategy that all role-players be involved and that an open and participating process be followed. The priorities of Government and the private sector differs and any strategy should realise this

- A cyber security strategy should be adoptable.
- The costs involved to come to grips with cyber security is extensive and usually always compete with other priorities in a developing country.
- South Africa, like most other countries in Africa does not have the necessary capacity to comprehensively deal with cyber security. Special initiatives should be promoted by government in order to ensure capacity building and adequate funding should be made available.
- Follow an incremental approach when implementing a cyber security strategy, by concentrating on the aspects, which need to be addressed on an urgent basis and then deal with less serious aspects.

Sudan

★ Khartoum

Population: **41,175,541**

Internet Penetration: **33.18%**

One of the key cyber security challenges facing the government of Sudan is the development and implementation of a comprehensive cyber security framework. Authorities noted that it will be a key method for managing cyber risk in the future. The biggest impediments to Sudan's cyber security advancement this year is working towards strengthening cyber security by expanding cyber education and awareness. This can be done by coordinating and redirecting research and development efforts across the Government.

The Government of Sudan is currently working on a national policy to coordinate cyber security efforts and the government has plans to adopt a personal data protection legislation in the near future. In the meantime, Sudan has established mechanisms for responding to cyber incidents and the government operates a CSIRT or CERT with national-level responsibilities, called Sudan-CERT. The Sudan-CERT was founded in 2010. In addition, Sudan has taken into consideration the ITU framework on cyber security, programme 3 on cyber crime fighting procedures and ITU-IMPACT global cyber security agenda in building a cyber security approach. This programme led to a number of achievements, including the establishment of Sudan-CERT. This was achieved by an initiative of the National Telecommunication Corporation, the telecom regulatory authority in Sudan created to enhance information and network security throughout Sudan. In 2014, Sudan-CERT handled 150 e-crime cases with social media crimes making up 85%. Sudan-CERT has bilateral relations with a number of National CERTs globally.

Cyber security efforts in Sudan are led by the Sudan-CERT. Other major stakeholders involved are the government sector and the private sector as both parties work together in order to build mutual understanding and improve cyber security. According to officials, Sudan-CERT is the division of the government that is specifically tasked with investigating cyber crimes.

Sudan has experienced an increase in the number of cyber incidents in the past year and uses a number of cyber security technologies to track and monitor these illicit activities. The most significant cyber incident which took place in Sudan last year was resource misconfiguration and abuses as well as network and resource abuses. Sudan was able to find out who perpetrated the incident and according to the evidence the actors who perpetrated the incident were located outside the country.

Notably, Sudan has been able to establish a number of fruitful working relationships with other countries when managing and responding to cyber security threats and promotes confidence building measures (CBM) and international cooperation in cyberspace by exchanging information on cyber incidents and best practices for cyber security.

Togo

★ Lomé

Population: 7,496,833

Internet Penetration: 5.31%

Within the Government of Togo, the oversight of issues pertaining to cyber security are led by the Regulator of Post and Telecommunications (ART & P). The ARTP is charged with regulating cyber security, investigate cyber crime and the creating the National CERT. Other stakeholders include the General Directorate of the Nation Police for the Suppression of cyber criminals, and the Justice department.

According to officials the Government of Togo maintains a division specially tasked to investigate cyber crimes within the Information and Communication Technologies Agency (CLCTIC) that is under the Ministry of Security and Civil Protection. While the Government has not developed a national CERT, there is currently a proposal being considered under an initiative by the Ministry of Post and Digital Economy.

Some of the biggest challenges encountered in Togo is the process of identifying and recruiting all of the cyber security stakeholders to participate in improving cyber security. Officials noted that there is no national cyber security awareness raising campaign in place at this time. However, awareness projects are under consideration. Universities in Togo do maintain a number of cyber security related degree programs. The biggest impediment to cyber security advancement that was identified is the lack of awareness about the importance of cyber security and the dangers of cyber crime.

Togo has experienced an increase in the number of cyber incidents including many web defacement attacks and intrusion into computer systems using brute force techniques. The government of Togo works in conjunction with several private sector players on cyber security issues. The government considers that involvement of all stakeholders in the process is the best guarantee against cyber crime. Togo does promote confidence building measures (CBM) by exchanging information on cyber incidents and best practices for cyber security.

Tunisia

★ Tunis

Population: 11,375,220

Internet Penetration: 53.22%

Tunisian officials noted that the institution that leads and maintains oversight over cyber security issues in Tunisia is known as ANSI/ATT (http://www.ansi.tn/fr/documents/loi_05-2004_fr.pdf). Another major stakeholder is the Ministry of Communication Technologies and the Digital Economy.

The Government of Tunisia has established mechanisms, procedures, and policies for responding to cyber incidents. In particular, Tunisia operates a CERT with national-level responsibilities, called tunCERT. The country has a national policy that coordinates cyber security efforts that has been in existence since 2002 and is called the National Trust in Cyberspace. The policy includes efforts to create more robust national information systems, legal aspects and strengthening the Tunisian cyber security workforce.

The main issues facing the Government of Tunisia in the process of implementing a national cyber security strategy are various cultural aspects. Tunisia has a national cyber security awareness campaign, for example it has one for children known as COP. Tunisia works with NGOs and civil society organizations in order to raise awareness about cyber risks. In addition, ANSI periodically organizes and conducts high level training courses for Tunisian professionals (both public and private). The biggest impediments to cyber security advancement are the cumbersome processes regarding the security of the cloud. In Tunisia, the private sector works with the government through the FIRST network. Tunisia has experienced an increase in the number of cyber incidents over the last year and monitors these incidents through a platform called SAHER.

Zambia

★ Lusaka

Population: **16,717,332**

Internet Penetration: **21.98%**

Cyber security efforts in Zambia are led by the Zambia Information and Communications Technology Authority. The national cyber security strategy implemented by ZICTA is focused on strengthening legislation around cyber security to respond to emerging trends. Other major stakeholders include the Government, security wings, and law enforcement agencies, ICT operator (providers), consumers (general public), business enterprises, financial institutions and the general public. Officials noted that the Government of Zambia maintains a division, which is specially tasked with investigating cyber crimes, named ZM-CIRT and it is part of the Ministry of Transport and Communications. The ZM-CIRT (www.cirt.zm/) exists with national-level responsibilities and was founded in 2012

Zambia has not yet developed and implemented a national policy or strategy that guides and coordinates cyber security efforts. They have, however, developed a draft strategy, which is yet to be approved. The government has adopted personal data protection legislation called the Electronic Communications and Transaction Act of 2009. The Government of Zambia is currently in the process of developing additional legislation to strengthen the current law, as recommended by the SADC cyber law model. With regard to the development and implementation of a cyber security strategy, officials observed that the role of the government is to develop policy and ensure compliance, implementation and monitoring.

The main challenges the government has faced in the process of development and implementation of a national cyber security strategy is the long and arduous process of developing and adopting laws. Zambia does not have a national cyber security awareness raising campaign but authorities note that they begun the initial stages of development. However, other campaigns driven by the Regulators currently exist such as: Train the trainer 2015 targeted at teachers, Child Online Protection 2015 as well as ad hoc awareness initiatives with government agencies and law enforcement agencies last conducted in 2012.

The Government of Zambia works with civil society organizations to educate and raise awareness about cyber risks. In addition, although there are no government established cyber security education training centers, a few universities in Zambia have started offering cyber security degree programs. Officials identified the greatest impediments for cyber security advancement were limited funding as well as limited numbers of qualified staff who are proficient in cyber security issues working in the ZM-CIRT. An important evolution has been the growing appreciation of cyber security issues at the national level.

In the past year, Zambia has experienced an increase in the number of cyber incidents mainly in ransomware attacks, email scams, identity theft and website hacking. The tools used to monitor these statistics and trends are the honey-pot networks and digital forensics services. Thus, illicit cyber activities have been met with the awareness programs indicated above as well as professional training for identified stakeholders such as government agencies or critical infrastructure providers from the ZM-CIRT team.

The most significant cyber incidents, which took place in Zambia last year were a series of ransomware attacks and email scams. In many cases, the perpetrators of the attack were revealed through digital forensics, and evidence indicated that the perpetrators were local.

A global event, which has significantly affected Zambia's cyber security posture is the AU Convention on Cyber Crime. The government of Zambia works with the private sector on a number of cyber security issues. This is due to the awareness programs in place and consumer protection issues that arise with regard to cyber security issues. Zambia has been able to establish constructive relationships with other countries when managing and responding to cyber threats. Zambia has also worked closely with the Mauritius-CIRT in providing technical support and in relation to ITU's setting up of CIRT. The Government of Zambia also promotes confidence building measures and international cooperation in cyberspace by exchanging information on cyber incidents and best practices for cyber security. In working with Africa CIRT as well as Mauritius and in the process of becoming affiliated with the Forum for Incident Response Team (FIRST), a global team of incident responders, the country of Zambia has become more open to partnerships in the future including at African Union level.

CREDITS

Head of Information Society Division

Moctar Yedaly

Senior Radio Transmission and Broadcasting Officer | Infrastructure and Energy Department

Souhila Amazouz

Senior Policy Officer | Infrastructure and Energy Division

Auguste K. Yankey

Director, Government Affairs & Senior Policy Counsel

Bill Wright

Graphics and Design

Scott Wallace

Contributing Editors

Shireen Alam

Jared Schober

Data Analyst

Ben Nahorney

11/16

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

ABOUT SYMANTEC

Symantec Corporation is the global leader in cyber security. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

MORE INFORMATION

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/

Symantec™

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.