Survey of African Infrastructure for Amplified DDoS, Spam, and Storm Botnet Command & Control

Frank S. Rietta, Seymour Goodman
College of Computing, Georgia Institute of Technology
19 December 2007

Abstract

This paper is a survey of the current status of network infrastructure security throughout Africa, based on three IPv4 studies. It will first give an overview of the regional efforts to expand internet access for the purpose of educational, private sector, and government development. It then looks at the size and scope of the malicious infrastructure already existent on the continent, with a particular focus on the enhanced DDoS potential caused by the exponential increase in the number of open recursive DNS resolvers, along with the relationship between spammer activity and the Storm/Peacomm botnet. Finally, it will give some recommendations of how improved ICT policy may reduce some of the security risks, particularly as IP-based networks increasingly converge with mobile networks.

1 Introduction

1.1 Internet Role for Economic Development

Africa is one of the last frontiers of internet connectivity, and some of its regions are posed to jump onto the latest IP-based data and voice communication networks. AfriNIC, the principle ICCAN Regional Internet Registry, held a conference in September 2007 that was attended by one hundred fifty delegates from thirty-five countries. The primary thrust of the conference was the importance of expanding internet access as a key component for economic and social development. A major technical focus of the conference was an effort to switch to IPv6 technology immediately, and subsequently leap ahead of other parts of the world that are currently struggling with the migration.

Expanding ICT infrastructure includes efforts to transition from Very Small Aperture Terminal (VSAT), small two-way satellite ground stations links to fiber-optic connections. The new connections have led to faster and cheaper network infrastructure in Algeria, Egypt, Morocco, Nigeria, and other countries. Most ICT expansion efforts have not had a strong security-related component [4].

Some countries have emphasized the importance of security in their ICT expansion efforts. Algeria and Tunisia have instituted public organizations tasked with encouraging ICT security within their jurisdictions. Algeria has implemented a Computer Security Incident Response Team (CSIRT), and Tunisia created a Computer Emergency Response Team (CERT). Egypt does not have a CERT, but it has implemented a nation-wide Public Key Infrastructure, based on its e-signature law, with an emphasis on supporting future e-business development [4]. Many countries are considering instituting regionally harmonized basic cyber crime laws. Some of these nations, including Nigeria and Ghana, are also establishing cyber crime units within their law enforcement agencies.

It is commonly accepted that increased emphasis on ICT plays an important role in economic development. Some major international efforts are underway to provide more access to computers for people living in developing countries. Perhaps the most well known effort is the One Laptop per Child Project (OLPC). This project will provide laptops designed to run under the harsh conditions found in many villages, and each will cost only $150 (US). Lenovo, a Chinese laptop manufacturer, along with Microsoft have started a competing effort, offering software based on a $3 (US) software bundle from Microsoft's Unlimited Potential program [5].

More people throughout Africa are beginning to access the internet through computers and IP-enabled mobile devices. They will be increasingly exposed to fraud through cyber crime. Additionally, as the ICT infrastructure grows, there will be an increase in resources available to cyber criminals, allowing them to expand their malicious efforts.

The rest of this paper will examine a part of the malicious infrastructure already in place. One need only imagine how much worse things might be, if additional security precautions are not implemented as an integral part of the ICT improvement process.

1.2 Important Regional Differences

When studying the role that expanded ICT infrastructure may play in economic and social development, one must consider the various states of development found within Africa. The continent is divided into fifty-three independent countries, each with significant variances in the availability of natural resources, the degree of economic liberty, and the level of armed conflict. The United Nations categorizes the various countries in five regions: Eastern, Middle, Northern, Southern, and Western. Within these regions are significant disparities in development that determine the short-term benefits that the people will receive from improved ICT infrastructure. Consider the following regional facts pulled from Table 4.

Eastern

- **Literacy Rate**
  - Highest: Seychelles, 92%
  - Lowest: Somalia, 38%
- **Internet Access Rate**
  - Highest: Seychelles, 24%
  - Lowest: Malawi; Comoros; Somalia, < 1%
- **Cell Phone Usage Rate**
  - Highest: Seychelles, 70%
  - Lowest: Ethiopia, < 1%
- **Purchasing Power Parity**
  - Highest: Mauritius, $13700
  - Lowest: Malawi; Comoros; Somalia, $600

Middle

- **Literacy Rate**
  - Highest: Equatorial Guinea, 86%
  - Lowest: Chad, 48%
- **Internet Access Rate**
  - Highest: Sao Tome & Principe, 10%
  - Lowest: Central African Republic; Democratic Republic of the Congo, < 1%
- **Cell Phone Usage Rate**
  - Highest: Gabon, 45%
  - Lowest: Central African Republic, 1%
- **Purchasing Power Parity**
  - Highest: Equatorial Guinea, $50200[1]
  - Lowest: Democratic Republic of the Congo, $700

[1] The PPP in Equatorial Guinea has increased significantly since the discovery of major oil reserves. It is now the third-largest producer in sub-Saharan Africa and derives most of its revenue from oil exports. 6. Blum, J. *U.S. Oil Firms Entwined in Equatorial Guinea Deals*. 2004 [cited 2007 Nov 15]; Available from: http://www.washingtonpost.com/wp-dyn/articles/A1101-2004Sep6.html..

Northern

- **Literacy Rate**
  - Highest: Libya, 83%
  - Lowest: Morocco, 52%
- **Internet Access Rate**
  - Highest: Morocco, 14%
  - Lowest: Libya, 3%
- **Cell Phone Usage Rate**
  - Highest: Tunisia, 55%
  - Lowest: Libya, 4%
- **Purchasing Power Parity**
  - Highest: Libya, $12300
  - Lowest: Sudan, $2400

Southern

- **Literacy Rate**
  - Highest: South Africa, 87%
  - Lowest: Botswana, 81%
- **Internet Access Rate**
  - Highest: South Africa, 12%
  - Lowest: Lesotho, 2%
- **Cell Phone Usage Rate**
  - Highest: South Africa, 77%
  - Lowest: Lesotho, 12%
- **Purchasing Power Parity**
  - Highest: South Africa, $13300
  - Lowest: Lesotho, $2600

Western

- **Literacy Rate**
  - Highest: Cape Verde, 77%
  - Lowest: Burkina Faso, 22%
- **Internet Access Rate**
  - Highest: Cape Verde, 6%
  - Lowest: Liberia, < 1%
- **Cell Phone Usage Rate**
  - Highest: Mauritania, 23%
  - Lowest: Sierra Leone, 2%
- **Purchasing Power Parity**
  - Highest: Cape Verde, $6000
  - Lowest: Liberia; Guinea-Bissau; Sierra Leone, $900

Table 1: For each African region, the highest and lowest performers in key indicator statistics that may shed light on expected ICT usage. One would expect that more people benefit from internet access in countries with higher literacy rates and purchasing power parity. ***Data Source: Table 4***

1.3 Open Recursive DNS Servers

The worldwide Domain Name System (DNS) is a large, distributed, hierarchical database designed to make the conversion of domain names to IP address numbers efficient on the internet-scale. The system plays an essential role in the operation of nearly all IP-based networks. For every domain on the internet, at least two DNS servers are indicated as being authoritative. When an internet user wishes to visit a particular internet host, his computer will typically contact a DNS recursive resolver provided by his network. The resolver will then follow the DNS resolution path until it can return an authoritative answer to the query.

There are four general types of DNS resolvers:

- Open recursive resolvers that provide open access to a full resolver [7].
- Open forwarding resolvers that proxy access to a full resolver [7].
- Open caching servers that have recursion disabled, but still provide access to temporarily mirrored entries [7].
- Restricted resolvers provide access to authoritative data [7].

A DNS resolver is said to be open recursive when it will non-authoritatively answer queries from any host on the internet, regardless of the query's network of origin. Under current best practices, it is strongly suggested that network operators should configure their DNS servers to only answer queries from hosts within their own network [8]. In section 2, this paper will discuss the results of the IPv4 Open Recursive DNS Resolver Survey, showing that the number of these servers has jumped significantly in Africa in the last year. Between January 2006 and August 2007, the number of open recursive resolvers increased by about 3800% in South Africa, 3163% in Egypt, 8014% in Algeria, and 1103% in Morocco. The resolver population grew in every African country except for Sao Tome and Principe, which now only has two (Table 1). The rate of increase well outpaces the needs of the markets in these countries and is indicative of a rise of world-wide malicious resolution authorities [7].

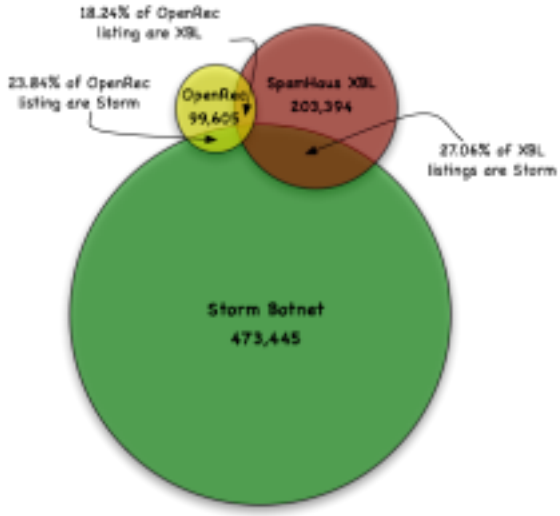

Figure 1: Summary of the unique African IPv4 addresses observed between 2007-02-09 and 2007-10-01. 473,445 were observed in the Storm botnet. 203,394 were listed at some time in the SpamHaus Exploit Block List (XBL). 99,605 responded to DNS queries. [1-3].

1.4 The SpamHaus XBL

The SpamHaus Project Ltd publishes a list of actively exploited hosts throughout the internet called the XBL Advisory, which is a real-time database containing the IP addresses of illegal third-party exploits, including open proxies, worms/viruses with built-in spam engines, and other types of trojan-horse exploits [9]. For this research, a data feed subscription was maintained, from which daily XBL listing updates were downloaded and logged into a long-term historical database [3]. As with the Open Recursive Resolver and Storm/Peacomm studies, a major

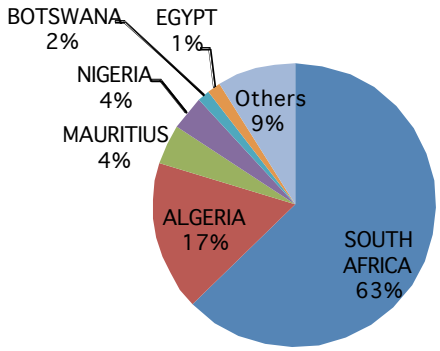

Figure 2: Summary of the top African countries that the SpamHaus XBL has listed as sending spam and being infecting with malware. *Source: Table 3.*

commercial IP-to-location database was used to determine which country each XBL-listed IP address belonged to.

The purpose of the XBL feed is to provide a source of independent baseline statistics on malware activity within the network infrastructures of the various African countries. Consider the chart in Figure 2. During the study period between February 9th and October 1st, South Africa was home to 63% of the unique IPv4 addresses listed at any time in the XBL. Algeria was second in line, housing 17% of the listed unique hosts.

As seen in Figure 1, XBL-listed hosts significantly overlap the open recursive resolver population and the enormous Storm/Peacomm botnet. The full breakdown of the XBL-listed hosts and the amount of overlap with the Storm/Peacomm botnet can be found in Table 2 in the Data Tables section of this paper.

1.5 The Storm/Peacomm Botnet

The Storm botnet, also referred to within the security research community as Peacomm or Zhelatin, is a massive worldwide network of compromised computer systems coordinated over a peer-to-peer command and control network based on Overnet. It is the same protocol that was used by the once popular e-Donkey file-sharing network. The Storm botnet first began appearing in the beginning of 2007 and is considered, by some prominent experts, to represent the future of malware [10, 11]. Between February and September 2007, 473445 unique African IPv4 addresses were observed to be participating in the Storm botnet.

1.6 Review of Distributed Denial of Service Attack Methods

In general, there are two methods of DDoS commonly used today that make use of botnets. The infrastructure necessary to either conduct or support these attacks is already present within the African IP space. In a direct DDoS attack (see Figure 3) the adversary uses an army of compromised computer systems to flood the targeted victim with voluminous amounts of unsolicited network traffic. This classic attack is well documented [12].

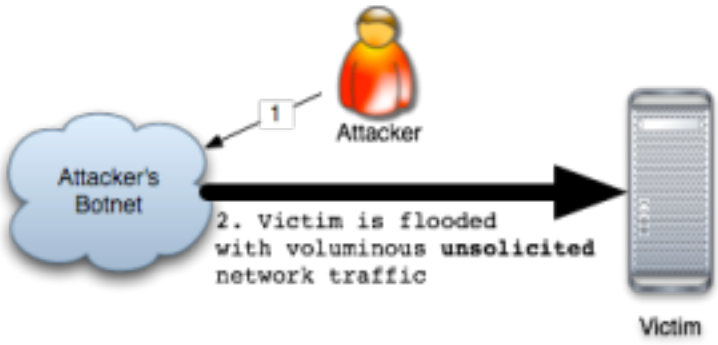

Figure 3: In a direct attack, the adversary uses a botnet to send traffic to the victim.

In a DNS amplified denial of service attack, (see Figure 4) the adversary uses an army of open recursive DNS resolvers to flood the victim with traffic. It is called an amplification attack, because a repeated small, spoofed request to a DNS server can result in a significantly larger response packet travelling to the victim from high-bandwidth DNS servers. In an extreme amplified attack, see Figure 5, a single response packet of about 60 bytes can trigger the delivery of a DNS response message of 4,000 bytes to the victim - roughly a seventy fold increase [13].

DNS amplified denial of service attacks are convenient for a malicious entity, because the schemes allow him to deliver a significant blow to his victim while remaining largely undetected. These attacks can be very dangerous; especially because:

- Any EDNS0-compatible open recursive resolver can be used [14]
- The DNS resolvers are part of the internet critical infrastructure, with access to a lot of bandwidth on major commercial and government networks [15]
- Small requests yield very large responses from these high bandwidth resolvers
- Indirect attacks help protect the privacy and integrity of the botnet nodes

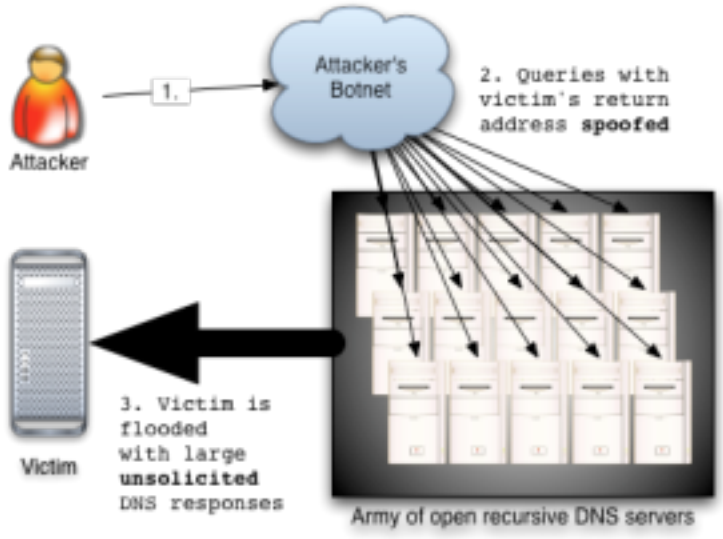

Figure 4: In an amplified attack, the adversary uses an army of open recursive DNS servers, many of which are on high bandwidth connections, to flood the victim with network traffic. The army of open recursive DNS servers is not necessarily comprised of compromised systems. The level of indirection makes it difficult for the victim network to fingerprint the botnet that is launching the attack.

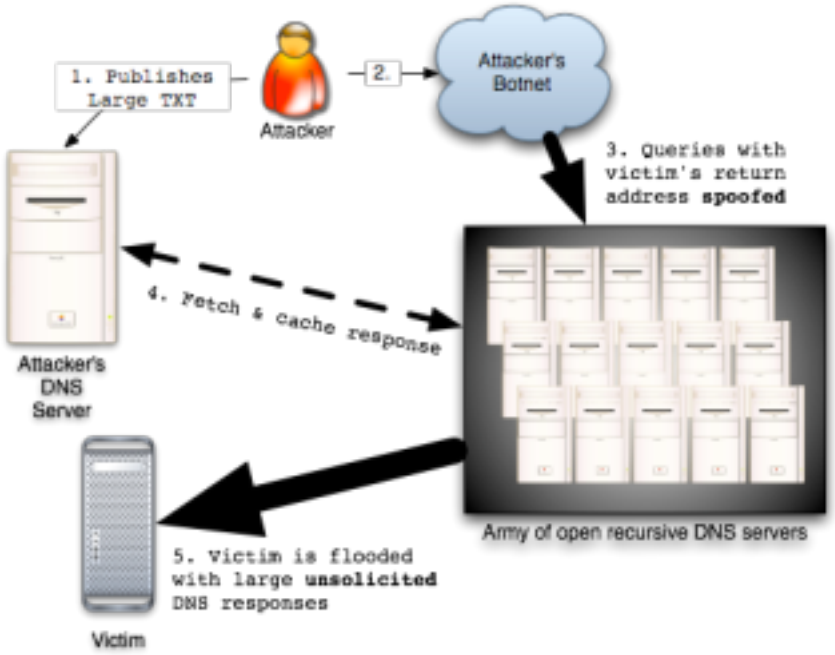

Figure 5: Similar to the amplified attack above, an extreme amplified attack uses a large TXT record to really hammer the victim because a single small request packet will result in a gigantic DNS response. The open recursive resolvers need not be malicious. Any one that supports EDNS0 and does not filter requests can be used.

2 African IPv4 Network Infrastructure Surveys

2.1 The IPv4 Open Recursive DNS Resolver Survey

An open recursive DNS resolver is any DNS server that will answer arbitrary queries from any host on the internet. There are legitimate non-malicious open recursive DNS resolvers that are configured to respond to DNS requests from any source despite the fact that this is considered bad practice. These legitimate recursive resolvers are typically operated by major internet service providers, large organizations with their own network management group, and universities. Additionally, non-malicious open recursive resolution services may be provided by small business and hobbyist server systems, because resolver software is often bundled with server operating systems such as Linux, FreeBSD, and Windows Server. However, one should not expect end-user desktop computer systems, such as those found in cyber cafés, private residences, or offices, to be providing DNS resolution services to the internet.

A large-scale survey was conducted in January 2006, and then again in August 2007, to enumerate open resolvers and identify those that are most likely providing malicious DNS services. In the study, the entire worldwide four billion address space was divided into classful addresses, excluding those that belong to U.S. Government or military networks, and non-routable addresses published in Team Cymru's list of inactive IP networks [7]. The results of these two surveys were long, separate lists of IP addresses for many DNS servers that were verified open recursive. These IP addresses were then

entered into a database to facilitate location-based research. Between the two surveys, the number of verified open recursive resolvers increased by about 3800% in South Africa, 3163% in Egypt, 8014% in Algeria, and 1103% in Morocco.

See Table 1 for a list of the number of verified open recursive servers from each study in Africa. The table is sorted by the difference between the numbers of open recursive resolvers in the two surveys. The "% Storm" column indicates the percentage of the unique IP addresses found in the August 2007 survey was also found in the survey of Storm/Peacomm botnet nodes. Similarly, the "% SpamHaus" column indicates the percentage of the unique IP addresses found in the August 2007 survey that were also found in the SpamHaus survey.

South Africa is undoubtedly on top in terms of raw numbers of open recursive resolvers. The country has the most privately owned networks of any African country. It also has a healthy broadband network infrastructure that supplies high-speed internet access to many citizen's homes and private businesses. It also has many universities and research centers. However, considering that there are only a few hundred universities and fewer than two hundred general internet service providers in the country [16], there is not a market-based explanation for the existence of nearly sixty thousand open recursive resolvers. When one further considers the prominent position that South Africa holds in the XBL, (see Figure 2) and the existence of a set of malicious hosts that have a 22% overlap with this open recursive survey set, it is most likely that these hosts are malicious resolvers installed by malware.

Egypt is home to nearly 24000 open recursive servers, 60% of which are part of the very malicious Storm/Peacomm botnet. Algeria is home to a comparably modest 4787 open recursive servers, of which almost all should be considered malicious. It is the only country among the top offenders that has a CSIRT as its national organization tasked with supporting information security efforts.

The primary take away from the open recursive resolver survey is that the number of malicious DNS servers is increasing throughout the world, not just in Africa. In light of the latest malware which changes the host resolution paths for infected computers, so that users can be more easily phished, the availability of open recursive servers threatens to create a nefarious domain authority [7].

2.2 The Storm/Peacomm Botnet Survey

The Storm/Peacomm botnet is currently considered one of, if not the, most powerful supercomputer in the world [10, 17, 18]. The Storm botnet is very large; some estimates state that the worldwide population of the botnet may be as high as 50 million nodes [17]. A survey was prepared to use a honey network to participate in the botnet in order to enumerate many of its nodes. The survey computers participated in the peer-to-peer communication network and recorded every IPv4 host that they communicated with. During the survey period between the 25th of May and the 1st of November, 473,445 unique IPv4 addresses were observed participating in the Storm/Peacomm botnet from African IP space. Figure 6 shows the time wise trend of the botnet population, during the four months of active monitoring. The botnet population exhibits cyclic periods of growth and decline, with no significant trend variance between the African and

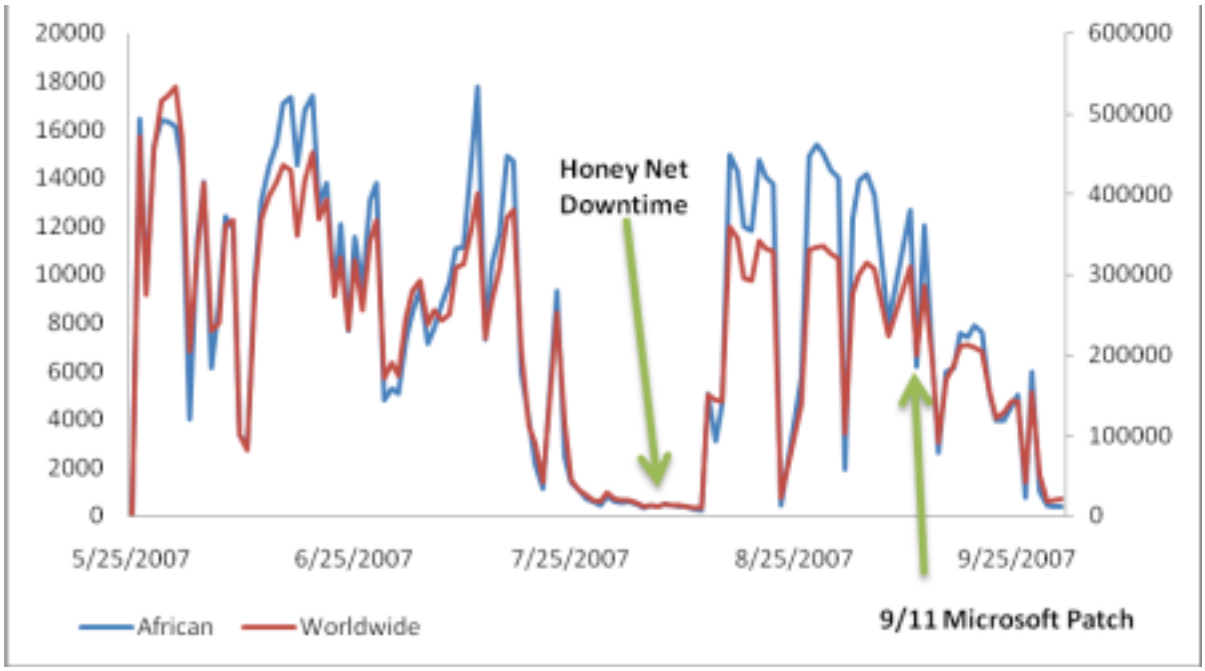

Figure 6: Number of unique IPv4 addresses participating in the botnet per day. The African hosts are plotted on the left axis and the worldwide hosts on the right axis. The anomaly in July was caused by technical difficulties with the sensor network. On September 11, 2007 Microsoft released a patch to thwart the botnet. Towards the end of the period, the count tappers off as the nodes migrated to a new encrypted protocol. A new enumeration technique will be needed to continue this research.

worldwide populations. The population grows very quickly when new spam runs infect additional computer systems with the malicious software and then. It then shrinks quickly as computers become disconnected from the network or are cleaned through security updates.

The various African countries are not homogenously participating in the Storm network. Nor is the overlap with the open recursive resolver or XBL surveys evenly distributed among the countries. The top participant in Storm/Peacomm, Egypt, has hosted 37% of the African nodes during the study period. Next is Morocco with 30% and South Africa with 15%.

Egypt is the third most literate country in Northern Africa. Internet access is abundant and cheap because of its "Subscription-Free Internet" and "PC For Every Home" initiatives, which subsidize internet access for Egyptian citizens through "a revenue sharing scheme between Egypt's national operator, leading local ISPs and traditional content providers" [19]. Many Egyptians access the internet through numerous cyber cafés, in which many computer terminals are likely infected with the Storm botnet, as per Table 2. Only one system user must execute the worm's software code for a computer system to become infected. The worm expands by sending out volumes of spam, purporting to be an electronic greeting card from a friend or an urgent news item that requires immediate attention. A significant portion, 60%, of Egypt's open recursive resolver population is composed of Storm nodes and thus undoubtedly malicious.

Morocco has the second largest Storm botnet population. It is has a solid high-speed IP-based network infrastructure and about 4.6 million people (a sizable portion of the

population) who access the internet (see Table 2). Of its open recursive resolver population, 46% are Storm (see Table 1). Algeria and Tunisia both have agencies tasked with supporting information security efforts. The Tunisian CERT issued an alert on September 17, 2007 about the Storm worm, that they call *Zhelatin.LJ*, threat [20].

The Storm/Peacomm botnet is a significant worldwide threat to the global ICT network infrastructure. Its worm continues to spread throughout the world. The reader should note that there is little significant difference in the worldwide and African trends within the botnet, except that there are fewer nodes. It represents a new class of malicious botnets that use highly resilient peer-to-peer command and control mechanisms that lack any central point of failure [11]. A method for controlling the spread of this botnet or stopping it from inflicting harm still eludes security researchers and law enforcement organizations.

3. Conclusion & Recommendations

This analysis of three IPv4 surveys of the status of information security in Africa has demonstrated that the prevalence of networked malicious software is significant even considering the modest size of the continent's growing network infrastructure. The cybersecurity threat has already been manifested. If nothing changes, the threat will likely increase as Africa continues to expand its network infrastructure in order to join the rest of the worldwide information economy through expanded use of computer systems IP-enabled mobile networks. Bandwidth costs will rise as malicious activity consumes network resources that should be used for legitimate purposes. It is imperative that additional security efforts be undertaken as an integral part of the ICT infrastructure expansion process.

More specifically, these additional security efforts should include policy efforts that:

- Continue to regionally harmonize cyber laws
- Establish regional CERT organizations
- Mandate that the CERTS, in cooperation with AfriNIC, conduct IP-based surveys

While each country has a responsibility to maintain its national sovereignty and tailor its strategies that justly promote its citizens' best interests, it is important that core cyber laws be compatible among the various countries. The East African Community (EAC) and South African Development Community (SADC) need to help spread awareness of important cybersecurity and cybercrime considerations among their members. When laws are similar throughout a region, cyber criminals have a harder time finding a safe haven in neighboring jurisdictions.

Regional CERT organizations should be established to advise more than one country on matters of cybersecurity. A regional CERT would be able to pool financial and intellectual resources to conduct comprehensive IP-space surveys looking for compromised computer systems. The CERT would then be involved with proactively contacting various network administrators to remedy any malicious network activity according to acceptable network usage policies, security procedures, and the law.

International governmental efforts to encourage improved cybersecurity should not underestimate the significance of the role that private networks and international non-

governmental organizations have to play in affecting cybersecurity. CERT efforts to conduct wide-scale security scanning and reporting should be coordinated with AfriNIC, who controls IP allocations throughout Africa. In extreme cases of abuse, AfriNIC has the capability to remove certain net-blocks from the internet by deleting the associated entries from its routing tables. Such extreme remedies can be balanced with proactive CERT notification to network administrators can go a long way to squashing malicious activity in African networks.

As a final note, this paper has focused on observations of internet connected hosts. Today these hosts largely consist of traditional computer systems either located in data centers, offices, and cyber cafes. However, in the future smart phones that connect to IP-based mobile networks will be targeted. The nature of the threats will continue to grow as critical infrastructure relies more heavily on ICT. Failure to systematically address cybersecurity, as ICT infrastructure is laid down, will likely lead to even bigger challenges in the future.

4. Related Work

Grizzard, et al, published an introduction to the new peer-based botnet rally, command, and control infrastructure that played an essential role in the organization of this research effort. This paper would not have existed without their work [11].

Tony Rutkowski has published a solid collection of cybersecurity reference materials that will be a good starting point for anyone tasked with developing national, international, or inter-organizational security policies [21].

Our research group at the Sam Nunn School of International Affairs has prepared *The Current State of Cybersecurity in Africa*. Whereas this paper has focused on technical data about malicious internet activity in Africa, the report takes a more holistic view of the status of cybersecurity.

5. Acknowledgements

This research was greatly supported by data that was collected by David Dagon, Robert Edmonds, and Christopher Lee with the Georgia Institute of Technology. They were each extremely helpful in both supplying raw data and discussing ideas. Kristina Cole provided excellent feedback for early drafts of this paper.

6. Survey Data Tables

Table 2: Counts of known open recursive DNS servers, in African IPv4 address space, collected in a world-wide IPv4 open recursive resolver survey [1].

Country	Jan-2006	Aug-2007	Change	% Storm	% SpamHaus
SOUTH AFRICA	1522	59352	57830	8.93%	22.49%
EGYPT	734	23948	23214	60.29%	0.51%
ALGERIA	59	4787	4728	29.22%	87.03%
MOROCCO	211	2539	2328	46.04%	0.55%
NIGERIA	72	1505	1433	4.19%	5.12%
KENYA	85	1050	965	24.67%	14.10%
MAURITIUS	18	734	716	54.63%	17.57%
SENEGAL	28	694	666	33.72%	0.00%
COTE D'IVOIRE	20	618	598	22.98%	0.00%
GHANA	38	459	421	3.92%	3.27%
TUNISIA	42	398	356	14.32%	0.25%
MOZAMBIQUE	31	322	291	10.56%	3.73%
LIBYAN ARAB JAMAHIRIYA	16	288	272	20.83%	0.00%
MADAGASCAR	16	274	258	5.11%	0.00%
ZIMBABWE	27	275	248	1.45%	3.27%
ANGOLA	19	228	209	2.63%	8.33%
TANZANIA	69	278	209	9.35%	14.39%
SEYCHELLES	8	161	153	0.00%	0.62%
CAMEROON	9	145	136	7.59%	2.07%
SUDAN	20	156	136	10.90%	3.85%
NAMIBIA	20	137	117	1.46%	11.68%
MALI	14	112	98	6.25%	13.39%
MAURITANIA	13	106	93	8.49%	0.00%
UGANDA	18	100	82	5.00%	0.00%
BURKINA FASO	9	85	76	30.59%	0.00%
ZAMBIA	6	79	73	1.27%	3.80%
BOTSWANA	19	87	68	1.15%	4.60%
MALAWI	9	72	63	6.94%	0.00%
LESOTHO	11	73	62	1.37%	26.03%
TOGO	5	50	45	2.00%	0.00%
BENIN	8	46	38	6.52%	0.00%
ETHIOPIA	0	38	38	7.89%	0.00%
NIGER	3	37	34	2.70%	0.00%
CONGO (DEMOCRATIC REPUBLIC)	7	39	32	10.26%	0.00%
GABON	10	42	32	16.67%	0.00%
RWANDA	7	39	32	5.13%	0.00%
GUINEA	4	34	30	8.82%	0.00%
GAMBIA	3	30	27	10.00%	0.00%
CAPE VERDE	6	32	26	9.38%	0.00%
CONGO (REPUBLIC OF)	2	22	20	0.00%	0.00%
LIBERIA	0	16	16	0.00%	0.00%
ERITREA	3	17	14	0.00%	0.00%
BURUNDI	2	15	13	0.00%	0.00%
SWAZILAND	9	22	13	0.00%	9.09%
SIERRA LEONE	0	10	10	10.00%	0.00%
DJIBOUTI	0	8	8	0.00%	50.00%
SOMALIA	2	10	8	0.00%	0.00%
EQUATORIAL GUINEA	0	7	7	42.86%	0.00%
GUINEA-BISSAU	0	6	6	16.67%	0.00%
REUNION	2	8	6	0.00%	0.00%
CENTRAL AFRICAN REPUBLIC	0	5	5	0.00%	0.00%
CHAD	1	4	3	0.00%	0.00%
MAYOTTE	0	2	2	0.00%	0.00%
COMOROS	1	2	1	0.00%	50.00%
SAO TOME AND PRINCIPE	3	2	(1)	0.00%	0.00%

Table 3: The counts of all unique IPv4, by country, that were listed in the SpamHaus Exploit Block List any time between 2007-02-09 and 2007-10-01. The Storm column is the percentage of these unique addresses that were also observed in the Storm/Peacomm Survey.

Country	SpamHaus	% Storm
SOUTH AFRICA	127646	24.05%
ALGERIA	34770	41.61%
MAURITIUS	9172	15.19%
NIGERIA	7758	34.85%
BOTSWANA	3100	16.48%
EGYPT	2930	19.83%
KENYA	2920	28.63%
SUDAN	2341	29.30%
TANZANIA	2111	37.71%
NAMIBIA	2028	51.53%
MOZAMBIQUE	1804	15.41%
ANGOLA	1728	10.19%
MALI	1331	31.40%
DJIBOUTI	1115	9.33%
GHANA	643	16.80%
ZIMBABWE	527	15.56%
MOROCCO	424	6.13%
LESOTHO	424	1.42%
SWAZILAND	152	31.58%
COMOROS	111	0.00%
UGANDA	84	26.19%
CAMEROON	76	10.53%
SEYCHELLES	64	12.50%
ZAMBIA	50	10.00%
RWANDA	48	31.25%
SENEGAL	31	0.00%
SIERRA LEONE	6	33.33%

Table 4: The counts of all unique IPv4 addresses, per country, that were listed in the Storm/Peacomm Survey [2] any time between 2007-05-25 and 2007-10-01. Each address was either a live botnet node or an e-Donkey file sharing client.

Country	Storm	Country	Storm
EGYPT	173,877	ZAMBIA	287
MOROCCO	144,091	MADAGASCAR	276
SOUTH AFRICA	71,179	GABON	257
ALGERIA	14,816	MALAWI	240
TUNISIA	12,193	BENIN	237
NIGERIA	7,745	CAPE VERDE	197
MAURITIUS	7,100	NIGER	140
SENEGAL	6,664	SEYCHELLES	140
GHANA	6,171	UGANDA	132
SUDAN	3,993	DJIBOUTI	106
KENYA	3,783	TOGO	105
LIBYAN ARAB JAMAHIRIYA	3,500	EQUATORIAL GUINEA	92
COTE D'IVOIRE	3,244	LESOTHO	89
ETHIOPIA	2,272	SOMALIA	89
TANZANIA	1,416	SWAZILAND	69
ZIMBABWE	1,265	BURUNDI	56
NAMIBIA	1,207	LIBERIA	47
MOZAMBIQUE	944	GUINEA	24
BURKINA FASO	839	CHAD	23
BOTSWANA	823	ERITREA	16
CAMEROON	686	CENTRAL AFRICAN REPUBLIC	14
MAURITANIA	683	REUNION	13
ANGOLA	626	CONGO	11
MALI	505	SIERRA LEONE	11
GAMBIA	427	SAO TOME AND PRINCIPE	10
RWANDA	402	GUINEA-BISSAU	8
CONGO (DEMOCRATIC REPUBLIC)	305		

Table 5: Side-by-side comparative summary of the various countries in Africa. The values were collected from The World Factbook [2, 22], by the U.S. Central Intelligence Agency, in August, 2007.

Legend: ✔ indicates that this country has a funded CERT. Mauritius is home of AfriNIC.

Country	Region	TLD	Population	International Languages	Literacy	PPP	Cell Phones	INET Users	IU/Pop	Cell/Pop
Seychelles	Eastern	sc	81,895	Creole, English	91.80%	$7,800	57,000	20,000	24.42%	69.60%
Zimbabwe	Eastern	zw	12,311,143	English, local	90.70%	$2,100	699,000	1,000,000	8.12%	5.68%
Kenya	Eastern	ke	36,913,721	English, Kiswahili	85.10%	$1,200	6,500,000	1,055,000	2.86%	17.61%
Mauritius	Eastern	mu	1,250,882	Creole, English	84.40%	$13,700	713,300	180,000	14.39%	57.02%
Zambia	Eastern	zm	11,477,447	English, local	80.60%	$1,000	946,600	231,000	2.01%	8.25%
Rwanda	Eastern	rw	9,907,509	French, English, Bantu	70.40%	$1,600	290,000	38,000	0.38%	2.93%
Tanzania	Eastern	tz	39,384,223	English, Arabic	69.40%	$800	1,942,000	333,000	0.85%	4.93%
Madagascar	Eastern	mg	19,448,815	French, Malagasy	68.90%	$900	504,700	90,000	0.46%	2.60%
Djibouti	Eastern	dj	496,374	Arabic, French, Samoli	67.90%	$1,000	34,500	9,000	1.81%	6.95%
Uganda	Eastern	ug	30,262,610	English, local	66.80%	$1,900	1,525,000	500,000	1.65%	5.04%
Malawi	Eastern	mw	13,603,181	Local	62.70%	$600	429,300	52,500	0.39%	3.16%
Burundi	Eastern	bi	8,390,505	French, Kirundi	59.30%	$700	153,000	25,000	0.30%	1.82%
Eritrea	Eastern	er	4,906,585	Arabic	58.60%	$1,000	58,000	70,000	1.43%	1.18%
Comoros	Eastern	km	711,417	Arabic, French	56.50%	$600	16,100	20,000	2.81%	2.26%
Mozambique	Eastern	mz	20,905,585	Portuguese	47.80%	$1,500	1,220,000	138,000	0.66%	5.84%
Ethiopia	Eastern	et	76,511,887	English	42.70%	$1,000	410,600	113,000	0.15%	0.54%
Somalia	Eastern	so	9,118,773	Arabic, Italian, English	37.80%	$600	500,000	90,000	0.99%	5.48%
Gabon	Middle	ga	1,454,867	French	63.20%	$7,100	649,800	67,000	4.61%	44.66%
Equatorial Guinea	Middle	gq	551,201	Spanish, French	85.70%	$50,200	96,900	5,000	0.91%	17.58%
Congo (Republic of)	Middle	cg	3,800,610	French, Lingala	83.80%	$1,400	490,000	36,000	0.95%	12.89%
Cameroon	Middle	cm	18,060,382	French, English	67.90%	$2,400	2,259,000	167,000	0.92%	12.51%
Angola	Middle	ao	12,263,596	Portuguese, local	67.40%	$4,400	1,094,000	172,000	1.40%	8.92%
Sao Tome and Principe	Middle	st	199,579	Portuguese	84.90%	$1,200	12,000	20,000	10.02%	6.01%
Congo (Democratic Republic)	Middle	cd	65,751,512	French, Lingala	65.50%	$700	2,746,000	140,600	0.21%	4.18%
Chad	Middle	td	9,885,661	French, Arabic	47.50%	$1,500	210,000	35,000	0.35%	2.12%
Central African Republic	Middle	cf	4,369,038	French, Sangho	51.00%	$1,200	60,000	9,000	0.21%	1.37%
Libyan Arab Jamahiriya	Northern	ly	6,036,914	Arabic, Italian, English	82.60%	$12,300	234,800	205,000	3.40%	3.89%
Tunisia ✔	Northern	tn	10,276,158	Arabic, French	74.30%	$8,800	5,681,000	953,800	9.28%	55.28%
Egypt	Northern	eg	80,335,036	Arabic, French, English	71.40%	$4,200	14,045,000	5,000,000	6.22%	17.48%
Algeria ✔	Northern	dz	33,333,216	Arabic, French	69.90%	$7,600	13,661,000	1,920,000	5.76%	40.98%
Sudan	Northern	sd	39,379,358	Arabic	61.10%	$2,400	1,828,000	2,800,000	7.11%	4.64%
Morocco	Northern	ma	33,757,175	Arabic, French	52.30%	$4,600	12,393,000	4,600,000	13.63%	36.71%
South Africa	Southern	za	43,997,828	English, local	86.40%	$13,300	33,960,000	5,100,000	11.59%	77.19%
Namibia	Southern	na	2,055,080	Afrikaans, German, English	85.00%	$7,600	495,000	75,000	3.65%	24.09%
Botswana	Southern	bw	1,815,508	English, local	81.20%	$10,900	823,100	60,000	3.30%	45.34%
Swaziland	Southern	sz	1,133,066	English, siSwati	81.60%	$5,200	200,000	36,000	3.18%	17.65%
Lesotho	Southern	ls	2,125,262	English, regional	84.80%	$2,600	245,100	43,000	2.02%	11.53%
Mauritania	Western	mr	3,270,065	Arabic, French	51.20%	$2,600	745,600	14,000	0.43%	22.80%
Cape Verde	Western	cv	423,613	Portuguese	76.60%	$6,000	81,700	25,000	5.90%	19.29%
Nigeria	Western	ng	135,031,164	English, local	68.00%	$1,500	21,571,000	5,000,000	3.70%	15.97%
Gambia	Western	gm	1,688,359	English	40.10%	$2,000	247,500	49,000	2.90%	14.66%
Senegal	Western	sn	12,521,851	French	39.30%	$1,800	1,730,000	540,000	4.31%	13.82%
Ghana	Western	gh	22,931,299	Local, English	57.90%	$2,700	2,842,000	401,300	1.75%	12.39%
Cote d'Ivoire	Western	ci	18,013,409	French	50.90%	$1,600	2,190,000	160,000	0.89%	12.16%
Togo	Western	tg	5,701,579	French, local	60.90%	$1,700	443,600	300,000	5.26%	7.78%
Mali	Western	ml	11,995,402	French	46.40%	$1,300	869,600	60,000	0.50%	7.25%
Liberia	Western	lr	3,195,931	English	57.50%	$900	160,000	1,000	0.03%	5.01%
Benin	Western	bj	8,078,314	French, local	34.70%	$1,100	386,700	425,000	5.26%	4.79%
Guinea-Bissau	Western	gw	1,472,780	Portuguese	42.40%	$900	67,000	26,000	1.77%	4.55%
Burkina Faso	Western	bf	14,326,203	French, Sudanic family	21.80%	$1,300	572,200	64,600	0.45%	3.99%
Niger	Western	ne	12,894,865	French	28.70%	$1,000	299,900	24,000	0.19%	2.33%
Guinea	Western	gn	9,947,814	French	29.50%	$2,100	189,000	46,000	0.46%	1.90%
Sierra Leone	Western	sl	6,144,562	English, Creole, Local	35.10%	$900	113,200	10,000	0.16%	1.84%

7. References

1. Dagon, D. and C. Lee, *Flow Analysis Database: Open Recursive Resolver Survey Data*. 2007, Georgia Institute of Technology.
2. Dagon, D. and C. Lee, *Flow Analysis Database: Storm/Peacomm Survey Data*. 2007, Georgia Institute of Technology.
3. Edmonds, R., *Predator: Historical SpamHaus Data*. 2007, Georgia Institute of Technology.
4. Cole, K., et al., *The Current State of Cybersecurity in Africa*. 2007, Georgia Institute of Technology: Atlanta, Georgia.
5. Lohr, S. *Software for the poor: Microsoft's $3 Windows*. 2007 [cited 2007 Oct 14]; Available from: http://www.iht.com/articles/2007/04/19/news/msft.php.
6. Blum, J. *U.S. Oil Firms Entwined in Equatorial Guinea Deals*. 2004 [cited 2007 Nov 15]; Available from: http://www.washingtonpost.com/wp-dyn/articles/A1101-2004Sep6.html.
7. Dagon, D., et al., *Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority*, in *NDSS Symposium*. 2008.
8. Damas, J. and F. Neves. *Preventing Use of Recursive Nameservers in Reflector Attacks*. 2007 [cited 2007 Nov 12]; Available from: http://www.ietf.org/internet-drafts/draft-ietf-dnsop-reflectors-are-evil-04.txt.
9. The Spamhaus Project. *Exploits Block List*. 2007 [cited 2007 Nov 13]; Available from: http://www.spamhaus.org/xbl/index.lasso.
10. Schneier, B. *Gathering 'Storm' Superworm Poses Grave Threat to PC Nets*. 2007 [cited 2007 Nov 15]; Available from: http://www.wired.com/politics/security/commentary/securitymatters/2007/10/securitymatters_1004.
11. Grizzard, J.B., et al., *Peer-to-Peer Botnets: Overview and Case Study*, in *USNIX Hotbots*. 2007: Cambridge, Massachusetts, USA.
12. Cooke, E., F. Jahanian, and D. McPherson. *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets*. 2005 [cited 2007 Oct 10]; Available from: http://www.usenix.org/event/sruti05/tech/full_papers/cooke/cooke_html/.
13. Piscitello, D.M. *Anatomy of a DNS DDoS Amplification Attack*. 2006 [cited 2007 Oct 6]; Available from: http://www.corecom.com/external/livesecurity/dnsamplification.htm.
14. VeriSign Inc. *Anatomy of Recent DNS Reflector Attacks from the Victim and Reflector Point of View*. 2006 [cited 2007 Oct 8]; Available from: http://www.verisign.com/static/037903.pdf.
15. US-CERT. *The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)*. 2006 [cited 2007 Oct 6]; Available from: http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf.
16. Internet Service Providers' Association. *ISPA Members*. 2007 [cited 2007 Oct 14]; Available from: http://www.ispa.org.za/about/memberlist.shtml.
17. Gaudin, S. *Storm Worm Botnet More Powerful Than Top Supercomputers*. 2007 [cited 2007 Oct 9]; Available from: http://www.informationweek.com/news/201804528.
18. Thomson Dialog NewsEdge. *Storm Botnet Puts Up Defenses And Starts Attacking Back*. 2007 [cited 2007 Oct 9]; Available from: http://ipcommunications.tmcnet.com/news/2007/08/17/315179.htm.
19. International Telecommunications Union. *ICT in Egypt*. 2004 [cited; Available from: http://www.itu.int/AFRICA2004/media/ict_egypt.html.
20. CERT-TCC. *Zhelatin.LJ Alerte*. 2007 [cited 2007 Nov 15]; Available from: http://www.ansi.tn/fr/alertes/archives/2007/novembre/2007-179.htm.
21. Rutkowski, T. *Cybersecurity Reference Materials*. 2007 [cited 2007 Nov 15]; Available from: http://www.ituwiki.com/Cybersecurity_Reference_Materials.
22. U.S. Central Intelligence Agency. *The World Factbook*. 2007 [cited 2007 August]; Available from: https://www.cia.gov/library/publications/the-world-factbook/.