USABILITY OF HONEYPOTS IN KENET MEMBER INSTITUTIONS IN WESTERN KENYA AS PROACTIVE DETECTION TOOLS FOR MONITORING CYBER RELATED INCIDENCES

Peter Odhiambo Ogada, George Raburu and S. Liyala
School of Informatics and Innovative Systems
Jaramogi Oginga Odinga University of Science and Technology
P.O. Box 210-40601, BONDO-Kenya

N. B. Okelo
School of Mathematics and Actuarial Science
Jaramogi Oginga Odinga University Science and Technology
P.O. Box 210-40601, BONDO-Kenya

ABSTRACT

With the advent of the ever changing technology and the intense sophistication in methods and means of committing illegal activities, crime is no longer narrowly defined vies-a-vie the law but there is need to be able to handle technologically oriented crimes commonly referred to as Cybercrimes. Cybercrimes are crimes that involve the use of computers to undertake illegal. Collection of statistics associated with cybercrimes can be quite tricky and daunting, since their collection and tabulation can only be done when aggrieved parties report them. Some of these illegal activities that constitute cybercrimes include, but not limited to, creation of counterfeit currency or official documents using computer scanners and graphics programs, embezzlement of funds using computers to skim very small sums of money from a large number of accounts, distribution of child pornography on the Internet, and theft of digital property. Other crimes that can also be committed include fraud, hate crimes, stalking, gambling, hacking; spread of malware, phishing, spamming, Botnet attacks, DDoS attacks, espionage and money laundering. In this paper we present results on usability of HoneyPots in KENET member institutions in western Kenya as proactive detection tools for monitoring cyber related incidences.

1. INTRODUCTION

As increased cyber related incidents continue to be noted and documented in Kenya, as a result of the rapid deployment of the fiber optic cable (Kenya cyber security report, 2014), the need to setup proactive detection tools for use by Computer Incident Response Teams (CIRTs) becomes more evident. CIRTs act as Police stations where cyber related security incidents are reported and recorded. Such teams, especially in institutions with high speed fiber optic connections, should have the mandate of coordinating response; managing cyber security incidents within their districts of jurisdiction and collaboration with partnering institutions. Numerous reports showing a steady increase in cyber related incidences that easily qualify as cyber crimes, yet crime is still being looked at in the traditional sense in terms of something that is against the law. Modern societies generally regard crimes as offences against the public or the state, as distinguished from torts - wrongs against private parties that can give rise to a civil cause of action (Canada Law Commission, 2004).

2. LITERATURE REVIEW

Cyber security; General State of affairs

Cyberspace and related technologies have eroded society's ability to enforce criminal laws as they apply to attacks on communications between computers, on data stored on computers and on real world systems controlled by computers (Brenner, 2005). This is because these technologies have contributed immensely to the introduction and spread of cyber crimes. Cybercrimes are a type of crime that involves the abuse of information technology. The term cybercrime covers a series of crimes which range from cyber terrorism to industrial espionage. Cybercrimes are thus extensive phenomenon expressed via of an intricate ecosystem of operators, victims and instruments (Brenner, 2005). Cybercrime is a criminal phenomenon centered on the abuse of information technology, and its manifestations range from cyber terrorism to industrial espionage (European cybercrime survey, 2011). Cybercrime today is a particularly extensive and complex phenomenon expressed via an intricate ecosystem of operators, victims and instruments which, over the years, has acquired a complex organizational hierarchy all over the world. Cyberfraud which is a subcomponent of cybercrimes differs from other cybercrimes, because of the undue profits enjoyed by the fraudster, gained by illegally manipulating IT systems, or for other peculiarities based on the legislation in force in the various countries. In 2010, the European Electronic Crime Task Force decided to explore the dynamics of Cyberfraud at European level (European cybercrime survey, 2011.

4. RESULTS AND DISCUSSION

Type of Honeypot on network

14.3% of respondents indicated running Physical HoneyPots, 1.4% indicated running Virtual HoneyPots, while 84.3% were running neither HoneyPots. HoneyPots are yet to penetrate the various constituencies.

Table 34: Type of Honeypot on network

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Physical	10	14.3	90.9	90.9
	Virtual	1	1.4	9.1	100.0
	Total	11	15.7	100.0	
Missing	System	59	84.3		
Total		70	100.0		

4.5.3 Number of Honeypots deployed and running

12.9% of respondents indicated running two or less HoneyPots, while 1.4% of the respondents were running 3-5, or 6 and greater HoneyPots. 84.3% were running none. HoneyPots are, once again a new concept, and are yet to penetrate the various constituencies.

Table 35: Number of Honeypots deployed and running

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<=2	9	12.9	81.8	81.8
	3 - 5	1	1.4	9.1	90.9
	>= 6	1	1.4	9.1	100.0
	Total	11	15.7	100.0	

Missing	System	59	84.3		
Total		70	100.0		

4.5.4 Number of Honeypots deployed and running

14.3% of respondents running HoneyPots indicated that their HoneyPots **Often** received suspicious activity, while 1.4% indicated that their HoneyPots **So Often** received suspicious activity.

Table 36: Honeypot recorded suspicious activity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Often	10	14.3	90.9	90.9
	So Often	1	1.4	9.1	100.0
	Total	11	15.7	100.0	
Missing	System	59	84.3		
Total		70	100.0		

4.5.5 Kind of honeypot imitated

Table 37: Kind of honeypot imitated

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Production HoneyPots	9	12.9	81.8	81.8
	Personal HoneyPots	2	2.9	18.2	100.0
	Total	11	15.7	100.0	
Missing	System	59	84.3		

Table 37: Kind of honeypot imitated

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Production HoneyPots	9	12.9	81.8	81.8
	Personal HoneyPots	2	2.9	18.2	100.0
	Total	11	15.7	100.0	
Missing	System	59	84.3		
Total		70	100.0		

4.5.6 Primary reason for running HoneyPot

12.9% of respondents running HoneyPots indicated that their primary reason for running their HoneyPot was monitor malware threats, 1.4% for Research on threats and Securing their networks respectively.

Table 38: Primary reason for running HoneyPot

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Research on threats	1	1.4	9.1	9.1
	Securing the network	1	1.4	9.1	18.2
	Monitor malware threats	9	12.9	81.8	100.0
	Total	11	15.7	100.0	
Missing	System	59	84.3		
Total		70	100.0		

4.5.7 Major challenges in running HoneyPots

1.4% of respondents running HoneyPots indicated that the major challenges they faced as they run HoneyPots was lack of qualified staff to handle the HoneyPots, while 14.3% of respondents running HoneyPots indicated that they faced no challenges.

Table 39: Major challenges in running HoneyPots

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Qualified staff to handle Honeypots	1	1.4	9.1	9.1
	None	10	14.3	90.9	100.0
	Total	11	15.7	100.0	
Missing	System	59	84.3		
Total		70	100.0		

4.5.8 Reasons for NOT running a HoneyPot in your LAN setup

84.3% of respondents that do not run HoneyPots indicated that they do not run them for the following reasons. 24.3% were not aware of Honeypots existence, 15.7% indicated a lack of skills to interpret HoneyPot traffic, 14.3% felt HoneyPots were a Security risk if compromised, 11.4% indicated budgetary constraints, 10% cited a lack of technical staff to handle them, while 8.6% felt their data centers had poor infrastructure to allow for setup of such equipment.

Table 40: Reasons for not running a HoneyPot in your LAN setup

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Lack of technical staff	7	10.0	11.9	11.9

	Lack of awareness	17	24.3	28.8	40.7
	Budgetary Constraints	8	11.4	13.6	54.2
	Poor data centre infrastructure	6	8.6	10.2	64.4
	They are a security risk	10	14.3	16.9	81.4
	Lack of skills to interpret traffic	11	15.7	18.6	100.0
	Total	59	84.3	100.0	
Missing	System	11	15.7		
Total		70	100.0		

4.5.9 Malware domain list is our external source providing information on our domain

64.3% of the respondents indicated that **Malware domain list** was their external source for providing information on malicious or problematic URLs, IPs or Domains. 35.7% of the rest of respondents felt otherwise.

Table 41: Malware domain list is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	45	64.3	64.3	64.3
	No	25	35.7	35.7	100.0
	Total	70	100.0	100.0	

4.5.10 SpamCop is our external source providing information on our domain

20% of the respondents indicated that **SpamCop** was their external source for providing information on malicious or problematic URLs, IPs or Domains, while 80% of other respondents indicated otherwise.

Table 42: SpamCop is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	14	20.0	20.0	20.0
	No	56	80.0	80.0	100.0
	Total	70	100.0	100.0	

4.5.11 Cert.br data feed is our external source providing information on our domain

7.1% of the respondents indicated that **Cert.br data feed** was their external source for providing information on malicious or problematic URLs, IPs or Domains, while 92.9% of other respondents indicated otherwise.

Table 43: Cert.br data feed is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	7.1	7.1	7.1
	No	65	92.9	92.9	100.0
	Total	70	100.0	100.0	

4.5.12 Cert.br Spampot is our external source providing information on our domain

10% of the respondents indicated that **Cert.br Spampot** was their external source for providing information on malicious or problematic URLs, IPs or Domains, while 90% of other respondents indicated otherwise.

Table 44: Cert.br Spampot is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	7	10.0	10.0	10.0
	No	63	90.0	90.0	100.0
	Total	70	100.0	100.0	

4.5.13 NoAH is our external source providing information on our domain

2.9% of the respondents indicated that **NoAH** was their external source for providing information on malicious or problematic URLs, IPs or Domains, while 97.1% of other respondents indicated otherwise.

Table 45: NoAH is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	2	2.9	2.9	2.9
	No	68	97.1	97.1	100.0
	Total	70	100.0	100.0	

4.5.14 HoneySpider Network is our external source providing information on our domain

5.7% of the respondents indicated that **HoneySpider Network** was their external source for providing information on malicious or problematic URLs, IPs or Domains, while 94.3% of other respondents indicated otherwise.

Table 46: HoneySpider Network is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	4	5.7	5.7	5.7
	No	66	94.3	94.3	100.0
	Total	70	100.0	100.0	

4.5.15 HoneySpider Network is our external source providing information on our domain

61.4% of the respondents indicated that **HoneySpider Network** was their external source for providing information on malicious or problematic URLs, IPs or Domains, while 38.6% of other respondents indicated otherwise.

Table 47: Google safe browsing alerts is our external source providing information on our domain

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	43	61.4	61.4	61.4
	No	27	38.6	38.6	100.0
	Total	70	100.0	100.0	

4.5.16 Use of closed sources of information that cannot be disclosed

27.1% of the respondents indicated that they were using other closed sources of information that they could not disclose, while 72.9% of other respondents indicated otherwise.

Table 48: Use closed sources of information that cannot be disclosed

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	19	27.1	27.1	27.1
	No	51	72.9	72.9	100.0
	Total	70	100.0	100.0	

4.6 Usability of HoneyPots as proactive detection tools for monitoring cyber related incidents

4.6.1 Collection of information on other constituencies

18.6% of the respondents indicated that they collect information about incidents related to other constituencies. 72.9% indicated that they don't, 4.3% were not sure, while 4.3% could not tell.

Table 49: Collection of information on other constituencies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	13	18.6	18.6	18.6
	No	51	72.9	72.9	91.4
	Not sure	3	4.3	4.3	95.7
	cannot tell	3	4.3	4.3	100.0
	Total	70	100.0	100.0	

4.6.2 Sharing collected information with other players

25.7% of the respondents indicated that they did share collected information with other constituencies, while 74.3% indicated otherwise.

Table 50: Sharing collected information with other players

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	18	25.7	25.7	25.7
	No	52	74.3	74.3	100.0
	Total	70	100.0	100.0	

4.6.3 Type of information shared

7.1% of the respondents who shared information collected, indicated that they shared mostly types of malware attacks, 2.9% were not sure.

Table 51: Type of information shared

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Types of Malware attacks	5	7.1	71.4	71.4
	Not sure	2	2.9	28.6	100.0
	Total	7	10.0	100.0	
Missing	System	63	90.0		
Total		70	100.0		

4.6.4 Form of information shared

7.1% of the respondents indicated that they shared the information in raw data, 14.3% shared in processed data, while 4.3% shared in interpreted data.

Table 52: Form of information shared

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Raw data	5	7.1	27.8	27.8
	Processed data	10	14.3	55.6	83.3
	Interpreted data	3	4.3	16.7	100.0
	Total	18	25.7	100.0	
Missing	System	52	74.3		
Total		70	100.0		

4.6.5 Conditions for sharing information

7.1% of the respondents indicated that they shared the information under public conditions, while 20% shared under Limited accesses.

Table 53: Conditions for sharing information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Public	5	7.1	26.3	26.3
	Limited access	14	20.0	73.7	100.0
	Total	19	27.1	100.0	

Missing	System	51	72.9		
Total		70	100.0		

IJRDO

4.6.6 Missing kind of tools for detecting incidents

47.1% of the respondent indicated that HoneyPots were the kind of tools missing for detecting incidents; 20% indicated IDS/IPS; 18.6% indicated Internet scanners; 2.9% indicated none, while 10% indicated Firewalls.

Table 54: Missing kind of tools for detecting incidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Honeypots	33	47.1	47.8	47.8
	IDS/IPS	14	20.0	20.3	68.1
	Internet scanners	13	18.6	18.8	87.0
	None	2	2.9	2.9	89.9
	Firewalls	7	10.0	10.1	100.0
	Total	69	98.6	100.0	
Missing	System	1	1.4		
Total		70	100.0		

4.6.7 Kind of information from closed sources

11.4% of the respondent that use closed sources of information indicated proxies' logs were the kind of information provided by their closed sources of information. 4.3% indicated Routers routing logs; 4.3% indicated Dbase logs; 2.9% indicated Anti Virus engines; while another 2.9% indicated Sandboxes for malware logs.

Table 55: Kind of information from closed sources of information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Proxies for logs	8	11.4	44.4	44.4
	Routers for routing logs	3	4.3	16.7	61.1
	DBMS for Dbase logs	3	4.3	16.7	77.8
	AV engines for virus logs	2	2.9	11.1	88.9
	Sandboxes for malware logs	2	2.9	11.1	100.0
	Total	18	25.7	100.0	
Missing	System	52	74.3		
Total		70	100.0		

4.6.8 TOP 3 best sources for gathering information from closed sources

A. TOP 3 best sources for gathering information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Honeypots	17	24.3	24.3	24.3
	Cuckoo	2	2.9	2.9	27.1
	AV engines	24	34.3	34.3	61.4
	IDS/IPS	5	7.1	7.1	68.6
	Sans Security alerts	19	27.1	27.1	95.7
	Darknets	3	4.3	4.3	100.0

A. TOP 3 best sources for gathering information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Honeypots	17	24.3	24.3	24.3
	Cuckoo	2	2.9	2.9	27.1
	AV engines	24	34.3	34.3	61.4
	IDS/IPS	5	7.1	7.1	68.6
	Sans Security alerts	19	27.1	27.1	95.7
	Darknets	3	4.3	4.3	100.0
	Total	70	100.0	100.0	

B. ***Table 57: TOP 3 best sources for gathering information***

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Honeypots	14	20.0	20.0	20.0
	Cuckoo	7	10.0	10.0	30.0
	AV engines	21	30.0	30.0	60.0
	IDS/IPS	8	11.4	11.4	71.4
	Sans Security alerts	10	14.3	14.3	85.7
	Darknets	10	14.3	14.3	100.0
	Total	70	100.0	100.0	

C. **TOP 3 best sources for gathering information**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Honeypots	30	42.9	42.9	42.9
	Cuckoo	4	5.7	5.7	48.6
	AV engines	13	18.6	18.6	67.1
	IDS/IPS	9	12.9	12.9	80.0
	Sans Security alerts	9	12.9	12.9	92.9
	Darknets	5	7.1	7.1	100.0
	Total	70	100.0	100.0	

This question required the respondents to pick the best three sources for gathering information in order of personal priority. The tables generated are as indicated above. From the above three tables, the average responses was determined to get the final TOP 3 best sources for gathering information as indicated by the respondents. The best were identified as Anti Virus engines 31.4%, HoneyPots 21.47% and Sans Security alerts 18.6% in that order.

Table 56: Summary of Top 3 Best sources of gathering information

SOURCE	TABLE A	TABLE B	TABLE C	TOTAL	AVE
HoneyPots	24.3%	20.0%	20.0%	64.3%	**21.4%**
Cuckoo	2.9%	10.0%	10.0%	22.9%	**7.6%**
AV Engines	34.3%	30.0%	30.0%	94.3%	**31.4%**
IDS/IPS	7.1%	11.4%	11.4%	29.9%	**10.0%**

Sans Security alerts	27.1%	14.3%	14.3%	55.7%	**18.6%**
Darknets	4.3%	14.3%	14.3%	32.9%	**11.0%**
Total	**100.0%**	**100.0%**	**100.0%**		**100.0**

4. CONCLUSION

There is need to conduct a research survey across all institutions that are affiliated to KENET as well as all government ministries and agencies to determine their preparedness in terms of detecting and monitoring cyber related incidents. This will help in facilitating a deeper understanding of cyber network traffic within KENET infrastructure and the country, and thereby be able to pinpoint ways of improving our networks security.

REFERENCES

Babbie, E. (2007). *The Practice of Social Research*. Twelfth Edition. USA: Chapman University.

Brenner S. W., L. L. (2005). Distributed Security: A New Model of Law Enforcement. *John Marshall Journal of Computer & Information Law, Forthcoming.*

CAK. (2014). *KE-CIRT*. Retrieved from www.cck.go.ke: https://www.cck.go.ke/

Canada, L. C. (2004). *What Is a Crime? Defining Criminal Conduct.* Vancouver/Toronto: UBCPress.

Carter, L. W. (2004). *SANS Institute.* Retrieved from http://www.sans.org: http://www.sans.org/reading-room/whitepapers/casestudies/setting-honeypot-bait-switch-router-1465

Cunningham, C. C. (2013). *Honeypot-Aware Advanced Botnet Construction and Maintenance.* University of Central Florida, School of Electrical Engineering and Computer Science. Orlando, FL: University of Central Florida.

Denzin, N.K., & Lincoln, Y.S. (1994). *Handbook on Qualitative Research*. Thousand Oaks, CA: Sage

Economic Times. (2009, August 19). *Cybercrime india and brazil major hub*. Retrieved from www.articles.economictimes.indiatimes.com:

ENISA. (2012). *Proactive Detection of Security Incidents.* Polska: ENISA.

European Cybercrime Survey. (2011). EECTF. Rome: EECTF.

Goodman Marc D. (1997). Why the Police don't care about computer crime. *Harvard journal of law and Technology*, 1-30.

IATAC. (2009). Measuring Cyber Security and Information Assurance. In (Information Assurance Technology Analysis Centr) IATAC, *Measuring Cyber Security and Information Assurance.* Fort Belvoir, Virginia: Defense Technical Information Center.

KENET. (2014). *Our History*. Retrieved from www.kenet.or.ke: https://www.kenet.or.ke/

KENET, CERT report. (2014). *Welcome to the KENET CERT*. Retrieved from www.kenet.or.ke: https://www.kenet.or.ke/

Kenya Cyber Security Report (2014). *Serianu Limited.* Nairobi: Serianu Ltd,.

Kombo, D. K., & Delno, L. A. T. (2006). *Proposal and Thesis Writing: An Introduction*. Nairobi: Pauline's publications Africa.

London Daily News. (2009). *www.cyberlawtimes.com*. Retrieved from CyberLawTimes.com: http://www.cyberlawtimes.com/cyberlaw/3-million-online-crimes-a-year-new-cyber-crime-squad-to-be-established/

Newswise. (2009). *China linked to 70 percent of worlds spam says computer forensics expert.* Retrieved from www.newswise.com: http://www.newswise.com/articles/china-linked-to-70-percent-of-worlds-spam-says-computer-forensics-expert

Pariyani, R. (2014). *www.manupatra.co.in.* Retrieved from manupatra.co.in: http://www.manupatra.co.in/newsline/articles/Upload/779E337A-DDF8-41AE-ACA4-89F3CB746F2D.pdf

Pathan, A.-S. K. (1990/91). *The State of the Art in Intrusion Prevention and Detection.* Natick, Massachusetts: CRC Press, Taylor & Francis Group.

Ping Wang, L. W. (2010). Honeypot detection in advanced botnet attacks. *Int. J. Information and Computer Security*, 30-32.

Punch, F.K. (2010). *Introduction to Social Research: Quantitative and Qualitative Approaches*. Second Edition. New Delhi: Sage Publications Ltd.

Sabine, L., & Everitt, B.S. (2004). *A Handbook of Statistical Analysis Using SPSS*. USA: Chapman & Hall /CRC Press on 30/08/2012.

Saini H., Rao Y. S., Panda T.C.(2012) International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209.

Schuttler, K. (2014). *Eastern Michigan University College of Technology*. Retrieved from www.emich.edu: www.emich.edu/ia/pdf/research/Honeypotresearch.pdf

Spitzner, L. (2002). *Honeypots: Tracking Hackers.* Boston, Massachusetts: Addison Wesley.

Spitzner, L. (2002, December 10). *Windowsecurity*. Retrieved from www.windowsecurity.com: www.windowsecurity.com/whitepapers/honeypots/Honeypots_Definitions_and_Value_of_Honeypots.html