A Mitigation Technique For Internet Security Threat of Toolkits Attack

Francisca Nonyelum Ogwueleka *ogwuelekefn@fuwukari.edu.ng*
Computer Science Department,
Federal University Wukari,
PMB 1020 Wukari,
Taraba State, Nigeria.

Edward Onyebueke Agu *aguedward@fuwukari.edu.ng*
Computer Science Department,
Federal University Wukari,
PMB 1020 Wukari,
Taraba State, Nigeria.

Abstract

The development of attack toolkits conforms that cybercrime is driven primarily by financial motivations as noted from the significant profits made by both the developers and buyers. In this paper, an enhanced hybrid attack toolkit mitigation model was designed to tackle the economy of the attack toolkits using different techniques to discredit it. The mitigation looked into Zeus, a common and the most frequently used attack toolkit to discover the hidden information used by the attackers to launch attacks. This information helped in creating honey toolkits, honeybot and honeytokens. Honeybots are used to submit honeytoken to botmasters, who sells to the internet black market. Both the botmasters, his mules and buyers attempts to steal huge amount of money using the stolen credentials which includes both real and honeytokens and will be detected by an attack detector which sends an alert on any transaction involving the honeytokens. A reconfirmation process which is secured using enhanced RC6 cryptosystem is enacted. The reconfirmation message in plain text is securely encrypted into cipher text and transmitted from the bank to the legitimate account owner and vise visa. The result of the crypto analysis carried out on the encrypted text using RC6 encryption algorithm showed that the cipher text is not transparent.

Keywords: Toolkits, Mitigation, Zeus, Botmaster, Cryptosytem, Botnets.

1. INTRODUCTION

Internet has been considered to be universal in scope, but its open medium is not secure. Internet has transformed the computing and communications world in order to develop and support client and server services. The existence of internet browsers and internet technologies has increased the efficiency and effectiveness of the internet service to the users throughout the whole world [1]. Today, The Internet consists of infrastructures and mechanisms for sharing information across the globe [1].

Due to many activities being carried out on the internet ranging from electronic mail to sharing of professional knowledge, has led to internet insecurity problems which is of high importance. Internet problems need critical attention, unsecured online businesses on which many lives depend for survival draws the attention of online criminals [1].

A packs of mischievous codes used to carryout rigorous and extensive attack on computers in a network is called attack toolkits or crimeware [2]. Attack toolkits consist of established mischievous codes for taking advantages of weakness in devices together with many other tools to modify, install, and computerize extensive attacks, which includes command-and-control (C&C)

attack at the server [3]. Attack toolkits are used for stealing vital information or to change attacked systems to zombie bots or network (botnet) so as to achieve more attacks according to [4]. The advertisement and selling of these attack toolkits are on the internet secretive black market which consist of illegal transactions among internet criminals. The ease-of-use nature of these toolkits has played a major role in turning internet crime to a lucrative means of acquiring wealth [2].

Some toolkits attack codes focuses on specific program while others have sophistical codes to carryout multiple attack on many programs across many operating platforms [2]. The combined effort of these attack kits and Internet-network controlled from a remote location is to performed mischievous and illegal acts on life supporting information and equipment. [5].

The mitigation techniques in this research showcase a number of ways that can be used to curb this insecurity irrespective of the cadre. Some part of this mitigation approach inter-worked together and appeared as aspect of the general approach for toolkits attack mitigation. [6].

2. REVIEW OF RELATED STUDIES

Determining botnets membership using Domain Name System (DNS) blacklist counter intelligence was proposed by [7], but it is only effective to certain categories of spam botnets. A system to sense a botnet using network traffic aggregation called Tand system, was proposed by [8]. This is not too effective to detect botnets as botnets changes their mode of attack frequently to circumvent this solution. Similarly, a system for passive detection of individual attack toolkits using correlation of Intrusion Detection System (IDS) alerts to a predefined infection model called BotHunter was proposed by [9]. [10] proposed a system which correlates network traffic to detect botnets called BotMiner, but with different parameters to Tand system. A system to detect Internet Relay Chat (IRC) botnets using signature detection on known IRC nicknames called Rishi was proposed by [11]. All these measures face the same limitation as Tand system, because botnets constantly changes their mode of operation in order to escape these measures.

So many researchers have equally done a great research works on the field of identity theft analysis, detection and mitigation. Two attacks on the trust and rating system of the internet black market was presented by [12], but their method has limitation as it did not handle the case where credentials are not sold on the black markets. Research on detection of attack sites by submitting fake credentials and monitoring site behaviour was presented by [6], but their approach did not mitigate attack toolkit. A research to analyzed data that is sized from 70 drop zones in order to provide metrics to determine the wealth of underground economy was presented by [13]. A system that used honeytokens to track attackers was presented by [14]. All these measures did not submit the honeytokens through attack toolkit and did not mitigate them. A system to destabilized Distributed Denial of Service (DDoS) attack using honeypots was created by [15]. The attack was to scatter the profit margins of botmasters by reducing the value of their services. While all these measures show good steps to detect and mitigate internet attack, they have not addressed the malware authors or the botmasters that created the attack toolkits. The enhance hybrid model in this research moved further to extend the economic attack to lower the botmaster's profits by aiming the kits they are selling. The closest work to this model is a framework proposed by [16] and [17]. [16] in approach utilize spam traps to send credentials to phishing sites as well as using phoneybots to send credentials to botnets such as Zeus. But the main aim is the end-users or the money mules, while [17] in their approach targeted to disrepute a specific kit and the creator of the toolkit. The model in this research will be a hybrid of the two frameworks by complementing the limitations of each one with the strength of another. We will adopt more security features such as encryption to further improve the hybrid model. This hybrid method stands to bring to minimum the variation of these kits that is accessible to cybercriminal and directly affect their extensive uses.

2.1 The First Framework by [17]

The ultimate aim of [17] in their proposed framework is to damage the reputation of a botnet toolkit and reduce its demand. They attack integrity of the toolkit in two ways: the toolkit profitability with respect to its use to sale credentials and the security of the toolkit users from prosecution. This research proposed two stages to this approach: to reduce a toolkit's profitability by submitting false credentials to it, and to make the toolkit insecure by submitting honeytokens to the botnets which will help in arresting and prosecuting the end-users of the stolen credentials. The framework which shows the two stages and its process is illustrated in Figure 1.

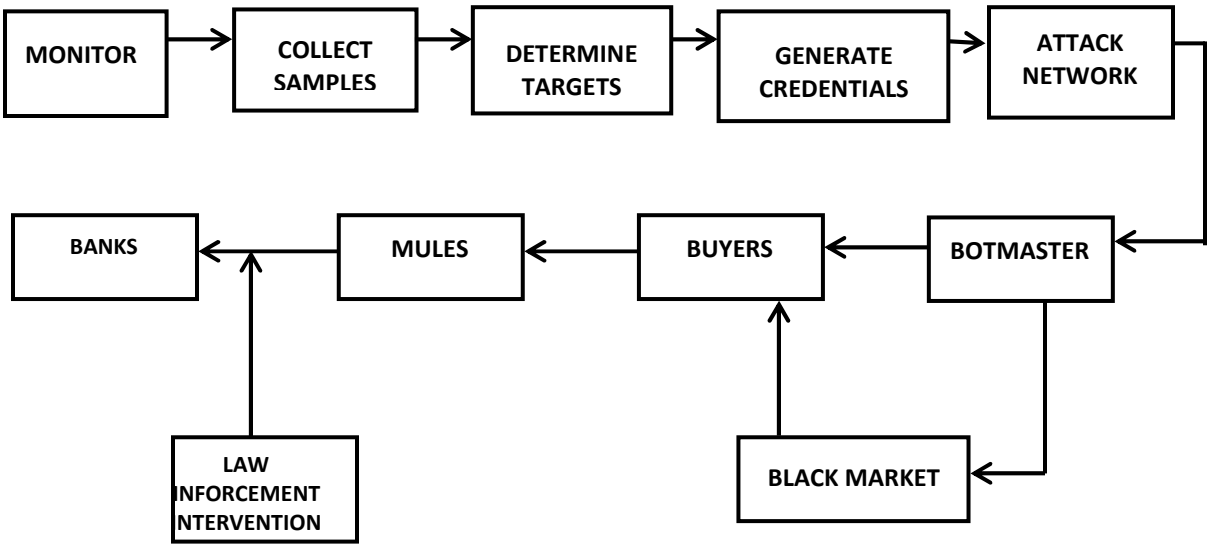

FIGURE 1: Botnet toolkit attack and detection process [17].

The first stage aimed at mixing the stolen credentials from a botnet with honey tokens have the following steps -

i. It monitors the current activities of the botnet toolkit and selects the most used toolkit for stealing credentials as their target.
ii. It collects many samples of botnet binaries from honeynets, antivirus companies, financial institutions and security forums.
iii. It analyzes the toolkit samples to determine the targeted websites and their targeted fields.
iv. It creates false credentials.
v. It submits the credentials to the botmasters using the toolkit.

The first stage of the frameworks ends at this point, and the false credentials are sent to the internet black market.

In the second stage of the framework which is an expansion of the first framework, aimed at discrediting the security of the end-users of the stolen credentials. The stage contains one additional step which takes place after the credentials have been sold and passes via the internet black market: The second stage of the framework monitors honey account usage in order to make arrests when money are withdrawn from the account and purchases made using the honey credentials are received. This framework only targets to damage the reputation of a toolkit and the authors that made them.

2.2 The Second Framework by [16]

The anti-phishing framework proposed is an organized solution showcasing steps used in the framework information flow. The steps are -

Step 1: The honeyed bank for example, sets up a number of virtual machines (m >= 1), running 'm' honeybots and 'm' spam traps. Each spam trap or honeybot is fed with a honeytoken. Following the normal characteristics of all bank customers, each honeybot accesses e-banking system frequently and carryout virtual online transactions. A designated group of personnel in a bank take the responsibility of managing the virtual machines, spamtraps and honeybots. They also monitor doubtful phishing e-mails.

Step 2: The e-criminal sends threat e-mails to his prospective victims, or contaminate prospective victims' computers with attack bot, or launches a sophisticated attacks.

Steps 3: During phishing attack using threat e-mails, the group of managers in the honey bank submits the tokens accompanied with the honeytokens to the attack site. In a sophisticated phishing attack based on attack toolkit, the e-criminal collects automatically both tokens and honeytokens each time attack toolkit is used. The collected tokens are used to access the e-banking system. Each honeytoken should be submitted only once after which a new honeytoken will be created and assigned to attack toolkit by the group of managers after the old honeytoken is used up. Each toolkit should be updated after submitting a honeytoken to avoid it being detected.

Step 4: The e-criminal gets some valid identities that is mixed with some honeytokens from the attack website, or from the attack toolkit.

Step 5: The e-criminal visits the honeyed e-banking system with the credentials or honeytokens that have been collect. They may wish to examine the validity of the honeytokens, and it is more reasonable, to assume that the botmaster knows how the framework works.

Step 6: The botmaster launches attack by trying to steal money from both the victims' accounts and the honeytokens.

Step 7: A detector placed in the honeyed e-banking system checks all e-transactions with respect to all false credentials or honeytokens. It sends a signal immediately it detects an attack by botmaster trying to steal a good or predefined amount of money from a honeytoken to a non-honeytoken account. The detector marks the receiver's account to be highly doubtful or suspicious which is in turn regarded as "phishing account". This phishing account is usually a mule's account opened and operated in another bank.

Step 8: The affected bank requests for the consent of the prospective victims or the prospective victims contact the bank, for reconfirmation of all money that are transferred from victims accounts to any other account that have being marked to be phishing accounts.

Step 9: The prospective victims then have the right to agree or refuse the transactions through the reconfirmation message. For the case of rejection, their account may be locked temporarily, and their credentials may be reset.

Steps 10: The bank informs appropriate authorities about the doubtful attack activities, it will also inform other banks that are connected and are in cooperation with them such as botmaster mules' accounts. The banks will also send feedback reports to the affected bank in order to update the phishing detector which helps it to make a better decision for future attacks detection.

Step 11: The mules thereafter check whether money has been deposited to their accounts. They make withdrawal on individual basis if money has been deposited to their accounts, either direct from the bank or through Automatic Teller Machine (ATM), and thereafter remit the money to their botmaster. During this process or after their transactions, the appropriate law enforcement agents swing into full investigation using information provided to them by the bank. The law enforcement agents play a major role in recovering the stolen money back since their investigation is the last step of the framework.

The detection of attacks launched on victims account is the most vital step in the framework and it is largely depends on successful submission of honeytokens. This model of anti-phishing framework based on honeypot is shown in Figure 2.

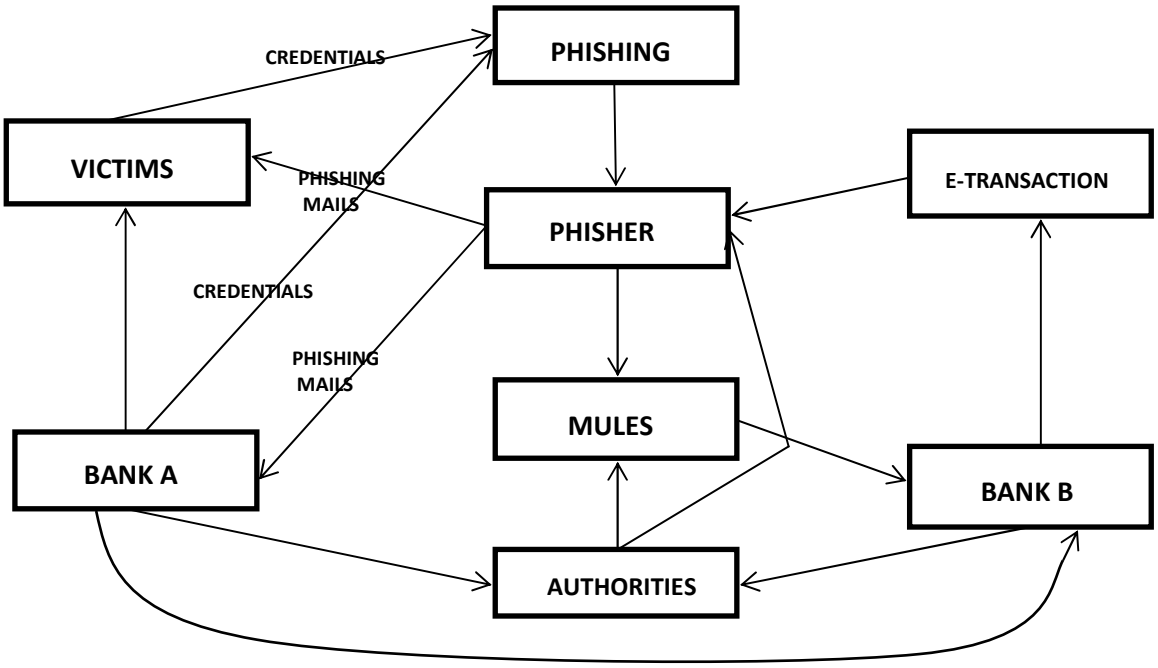

FIGURE 2: The novel anti-phishing framework based on honeypots [16].

[15] in this method make use of toolkits to submit honeytokens to attack website sites and uses honeybots such as Zeus to submit honeytokens to botnets, but it should be noted that they focused on the end-users or the money mules.

2.3 Limitations of the Existing Systems

[17] in their framework only targets to discredit a particular toolkit and the botmasters that created them. They fail to consider the proliferation of attack toolkits which is at increase in the labour market. [16] in their own model made use of toolkits to submit honeytokens to attack websites and uses honeybots such as Zeus to submit honeytokens to botnets. Though they tried to investigate different forms of attack but their targets were restricted to the end users, or money mules, without considering the actual toolkits that empowered them [17]

3. METHODOLOGY

The method adopted in this research is a process method. Starting with a review of the degree of attack and attack toolkits used to launch these attacks and mitigate them one after the other. The first step was to reach different antivirus companies especially Symantec antivirus company who has done a lot of researches on attack toolkits mitigation. Banks, individuals and other security forums were reached to gather information about the most widely used attack toolkits and the type of attack being launched using these toolkits. After the most frequently used attack toolkits were ascertained, it was reverse engineered. After which it was used to discredit the particular author that produce it as well as the end users.

Figure 3 illustrates the enhanced hybrid mitigation model with the following components - a honeyed e-banking system as a honeypot, honeytokens as fake or false identities created and managed by the e-banking system, attack toolkits for getting attack emails and sending honeytokens to attacked network or websites, honeybots for sending honeytokens to botmaster

using attack toolkits. Honeytokens played a vital role in this model and they are used by both the honeybots and the banking system. An attack detector is placed in the banking system to automatically detect when an attack is taking place. We should emphasize that the banking system is not a pure honeypot since it also has all the functions of a normal e-banking system. It can be considered as a semi-honeypot. Figure 3.1 show the diagram of the proposed enhanced hybrid internet attack model, which when closely observed showcases the good work done by [17] and [16] with improvement over their limitations.

3.1 Stepwise Methodology Using the Architecture of the Enhanced Hybrid Mitigation Model

This sub-section gives the step by step attack toolkits mitigation method that is adopted in this research using the enhanced hybrid model. The hybrid model is an organized resolution encompassing different steps of the whole mitigation model adopted to mitigate the effect of attack toolkit in Nigeria commercial banking system and the model is shown in Figure 3.1.

Step 1: The financial institutions sets up a number of virtual machines running a number of honeybots and a number of spamtraps. Each spamtrap or honeybot is fed with a honeytoken. Following the normal characteristics of all bank customers, each honeybot accesses e-banking system from frequently and carryout virtual online transactions. A designated group of personnel in a bank take the responsibility of managing the virtual machines, spamtraps and honeybots. They also monitor doubtful phishing e-mails.

Step 2: The botmasters sends attack mails to prospective victims or infects victims' computers with attack software or attack toolkits, or mounts enhance attacks. The victims can be private or individual organizations, corporate organizations, multi-billion organizations, government of all levels, ministries and parastatals, and honeybot managers.

Step 3: The honeybot manager collects a lot of attack samples of mails from botmasters with the help of spamtraps. The honeybot manager equally monitors some anti-virus companies, other associative bank threat or attack records and other security forum to determine which attack is most paramount and which toolkit is mostly used to perpetrate the attack.

Step 4: The honeybot manager determines targeted websites URL fields by analyzing the identified toolkit using reverse engineering process.

Step 5: The honeybot manager generates false credentials or honeytokens which must appear real to botmasters, and incorporate it to the reverse-engineered toolkit to form honeybot or honey toolkit. These toolkits are also sold to the black market.

Steps 6: Each honeytoken should be submitted only once after which a new honeytoken will be created and assigned to attack toolkit by the group of managers after the old honeytoken is used up. Each toolkit should be updated after submitting a honeytoken to avoid it being detected.

Step 7: The botmaster collects some valid identities together with some false credentials from the attack website, or from the attack toolkit.

Step 8: The e-criminal visits the honeyed e-banking system with the credentials or honeytokens that have been collected to examine the validity of the honeytokens.

Step 9: The botmasters, mules or buyers of stolen credentials launches attack by trying to steal money from both the victims' accounts, and from the honeytokens.

Step 10: A detector placed in the honeyed e-banking system checks all e-transactions with respect to all false credentials or honeytokens. It sends a signal immediately it detects an attack by botmaster trying to steal a good or predefined amount of money from a honeytoken to a non-honeytoken account. The detector marks the receiver's account to be highly doubtful or

suspicious which is in turn regarded as “phishing account”. This phishing account is usually a mule’s account opened and operated in another bank.

Step 11: The detecting bank requests for the consent of the prospective victims through SMS for reconfirmation of all money that are transferred from victims accounts to any other account that have being marked to be phishing accounts. The reconfirmation signal or message will be encrypted using RC6 enhanced encryption and decryption algorithm.

Step 12: The prospective victims then have the right to agree or refuse the transactions through the reconfirmation message. For the case of rejection, their account may be locked temporarily, and their credentials may be reset.

Steps 13: The detecting bank information appropriate authorities on the doubtful attack activities, it will also inform other banks that are connected and are in cooperation with them. The banks will also send feedback reports to the affected bank in order to update the phishing detector which helps it to make a better decision for future attacks detection.

Step 14: The mules check whether money has been deposited to their accounts. They make withdrawal on individual basis if money has been deposited to their accounts, either directly from the bank or through Automatic Teller Machine (ATM), and thereafter remit the money to their botmaster. During this process or after their transactions, the appropriate law enforcement agents swing into full investigation using information provided to them by the bank. The detection of attacks launched on victims account is another vital step in the framework and it is largely depends on successful submission of honeytokens.

Step 15: Public awareness and education to alert the potential victims about easy use of attack toolkits to steal their credentials over the internet and possible measures they can take to avert these threats.

Step 16: Enacting policies and law through the federal government and other anti-cybercrime bodies to fight tirelessly, the botmasters, mules and the black market dealers who make billions of money at the expense of the innocent victims.

Step 17: Internet Service providers (ISP) should put in place adequate internet security technologies to protect their potential customers from this epidemic security threat.

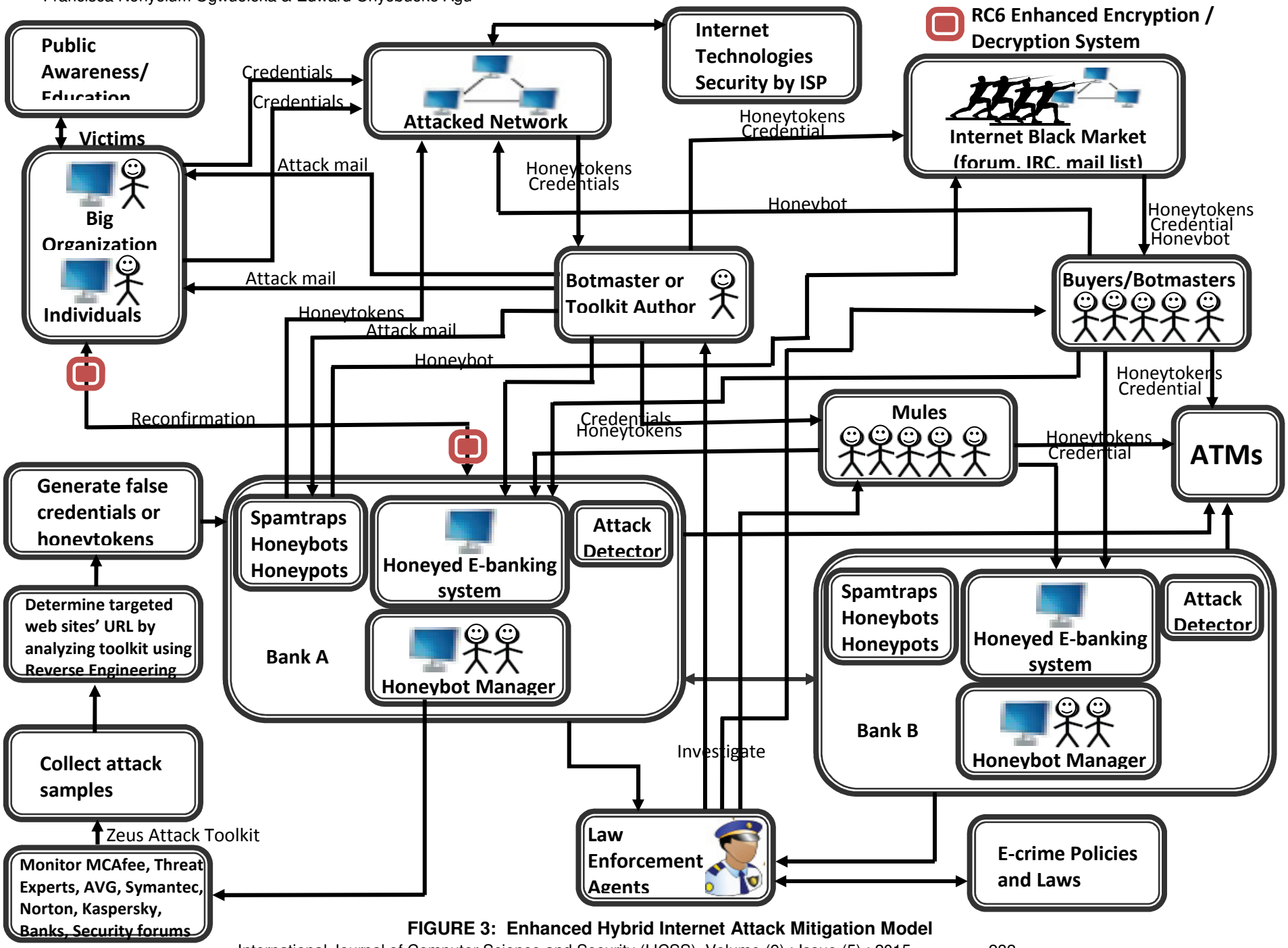

FIGURE 3: Enhanced Hybrid Internet Attack Mitigation Model

3.2 Securing User Reconfirmation Using RC6 Encryption and Decryption Algorithm

[17] in their model proposed that the doubtful businesses or transactions should be reconfirmed at the bank by the bank staff, and not at the user end. Since the victim's system may have being compromised with attack toolkit, an out of band (OOB) medium can be used for the user reconfirmation process. They suggested that the OOB should include short message services (SMS), fax, telephone and postal service, the most convenient and practical medium should be SMS or telephone. With a known OOB medium, the user can carry out the reconfirmation process as follow: when the bank requests the user's consent through an OOB medium and ask the user to plainly reconfirm or refuse the doubtful transaction. The process went further to prohibit modification of the user's contact information in the banking; else the e-criminal that stays in between the two ends will use attack toolkit to utter it. The research equally propose the use of personal identification number (PIN) and transaction authentication number (TAN) to protect updating of the user contact information via telephone.

This existing proposed method of securing reconfirmation process using TAN is not reliable being that the man in the middle that is being avoided from internet medium also exist or have agents in our communication companies which TAN methodology chooses as alternative. The voice calls made from banks through communication medium can still be intercepted either physically by one of the attackers or different attacker working in that communication company, or technically via their broadband. The SMS also faces the same challenge. To enhance the security measure for securing the reconfirmation process as it is the ultimate last step for an attacker to be successful or failed. We proposed deployment of a cryptosystem which encrypt and decrypt the reconfirmation message to cipher text and back to plain text at both server or bank side and client or user side. The cryptosystem uses enhanced RC6 encryption and decryption algorithm together with private key to convert the reconfirmation message to cipher text which are random sequence of notations, symbols, numbers, alphabets etc, as the message propagate through the transmission medium to evade interception by attackers. The message is decrypted back to back to original plain text by the real user or bank official. It is the only legitimate owner who is in possession of the private key can decrypt the message. If the man in the middle intercepts the message, he will find it difficult to decrypt the message which is in turn useless to him. Again, the reconfirmation process should be timed and if there is no response at the end of the duration, the reconfirmation response should be considered negative. The schematic diagram of the cryptosystem is shown in Figure 4.

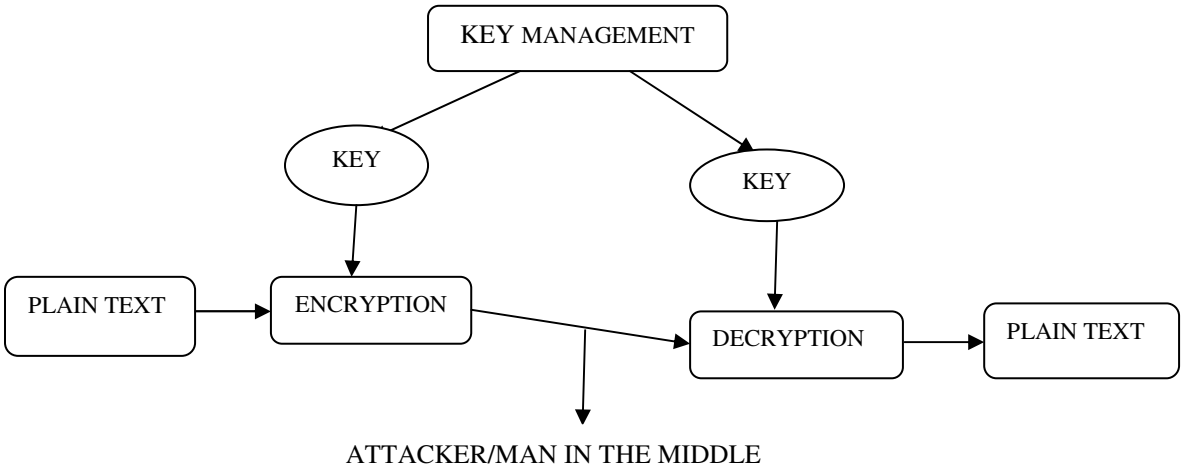

FIGURE 4: A schematic diagram of RC6 encryption and decryption system.

But the ultimate question here remains how do we transmit this secret or private key to avoid it been intercepted? This is been generated and confidentially sealed and handed over to the legitimate account owner directly at the point of creating the account.

4. DISCUSSION AND RESULT

The two subsystems; encryption subsystem and decryption decryption subsystem were tested individually. The result of the unit testing conforms to the set result. The two subsystems were integrated to form the main enhanced cryptosystem.

The testing process: The process of testing adopted in this research involve two major phases which conforms to verification and validation goals (V&V goals); verification ensures that the system conforms to its specification which implies that the system should encrypt/decrypt the reconfirmation messages as specified by enhanced RC6 algorithm; while validation ensures that the system does what the users expected of the system; that is encrypting the reconfirmation to cipher text and decrypting it to plaintext or original message without loss of confidence.

4.1 Test Data

Key 1

"It is just coded"

Plaintext 1

Dear Customer, this is to alert you that a transaction involving a cash transfer of two hundred million naira (N200m) from your account is currently going on. Please send confirmation to us if you actually wish the transaction to go successful. Thank you for banking with us and we look forward to serve you better. Management. .....

Cipher text 1

ØøE æjt w‡ ÿc eN÷ 'K… FV ¿Äß ý:Ñ ¸¢F ß¨—˜uM]^ñÙU ë¸šÖ_ÜèÂoû§ îå K1â QÛ„ zÑ ¶"Ý ÷æk küx Ko× È(9 ýšà ÉD› ×–Ì -ËÙ 'µ žýy á>4 ý+ À%© [‹X H' ˜Ã1 [fj Ih‰ Jl -¿¤ ov> r²r PŸ `Ó~ *|¶ âë3 nëá ¿ ‚‡A êØa yŒ€ 0™g…Ú p"– F ØøE æjt w‡ ÿc eN÷ 'K… FV ¿Äß ý:Ñ ¸¢Fß¨—˜uM ]^ñ ÙU ë¸ šÖ_ ÜèÂ oû§ îå K1â QÛ„ zÑ¶"Ý ÷æk küx Ko× È(9 ýšà ÉD› ×–Ì -ËÙ 'µ žýy á>4 ý+ À%© [‹X H' ˜Ã1 [fj Ih‰Jl -¿¤ ov> r²r PŸ `Ó~ *|¶ âë3 nëá ¿ ‚‡A êØa yŒ€ 0™g…Ú p"– F

Comparing the two results: From expected result/test case and actual test result, it was observed that the test data that is fed into the system for processing is the same as the result obtained after the encryption and decryption process, hence validation goal is achieved.

The result of this research is based on the justification of the new hybrid model. The term hybrid came into play as a result of the combination of the powerful features of the two models (that is, Botnet toolkit defamation process model and the novel anti-phishing framework based on honeypots). The new hybrid model targeted the most frequent used attack toolkits, looked into each one in turn as the most frequent used attack toolkit, perform reverse engineering on it and use it to discredit the particular author in charge of it. The model continues in that trend hunting all the powerful attack toolkits and discrediting them one after the other. The model also attacks the end users or the money mules. The model enhancement is as a result of its adoption of an enhanced Rivest Code version 6 (RC6) cryptosystem which plays a major role by guarding against the malicious manipulations of the man in the middle who is capable of intercepting the reconfirmation message. This is the last step to pull through the transaction if it is returned positive. The cryptosystem encrypts the reconfirmation message thereby hiding it from the attacker through the wireless transmission channel. RC6 cryptosystem is adopted in this research because it has been proved to be free from analytical attack which is also experimented in this research.

4.2 Comparative Evaluation of the current study showing its improvements over the Existing Related studies carried out by [16] and [17].

Existing researches' models by [16] and [17]	The current research hybrid model
• The research carried out by [17] damages the reputation of a particular botnet toolkit by destroying the confidence its users has on the toolkit. • It increases the insecurity of the toolkit users and make them liable for prosecution. • It reduces the profitability of the toolkit with respect to its use to sale credentials. • [16] concentrated on detection of attacks carried out on victims accounts. • [17] in their model proposed that the doubtful businesses or transactions should be reconfirmed at the bank by the bank staff. They suggested that an out of band (OOB) medium should be used for the user reconfirmation process which include short message services (SMS), fax, telephone and postal service,	• The hybrid model creates an opportunity to consider so many other types of botnet toolkits. • It destroys their reputations by making them insecure or unsafe to be used by their users. • The hybrid model creates opportunity to detect and prosecute the attacks launched on the victims' accounts. • It equally go further to root out individual forms of attack and reduces their effects to minimal. • The model also incorporates an enhanced security medium using enhanced RC6 cryptosystem. The OOB suggested by the previous researchers such SMS, fax, telephone and postal service, to be used for reconfirmation of transaction at bank side using PIN and TAN can easily be compromised by both internal attack (biased staff) and external attack (man in middle). • It also improvises e-crime policies and laws as tools to appropriate authorities if adopted will help to checkmate e-crimes. • It equally put in place measures to encourage ISPs to adopt sophisticated internet security technologies to checkmate e-crimes. • The hybrid also proposed public enlightenment campaigns as means of educating the public about the e-crime activities.

TABLE 1: Comparative evaluation of this study with the existing studies by [16] and [17].

4.3 Review of Achievements

This research establishes an enhanced hybrid attack toolkit mitigation model to discredit the toolkit authors. It equally establishes a cryptosystem using enhanced Rivest Code Version 6 (RC6) encryption and decryption algorithm to secure the reconfirmation message which played a very important role in the hybrid attack mitigation model. It proposes some effective policies and laws to the appropriate authorities which will empower the law enforcement agents to prosecute the cyber criminals adequately. One of the intellectual nuggets says that if one is not informed, he will be deformed. Hence, opening the eye of the potential victims to the reality of e-crime through public awareness will go a long way to help them to re-adjust their mentality and method of surfing the internet with security precautions. Therefore, this research also propose public lectures or awareness campaign to education the public which are the potential victims about cyber criminal activities, and also encourage the Internet service providers (ISPs) to adopt more

sophisticated security technology measures to guard against cyber criminality and protect their potential customers.

5. CONCLUSION

Generally, talented e-criminals do not waste their precious time on attacks that will not profit them, and these smart attackers are the ones we are after in this research by putting in place various mitigation measures to discredit the toolkit. From the samples displayed in test data, it is obvious that the code is not transparent. Each letter of the plaintext does not have a fixed relationship to the cipher text. The number of characters in plaintext is 334 and its corresponding cipher text contains 453 characters which is higher. Since the corresponding number of characters in cipher text for every encrypted plaintext is not deterministic, it makes it very difficult to actually correlate a particular character or word in the plaintext to the cipher text.

6. SUGGESTION FOR FURTHER WORK

The implementation of other aspect of this hybrid model should be further looked into. It will be necessary to research for more behavioural methodologies that can be incorporated into this mitigation model. Also to design a measurement metric which will help to find out how much honeytokens are necessary to be injected into the internet black market in order to have major effect on botmasters, buyers and money moles.

7. REFERENCES

[1] M. Y. Rhee. Internet security: cryptographic principles, algorithms, and protocols. John Wiley & Sons Ltd., The Atrium, South Date, Chichestre, West Sussex. PO09 8SQ, England. 2003 Pp 26-298.

[2] F. Marc. “A white paper on Symantec Report on Attack Kits and Malicious Websites”, Symantec World Headquarters, 350 Ellis St. Mountain View, CA 94043 USA. Pp. 17-65. 2011. http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits

[3] Web source write-up on “Security Response from Symantec Corporation” 2010a. http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-

[4] M. Chandrasekaran, R. Chinchani, & S. Upadhyaya. “Phoney: “Mimicking user response to detect phishing attacks”, In Proceedings of the 2006 International Symposium on the World of Wireless, Mobile and Multimedia Networks, pp. 5pp.–672. 2006.

[5] ITU Botnet Mitigation Toolkit Background Information, ICT Applications and Cyber security Division Policies and Strategies Department ITU. Pp. 12-43. 2008. Telecommunication Development Sector. www.itu.int/ITU-D/cyb/cybersecurity /projects/botnet.html

[6] Web source white paper on internet security threat report, from Symantec Corporation http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf;p.1831. 2010b.

[7] A. Ramachandran, N. Feamster, & D. Dagon “Revealing botnet membership using dnsbl counter-intelligence,” in Proceedings of USENIX SRUTI06, vol. 23. pp. 49–54. 2006.

[8] T. F. Yen & M. K. Reiter. “Traffic aggregation for malware detection,” in Proceedings of the Fifth GI International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA08), pp. 207–227. 2008.

[9] G. Gu, R. Perdisci, J. Zhang, & W. Lee, “Botminer: Clustering analysis of network Traffic for protocol and structure independent botnet detection,” in Proceedings of the USENIX Security Symposium. Berkeley, CA, USA: USENIX Association. Vol. 31, pp. 139–154. 2008.

[10] G. Gu, P. Porras, V. Yegneswaran, M. Fong & W. Lee W. “Bothunter: detecting malware infection through ids-driven dialog correlation,” in SS’07: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association. Vol. 19, pp. 1–16. 2007.

[11] J. Goebel, & T. Holz. “Rishi: Identify bot contaminated hosts by IRC nickname evaluation,” in Proceedings of USENIX HotBots07. Berkeley, CA, USA: USENIX Association. Vol. 32, pp. 7-25. 2007.

[12] J. Franklin, V. Paxson, A. Perrig & S. Savage. “An inquiry into the nature and causes of the wealth of internet miscreants,” in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS’07), Vol. 37, pp. 375–388. 2007.

[13] T. Holz, M. Engelberth, & F. Freiling. “Learning more about the underground economy: A case-study of keyloggers and dropzones,” University of Mannheim, Tech. Rep. Reihe Informatik TR-2008-006, pp. 7-28. 2008.

[14] D. Birk, S. Gajek, F. Grobert, & A. R. Sadeghi,. “A forensic framework for tracing phishers, in IFIP Summer School on The Future of Identity in the Information Society”, Karlstad, Sweden, pp. 12-31. 2007.

[15] Z. Li, Q. Liao, & A. Striegel, “Botnet economics: Uncertainty matters,” in Proceedings of the 7th Workshop on the Economics of Information Security (WEIS’08), pp. 9-23. 2008.

[16] S. Li & R. Schmitz. “A novel anti-phisihng framework based on honeypots,” in Proceedings of the 4th annual Anti-Phishing Working Groups eCrime Researchers Summit. Vol. 16, pp. 3 - 38. 2009.

[17] Thomas Ormerod, Lingyu Wang, Mourad Debbabi, Amr Youssef, Hamad Binsalleeh, Amine Boukhtouta, & Prosenjit Sinha “Defaming Botnet Toolkits: A Bottom-Up Approach to Mitigating the Threat,” National Cyber-Forensics and Training Alliance Canada, Computer Security Laboratory, Concordia University, Montreal, Quebec, Canada, H3G 2W1, 2010.