ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

Vulnerability-Threats Assessment for Enterprise Network

Aliyu Mohammed, Sulaiman Mohd nor, Muhammad Nadzir Marsono

Abstract*— the information security management system is to provide clear guideline for risk evaluation and assessment for enterprise networks. The risk evaluation is based on the relationships among the most critical assets, and threats that are likely to those assets and the vulnerability impacts. Threat and risk assessment are conducted to identify the safeguards to be adapted to maintain confidentiality. In this paper, we provide the network security integrity strategy by identifying the areas of greatest risk and concentrate on those triggers like Trojan horses, viruses, and malwares. These factors can degrade network system performance through disclosure of sensitive information and denial of service that result in economic losses. With a look at the risk evaluation, assessment, and factors of return on investment as a whole on the enterprise network infrastructure.

***Index Terms*— Evaluation, Enterprise Network, Information Security, Risk and Threat.**

I. INTRODUCTION

The information security system in enterprise network must ensure that confidentiality, integrity, and availability are uphold within the lifecycle of the enterprises information assets [1],[2]**.** Risk assessment is conducted to identify the safeguards to be adapted [3],[4],[5]. Looking at the vulnerabilities of the system with a view to have effective enterprise network infrastructure control[6]. the framework of information security management system (ISMS) is for risk assessment. Typical ISMS is carried out by the enterprise through the utilization of appropriate tools [1, 7] to evaluate and assess the probability of the occurrence of information security incidence. threats are direct result of the exploitation of vulnerable assets of the network which must be measured and analyzed[8]. While exploitation is as a result of attacks on the compromised number of assets within the system framework infrastructure[9]. Enterprise can design and present effective security policies that are based on the security risk evaluation results[10]. The trends of risk evaluation are carried out within the enterprise framework at regular basis or intervals. In [10],[11],the authors considered information security risk management as multifaceted processes of verification, validation and evaluation of assets within the enterprise, with a security wheel driven characteristics. in this paper, we provide the network security integrity strategy by identifying the areas of greatest risk to the enterprise. Threat triggers like Trojan horses, viruses, and malware are considered and analyzed. With a look at the risk evaluation, assessment, and factors of return on investment as a whole to enable for effective security management on the enterprise network infrastructure[5, 12]. The risk management perspective emphasizes that a proactive nature of risk management is to be considered within the stipulated integrated risk management framework. Thus, risk management in general involves the complete understanding, communicating, and acting to acquire control on risk issues. Assessment scenario involves likelihood, motivation, difficulty, and impact. Assessment concepts be undertaken to see the realities of the situation as it affects the assets. The ISO27001 standards[13] states that, information security evaluation be divided into components that are highly integrated and this include assets, threats, vulnerability, and impact. Doing so will provide meaningful result, as threats are caused by internal, external or both to the vulnerable assets in the system. The internal threats could be as a result of personnel or administrative issues[14],[4],[3, 15]. In these regard qualitative and quantitative security risk assessment in the system is highly desirable[16],[17]. Also causal risk analysis is typically extended to cover joint propagation and interdependent structures within a given network environment[18-19]. The rest of the paper is organized as follows. Section II assesses threat occurrences, exploitation, and vulnerability due to the emergence of malware on the enterprise network environment. Section III introduces risk management evaluation and assessment on the vulnerable enterprise network infrastructure. Section IV considers the possible defense mechanisms against Botnets. We conclude with Section V.

II. THE EMERGENCE OF THREATS ON ENTERPRISE NETWORK INFORMATION SYSTEMS

The security concern on an enterprise network is in its access control, privacy, and integrity of the system information and other assets. The integrity of assets and/or information security gets the least interest; this is for the fact that detecting threats to the network can be very difficult. Some threats to network and data integrity are easy to identify and remediate, others can be extremely hard to detect and / or even more difficult to protect against any form of threat that might be encountered. Enterprise focus on the firewall to handle all aspects of threat management, as these threats can come from anywhere. Common threats are worms and viruses, wireless, guests, and careless or malicious insiders [4]. The security threat identification came in the form of IDS, intrusion detection systems and has proven its worth as a tool in the arsenal of the security analyst. Most enterprises have discovered that the information they get from their IDS is not primarily useful in detection and remediation of immediate threats. An IDS is a protocol analyzer: it's a tool for the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

security analyst to use in diagnosing and identifying problems. In-line with the continuing need for threat detection and management, security vendors have flooded the market with products ranging from in-line intrusion prevention systems (IPS) based on the same core technology as IDS. The application-layer firewalls and highly specific tools are designed to catch a particular type of threat, such as a network worm, Trojans (Bots) and alike. The paramount challenge in managing network threats is in defining the appropriate risk/reward balances on the network. Thus, the difficulty of determining factors like return- on- investment of security products in general purses a serious challenge to the network administrators. With threat management and network integrity assurance, the calculation of return on investment is as hard as it could be[20].The obvious issue is protecting the system against total network failure, since adding integrity checking tools to the network doesn't give a good metric of how much less frequently the network is unavailable or degraded for security reasons. A commonly encountered challenge with deployment of network integrity products, such as intrusion detection systems, is the highly distributed nature of most networks. In a highly switched network, monitoring the integrity of the network becomes a very difficult task. Successful integration of these tools requires understanding of what the threats are and how to detect them. The most successful network security integrity strategy will be identifying the areas of greatest risk and concentrate on those first. That is to say half of the best path forward analysis of the problem. The other half is to examine the technologies that have the lowest cost, both in terms of capital and continuing operational characteristics and support. There are threats that have the ability to degrade not only network and system performance, but they can also expose and disclose sensitive information or cause a complete denial of service that brings about economic losses to the enterprise[21]. A good example of that are Trojan horses, viruses, and malware. Most importantly, it is very easy nowadays to get infected with the various kinds of malware and viruses on the network. These shows that there is high risk of infection, as well as the risk to the network infrastructure. These bring about the reasons that most enterprises network has virus identification and mitigation strategies in all the places as a safeguard.

A. *Threats and the Vulnerabilities*

The users on the network are clearly understood and known, but then, they are into the compromised platform and can inhibit a serious threat to the network despite the fact it is unintentionally carried out. It is therefore necessary to understand the users' entry points and the particular policy management associated to the entry point. This is done by incorporating the end point security determination when defining the policy[22]. Insider threats are often considered as the biggest threat because employees can easily exploit legitimate access to commit fraud. These is through downloading large amounts of sensitive or proprietary data, or commit acts of vandalism such as inserting logic bombs in critical databases. It is so critical to an academic network environment where e-learning is of paramount importance so also research documentations and records. The most common and rampant external network threats for years now have been financially motivated malware and botnets. The builders tries to infect millions of computers with malicious software that is used for stealing credit cards, send spam, and launching of denial of service attacks. In most cases these attacks are broadly targeted and utilizing all known off-the –shelf attack techniques and capabilities to exploit the vulnerable. The trend in the past has been that the zero-day vulnerabilities are being used in conjunction with the sophistication of the construction of botnet. Looking at the current trend it seems the black market sellers are facing great challenges from the buyers who are coming out with new kinds of aspiration to achieve their goals. This quest for great deal of money from broadly targeted botnet is attracting a lot of players worldwide. These attributes are tabulated in the Table 1, indicating the effects of broadly targeted botnet activities on the internet due to either internal or external consequences. To keep all of this activities out of an enterprise network through vulnerability patches and detecting attacks at the perimeter, can go a long way in having a significant challenge.

Table1.Broadly Targeted Attack Techniques and its Sophistication

	Broad	Targeted	Internal External
Off-the-shelf, Tools and techniques	Indiscriminate; Lack sophisticated technical skills; Use tool chest of exploit and malware kits; Botnet builders Financially motivated; malware activity Spam and DoS	Financially motivated; targeted hacks; DDoS attacks; Hacktivists	Internal and External
Sophisticated	Cyber war	Advanced Persistent Threat; Organized; state sponsored teams; Discovering new zero-day vulnerability ; Unprecedented attack techniques;	Internal and External

B. *Network Exploitation*

The terms academic computing is defined as the factors that are associated with utilization of staff, services, and infrastructure. These are the key elements that are involved in assisting in the management and delivery of institutional programmers' like teaching, learning, and research[23].

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

Contextually, the infrastructures include hardware and software systems, while the typical service areas include the undertakings of aspects like technology, information contents and above all the human resources. Thus, it is necessary to understand the main characteristics of academic computing through looking at a framework which encompasses the key operational layers. These layers are segmented and grouped into three compartments as core layer group, support layer and the control layer group. In the academic environment the core layer undertakes activities like teaching and learning, research and publication. While the support layer handles the consequences of infrastructural issues, information and institutional support systems services. The control layer is where implementation of I.T services is carried out, including planning, policy and assessment activities. A view of the framework is depicted in Figure 1.

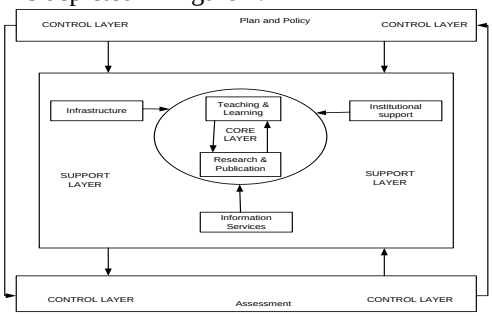

Fig1. Framework Academic Computing [23]

The characteristic of malware infection propagation on the network is being analyzed through the process of attacker's methods of exploiting the vulnerable machines on the Internet. The whole developed world; government; defense industries; and companies in the finance, power, and telecommunication are increasingly being sources of targets. This is due to the overlapping surges of cyber attacks that come from criminals and some of the nations that are seeking for economic or military supremacy over others. In the recent times, the vulnerabilities of applications are far more than that of operating systems. This has been on the increase for the past three years from 2006- 2009(2010) [24]and beyond. The current trend of having web- server being malicious, it leads to the fact that most browsers and client- side applications are being targeted for attacks. These could be observed from the vulnerability diagram in the Figure 2.

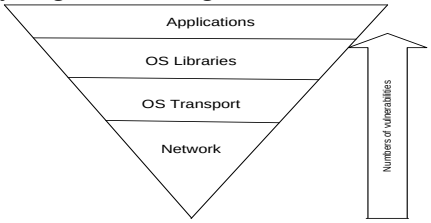

Fig 2. Numbers of Vulnerabilities in Network, OS and Applications

The process of web- application attacks is through exploiting and compromising the web servers. The password –guessing and web – application attacks are paramount, thus the popular targets of attack are Microsoft SQL, FTP and SSH servers that tends to make it easy for password guessing. The attackers are so inclined to the most popular targeting techniques like SQL Injection, Cross – site scripting and PHP file include. With the emergence of conficker / Downadup windows malicious software, the attacks on the Microsoft windows operating systems has been on the increase on the recent past. The variant recorded for the first time as at 2009, stands at about 90% of all the attacks as reported in Microsoft Security Bulletin MS08-067[24] and indicated in figure 3. The number of attacks was seen steadily increasing in the months of March- August of 2009, with July recording the highest as in Figure 3.

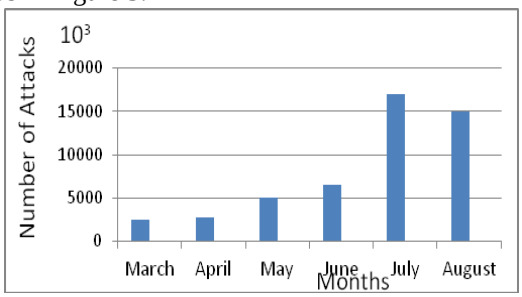

Fig3. Attacks on Critical Microsoft Vulnerabilities (6months)[24]

The trends of malicious attacks from countries that originate the attacks and their possible destinations for some typical prevalent attack categories have been analyzed for a period of six months. These attack categories have shown to be the most prevalent and tends to present high risks of threat to all forms of networks. The typical threat categories are the Server – side HTTP, Client – side HTTP, PHP Remote File Include, Cross- site Scripting and SQL- Injection attacks. It is observed that, there are some levels of overlapping in the characteristics of the attack prevalence. In Figure4, the last three are more or less the subset of the first two, though in their general threat behavior there are some distinct differences and magnitude. The singular consideration of server- side HTTP attacks shows that USA is the most severely hit from the analysis in the Figure 4 below.

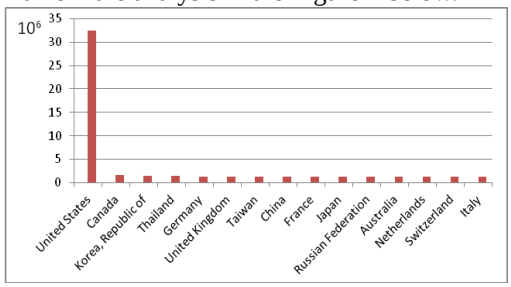

Fig 4. Server-Side HTTP Attacks by Destination Country (last 6 months).

C. Client – Side and Client to Client Exploitation

The trend with which attackers follow to exploit vulnerable clients on the Internet is through the third – party website that is most trusted. These websites are categorized as social networking, photo – sharing, or video sharing or some time

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

through any other web-servers. The process of compromising the clients is by making the contents of the variants on the trusted sites. It establish the reverse shell backdoor on the client side through HTTPS; dumping of the hashes and using pass- the – hash method to attack, and finally passing the hash to try and compromise the domain controller. After gaining the full domain administrator privileges, the attacker will compromise the server machines upon which the secret documents are placed. Finally, the attacker will access the data through virtually the same process with the HTTPS, and try to avoid possibility of being detected while encrypting the gathered information. The diagrams in figure 5 and figure 6 tries to depict the whole process with some unique clarity between client- server and peer to peer modes of propagation and infection processes on enterprise network environment.

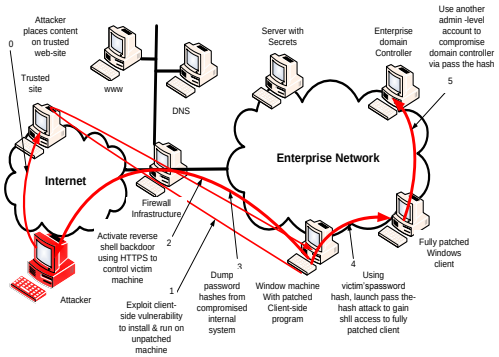

Fig 5 Client Side Vulnerability Exploitation[24]

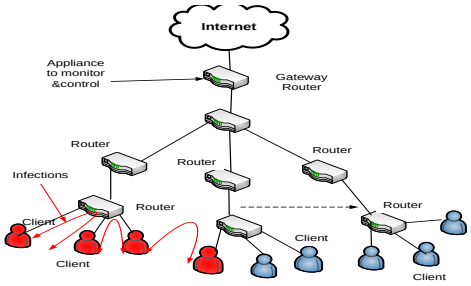

Fig 6. Client To Client Infection Propagation

In the creation and management styles of botnet, there are certain characteristics that it tries to exhibit which is highly skilful and with unique technical ability for exploiting the compromised systems as depicted in the client – server propagation characteristics of Figure 5. Botnet developers came up with resilient intentional procedure termed as Fast-Flux Service Networks (FFSN). These provides for increased significance within the botnet community. These principles of fast- flux have similarities with Content Delivery Networks (CDN) in operational characteristics as indicated in the figure 7. Most bots function as proxy servers and try to send all sorts of client communications to designed server that hides behind a proxy layer in the system. Therefore, all malicious activities could be carried out which includes web page phishing, and / or suspicious kinds of advertisements alike. The developers have a complete configured bots with step by step procedures of its operational characteristics on how to compromise the vulnerable and made available for sale to the customers on the Internet [25], [26]. The complete discussion and analysis of the Botnet propagation mechanisms and the associated modes of network access control are articulated in Section IV.

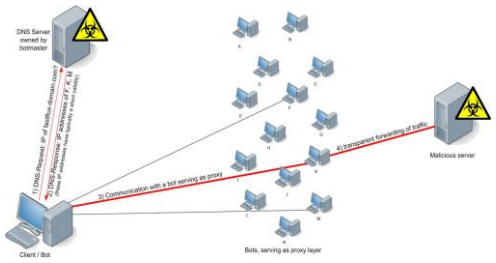

Fig 7: Fast-Flux Service Networks [ENISA Report].

III. RISK ASSESSMENT

The enterprise network information system is huge and complicated with numerous kinds of assets that are scattered all over the environment. Risk analysis activities are focused on assets in order to determine the most critical components to the enterprise network infrastructure. The risk evaluation is based on the relationships among the most critical assets, threats that are likely to those assets, vulnerability that can be exploited and the likelihood and impact of the threats on the assets. Assets- identification is a process that enables for the quantification of the three attributes of information security risk. These attributes are confidentiality, integrity, and availability, this will provide for categorizing the critical assets based on the ability to make good decision. Threats- are an act or usage that can inhibits savior damage to the information assets. While the rate at which the threats happens is considered as the scenario for quantifying the magnitude of the threat. Thus, to ensure the rationale behind the threat, it is necessary to determine the extent through experts by investigating the statistics of the data. Vulnerability- this is an important aspect taken in the consideration of risk evaluation process. Although, vulnerability is in two forms, either technological or organizational. The quantified figure of vulnerability is regarded as the damage caused to the assets as being exposed to the threats that tends to exploit the vulnerability.

A. Risk Assessment Framework

Threat is an attack when successfully carried out against a given system, will cause a harmful conclusion such as information leak, communication loss, network breakdown, and revenue loss. The network attackers achieve their objective through exploiting weakness and vulnerability of threats with possible magnitude of harmfulness to the system. Threat and risk assessment provides the indicator for understanding the characteristics of the system despite the fact that it has been under threat and exploited. Threat and risk assessment are conducted to identify the safeguards to be adapted to maintain confidentiality. Risk management is an activity where threat and risk assessment are continuous processes following the evolution of technology, threat, and safeguards. Threat and risk assessment is best conducted with

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

the use of necessary methodology within which it could be quantitatively or qualitatively articulated[17],[27]. As quantitative methodology tends to output numerical levels of risk representing the clear probability that a threat has been successfully carried out. Thus this entails the following:

(1) Likelihood assessment: this is a risk factor that gives the indication that a particular attacks associated with given threat are actually carried out against a vulnerable asset. Motivation assessment: it is a trend to explore factors that drive an attacker [28]. The authors did identified a general profile of network attacks, where motivation helps to better evaluate and react to threats, and also gives a multiple economic factor as against sole factor effect. The motivations and their considered profiles are as indicated in table 1 below:

Table 2. Round and Pendgraft Profiles of Network Attackers

motivation	profile
Fun and adventure	Script kiddy
Recognition in their virtual community	Malware developers
Propagation of a Message	Hacktivists
Investigation of Potentially criminal activity	Vigilance
Victim's Identity	State Sponsored agent
Steal Money	Thief
Active response against attackers, retaliation	Defensive Hacker
None, compromised / used by other attackers	Innocent Hacker
Law enforcement, pinpoint attackers	Enforcement

(2) Difficulty assessment: is based on the technicalities involved to review the technological barriers being encountered by the attackers in a bid to carry out the threat. Most importantly, the difficulties are dynamic in nature and depend on time and situation.

(3) Impact assessment: it tends to the understanding of the consequences that might arise on the victim's of attack. It tries to evaluate the compromised system or user on the ground that a successful threat has been carried out. In the single user's view point, impact of a threat is rated as Minor when the attack results in only single consequence, and can be attended to and perfected. But when the system serves several users, a threat is ranked with Minor impact if the possible outages are very limited in scope, with few users affected for a short duration of time. This entails that for the user, the impact is considered moderate if and only if a loss of service occurs for only a short amount of time. The consequences of a moderate impact threat consist of outages that are limited in both scope and possible financial losses. Thus, threat carries a significant impact for a user if an attack causes a loss of service for a considerable period of time. This is to say, the targeted system had an attack associated with a significant impact of threat resulting in several outages over a long period of time. With a large number of users affected, possibly accompanied by law violations or substantial financial losses. In confidentiality perspective, having correct evaluation of the motivation/impact of a threat depends largely on the attacker/victim. These tend to consider the levels of sensitivity of the information that can be used to rank the motivation or impact of a threat[29].

B. The Concepts of Return on Investment

Effectively operating an enterprise information system means that the information system can be a large and growing portion of annual budget of organization. Increasingly, IT managers have to consider and review all costs of operating information systems. Once a new enterprise information system is successfully implemented, annual maintenance expenditure on infrastructure, including telecommunication, system's warranty, electricity power supply, will be considered[30]. The process of estimating risk is as articulated in the Figure 8.

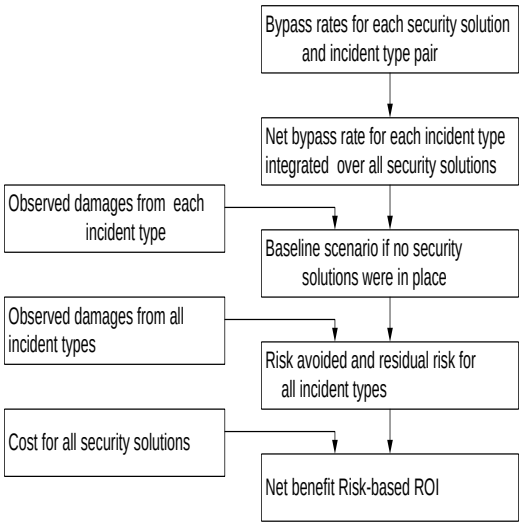

Fig 8. Basic Process for Estimating Risk – Based Return on Investment

The first process to consider is the incident type, these refers to the various types of cyber security- related incidents that an enterprise records. The second crucial concept is bypass rate. Bypass rate is the rate at which an attack results in observable damage to the enterprise. Each security solution has a bypass rate for every incident type. A 100 percent bypass rate means the security solution does not stop incidents of that type. By using incident types and bypass rates, IT professionals can better judge the efficiency and return on investment (ROI) for an enterprise's security solutions. If only one security solution is in place, the expected number of successful attacks in a year is N times the bypass rate for that security solution and given incident type as D. The total unprotected risk to the organization is then N × D, and the expected damage is N × D × net bypass rate for the given incident type[20]. To undertake the required analysis, the data to be in place include the following: Observed damage- this is the damage that the systems in the enterprise sustains in a period of time for a given incident type. The Cost for a given security solution is being its implementation and operational

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

costs. Bypass rate, is estimated for each pairing of incident types and security solution. In general, the framework is based on three phase's factor that includes: - Estimating the net bypass rate for all security solutions; Calculating the incident risk and baseline scenario; Calculating net benefits and risk based ROI (RROI).

$$Baseline, scenario = \sum[Incident, risk(incidentty\,pe)]$$

$$\text{Re}\,sidual, Risk(\text{sec}\,urity, solution) = \sum[Incident, risk(incident, type)XBypass, rate(\text{sec}\,urity, solution)]$$

$$Incident, Risk = \frac{Observed, damage(Incident, type)}{Net, bypass, rate(incident, type)} \quad (1)$$

The equation presents the mode of determining the incident risk as articulated in figure8.

III. CASE STUDY: RISK ASSESSMENT OF BOTNETS

The security at the lower layers of OSI has been significantly improved making attackers to change their strategies to the upper and higher layers of the OSI model. Most attackers get access to the systems through the applicative layers. Thus, Botnets are classified as collection of hundreds of compromised computers to carry out exploits on the available vulnerabilities on the network infrastructure. The harm that arises from these exploitations is much more than the traditional and discrete kinds of attacks that have been witnessed in the past. Having these massive sizes of botnets, the tendencies are that it could be used to form bigger nets to threaten the operational characteristics of an enterprise infrastructure. The botnets network achieves its control through the process called 'command and control' (C&C) strategy by the Botmaster. Notwithstanding, in the operation of botnet, there are forms of bots that exhibits certain characteristics that relay on peer-to-peer control propagation strategies[31-32]. In p2p no botmaster, the attackers form chain reaction of compromised systems to create storming characteristics for exploiting the vulnerable. This singular act is some time referred to as storm malicious behavior. Most new versions of Botnets use p2p communication through the implementation of p2p protocol that is encrypted. These are different types of protocols as against the IRC and HTTP. The malicious Botnets are categorized based on their attack trend to compromise users. These attack trends are Denial of Service, Spamming, traffic monitoring and sniffing, keylogging, mass identity theft, Botnet spread, pay- per- click system abuse and host of others that are not yet common on the Internet. The developments of botnets software are normally done by the malware industries. The developers create the malware and the viruses for their nefarious intents along with economic purposes. The botmasters handles the customized modules that are in form of pre- compiled software packages from the developers [33]. A malware economic characteristics diagram indicating relationship between the developers and the customers is illustrated in Figure 9. It depicts the way the botmaster and botherders handles the control of the bots that are compromised for the various attacks.

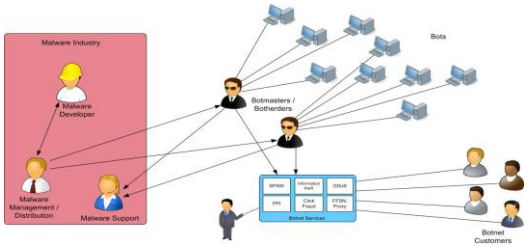

Fig 9: Simplified Role Model Of The Malware Economy [ENISA Report].

C. Botnets Propagation Mechanism

The techniques and the policies that are being used by attackers to spread the malicious bot programs on the Internet are considered as propagation mechanism. The trend of malware propagations previously seen on the Internet is being adapted by current botnets and their botmasters to carry out their threats. The mechanisms for propagation are exploitation, e-mail, Instant Messages, Web-browser, File-sharing, and movable media. These effective propagation mechanisms are carried out by the attackers running the bot-malicious programs in either passive or active processes. These processes are grouped based on their ability to propagate on the Internet. Active processes are the emails, exploits, Instant messages, etc. While, the passiveness by the process of web-browser, movable media, file sharing and a few host of others [35]. The propagation process of botnet is to exploit and install itself by uploading or commanding the victim machine to download a copy of the bots malicious strings[36]. The protocols that are involved in the transactions are FTP, HTTP, TFTP and other services. The Botmaster will have the desired capabilities and strength to consolidate itself strong enough to have control over the bots [37]. The botnets models for propagation are categorized into centralized, decentralized or a hybrid of the two so as to give the botnet a stronger capability to invade possible detection. The analogy of decentralized use the p2p communication to provide resilience to any form of failure in the network[38]. On the hybrid botnet model, the authors in[39] proposed the hybrid that forms botnets into two main groups as servant bots and client bots. The servant bots have both clients and servers with routable IP addresses. The client bots don't have the ability to accept incoming connections and formation of other groups in the network of bots. These groups are dynamically designed with IP addresses, with non- routable IP addresses. They are behind the firewalls and cannot connect to the global Internet.

D. Vulnerability Access Control

Network Access Control technologies addresses the malicious access to enterprise by auditing the security stance of endpoints. They are appropriate updates before any connection to the standard corporate network through the given policy. Once policies have been created, a baseline is used to compare systems connecting to the network with the configured policy. Access Control is used to give the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

connecting system the appropriate level of network access. For example, a system that is in compliance with the baseline will receive full access to the network. The Figure10 shows the typical layer3 vulnerability protection characteristics. The CISCO NAC components and its decision making flow is in Figure 11[40].

Fig 10 Vulnerability Protection

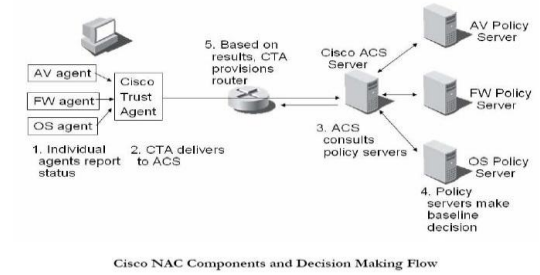

Fig 11 Component and Decision Making [40]

To curtail the excess of botnet and bot, it is required that certain measures and performed activities be carried out in order to limit the menace of the malicious software's used in carrying out the attacks [41] To achieve that level of defense and protection, requires understanding of the controls processes how the Botnets carry out its infection strategies. The users are to be properly educated and offered good knowledge on the characteristics of the bots. The policy that is properly legislated and put into law could go a long way in providing a better control measures on the bots activities[42]. Providing a proactive solution will give a controlled zero-day protection for the network against the effects of attacking scenarios from Bots and malicious software's alike[43].

E. Estimating Risk and Return on Investment

We are able to define risk as the chance that a specific threat will negatively impact an info system by taking advantage of a specific vulnerability. The 3rd component within the risk analysis may be the countermeasure or lack Thereof. A countermeasure is definitely an action, device, procedure, technique, or any other measure that reduces risk for an information system. Consequently, the rest of the risk may be the part of risk remaining following a countermeasure is used. Residual risk might be "none" if your perfect countermeasure is available. These suggested physical model identifies the deterministic (constant) and probabilistic (random) inputs for that target creation of a residual risk-namely, a panic attack along with the expected cost to prevent or mitigate the calculated risk. Probabilistic inputs: The recommended vulnerability values range from zero to at least one (0 to 100 %), accumulated to 1. Inside a probabilistic sample space of achievable final results of "vulnerability," the sum of the odds accumulates to 1. This really is such as the odds from the faces of the die, for example 1 to six, amassing to 1, if the die is fair or moved. A threat is understood to be the prospect of the exploitation of some vulnerability or weakness inside a specific time-frame. Undesirable risks that make the most of software and hardware weak points or weaknesses could affect the breach and introduction to availability, integrity, discretion, and non repudiation. These goes along with other facets of software security for example authentication, privacy, and file encryption.[44] Deterministic inputs: System criticality, another constant that signifies the quality of how critical or troublesome the machine is in case of entire loss, is taken to become a single value akin to all weaknesses having a value varying from to at least one. Criticality is low if residual risk is of little if any significance, like the deterioration of the office printer; however in the situation of the nuclear energy plant, criticality is near to 100 %, because its security has vital safety implications for humans. Capital (investment) price is the entire expected reduction in financial models (dollars) for that particular system if it's completely destroyed and can't be applied any longer, had the machine ongoing to create added value for other areas from the system or society. These are as depicted in the Figure 12, for the determination of the residual risk.

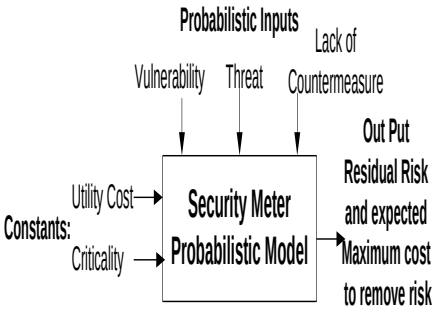

Fig 12. The Quantitative Security Meter Probability Model for Probabilistic and Deterministic Input

By applying the probabilistic inputs to the security meter system, the residual risk factor could be determined analytically through the factors as indicated below: Residual Risk = Vulnerability x Threat x Lack of Countermeasure

$$= V \times T \times LC \quad (2)$$

While the final risk level can be obtained as:-

Final risk = Residual risk x Criticality

$$= RR \times Cty \quad (3)$$

To finally determine the expected cost of loss that relates to the enterprise capital cost is to find the product of the final risk and the enterprise capital cost for the given investment.

Expected Cost Loss (ECL) = Final risk x Capital cost

$$= FR \times CC \quad (4)$$

Thus, the determination of the expected loss cost is obtained through taking the final risk of the enterprise systems and the infrastructures capital cost as a product of sum. These show a method of considering for the computation of effective return on investment for the enterprise network.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

VI. CONCLUSION

Threat analysis methods provide an effective ways of differentiating between actual and perceived risk on the network. Risk evaluation is a challengeable task and a long term issue for running of robust enterprise networks infrastructure. The evaluation result goes a long way in helping the management to improve on the levels of information security system of an enterprise. Understanding of malicious bots and botnets and their associated characteristics is a critical part in recognizing how to effectively protect against the overall malware threats on the enterprise network environment. The Botnet attackers are moving away from the normal centralized concept of C&C channels to the decentralized (p2p) to gain resilience against being detected. We have shown through our analysis the ability to have a comparable concept of verification, validation and evaluation results. We have given the overall importance for measuring and understanding of threats and information security risk management as a view point of enterprise environment. With clear concept it will provides for a trust in the expected levels of security to also ascertain whether organizational security investments paid off or not through a measure of return on investment.

REFERENCES

[1] R. Bernard, "Information Lifecycle Security Risk Assessment: A tool for closing security gaps," Science Direct- Computers and Security, 2007.

[2] "Managing Information Security Risk :Organization, Mission, and Information System View," NIST Special Publication 800-392011.

[3] R. McNamara, "Networks--Where does the real threat lie?," Information Security Technical Report, Elsevier science, vol. 3, pp. 65-74, 1998.

[4] C. Colwill, "Human factors in information security: The insider threat : Who can you trust these days?," Science direct-information security technical report, 2010.

[5] V. Viduto, et al., "An analytical evaluation of network security modelling techniques applied to manage threats," IEEE, 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, 2010.

[6] M. T. Siponen and H. Oinas-Kukkonen, "A Review of Information Security Issues and Respective Research Contributions," The Data Base for Advances in Information Systems, vol. 38, 2007.

[7] X. Lv, "Information Security Risk Evaluation for E-Campus," IEEE, pp. 2153-2154, 2011.

[8] O. H. Alhazmi, et al., "Measuring, analyzing and predicting security vulnerabilities in software systems," Science Direct-computer and security, 2006.

[9] T. N. Dinh, et al., "On New Approaches of Assessing Network Vulnerability: Hardness and Approximation," IEEE -ACM Transactions on Networking, 2011.

[10] S. Fenz and A. Ekelhart, "Verification, Validation,and Evaluation in Information Security Risk Management," Copublished by the IEEE Computer and Reliability Societies2011.

[11] T. R. Peltier, et al. (2005). Information Security Fundamentals.

[12] E. K. Banks, et al., "Trusted Geolocation in the Cloud: Proof of Concept Implementation (Draft)," NIST Interagency Report 7904 (Draft), Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2012.

[13] "ISO/IEC 27001:2005 Information technology — Security techniques," 2012.

[14] Q.-J. Yeh and A. J.-T. Chang, "Threats and countermeasures for information system security: A cross-industry study," Science Direct, Information & Management, pp. 480 - 491, 2007.

[15] M. L. report, "2012 Threats Predictions," 2012.

[16] S. Kondakci, "A Composite Network Security Assessment," The Fourth International Conference on Information Assurance and Security,IEEE, 2008.

[17] Y.-k. Zhang, et al., "A Qualitative and Quantitative Risk Assessment Method in Software Security," 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICA CTE),IEEE, 2010.

[18] S. Kondakci, "Network Security Risk Assessment Using Bayesian Belief Networks," IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, 2010.

[19] S. Kondakci, "Intelligent network security assessment with modeling and analysis of attack patterns," Security and Communication Networks,Published online in Wiley Online Library 2012.

[20] A. Arora, et al., "Measuring the Risk-Based Value of IT Security Solutions," IEEE, 2004.

[21] D. F. Drab, "Network Peripherals: A Weak Link in Security and an Open Gateway for Attackers " 2006.

[22] I. X.-F. 2011, "Mid-year Trend and Risk Report, September 2011," 2011.

[23] S. A. Mokhtar, "Academic Computing Components in Malaysian Higher Education," Proceedings of the Postgraduate Annual Research Seminar 2005, 2005.

[24] " SANS: The Top Cyber Security Risks," SANS2010.

[25] P. Barford and V. Yegneswaran, "An Inside Look at Botnets," 2006.

[26] A. H. Lashkari, et al., "IRC Botnet Major Issues and Solutions," 2011 2nd International Conference on Networking and Information Technology IPCSIT vol.17 (2011) © (2011) IACSIT Press, Singapore, 2011.

[27] Y. Carlinet, et al., "Analysis of Computer Infection Risk Factors Based on Customer Network Usage," The Second International Conference on Emerging Security Information, Systems and Technologies(IEEE), 2008.

[28] N. Pendgraft and M. Rounds, "Diversity in Network Attacker Motivation: A Literature Review," presented at the International Conference on Computational Science and Engineering, 2009.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

[29] M. Barbeau, "Assessment of the True Risks to the Protection of Confidential Information in the Wireless Home and Office Environment," 2010.

[30] S. Panjwani and S. Tan, "Assessing Trusted Network Access Control Cost- Benefit Factors," 2007.

[31] "Defeating the Botnets of the Future," 2012.

[32] M. Merritt, "Bots and Botnets—A Growing Threat," 2009.

[33] "Call Centers for Computer Criminals," 2010.

[34] "Botnets: Detection, Measurement, Disinfection & Defence," ENISA2011.

[35] X. Li, et al., "Understanding the Construction Mechanism of Botnets," Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing,IEEE, 2009.

[36] C. Shannon and D. Moore, "The Spread of the Witty Worm," Cooperative Association for Internet Data Analysis (CAIDA), 2004.

[37] Kim-Kwang and R. Choo, "Zombies and botnets," Trends & Issues in crime and criminal justice,Autralian Institute of criminology, 2007.

[38] R. Puri, "Bots & Botnet: An Overview," GSEC Practical Assignment Version 1.4b Option 1 – Research on Topics in Information Security, 2008, 2003.

[39] P. Wang, et al., "An Advanced Hybrid Peer-to-Peer Botnet," IEEE Transactions on Dependable and Secure Computing,, vol. VOL. 7, NO. 2, 2010.

[40] R. Langston, "Network Access Control Technologies," 2010.

[41] S. Stankovic and D. Simic, "Defense Strategies Against Modern Botnets," (IJCSIS) International Journal of Computer Science and Information Security, 2009.

[42] "Cisco Intrusion Prevention System Solutions," 2009.

[43] "Guide on Policy and Technical Approaches against Botnet," National Computer Emergency Response technical Team/Coordination Centre of China (CNCERT/CC)2008.

[44] M. Sahinoglu, "Security Meter: A Practical Decision-Tree Model to Quantify Risk," Infrastructure Security- IEEE, 2005.