ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

# State of Cyber Security: Emerging Threats Landscape

[I]Alhaji Idi Babate, [II]Maryam Abdullahi Musa, [III]Aliyu Musa Kida, [IV]Musa Kalla Saidu
[I]F.C.E. (Tech), Potiskum, Yobe Nigeria
[II]ATBU, Bauchi Nigeria
[III]Middlesex University London, United Kingdom
[IV]F.C.E. (T) Potiskum, Yobe Nigeria

**Abstract**
*Computer Security has become a major challenge in the present years due to the continuous global technological development and the different possibilities for the use of computer. Cyber threats are growing at an alarming rate and at the same pace with the online use of Personal Computers and mobile devices. This work surveys the state of Cyber Security emerging threats landscape, through the overview of related works reported between 2011 and 2013 in the literature by stakeholders and experts in Information Technology (IT) industry. Different type of Cyber emerging threats such as malicious attack, network attack and network abuse have been identified with specific interest on virus, Phishing, Spam and insider abuse to mention but a few. It has been established that these Cybercriminals tools are exhibiting common level of sophistication and advancement as the advances in Computer and mobile technologies. The available countermeasures are found to be satisfactorily effective, yet Cyber criminals are creating new measures to overcome Security mechanism. It is also envisaged that as the technologies advances, a resultant proliferation of cyber threats will be witnessed. Thus, a few government and Information Technology (IT) stakeholders' strategic policies to help in combating cyber threats were presented.*

**Keywords**
*Cybercrime; Attack; Landscape; Threat; Malware*

## I. Introduction

The perceived benefits of Computer technology were affected greatly by the increasing concern with internet crime today. This truly presents a major challenge to Security of the internet world. Cyber Security can essentially be defined 'as the body of technologies, practice with coordinated series of actions, designed to defend Networks, Computers, System Application Programs and data from an Attack, Damage or Unauthorized Access' [20]. Cyber Security experts classified Cyber Emerging threats as malicious attacks, network attacks, and network abuse. Malicious attack is any effort to exploit another person computer and infect the system resources through Virus, Trojan horses, Spyware etc. Network attacks are intended actions meant to damage or disturb data information flow of the Computer System on a Network Service account, which causes effects such as Denial of Service (Dos), Session Hijacking, Email Spoofing etc. [5]. Network abuse is fundamentally an exploit to the point of interaction of a network, and it could be utilized by actions such as spam, phishing, pharming etc. [17]. Cyber-attacks are widely, viewed as criminal action led by means of the Web. These exploits can incorporate taking an Organization's intelligent property, seizing online bank accounts, designing and circulating Viruses on different Computers, posting secret Business Data on the Web and destroy a nation's basic national Infrastructure. Internet threats are seen as the highest failure to business and revenue loses of all Organizations [27]. As put on by Tatum, Cyber Attack can be defined as…

"An attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission; Attacks of this type may be undetectable to the end user... or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks" [35].

This definition clearly described the manifestation of how serious of the problem with Cyber Attacks, and because of the increasing sophistication of these kinds of network attacks, a research by International Telecommunications Union (ITU) reveals an estimated survey report of about $1trillion was lost to Cyber related frauds globally in 2012, out of which $390billion was accounted for justification [16].The initial phase of this research will encompass an extensive literature review on the increasing sophistication and maliciousness of Cyber Security emerging threats that create unique challenges to federal information systems and government wide cyber security efforts. The review will critically discusses the current state and future forecast of States of cyber Security, the existence of internet threats landscape in administering government agencies. It will also put down some recommendations needed to combat the threats. An administrative and IT Stakeholder's Policies which if completely executed will work find in the fight against internet crime. These policies were recommended as a tool in fighting against the current and future risen cases of Cyber related crime.

## II. Research Methodology

The data for this research were derived from secondary sources: previous researches and analyses of scholars; books, Journals, Conference proceedings, white papers and Government publications on cyber security that are related to the current trend of cyber emerging threats. As the study involved an extensive literature review which critically analysed the present state of cyber security: emerging threats landscape. It lays down the policy to enhance cyber-Security and the critical steps to acquiring the know-how on how to deal with the emerging cyber threats; and the content analysis approach was utilized for analysis.

## Threat Landscape

The Persistent growth of internet threats in the world today standout amongst the greatest challenges to Cyber Security in the 21st Century; this research finds out that the dissemination of threats in the 21st century is from a wide number of sources. These emerging threats show themselves and get to be extremely destructive focusing on Government intellectual property, Financial Organizations, and Industries etc. Crafting from this explanation threat actors can specifically be viewed as 'element that cause or help in attaining digital incident' (Verizon, 2013). The work of

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Djambazova and his Colleagues further explain the meaning of threats and finally, point out the following definition as:
"A threat is any indication, circumstance, or event with the potential to cause harm to an ICT Infrastructure and the assets that depend on this infrastructure" [10]
The literature of ISO/IEU (2012) and EU green paper also support this definition. This definition is a description on the dynamic approach to threats landscape that develops with increasing sophistication in technology. According to September, 2012 report by ENISA threat landscape, the report defines Threats landscape as a rundown of threats holding data about threat risk and attacking vectors that might results in taken over valuable resources or asset of a Computer System when an attacker exploits the system weakness [22]. It is important to control our system asset against threats, because our asset is what we value when dealing with the technology. The scenario here describes the destructive danger of threats landscape for example threats for Smartphones, threats for PCs and threats for app-Stores [3]. Building on this Conception by describing the effect and level of threat landscape with respect to its exploitable priority on a Computer System, ENISA reports point out how different Combination of threat information were identified based on precedence, with regards to threat agents, exploits, vulnerabilities and in some cases made the online clients come very close to the risk landscape. Threats are actually dangerous for open security of the online community and this is due to its unpredictable behaviour globally. Covering malicious use of information technology wasn't difficult; this means threat actors can operate with significant exemption from essentially anywhere (Verizon, 2013). A summary of threat infection was also reported by Microsoft (2009, 2010) which reveals that threat landscape in developing countries such as Nigeria was dominated by Malware, as it was reported of bout 75.1 and 76.2 percent of all threats discovered on most affected computers as of early and towards end of year 2009 in a separate independent research [7].
Generally, the fundamental reason for destruction differs generally from the expertise being showed, to the theft of cash or information etc. The real sources of these threats incorporate criminals, terrorist and people supporting the attacks. The inception of malicious Code and strategies are from attackers and criminals.

## III. Emerging Cyber Security Threats

Each nation over the globe is encountering different sort of threats. Essentially, any task of Securing the Web and staying ahead of emerging threats could be a daunting Job; even for PC clients who are freely at ease with the technology and language of security specialist. There is not a week that passes without reports of a Virus infection, Hacking attempt or 'Phishing scam'. Consequently, various PC clients, even those people who have installed security software such as Firewalls, anti-virus and precise filtering software could be at risk to security threats and software breaks [21]. Ordinarily these threats could be identified into malicious, network attacks and network abuse. Malicious include computer viruses, spyware, Trojan horses, key loggers and BOTS. Network attacks include session hijacking, denial of service (DOS), and spoofing and web defacement. Likewise Network abuses include SPAM, phishing, and pharming and basically some of these threats are explained below with respect to their Network related forgery cases:

### Phishing and email Spamming

This can be defined as a type of threat through the internet, or flooding of the Internet or any unwanted online correspondences. The requests gathers client's credentials using a deception technique. In order way phishing could be described as an Internet fraud in such a way that the attacker will acquire details like, stealing of passwords, bank account details, credit card numbers and other private information [1]. In recent times, law enforcement agencies and the judiciary appear to be taking cyber-crime more seriously. As in the case of July 2011, an individual was evidently 'sentenced to more than twelve years in federal prison for his conduct in an international phishing and email spamming ring that stole the identities of more than 38,000 people' [28].

### Botnet

A Botnet is a guard of compromised Systems, sometimes called "zombies," that are under the command and control of a solitary "Botmaster." [1, 6]. A botnet are accumulation of computers networked together that are no doubt regulated by Cybercriminals for malicious and unlawful purposes. Botnets are currently turning into a key threat for the cybercrime since they are designed deliberately to disturb targeted computer systems in so many different ways. Many infected computers can figure out how to disturb and disseminate malicious code, virus and spam [6, 25]. Figure 1 describes the life cycle and approaches for detecting botnets, and how to combat the growing concern of Bots. As Banday argue 'the process of building a Botnet requires least and technical programming skills' [2].

### Malware and Spyware

These are malicious program designed to gather computer information without the awareness of the client [8]. [34] reportedly identified Malware as one of the key threats to Businesses, Governments and people [7]. For instance, in 2009 the number of new malware signatures was accounted to be just under 2.9 million, a 71 percent increase over 2008 [34], yet more than 286 million new malware variants were discovered by Symantec in 2010 [34]. The movement in motivation from interest and fame looking to illegal budgetary increase has been marked by a growing sophistication in the evolution of malware [7].

### Key loggers

Key loggers are programs that can screen and record the client keyboard information while typing into Computer System for later access. Key loggers store the data or send the information secretly to the other programs. They can record usernames, massages and secret key for remote systems and computer application. Some key loggers oblige the right to gain access of the criminal invader or attacker to get the data from the machine while other forcefully transfers the data to different machines by means of email; file transfers etc. [29]. Sagiroglu and his Colleagues further find out that the personal use of keyloggers can be beneficial, because the use of keylogger may assist private computer owner to enhance his daily routine with much privacy. With keylogger is possible to recuperate content wrote into word processors, spreadsheets, and computer programming environment after an application or system crash [29].

### Social Engineering

'Social Engineering (SE) is a developing Science that plays on the trust Component of the human intelligent' [30]. Social engineering

is a kind of technique in which it traps or tricks the client to reveal valuable information. The user will think the reason is honest to goodness yet the aim is truly criminal. Okenyi and Gaudin, further explains that SE relies on the trusting nature of individuals as it depends after getting unapproved secret information through mimicking people by means of Nontechnical means; Consequently SE can be viewed as "the human side of breaking into a corporate network" [26, 15 and 30].

### Denial of Service (DOS)

This is an attack that upsets the ordinary function of the computer system and thus prevents access to authorized users. Karthik, define DoS attack as an incident in which a Client or organization is deprived of the services of a resource they would regularly expect to have [19]. DoS is legitimately a resource overloading attacks that may have the likelihood of either smashing the host such that it can't communicate properly with the rest of the System, in this way the services may remain inaccessible to customer clients.

### Virus

A virus is a program that spreads itself from one computer to another computer without the users' authorization to do so, and they distribute themselves to the infected files or programs of a PC. Viruses cause negative and unforeseen event when the machine runs. Different kind of viruses has distinctive purpose. Some are designed to trap clients and some are designed to destruct Machine programs. They can harm computer programs and they are actually presented through email attachments [31, 38]. Consequently computer virus can additionally be spreads by connecting itself to executable files of systems areas, on external storage devices such as USB plash drives.

### Worm

A worm is usually a computer Program that moves itself from one machine environment then onto the next machine environment often keeping record of the last environment it has entered. Worms are self-duplicating programs towards oneself which essentially implies that they don't require a host program to attack a victim. When a worm moves to another environment it can do whatever it needs as per the obligatory access controls [37]. In the case of Virus it requires human intervention but worms do not and it moves round via the internet connection.

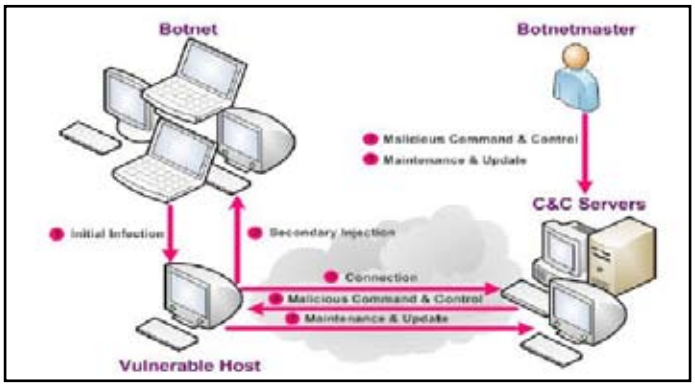


Figure 1: A typical Botnet life Cycle

## IV. Historical Threat Situations

The way at which Cyber-security is threatened by threats actors is different across the board; the target could be local or general and as a consequence of these the system is currently growing as a powerful threat Vector [36]. At this section the research discusses and overview of the threats landscape challenges and the growing concern that has evolved in the internet for malicious activity. However, based on the analysis of the identified Vulnerabilities of the threat landscape the research observed that malicious techniques and technology continued to grow more sophisticated. And this growing concern is now a challenge to Cyber security experts. Protecting against these attacks will be the next challenge this literature review is out to address. Consequently, because of the complexity of the subject matter the research will only discuss an overview based on a collection of threats landscape starting from 2010- 2013. These periods were chosen because the emerging threat discusses the current concern of today's cyber security age. As pointed out by Symantec study 'threat landscape is dynamically changing' [34]. This assertion truly supports the current proliferation of internet technology.

### Landscapes in 2010

The continued progressions of emerging threats are getting to be more alarming. Malicious attacks continue targeting developing countries, where the primary targets are financial Companies, and Industries. Web based attacks are increasing and all of this affects the online underground economy which are benefitting in the global economy. Threats landscape in 2010 creates a road for Cyber criminals infiltrating social Networking sites, Industrial infrastructures, health/medical and banks with spam and malware [36] It is at this instance that Spam and malware pick up a high momentum penetrating social networks such as Facebook and twitter; additionally Spam utilizes a HTML technique and plain text to achieve its aim.

## V. Attacks on Industrial Infrastructures

Stuxnet worm was found to be the most popular malware threat in recent histories. It has been designed to target critical Commercial enterprises. It's a complex worm which it spreads itself through USB devices, likewise it can duplicate itself and be shared across the network. Stuxnet was found to be one of sophisticated worm which can easily adjust complex system Configuration for example adjusting motors; stopping factory and can cause things to explode [12].

### Attack on banks

Threats landscape 2010 as it was nicknamed 'the year of Spam distribution'. It was in 2010 that a threat called 'ZEUS' was designed to steal internet banking details for Customers. ZEUS is a standout amongst the most widely recognized Malware. The year 2010 experienced the most high profile incidents which creates greatest impacts on customers and Security Industry. The spam distribution of 2010 were listed as: Stuxnet worm, ZEUS, ZBOT, the IE and other zero day attacks, Mariposa Botnet users, FAKEAV etc. [36]. Figure 2 describes the spam type distribution threats charts in 2010.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

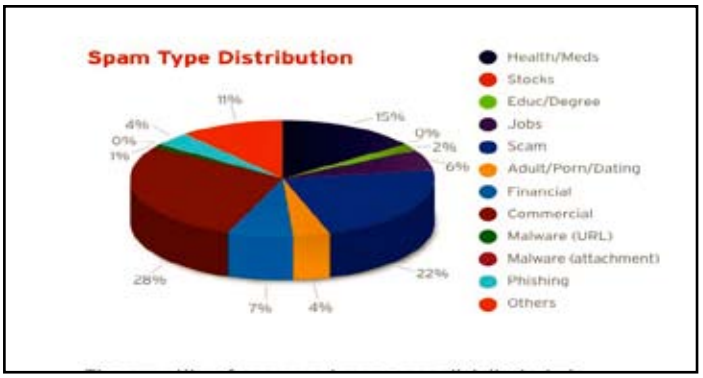

Fig. 2: Spam type distribution Sectors Chart

## Landscapes in 2011

2011 denoted the fast development of threats which comprises data breaches, Social Networking scams, Android Malware, Malicious Spam, and Phishing Attacks. Malware threats for Android Platform kept on increasing all around the year despite the fact that there is an increasing visibility and media consideration on Mobile Malware, the most focused devices are desktop Computers. Desktop Computers stay to be the most widespread PC based Malware threats. Threats landscape 2011 witnesses' major growth forces in online threats and online Cybercriminals [13]. Phishing earmarks the most focused attack in 2011, targeting on a selected group of users rather than spreading messages to random addresses. Phishing attempt is a technique used to trick people certifications and have access to their accounts. However, the increase popularity of the social networking sites particularly Facebook has been focused by online Phishing. Usually Facebook users encountered spammed messages to persuade users to act in numerous way; these are all malicious threats that put users at risk [34]. Aattackers normally spread Malicious Spam using Social Engineering techniques by attracting Clients to open an attachment or direct them to click a connection [13].

## Landscapes in 2012

As pointed out earlier that emerging threats landscape are challenges in the field of Cyber security we may observed that during 2011, Cyber Security incidents included theft of intellectual property and government data, Hackivism, Malware targeting Mobile devices and a recurring target to financial information [34]. So what is in store for 2012 will be a concise roundup of Cyber Security threat landscape migrating to Mobile Application devices. Consequently, as the utilization of mobile devices continues to grow, the volume of attacks focused to these devices will also grow (William and Pelgrin, 2012). Every new smart phone, tablet or other portable device gives another window for a potential Cyber-attack. The dangers include access to data, such as physical location or contacts records, and the capacity for the Apps to download Malware, such as keyloggers or programs that spy on phone calls and quick messages. Attackers are quickly figuring out how to collect legitimate applications and repackage them with malicious code before selling them on different channels to the unsuspecting client [22]. The situation here is not a prediction is a warning because smartphone compromise is a reality, and a compromise phone can release information about you or your business, and this kind of abuse can have serious consequences. Analysing on this situation we will understand from a report by TechTarget, which shows that the worldwide transformation of mobile devices, smartphones specifically, is opening considerably more chances for Cybercriminals and thefts, with Cybercriminals moving their target toward mobile users and far from the accepted PC environment (Techtarget, 2013). In fact, 2012 threats landscape is a move by Cybercriminals specifically targeting users of mobile devices; on the grounds that mobile devices are presently more powerful than the computer alone; and the assumptions were they are no longer just phones, they can actually be seen as our Assistance, Advisers, or closest companions.

## Landscapes in 2013

The year 2013 has conveyed big news, important changes and accomplishment in the Cyber threat landscape. But yet the moral force between defenders and attackers will continue to exist and the projection is that it will continue even far in the future [23]. But as the technology evolves, so too do the techniques used by Hackers and Cybercriminals to infiltrate our information system, this could be understood from the perception of Browning which says "….Every progress we make, someone else is making their own leaps and bounds in terms of their ability to attack and infiltrate our system"(TechTarget, 2013). These current challenges in technology forces cyber-security experts to always stay one step ahead of these threats to protect the integrity of our information system. Digesting from an overview of ENISA threat landscape 2013, the report is a collection of analysis of over 250 different sources of Cybercriminals cases; and the perspective of the research shows that 2013 has brought good and bad developments [23]. The two perspective of threats landscape of 2013 can be viewed as follows:

### Bad developments (Negative)

- Development of Cyber criminal's activities has grown maturely focusing mostly on Government and Private Commercial Institutions.
- Cyber-crime goes Mobile: Cyber criminals are now experts in social engineering with attack patterns and tools targeting and compromising our mobile devices.
- The two emerging digital battle fields: big data and the internet of things a concern to Cloud Storage Security services [23].

### Good developments (Positive)

- Law enforcement agent had succeeded in binding up a strong international Cyber policy as this lead to the arrest of gang responsible for the spread of Police Virus.
- Because of the risen cases of Cyber-crime threat analysis was encouraged and this provides valuable information to Cyber experts.
- Vendors had now constantly updates there products for security patches.
- Cooperation among organisations was achieved all in an effort to fight Cyber-crime.

The report of ENISA 2013 concluded with recommendation to train and involve end-users strongly with the view to assist in fighting cyber-crime [23].

## VI. Assessment of Current Day Situations

Cyber security has been called one of the best constraining national security issues facing the information age of the 21st century. Because the current situation shows that attackers were against information infrastructures and the perpetrators have ended up becoming more expert and likewise attacks get to be more

continuous and complicated. Cyber-Criminals utilize the internet as a medium for their exercises and managed covert attacks. The likelihood of retracing and reacting to the attacks are fairly restricted. The primary inspirations of such attacks are mostly by financial concerns, which in a manner involve new vulnerabilities. Specifically, looking at the cyber threats environment and the complexity of the sophistication of vulnerability of information infrastructures, the Cyber security situation will remain basic even in future. However comparing 2010-2011 all in all, there are few progressions of the way of DOS attacks. In 2011 the amount of attacks expanded marginally by 2% compared to 2010. The previous years the attacks were scarcely consistent with a slight difference. [36].

It has been found out from the survey research of Kaspersky that the attacks in 2012 will increase and packet per second volume will continue to ramp up [18]. It is also said the DOS attacks are really changing and are dramatically becoming more damaging. The study showed that in 2012 online businesses experiences a very big challenge in developing effective countermeasures that act toward enhancing the devastation of DOS attacks [5].

Key threats and Countermeasures

According to [33] he proposes that security experts might as well put countermeasures in place and they must be so vigilant in mitigating such kind of threats. As new countermeasures are being created new threats are really uncovered. However the key threats are Malware, Spam and Phishing. A few countermeasures that ought to be taken are; organization might as well establish a secure policy foundation, Strong authentication should be used, avoiding storing sensitive passwords as simple text, securing protocols during sessions, educating and creating awareness to clients on proper security protocols, strong authorization ought to be utilized, international co-operation should put hands together and battle threats etc. A collection of literature from the evidence of survey by 'Australia's National research and knowledge centre on crime and equity' [7], in the study Choo speaks out his perception on the best strategy to be adopted in battling with all issues relating to Cyber-attacks, even though he began with the assumption that 'currently no single technology could totally eliminate cyber security threats' but however, some few existing internet vulnerabilities could in due course be removed by effectively utilizing good security practice and tools. Building on this idea the Defence Signals Directorate (DSD), argue that no less than 70% of the targeted Cyber intrusions that DSD uncovered in 2009 could no doubt be controlled if organizations strictly adhered to the four methodologies already prescribed by DSD, and the recommendations goes as follows:

1. Organizations should ensure the use of an updated latest patching of windows platforms.
2. All used applications as well as third party applications must be properly patched before installation.
3. Organization must consider limiting the administrative rights of user logon; and
4. Ensure the use of whitelisting blog on application software's properly licensed, this is all in an effort to controlled unwanted applications from running at the background which at the end be a security threats to the system in use (DSD, 2010).

Considering the increasing growth of internet technology and the increasing concern of internet related criminal activity which in every way becoming more complex, this however, made it easy for Cybercriminals to have known systems security vulnerabilities, which if in anyway left un-patched, such a vulnerability can easily be exploited thereby compromising the system and build malware infections which at the end will have serious consequences on organizational activities (DSD, 2010; Choo, 2011).

## VII. Government and Industrial Policies

The gravity of the growing online emerging threats posed by Cyber-attacks especially when measured against the particular vulnerabilities of the current global trend landscape; these gravity critically challenges the foundation of our national security and demands a concerted response by the government in establishing a well comprehensive security policy that will at the end address the challenge of the states of our Cyber security efforts. As Thio argue with growing security threats, we will require new approaches in dealing with cyber threats. "The traditional 'Whack-a-mole' and 'Block the World' is no longer effective; It is important to focus on the technique and not the tool" (Adli and Thio, 2012). This was a discussion on the analysis on how to tackle advance persistent threats, system vulnerability, remediation techniques and strategy implementation. This describes adoption of a good security policy; thus a Security policy in the concept of Cyber Security can be viewed as a guideline of action adopted or proposed by a government, which figure out how organization treats Computational resources (Jansen and Scarface, 2008). This definition made it necessary for all organizations to have Security policies for Computer systems and handheld devices as this might help in addressing the risen concern of Cyber-criminals.

A report on National plan to combat cybercrime by Australian Government suggests that the best way to protect against cyber security emerging issues, four key ideas should be taken as a general philosophy toward combatting cybercrime. These includes Understanding the problem, Partnerships and shared responsibility, focusing on prevention and Balancing security, freedom and privacy [9]. This describes the internet is built upon the freedom, creativity and innovation of users, the scenario here is that implementing these integrated strategies should represents a national plan, a techniques that if it could be technically addressed it will no doubt work out to be the most effective way of achieving a safer and more secure digital society. In view of these Government must rise and join hand in establishing a well comprehensive security strategic policy that go hand in hand with the global Cyber challenges as suggested by [24]. Finally, the literature concluded by recommending the following policy as the best effort to put in place in fighting Cyber-crime:

- International co-operation and Collaboration with industries: to address the emerging threats need collaboration among nations as only by such measure can absolute Cyber security be improved [24].
- Policies that entails the Deployment of technical measures, implement best security practices in government and critical sectors. A well comprehensive security plan and periodic IT security risk assessments [24].
- Ensure Continuous testing and evaluating the capability and effectiveness of technical Security control measures as applied for IT systems and networks [24].
- Government should authorize strong Security laws, and ensure it makes fighting Cybercrime a top priority by training prosecutors, law enforcement, and judges [4].
- Educating clients on the use and utilization of IT equipment must be encouraged because rules won't be followed if nobody knows it does exist.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

## VIII. Conclusion

This paper has outlined the reasons for widespread of different types of threats thereby affecting the states of Cyber security. The aim of this survey is to assess and evaluate the state of Cyber security emerging threats and the best approach needed to mitigate Cyber security breaches. The accompanying conclusions might be drawn from the present study that shows governments and large cooperation all over the world should be wary of the growing danger of cybercrime in the near future. This study has reported and envisaged a dramatic increase in the amount of targeted attacks on institutions and large government cooperation around the globe. This is based on the prediction that Cybercriminals tactics in the near future is focused to be more complicated and difficult to prevent, detect and address compared to the current known ones.

However companies and state organizations at the moment are influenced by the principal attacks, because today the more Security is reactive the more Cybercriminals are keen in exploiting that weakness. In particular, it could be deducted from the relevant studies that, what is store in 2012 was a brief roundup of the threats landscape migrating to our mobile devices and Apps (William and Pelgrin, 2012). As the uses of mobile devices continue to grow, the volume of attacks targeted to these devices will grow proportionately. The research point out the year 2013 which carried big news both in positive and negative development as an achievement in the Cyber threats landscape, but yet the dynamic race between defenders and attacker has continued and the projection is that it will continue even far spreading beyond western Europe and the US and actually affecting Eastern Europe, the middle East and Africa [23; 5]. Having a better understanding of how cybercrime affects our businesses will play a greater role in addressing it; we need to know who it targets how and why? Who are the perpetrators and how much harm are they causing. Taken together, these findings suggest a role for the government take absolute countermeasures against Security threats. Unless governments adopt this measure to mitigate threats, security threats will continue to manifest unabated.

## References


[1] *Ahamad, M., Amster, D., Barrett, M., Cross, T., Heron, G., Jackson, D., & Traynor, P. (2008). Emerging cyber threats report for 2009.*

[2] *Banday, M. T., Qadri, J. A., & Shah, N. A. (2009). Study of Botnets and their threats to Internet Security. Sprouts: working papers on Information Systems, 9(24)*

[3] *Brahme, A. M., Mundhe, S., Chavan, A., Joshi, S. B., & Sawant, P. (2013). International Journal of Computer Engineering & Technology (ijcet). 4(3), 324-330.*

[4] *BSA, 2010. Global Cyber security Framework. [Pdf] USA: Business software alliance. Available at < http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/*

[5] *Canty, D., 2012. Digital Danger Zone: tackling cyber security. Arabian Oil and Gas, [online] 19 January. Available at < http://www.arabianoilandgas.com/article-9868-digital-danger-zone-tackling-cyber-security/4/ > [accessed 28 December 2013]*

[6] *Cooke, E., Jahanian, F., & McPherson, D. (2005, July). The zombie roundup: Understanding, detecting, and disrupting botnets. In Proceedings of the USENIX SRUTI Workshop (Vol. 39, p. 44).*

[7] *Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.*

[8] *Creeger, M. (2010). CTO Roundtable: Malware Defense. Communication. ACM, 53(4), 43-49.*

[9] *Dreyfus, Mark QC, (2013) National plan to combat cybercrime, Australia: Australian Government.*

[10] *Djambazova, E., Almgren, M., Dimitrov, K., & Jonsson, E. (2011). Emerging and future cyber threats to critical systems. In Open Research Problems in Network Security Springer Berlin Heidelberg Pp 29-46*

[11] *Ehimen O.R., Bola A. - Cybercrime in Nigeria (2010) Cybercrime in Nigeria Business Intelligence Journal - January, 2010 Vol.3 No.1 Pp93-98*

[12] *F secures, 2010. Threat summaries: 2012 security Wrap-up. Finland: Available at < http://www.f-secure.com/en/web/labs_global/2010/q4-threat-summary > (accessed 6 January 2014)*

[13] *F secures, 2011. Threat Summaries. Finland: Available at: < http://www.f-secure.com/en/web/labs_global/about/history> (accessed 6 January 2014)*

[14] *Feily, M., Shahrestani, A., & Ramadass, S. (2009, June) A survey of botnet and botnet detection In Emerging Security Information Systems. Information Systems and Technologies, 2009; SECURWARE'09 IEEE Third International Conference on Pp268-273*

[15] *Gaudin, S. (2008) "Social engineering: the human side of hacking", http://itmanagement.earthweb.com/secu/article.php/10408 1,2002, (24 January, 2014).*

[16] *Gerke M., (2012) Understanding cybercrime: Phenomena, Challenges and legal response ITU Telecommunication Sector Sept, 2012. Is a new edition of a report previously entitled Publication Understanding Cybercrime: A Guide for Developing Countries? Online available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html*

[17] *Justin, M. Rao (2011) the economics of spam email metric MAAWG report Microsoft research. Available at: http://www.maawg.org/system/_les/news/MAAWG 2013*

[18] *Kaspersky, 2011. Cyber threat Forecast for 2012 [pdf] Russia: Available at: <http://www.kaspersky.com/images/Kaspersky%20report-10-134377.pdf > (accessed 5 December 2013)*

[19] *Karthik, S.; Bhavadharini, R. M.and Arunachalam, V.P. (2008) "Analysing interaction between Denial of Service (DoS) attacks and threats," International Conference on Computing, Communication and Networking, 2008. ICCCn Dec. 2008. , vol., no., pp.1,9, 18-20*

[20] *Kosutic, D 2007, what is Cybersecurity and how can iso 271001 help? Blog. Accessed 25 January 2014 < http://blog.iso27001standard.com/2011/10/25/what-is-cybersecurity-and-how-can-iso-27001-help/#*

[21] *Kruger, R. C. (2008). Investigating the possible introduction of managed broadband internet security: a pilot study (Doctoral dissertation, Stellenbosch: Stellenbosch University).*

[22] *Marinos, L., and Sfakianakis A., (2012) ENISA Threat landscape responding to the Evolving Threat Environment. Report by European network and Information Security Agency, September, 2012 Available at: http://www.enisa.europa.eu*

[23] *Marinos, L. (2013) ENISA Threat Landscape Overview of current and emerging cyber-threats European Union Agency for Network and Information Security December, 2013.*

*Available at: www.enisa.europa.eu*

*[24] MIT, 2011.National Cyber security policy. [Pdf] INDIA: Ministry of Communication and information Technology. < http://mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf>*

*[25] Mielke, C. J., & Chen, H. (2008, June). Botnets, and the cybercriminal underground. In Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on (pp. 206-211).*

*[26] Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking. Information Systems Security, 16(6), 302-314.*

*[27] Ponemon, (2012) Cost of Cyber Crime Study: United Kingdom benchmark Study of UK Organisations, Ponemon Intstitute Research Report October, 2012*

*[28] Raymond. K., (2011) the cyber threat landscape: Challenges and future research directionsJournals of Computers & Security 3 0 (2 0 1 1): Pp719-731*

*[29] Sagiroglu, S., & Canbek, G. (2009). Keyloggers. Technology and Society Magazine, IEEE, 28(3), 10-17.*

*[30] Sandouka, H. Cullen, A. J., and Mann, I., (2009) Social Engineering Detection Using Neural Networks; International Conference on Cyber Worlds, pp.273-278.*

*[31] Szor, P. (2005) the art of Computer Virus research and Defence Published February, 2005 Addison Wesley Pearson Education; ISBN: 0-321-30454-3.*

*[32] Sesan, G., Soremi, B., and Oluwafemi, B., (2012) Economic Cost of Cybercrime in Nigeria Paradigm Initiative Nigeria, report on the output for the Cyber Stewards Network project of the Citizen Lab, Munk School of Global Affairs, University of Toronto, and supported by IDRC. September, 2012: http://www.pinigeria.org/download/cybercrimecost.pdf (Accessed 28th November, 2013)*

*[33] Swan, D. 2011. Cyber security vulnerabilities facing IT managers today. [Pdf]: < http://umuc.academia.edu/DarinSwan/Papers/1464664/Cybersecurity_Vulnerabilities_Facing_IT_Managers_Today> (accessed 23 Dec. 2013)*

*[34] Symantec, 2011. Threat Activity Trends. USA: Available at < http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=malicious_shortened_urls > (accessed 4 January, 2014)*

*[35] Tatum, Malcolm (2010) "What Is a Cyber-attack?" Available on-line from: http://www.wisegeek.com/what-is-a-cyberattack.htm (Accessed 29th January, 2014)*

*[36] Trend Micro (2011) Issues Monitor Cyber Crime – A Growing Challenge for Governments KPMG International Cooperative ("KPMG International") July 2011, V (8).*

*[37] Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. (2003, October) A taxonomy of computer worms In Proceedings of the 2003 ACM workshop on Rapid malcode Pp11-18*

*[38] Zuo,Z. Zhu,Q. and Zhou, M., (2006) Infection, imitation and a hierarchy of computer viruses, Computers & Security, Volume 25, Issue 6, September 2006, Pages 469-*

## Author's Profile

*Alhaji Idi Babate has obtained his MSc from the University of South Whales UK, and had worked in many International and local project in the field of cyber security. The author had published several International Journals and currently a lecturer in the department of Computer Science Federal College of Education (technical) Yobe state Nigeria.*