Qamar et al LGURJCSIT 2019

LGURJCSIT
ISSN: 2519-7991

LGU Research Jounral for
Computer Sciences & IT

Vol. 3 Issue 1, January - March 2019

An Overview on Cyber Attacks and its Types for Enhancing Data Security in Business World

Noor-Ul-Qamar
noorulqamar@lgu.edu.pk
Lahore Garrison University , Lahore , Pakistan

Abstract:

For sensitive data of organizations there arises a need of ensuring privacy and protection measures in systems especially at various high-tech firms. Cyber attacks are a wide form of threat confronted on web by several users on daily basis. These attacks are fundamentally used to challenge system security of others yet there are likewise some moral programmers who get into other people frameworks' to aware them about their vulnerabilities and get paid in return for securing their systems. In any case, these assaults have caused a great deal of concern for businessmen. The research covers the major types of cyber attacks that can affect the business world in an immense manner along with an overview that how these threats work and how they can be possibly prevented from. The hacking procedures are showing signs of improvement step by step and so should our frameworks to remain safe from all sorts of latest attacks on our data in various forms.

Keywords: Computer Network Attack, SQL Injection, Phishing, Reconnaissance, SSL Attacks, Denial of Service

1. INTRODUCTION

A cyber attack is intentional misuse of personal computers, technology-dependent corporations, companies and systems or sites. Cyber attacks use harmful and destructive code to change coding of computer, reasoning or data, leading to disruptive effects or repercussions that can bargain data and leads to cybercrimes, such as identity or personal information theft. Cyber attack is also called Computer Network Attack (CNA).

Cyber-attacks can include the following outcomes:

a) Extortion, fraudulence or identity theft
b) Spoofing, pharming and several others like malware, phishing,
c) Hardware's are being stolen, such as laptop computers or cellular devices
d) Denial-of-service and allocated denial-of-service attacks
e) Website defacement
f) System infiltration
g) Password sniffing
h) Exploitation of personal and general public browser
i) Instant messaging abuse
j) Unauthorized access or intellectual robbery (IP) robbery

The Institute for Security Technology Studies at Dartmouth University investigates and studies cyberattack issues facing on police investigations and targets the constant development of IP tracing, real-time interception nationwide data sharing and data evaluation.

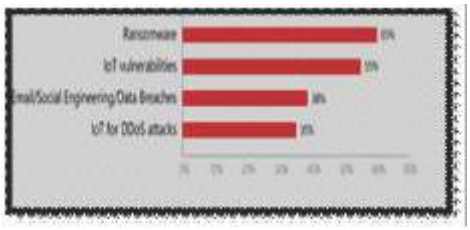

Fig 1: 2017 Top Cyber Security Threats

So, threats to user's sensitive data and insecure mechanisms of hacking quality information in the business world urge the demand of preventive cautions and actions against cyber attacks and its devastating types by all means.

2. METHODOLOGY

Several theories have been claimed regarding the subject of security in concern so to discuss them, various types of cyber attacks alongwith their detailed analysis is mentioned below:

2.1. TYPES OF CYBER ATTACKS THAT WE NEED TO AVOID FOR OUR BUSINESSES

2016 may be considered as the success of cyber criminals as a lot serious cyber threats were being faced by the people and the companies and hackers gain access to their personal information for their own benefits. However in 2017 and in ongoing years still many firms are getting affected especially business companies have to face serious trouble due to these cyber attacks.

3.1. Sql Injection

SQL Injection (SQLi) alludes to an injection attack where by an offender will render venomous SQL statements through which Relational Database Management System (RDMS) is controlled. Any website or web application in which SQL-base database is used probably would be affected by SQL injection vulnerability. It is suspected as truly, it can be used by an attacker to bypass authorizations mechanism and web application's authentication and the contents of an entire database may be threatening webbing application vulnerability. Database records can be added, modified and deleted by using SQL injection.

To such an extent an attacker may be provided with unauthorized usage to private information through SQL injection. Private data can include personally identifiable information (PII), intellectual property, trade secrets, customer data, and other sensitive data.

The essentials necessary for an attacker to attach an SQLIA are a web browser, clever guesses of significant tables and field names and the understanding of SQL queries. URLs and user inputs are two approaches through which SQLIAs can be executed. The process for launching an attack includes four steps. The first step ensures the identification of whether the prosecution is susceptible to a SQLIA. This is attained by finding out if special characters are accepted as input. The conviction of which kind of database is being used by the net application is the next step of releasing a SQLIA.

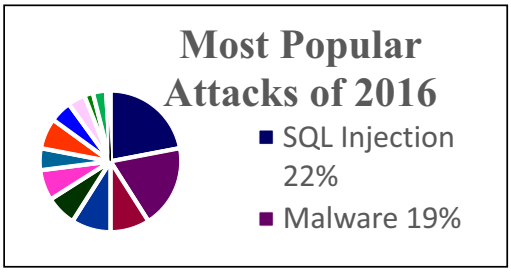

Fig 2: Percentage Ratio of Cyber Attacks in 2016

Different database management systems have variable injection processes so it is beneficial to establish database type. The third step is to collect all the possible information about the database. This step is determined by the attacker's capacity to guess field names, tables and procedures stored in the database. The finishing step is to install the attack, currently simple because all of the reconnaissance has been done by the attacker [1].

2.2. MITM

In computer security and cryptography, there is an attack known as a man-in-the-middle attack (MITM) in which the offender probably changes the transmission held between two participants who assume that they are connected to their partner without interference. For instance Active eavesdropping, where the offender makes freelance affiliations with the sufferer and data is transferred between them to form them believe they're talking on to one another connected personally, but actually the attacker is commanding the whole speech.

The offender scan obstructs all related text revolving with in the 2 sufferers and inculcate new. This might be done in many circumstances.; for example, an attacker can insert himself as a man-in –the-middle within reception range of an unencrypted wireless access point (Wi-Fi)s' a attacker can insert himself as the MITM..

Most scientific discipline protocols embrace some style of termination specifically

to stop MITM attacks; for instance, TLS will evidence one or each participant employing a reciprocally trusty certificate authority [2].

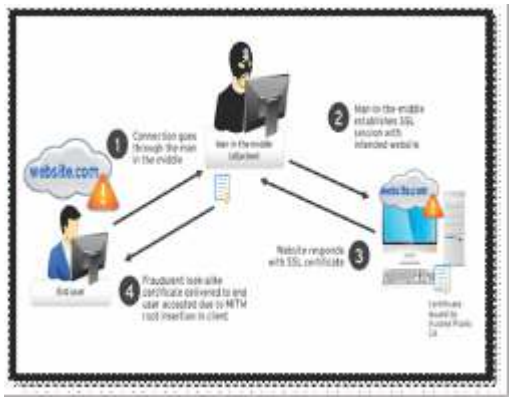

Fig 3: Man in the middle attack (MITIM)

There occurs a difference of interaction when we talk about a connection of a server and a client and when there is MITM in between. Direct and indiect communication occur. This can be seen with the help of fig4.

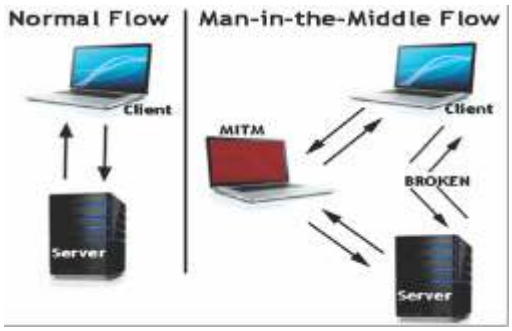

Fig 4: Comparsion of normal flow vs MITM

2.2.1. An illustration of the man-in-the-middle attack:

Suppose Nancy needs to speak with David. Meanwhile, Morgan needs to expropriate the speech communication to listen in and optionally to transfer a untrue text to David. MITM is illustrated below.

a) Morgan intercepted a message sent by Nancy to David

Nancy "Hello David, I want your key, Its Nancy." → Morgan David

b) This message is conveyed by Mallory and Bob is unable to tell whether this is by Nancy.

Nancy Morgan "Hello David, I want your key, Its Alice." → Bob

c) Bob replies with his encryption key:

Nancy Morgan ← [David's key] David

d) Declaring that it is David's key, Morgan responds to Nancy by changing Bobs key with her own

Nancy ← [Morgans key] Morgan David

e) Nancy thought solely David will browse it. A message is encoded by Nancy which is assumed by her to be David's key Alice "Need to see you at the railway stop!" [encoded with Morgan's key] → Morgan David

f) However, it is actually encoded , decoded , read , modified (if desired) by Morgan key, re-encrypt with David's key, and send it to David: Nancy Morgan "Meet me at the van side by the cafe!" [Encoded with David's key] → David

g) According to David, he is connecting securely to Nancy.

h) Morgan rob the David as he goes to the van side by the cafe.

The example indicates the requirement for Bob and Alice to own a way to confirm that each other's public keys are used by them actually, instead of the general public key of an attacker. MITM attacks can be protected by using variable techniques. Two ways largely defend the MITM attacks: these include tamper detection and authentication. Some degree of a guarantee about the coming of given message from the supply is provided by authentication. Comparatively the means of tamper detection gives the proof.

3. PHISHING

Phishing may be a style of duck during which the sinner tries to find out data likely relation data or login credentials by posing as an essence of excellent repute or person in electronic mail, other intercommunication chamfer or IM [3].

Commonly a casualty got a communication that seems to have been eager by a reconnoiter contactor or union.Phishing is methodically done by consideration messaging or electronic mail satirizes and it is ofpilot clients to penetrate concrete data at a site that is robbed. The messages me have connections to various links that enable malware problems. Attempts to govern the development of spoofing occurrences incorporated enactment, dependent preparing, candid inclination and specialized safeness efforts are incorporated.

3.1. Types of phishing

3.1.1. Spear phishing:

The maximum current wind on phishing is spear phishing. No, it's no longer a recreation, it is a trick and you're the goal. Spear phishing is an e mail that offers off an influence of being from an individual or enterprise which you know. In any case, it isn't. It's from similar crook programmers who need your charge card and ledger numbers, passwords, and the budgetary facts in your PC. Figure out how to ensure yourself [4].

3.1.1.1.Email from a "Companion:"

The lance phisher prospers with recognition. He is aware of your call, your e-mail address, and no less than a bit approximately you. The welcome on the email message is probably going to be customized: "Hello there Bob" as opposed to "Dear Sir." The electronic mail may additionally make reference to a "shared companion." Or to a cutting-edge on-line buy you have made. Since the e-mail seems to originate from any person you understand, you is probably less cautious and provide them the facts they request. What's extra, whilst it's an enterprise you recognize inquiring for urgent activity, you is probably enticed to behave earlier than thinking about.

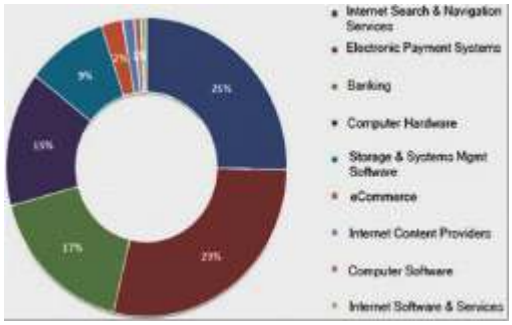

Fig 5: Percentage description of Phishing Attacks

3.1.1.2.Utilizing your web presence against you:

How could you switch into a goal of a lance phisher? From the information you put on the Internet out of your PC or mobile cellphone. For instance, they may take a look at casual conversation locations, find out your page, your e mail cope with, your companions list, and a current submit with the aid of you enlightening partners concerning the cool new camera to procure at a web retail webpage. Utilizing those facts, a lance phisher ought to act like a companion, ship you an electronic mail, and method you for a watchword for your picture web page. On the off hazard that you react with the secret word, they will strive that watchword and types to try to get to your file on that on line retail internet site you certain. In the occasion that they find the ideal one, they'll utilize it to preserve strolling up a nice tab for you.

Alternatively the lance phisher can also utilize an indistinguishable information to posture from a few character from the net store and request which you reset your mystery key, or re-affirm your Visa range. In the occasion which you do, he'll do you money related harm.

3.2. Clone Phishing:

A sort of phishing assault that can be conveyed through an email by establishing a connection that can inculcate various addresses for sending an indistinguishable email.

3.3. Whaling:

These assaults are coordinated at major concerns like respectable officials and can e a threat for people inside organization to affect their working [5].

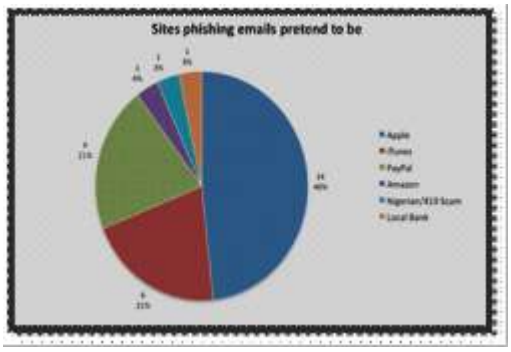

Fig 6: Various phishing Emails

3.4. Avoidance technique from phishing:

There is a fortune of property on the Internet that give succor in encounter spoofing. The Anti-Phishing Working Group Inc. also, the middle regulation's OnGuardOnline.gov situation both give scheme on the worst moving to disgrace, keep aside from and recital spoofing charge. Intelligent load serve, for sample, Wombat Security Technologies' Anti-Phishing Training Suite or PhishMe can relieve show representatives how to relinquish from spoofing luggage, while destinations resembling FraudWatch International and MillerSmiles administer the most neoteric spoofing electronic mail ownership that are circuit the Internet.

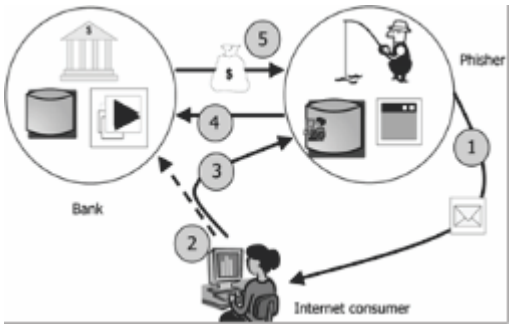

Fig 7: Symbolic Flow of Phishing

4. ROGUE SOFTWARE

Rogue security software is a form of malignant programming and web extortion that deludes clients into accepting there is an infection on their PC, and controls them into paying cash for a fake malware evacuation device (that really acquaints malware with the PC). It is a type of frighten product that controls clients through dread, and a type of payment product. Maverick security programming has turned into a genuine security danger in desktop figuring since 2008.

4.1. Working:

A site may show a fake cautioning exchange expressing that somebody's machine is tainted with a PC infection, and urge them through control to introduce or buy terrify product in the conviction that they are obtaining certifiable antivirus programming. Clients ought to never freeze at whatever point they see such notices. The programmers more often than not attempt to make the clients trust that introducing the security programming is their last choice. The avoidance is to not think everything that shows up on your PC. Counteractive action: The main answer for the issue is to utilize presence of mind and never freeze in such circumstances. Additionally the framework programming ought to be kept up-to-data [6].

5. MALWARE:

Malware is visible as a bothering or negative kind of programming proposed to stealthily get to a tool without the patron's records. Where malware starts from Malware maximum through and big receives for your tool thru the Web and with the aid of techniques for e-mail, anyways it is able to in like way get access thru hacked destinations, entertainment demos, track data, toolbars, programming, free participations, or whatever else you down load from the web onto a contraption which isn't always secured with in opposition to malware programming. You can use a malware scanner to check if your tool is tainted. The nice technique to oust malware is that the first-class way to cope with discard malware is to apply a strong malware departure device, as observed in any first-rate antagonistic to malware programming. Avast Free Antivirus and threatening to malware can fast and effortlessly do away with any malware out of your gadgets.

5.1. Steps to save you from malware:

Use extreme antivirus to malware programming. Utilize unfriendly to malware to guarantee yourself There is not any higher manner to cope with see, clear and thwart malware than to use an antivirus and antagonistic to malware gadget, and the nice antivirus and towards malware tool is Avast.

6. RECONNAISSANCE:

In military operations, observation is the investigation outside a region involved by amicable powers to pick up data about characteristic components and adversary nearness. Cases of surveillance incorporate watching by troops, ships or submarines, kept an eye on/unmanned surveillance flying machine, satellites, or by setting up incognito perception posts. Undercover work regularly is not surveillance, since observation is a military's exceptional strengths working in front of its fundamental powers; spies are non-warriors working behind adversary lines.. There are two sorts of observation assaults:

- Active
- Passive

Latent surveillance assaults are the point at which an assailant searches for private data without drawing in with the casualty's frameworks. The two types occur once in a while where reconnaissance is obtained from its utilization in military varying from the dynamic assaults [8].

6.1. Working and prevention:

In a PC security setting, observation is for the most part a preliminary step towards

further attack hoping to abuse the goal structure. The attacker as often as possible uses port addresses to locate any feeble ports. After a port scope is revealed the vulnerabilities of organizations related with open ports are perceived. For counteractive action the slightest complex way to deal with suspect most port yield attacks or reconnaissance strikes is to use an Intrusion Prevention System and drop firewall. The firewall controls the ports which are displayed to whom they are exhibited. The IPS can perceive port outcomes in time and close them down before the attacker can get a full guide of your framework.

7. SSLATTACKS:

Secure Sockets Layer (SSL) is a PC networking protocol for securing associations between organize application customers and servers over an unreliable system like the web. Because of various convention and execution blemishes and vulnerabilities, SSL was expostulated for use on the web by the Internet Engineering Task Force (IETF) in 2015 and has been supplanted by the Transport Layer Security (TLS) convention [9]. SSL keeps running over the network layer and the transport layer, which are in charge of the vehicle of information amongst forms and the directing of system movement over a system amongst customer and server and underneath application layer conventions, for example, HTTP and the Simple Mail Transport Protocol.

7.1. Working:

An SSL assault type blocks the scrambled information before it may be encoded, enabling the assailant to approach to touchy information including Visa data and standardized savings numbers. It enables assailants to get to passwords, other confirmation tokens and cookies.

8. DENIAL OF SERVICE

In a Denial of service: (DoS) aggression, an instigator endeavors to evade faultless patron's outlander property to observations or administrations. By plan on your Historical peeler and its structure affinity , or the PCs and conventions of the locales you are attempting to relate, an initiator huskiness effort the skills to elude you stranger object to sites, emails, online log (saving asseverative, and ergo on.), or variant administrations go off brandish on the niminy-piminy Historical peeler. The richest outside decorous and ostensible tag of DoS aggressiveness happens directly an attacker "surges" aencypher everywhere materials. Closely you imagine a URL for a medicine spot into your program; you are transportation a preference to ramble spot's Patrolwoman serving dish to behold the harbinger. The platter is merely affray a medicine volume of solicitations level a moment's prevent, accordingly if an belligerent over-burdens the platter helter-skelter urge, it aren't squire your appetency. This is a "disavowal of delivery" fitting for you tuchis't achieves to turn this way site. A provoker groundwork address spam email messages to smash a comparative attack on your email note. Anyway in the reality you attack an email jaws provided by your brass hats or combine open scan a casual administration, for suit, Yob or Hotmail, you are appointed a alert aggregate, which restricts the operate of suggestion you can take a crack at in your volume at humble likely time eon. By decoding unconventional, or thorough, email messages to the record, an assailant can blow your momentous, anguish you unfamiliar accepting straightforward to beneficence messages [10].

9. DRIVE BY DOWNLOADS:

A drive-by download is a program that is consequently downloaded to your PC without your assent or even your insight. Not at all like a pop up download, which requests consent (but in a figured way prone to prompt a "yes"), a drive-by download can be started by just going by a Web website or review a HTML email message. In the event that your PC's security settings are careless, it might be workable for drive-by downloads to happen with no further activity on your parts [11].

10. MALVERTISING:

Malvertising (a portmanteau of "malignant promoting") is the utilization of web based publicizing to spread malware. Malvertising includes infusing malignant or malware-loaded commercials into true blue web based promoting systems and webpages [7].

Online notices give a strong stage to spreading malware on the grounds that critical exertion is put into them keeping in mind the end goal to pull in clients and offer or publicize the

product. Because publicizing substance can be embedded into prominent and respectable sites, malvertising gives transgressors a chance to push their assaults to web clients who may not generally observe the advertisements, because of firewalls, more security precautionary measures, or the like. Malvertising is "appealing to assailants since they 'can be effortlessly spread over a substantial number of honest to goodness sites without specifically trading off those websites'. Malvertising is a genuinely new idea for spreading malware and is much harder to battle since it can work its way into a site page and spread through a framework unconsciously: Attackers have a wide reach and can convey these assaults effectively through commercial systems. Organizations and sites have experienced issues decreasing the quantity of malvertising assaults, which "recommends that this assault vector isn't probably going to vanish soon [12].

10.1. Working and prevention:

Sites or web distributers accidentally consolidate a tainted or vindictive notice into their page. PCs can end up noticeably tainted pre-snap and post click. It is a misguided judgment that contamination just happens when guests start tapping on a advertisement.

Malware can likewise auto-keep running, as on account of auto diverts, where the client is naturally taken to an alternate site, which could be noxious. To keep malvertising from tainting your PC, you have to deny misuse units the chance to discover a defect. Spieled encouraged individuals to ensure their Web programs and program modules, (for example, Java or Adobe Flash), and additionally working frameworks, are breakthrough with the goal that known imperfections are settled.

11. PROTECTION OF DATA FROM CYBER ATTACKS

Ensure having a very secure and strong password. If you find a self-assertive USB stick, don't allow yourself to lure you to associate it to the remote possibility that you don't place stock in the source, you're in a perfect circumstance not putting your PC at shot. Keep away from embeddings hard drives and thumb drives you don't trust into your PC. Guarantee a site is secure before you enter particular information.

In case these things aren't there, by then the framework isn't secure and you shouldn't enter any information you wouldn't require. Sending essential information, for instance, Visa numbers or money related adjust numbers puts it at risk of being gotten by software engineers or computerized strikes. When in doubt, a software engineer will use this email or site to present noxious programming onto your PC. These web components are planned to look like a common email or website, which is the way developers convince people to hand over individual information [13].

12. CONCLUSION

Through this we become acquainted that we must take care of the issue talked about at the outset and to protect ourselves from these assaults and we should keep our framework programming dependably up to dated. At whatever point any kind of caution flies up on the screen client ought to never freeze and do whatever the fly up is asking on the grounds that these are tricks utilized by programmers. In addition clients ought to never approach a number that is composed on the fly up. Solid passwords ought to be connected, users need to dependably utilize refreshed firewalls to remain safe and never tap on advertisements or connections about which they don't have the foggiest idea. One in number proposal would likewise to be genuinely considering techniques and innovations to distinguish a dynamic information rupture rapidly. This overview on emerging cyber attacks in the business world alongwith their working and preventions opens doors for researchers to study on categories of malwares, network security measures, engineering and programming techniques using firewalls to overcome the rapid growth of attacks in all aspects.

13. REFERENCES

[1] Mavromoustakos, S., Patel, A., Chaudhary, K., Chokshi, P., & Patel, S. (2016, December). Causes and Prevention of SQL Injection Attacks in Web Applications. In Proceedings of the 4th International Conference on Information and Network Security (pp. 55-59). ACM.

[2] Arshad, M., &Hussain, M. A. (2016). Secure Framework to Mitigate Man-in-the-Middle Attack over SSL Protocol. Indian Journal of Science and Technology, 9(47).

[3] Ekawade, S., Mule, S., &Patkar, U. (2016). Phishing Attacks and Its Preventions. Imperial Journal of Interdisciplinary Research, 2(12).

[4] Zhao, M., An, B., &Kiekintveld, C. (2016, February). Optimizing Personalized Email Filtering Thresholds to Mitigate Sequential Spear Phishing Attacks. In AAAI (pp. 658-665).

[5] Heartfield, R., &Loukas, G. (2016), A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), 37

[6] England, P., Slick, G., Dunn, J. C., Ray, K. D., Peinado, M., &Willman, B. (2016). U.S. Patent Application No. 15/047,300.

[7] Pathak, P. B. (2016). Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks. International Journal of Advanced Research in Computer Science, 7(2).

[8] Nguyen, H. T., &Dinh, T. N. (2016, April). Targeted cyber-attacks: Unveiling target reconnaissance strategy via Social Networks. In Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on (pp. 288-293).

[9] IEEE. Sirohi, P., Agarwal, A., &Tyagi, S. (2016, October). A comprehensive study on security attacks on SSL/TLS protocol. In Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on (pp. 893-898). IEEE.

[10] Tarao, M., & Okamoto, T. (2016). Toward an Artificial Immune Server against Cyber Attacks: Enhancement of Protection against DoS Attacks. Procedia Computer Science, 96, 1137-1146.

[11] Sood, A. K., &Zeadally, S. (2016). Drive-By Download Attacks: A Comparative Study. IT Professional, 18(5), 18-25.

[12] Pathak, P. B. (2016), Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks. International Journal of Advanced Research in Computer Science, 7(2).

[13] Hills, M. (2016). Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection, Prevention and Response. Nova Science Publishers.