Dr. Pranav Patil *et al*, International Journal of Computer Science and Mobile Applications,
Vol.7 Issue. 10, October- 2019, pg. 31-35 **ISSN: 2321-8363**
Impact Factor: 5.515

Study of Emerging Threats in Cyber-Security

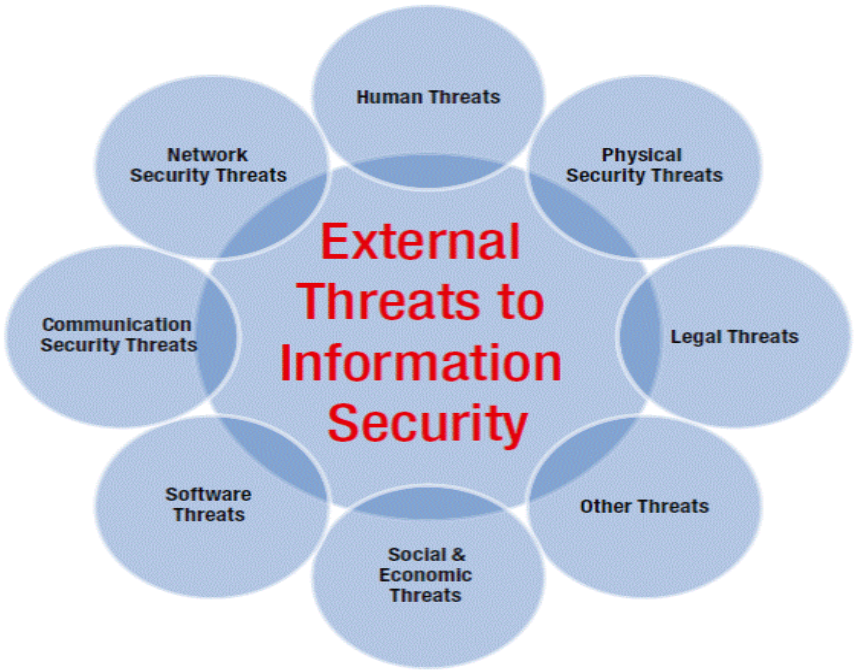
Dr. Pranav Patil
Department of Computer Science, Assistant Professor, M. J. College, Jalgaon, Maharashtra, India
Yogesh Sharad Chaudhari
BCA Student, M. J. College, Jalgaon, Maharashtra, India

Abstract: As constantly new technologies are evolved new threats and risks are creation way and making information security a deadly task, where organizations, institutions and individuals are spending on most modern technologies the question that arise is are we secured sufficient ? Information security plays an important role in the current development of information technology, as well as Internet services. Making the Internet safer has become vital to the development of new services and policies for any organization. In this paper we will highlight the most modern threats evolved with emerging cyber technologies their impact and how it can be prevented.

Keywords: Cloud Threat, Big data, Ransomware, Malware, Dark Web.

1. Introduction

Even the most recent technologies like cloud computing, mobile computing, E-commerce, internet banking etc. conjointly desires high level of security. Since these technologies hold some necessary info relating to an individual their security has become a requirement issue. Enhancing cyber security and protective crucial info infrastructures square measure essential to every nation's security and economic well-being. Making the web safer has become integral to the event of recent services further as governmental policy. Deterring crime is Associate in Nursing integral part of a national cyber security and demanding info infrastructure protection strategy. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach. Cyber security strategies for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime can help to reduce the risk of cybercrime.



2. Threats

A threat, within the context of computer security, refers to something that has the potential to cause serious hurt to a system. Threats are a few things which will or might not happen, however the potential to cause serious damage has. Threats will result in attacks on computer systems, networks and other things. In the present age, computer security threats are constantly increasing as the world is going digital.

Types of Threats:-

- Phishing
- Malware
- Trojans
- Man in the Middle (MITM)
- Distributed Denial of Service (DDoS)
- Internet of Things (IoT) or Algorithm Manipulation
- Ransomware
- SQL Injection

Phishing:-Cybercriminals will try to gain access to your secured network through different means, the most common of which is through phishing. By using social sites or email, these scammers can win over users to click on misleading links, offer sensitive information or company information, or maybe transfer content to their computer or server.

Malware:-If a victim of phishing does end up initiating a download, there's a good chance that the program received is harmful or malicious. A Trojan virus, for example, is a form of malware brought onto the network disguised as legitimate software, often carrying out its true purpose without the user knowing. Malware comes in various forms, tasked with anything from spying on the system to manipulating its code.

Trojans:-A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

Man in the Middle (MITM):-A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own. In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication.

Distributed Denial of Service (DDoS):-This is a type of attack that floods the server with requests from multiple sources, leading it to become overwhelmed to the point of slowing down substantially or even crashing. Once this occurs, the system becomes impossible to use effectively until theses numerous interactions are cancelled and blocked.

Ransomware:-Ransomware is a growing threat that encrypts a user's files and holds the decryption key until a ransom is paid by the victim. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of the many antivirus and intrusion detection systems. In this work, we tend to present CryptoDrop, AN early-warning detection system that alerts a user during suspicious file activity. Using a set of behavior indicators, CryptoDrop will halt a method that appears to be tampering with a large amount of the user's data. Furthermore, by combining a collection of indicators common to Ransomware, the system may be parameterized for fast detection with low false positives. Our experimental analysis of CryptoDrop stops ransomware from executing with a median loss of only ten files (out of nearly five, 100 available files). Our results show that careful analysis of ransomware behavior will turn out an effective detection system that significantly mitigates the number of victim data loss.

SQL Injection:-SQL Injection (SQLi) is a code injection attack where an attacker manipulates the data being sent to the server to execute malicious SQL statements to control a web application's database server, thereby accessing, modifying and deleting unauthorized data. This attack is mainly used to take over database servers.

3. Scope and Objectives

The study seeks to find out patterns of attacks in cyber security and studied about emerging threat .In this study we have tried to find out top five defense strategies to protect emerging technology. And in future what will be the effect of all these things on technology and future research directions in cyber security.

- Analysis of new cyber-attack pattern in emerging technology.
- Study of Defence strategies in cyber security.
- Potential future research directions in cyber security.

4. Review

SH Kok, Azween, Abdullah and Mahadevan Supramaniam-February 2019, In this work, we performed our research based on specific criteria related to ransomware. First, our research is based on recent studies, from year 2015 onwards. Thus, the information is the latest and is still relevant. Second, our sources comprise only scientific journals and conference papers; this is to ensure that the collected information is authentic. Third, we only focus on our topic of interest: the threats caused by ransomware and techniques for ransomware detection.

Alhaji Idi Babate-Mar. 2015, Stated in this paper that- 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. 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 threat swill be witnessed. Thus, a few government and Information Technology (IT) stakeholders' strategic policies to help in combating cyber threats were presented.

Ravi Sharma-June-2012, Stated in this paper that- Cyber Security plays an important role in the development of information technology as well as Internet services. Our attention is usually drawn on "Cyber Security" when we hear about "Cyber Crimes". Our first thought on "National Cyber Security" therefore starts on how good is our infrastructure for handling "Cyber Crimes". This paper focus on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure.

Ms.Shazia Ali, Dr.Sadia Husain, Manju Sharma, Stated in this paper that-As continuously new technologies are evolved new threats and risks are making way and making information security a tedious task, where organizations, institutions and individuals are spending on latest technologies the question that arise is are we secured enough ? Information security plays an important role in the ongoing development of information technology, as well as Internet services. Making the Internet safer (and protecting Internet users) has become integral to the development of new services and policies for any organization. In this paper we will highlight the latest threats evolved with emerging cyber technologies their impact and how it can be prevented.

5. Research Methodology

Sample Procedure: The survey was distributed electronically to 100 students and teachers in college. Participation was voluntary and anonymous. The survey response rate was high, with 90% of students in most districts participating.

6. Results

Computer geniuses, usually in their twenties, are thrown challenges to break one or another security program, capture the passwords to remote computers and use their accounts to travel the cyberspace, enter data networks, airline reservation systems, banking, or any other "cave" more or less dangerous. Managers of all systems have tools to control that "all is well", if the processes are normal or if there is suspicious activity, a user is using to access roads which is not authorized. All movements are recorded in system files, which operators review daily. Furthermore, the network is becoming the ideal place for criminals and terrorists to carry out their actions and activities. Hence, cybercrime and cyber terrorism have become two of the most serious threats seem to haunt Western societies. Moreover, the impact of the crimes on the victims and their measures to cope up with such crimes in the future will also be a part of the paper. This paper will also discuss the how network security is critically important in preventing the recurrence of these types of cyber-attacks in the future.

7. Conclusion

Cyber security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure.

References

[1] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 19, Issue 2, Ver. IV (Mar.-Apr. 2017)
[2] D. Timko, "The Social Engineering Threat", Information Systems Security Association Journal (ISSA), January 2008. Ahamad, M., Amster, D., Barrett, M., Cross, T., Heron, G.,Jackson, D., &Traynor, P. (2008). Emerging cyber threats report for 2009.
[3] MIT, 2011.National Cyber security policy. [Pdf] INDIA: Ministry of Communication and information Technology.
[4] International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015) State of Cyber Security: Emerging Threats Landscape Vol. 3, Issue 1 (Jan. - Mar. 2015)
[5] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy
[6] International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 "Study of Latest Emerging Trends on Cyber Security and its challenges to Society".
[7] International Journal of Computer Trends and Technology (IJCTT) – Volume 67 Issue 6 - June 2019 ISSN: 2231-2803, "Cybercrime Awareness among Students at a Teacher Training College".
[8] Aggarwal, G. (2015). General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering, 5(8)
[9] Kim, E. B. (2013). Information security awareness status of Business College: Undergraduate students. Information Security Journal: A Global Perspective.
[10] Malhotra, T., & Malhotra, M. (2017). Cybercrime Awareness among Teacher Trainees. Scholarly Research Journal for Interdisciplinary Studies.
[11] Moallem, A. (2018, July). Cyber Security Awareness among College Students. In International Conference on Applied Human Factors and Ergonomics. Springer, Cham.
[12] Narahari, A., & Shah, V. (2016). Cyber Crime and Security- A study on Awareness among Young Netizens of Anand. IJARIIE

Authors Bibliography

Yogesh Sharad Chaudhari, Third year BCA Student, KCES's M. J. College, Jalgaon, Maharashtra, India. His research focuses on Cyber Crime and Security.

The motivating factor for this research paper was the inspiration given to me by my respected sir, **Dr. Pranav Patil (**PhD, D.Lit.) he has given many valuable suggestions and encouraging generously throughout.

