Analysis of Threats to Information System in multicast communication

[1]Rajeev Kumar, [2]Manisha Yadav
[1,2]Assistant professor
[1]Department of Computer Science and Engg, [2]Department of Electronics and Communication Engg.
Institute of Engineering and Technology, Dr. Rammanohar Lohia Avadh University, Ayodhya, Uttar Pradesh, India

Abstract

In this fast-growing world, there is nothing without technology, it has evolved our working in many ways. We are just a click away from all the information and entertainment, from various services and applications. As the use of technology has increased tremendously, the security of the user data is at a high risk. Fraudsters are finding new ways to breach the security and steal important information's. So many measures have been taken till now to stop their activity, but now extra focus is required by IT owner because maintaining the authenticity of user data is crucial. In order to assure deliberate improvement instantaneous actions are required. We have seen a high rise in fraudulent activities during this COVID-19 pandemic. This paper mainly focuses on the readers whose life revolves around technology to observe the threats over Internet Security and inspect the aftereffects of numerous possible cyber intrusions.

Keywords- Threats, Protection, Crime, Security, Technology, COVID-19, Cyber attacks.

I. INTRODUCTION

We all are dependent on technology; it has become a vital part of our day to day life. Every business activity is being performed over network, for them their business and customer data is crucial. Most of the people are doing online transaction. Network has become a hub for sharing information, almost whole world is connected to a social networking site and sharing their life. Hackers are stealing all these data and sell them in order to make money, they are transferring money from user account, terrorists are stealing high authority data and much more is happening in cyber world. Whenever we talk about internet security we also talk about cyber-crimes because both the concept goes hand in hand.

In today's technical environment, latest technologies are changing. But because of these emerging technologies we are not able to safeguard our personal information in very effective way and hence the graph of cyber-crimes is going higher. Near about 70 % of the total business transactions are done through internet, so for transparent and best transactions this field needs high quality security. So, today's latest issue is cyber security. The outlook of cyber security is not just limited to securing the information in IT industry but also, to various other fields like cyber space, cloud computing, mobile computing, E-commerce, net banking,

e-mail services, etc., latest technology also needs high level of security, because these technologies have very confidential data so its security has become very important thing. Making the Internet safer has become integral part for the development of new policy as well as government services.

The fight against cyber-crime based on a global and a safer approach. Only technical measures are not able to prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber-crime effectively. To prevent the loss of some important information many nations and their government are imposing strict laws. To save our information from these increasing cyber- crimes, every user must be trained on the cyber security measures. Protecting critical information and boosting cyber security is essential for the nation and for its economic growth

II. CYBER CRIMES

Whenever we are talking about Cyber Security, we need to know what cyber-crimes are. Cyber-crimes are also known as computer- oriented crimes because it involves computer and a network. It is an illegal activity in which criminal minded people accomplish information related to user's personal or business. Commonly used Cyber Crime Techniques are:

Trojan: The aim of this malware is to make the device of the user available to cyber criminals. Once it is accessible, the devices are then used to conduct fraudulent transactions with an innocent IP address or build the botnets previously described, among other activities, they change/disrupt the information.

Spyware: The primary goal of this malware is to obtain user data that can later be used or sold, generally information of a medical or financial nature.

Ransomware: It is also a malware which encrypts the system of the victim with an unknown code and then attackers will display the message demanding a ransom in exchange for the code that victim will use to recover his or her device and data.

Social Engineering: This is a ploy used by cyber criminals to hook their victims. It consists of sending messages, e-mails, or creating viral chains on social media platforms with some malicious links to files that are downloaded or forms that will reveal sensitive user information and/or credentials if they are filled out.

III. RISE IN CYBER CRIMES DURING COVID-19

World is facing huge COVID -19 pandemic, for everyone it is terrible moment. It has already taken so many lives and still we don't know when it's going to end. The speed at which the virus is spreading around the world, cyber-crimes is also growing with the same speed. Since the beginning of this pandemic, we have seen a surge in cybercrime activities. Even WHO (World Health Organization) has seen number of cyber-attacks on its staff and fake mails are being sent to the public.

Number of mail ids are currently using the name of WHO and sending fake data to public in order to spread rumors and to steal their information. Around 400-500 working email address and password of WHO staff were leaked, although the data was old so it didn't put the system on risk, but it did affect the older system.

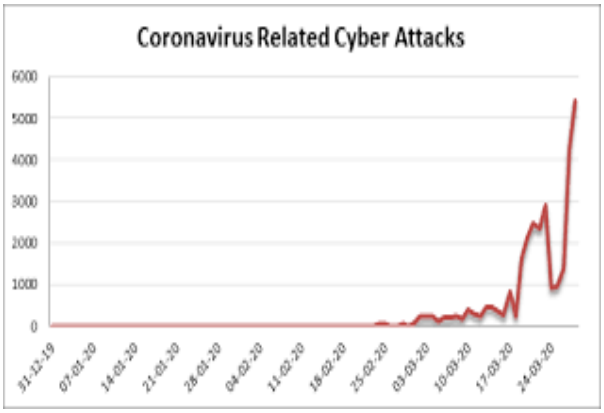


Figure 1- rise of cyber-crime during COVID-19

The new normal concept of **work from home**, **online classes, online meetings** etc. gave fraudsters new chances to expand unauthorized access to user data and they are fully utilizing this advantage in every possible way. All of these require video conferencing and for that so many new applications came to market, but most of them does not provide enough security. Many people received fake e-mails by using the name of official websites and their data got stolen.

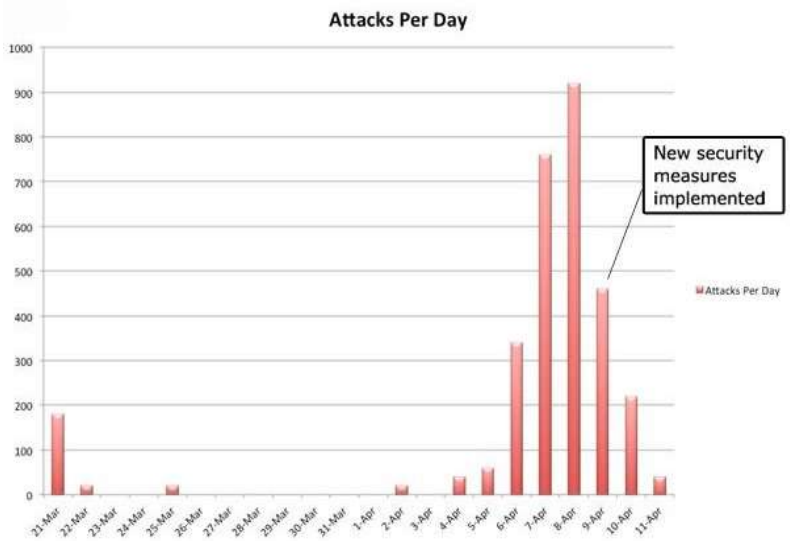
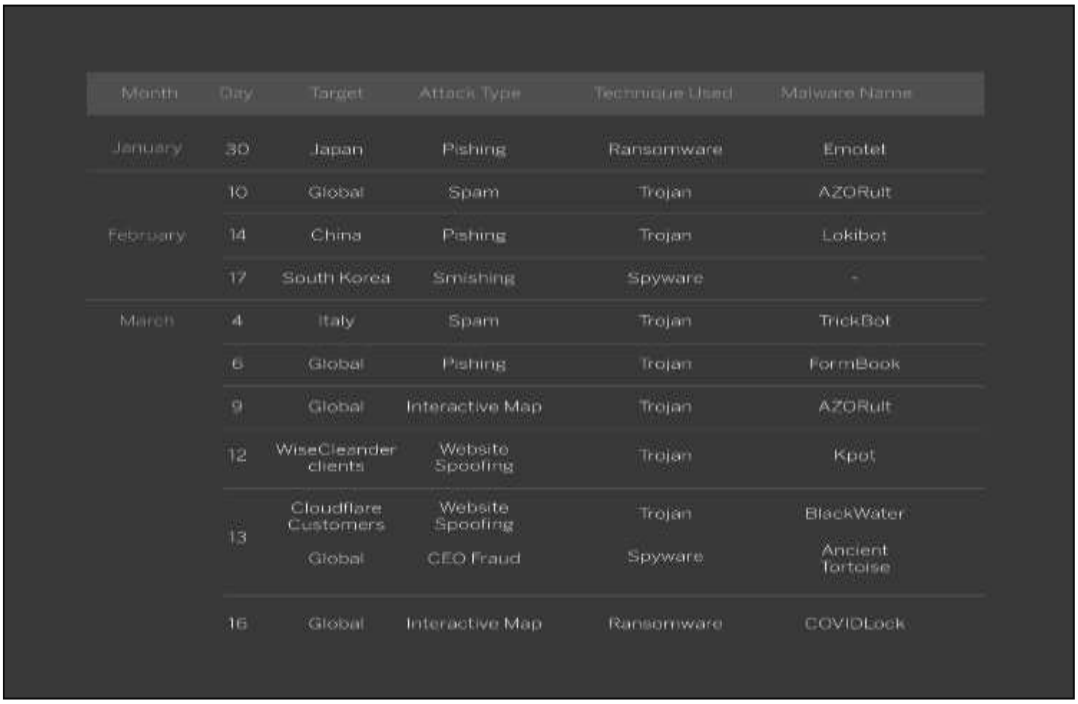


Figure 2 Implementation of security

Following is the table that displays the most successful cyber-attacks that have been occurred around the world since the World HealthOrganization's Emergency Committee met on January 22, 2020.



Month	Day	Target	Attack Type	Technique Used	Malware Name
January	30	Japan	Pishing	Ransomware	Emotet
	10	Global	Spam	Trojan	AZORult
February	14	China	Pishing	Trojan	Lokibot
	17	South Korea	Smishing	Spyware	-
March	4	Italy	Spam	Trojan	TrickBot
	6	Global	Pishing	Trojan	FormBook
	9	Global	Interactive Map	Trojan	AZORult
	12	WiseCleander clients	Website Spoofing	Trojan	Kpot
	13	Cloudflare Customers	Website Spoofing	Trojan	BlackWater
		Global	CEO Fraud	Spyware	Ancient Tortoise
	16	Global	Interactive Map	Ransomware	COVIDLock

Figure 3- Successful Cyber Attacks during COVID-19

IV. MEASURES TO PREVENT CYBER CRIMES

Hackers itself are using high level technology in order to perform these crimes. Although user cannot do much but always try to keep few things in mind while using internet.

- We need to be extra cautious while opening any link, if it seems to be suspicious don't open it.
- Always try to confirm the origin of any communication like from where it is started? why it is started?
- Don't share anything you receive.
- Always seek the information from official and trusted websites.
- Do not share your financial information like OTP, ATM pin etc. with anyone.
- Don't download applications from unofficial websites; they might be spreading fake news or fake links.

V. CONCLUSION

Cyber Security is and always will be the major concern. Majority of the hackers itself are IT Professional and dealing with them is a challenge. These crimes can never be fully stopped but still we need to minimize them. During this pandemic, we should only try to gather news from trusted source only. More secure steps need to be taken in order to prevent the future of technology from these crimes.

REFERENCES

1. A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging trends on latest technology- G. Nikhitha Reddy, G.J.Ugander Reddy.
2. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077
3. Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635- 018-0080-0
4. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole https://www.bbva.com/en/the-impact-of-covid-19-on-the spread-of-cybercrime/
5. Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.
6. Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.
7. Sutton, D. (2017). Cyber Security : A Practitioner's Guide. Swindon, UK: BCS, the Chartered Institute for IT.
8. WHO- https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
9. https://blog.avast.com/the-other-coronavirus-epidemic-cybercrime
10. Hua-Yi Lin1 and Tzu-Chiang Chiang "Efficient Key Agreements in Dynamic Multicast Height Balanced Tree for Secure Multicast Communications in Ad Hoc Networks" Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2011
11. P.Vijaya kumar and A.Kannan, S.Bose and S.Siva Subramanian "An Effective Key Distribution Protocol for Secure Multicast Communication, 2010
12. Guokai Zeng,, Bo Wang, Student,Yong Ding, Student, Li Xiao, andMatt W. Mutka, Senior,"Efficient Multicast Algorithms for Multichannel Wireless Mesh Networks" IEEE transactions on parallel and distributed systems, vol. 21, no. 1, january 2010
13. C.K. Wong, M.G. Gouda, and S.S. Lam, "Secure Group Communications Using key Graphs," ACM SIGCOMM Computer Comm..Rev., vol. 28, pp. 68-79, 1998.
14. D.M. Wallner, E.J. Harder, and R.C. Agee, "Key Management for Multicast: Issues and Architectures," IETF RFC 2627, June 1999.
15. Y. Challal and H. Seba, "Group Key Management Protocols: A Novel Taxonomy," Int'l J. Information Technology, vol. 2, no. 1, p p. 105-118, 2005