Impact of Cyber Security During Pandemics

Sourabh Sanjay Abhang

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

---***---

Abstract -During pandemic the work culture has been completely changed in order to contain the spread of viruses work from home culture has been introduced by several companies as users have moved working from offices to remote places/homes the companies had to upgrade their IT infrastructure like implement VPN'S to compensate for increased network traffic on the other hand to quickly overcome the infrastructure modifications some areas like network security often get overlooked which leads to increased number of cyber-attacks on the company precisely during pandemics. According to WHO there has been five-fold increase in the number of cyber-attacks since the COVID-19 pandemic. It has been observed that phishing sites/fraudulent emails are on a substantial rise in order to trick the person into downloading the malicious software which gives hacker the complete control over the infected machine which can contain confidential data about the user/company which he is working for putting the company as well as the person in distress. It is vital that we continuously educate ourselves with awareness programs. Lack of awareness and education of cybersecurity can lead to these situations. Organizations should focus on educating their employees about threats of cybercrimes in order to prevent breaches in the first place. It should be always be taken into consideration that a company's security is only as good as its weakest employee.

***Key Words*:**cybercrime, cybersecurity, network attacks, phishing, Ransomware.

1.INTRODUCTION

This pandemic has made businesses worldwide a challenge to be operational in spite of massive lockdown regulations by the government. Due to work from home culture there has been an increase in network traffic hence overnight the demands placed on digital equipments and networks have skyrocketed. In span of 2-3 months the world became more digitally connected more than evernot to forget vulnerable too. When working from home, employees may be tempted to use their company equipment (e.g., laptops or phones) for their personal uses. This could increase the risk of the devices being infected with viruses and malwares. Businesses rely on the digital infrastructure for their operations which have been impacted by several attacks resulting in loss of revenue for business owners. The reason behind such a spike in number of cybercrimes is the use of outdated softwares, misconfigured firewalls, expired security tools, lack of awareness to detect fraudulent emails and sites. Reports suggest that malware is being injected into systems by logging on to websites that host specific information on covid-19. All visitors to these websites were exposed to malicious software, leading to the extraction of personal data from their devices. New and emerging cyber-risks should be understood by the security professionals for instance they should make sure that the digital equipments can withstand cyberattacks during lockdown The continuous change in tools and methodologies used by cyber criminals makes it difficult for the security industry to keep up with the updates and patches to prevent these attacks Building softwares and hardware are long complex error prone processes on average for every 1000 lines of code there are 20 bugs which can affect security of system.

WHAT IS CYBERSECURITY?

Cybersecurity or information security are techniques of protecting computer systems and networks from unauthorized access or attacks which has the intent to cause harm or exploit the system

This term is divided into a few common categories as follows

Network security- It is the practice of securing networks, firewalls, routers from intruders it includes both hardware as well as software technologies.

Application security - Application security mainly focuses on keeping softwares and web Applications threat free. A compromised application can expose sensitive user data to the unintended viewer

Information security - It focuses mainly on integrity, privacy of data in multiple stages throughout the storage and transmission. This involves protection of electronic or any other form of confidential data.

Operational security - This includes the various processes and decisions taken for handling the data and protecting the assets. The permissions of users and privileges, data access control all fall under this domain.

End user education - It is an inexpensive way of enhancing security of your organization. This involves spreading awareness about threats and risks of cyberattacks and educating the employees to prevent and detect these types of attacks

Cyberthreats

1.Cybercrime consists of single individuals or group which target systems for financial gains or to steal sensitive data

2.Cyberattack could also be used for politically motivated information gathering

So, how can a malicious actor gain control of your system?

Here are a few common methods used to threaten cybersecurity

Malwares

Malware extends to malicious software. It is one of the most common cyberthreats used to infect machines it is a software which appears legitimate to the user but when installed on a system infects the system and gives the hacker complete control of the machine.

Malware can be distinguished into several types

VIRUS - Virus is a program when executed runs automatically and attaches itself to a clean file and spreads throughout a computer system

TROJAN - The term trojan is derived from ancient Greek history it misleads the user of its true intent it usually comes attached to a legitimate software and when installed it can damage the system or collect sensitive information.

SPYWARE - Spyware is a program that records the keystrokes and in some cases log files of the infected machine. It has the ability to capture and send all the keystrokes of infected machine to the originator.

ADWARE - These malwares display pop-up ads on the user's machine which when clicked usually leads to a malicious website which hosts other types of malwares

SQL INJECTION - An SQL (structured language query) injection is a type of cyberattack used to steal data from database from exploiting the input fields of web applications and servers. Criminals usually exploit vulnerabilities on the data-driven applications to insert malicious code in the form of malicious SQL statement which gives them access to the sensitive data in the database

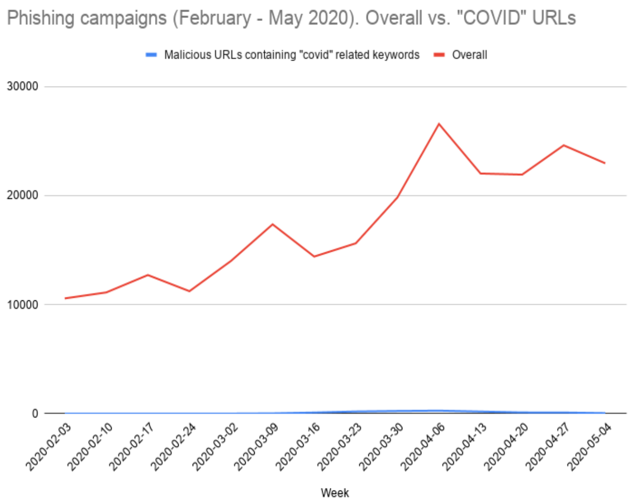
PHISHING - Phishing can be of multiple forms like fraudulent emails/websites which to the victim appear from a legitimate company asking for sensitive information usually bank account numbers or user id's and passwords. If the user submits the asked details these details go directly to the hacker.

MAN IN THE MIDDLE ATTACK - A man in the middle attack is a type of attack where a cybercriminal intercepts the communications between two parties in order to steal or to modify the data in transmission. These types of attack usually happen on public Wi-Fi networks or non-SSL websites.

DENIAL OF SERVICE ATTACK - Denial or service attack is meant to disrupt a network/organization by overwhelming their servers with multiple repeated requests rendering them unusable to their legitimate users

RANSOMWARE - Ransomware when executed locks down or encrypts users' files until the demanded ransom is paid which is usually in cryptocurrency. The intent of ransomwares is financial gain.

CURRENT EVENTS OF CYBERCRIME RELATED TO COVID-19



Phishing attempts specifically associated with Covid-19

Since February cybersecurity professionals have seen a rapid burst of infrastructure used by cybercriminals used to launch covid-19 themed spear-fishing attacks to lure victims into visiting fake websites to steal sensitive user data.

Few covid-19 related phishing campaigns are mentioned below

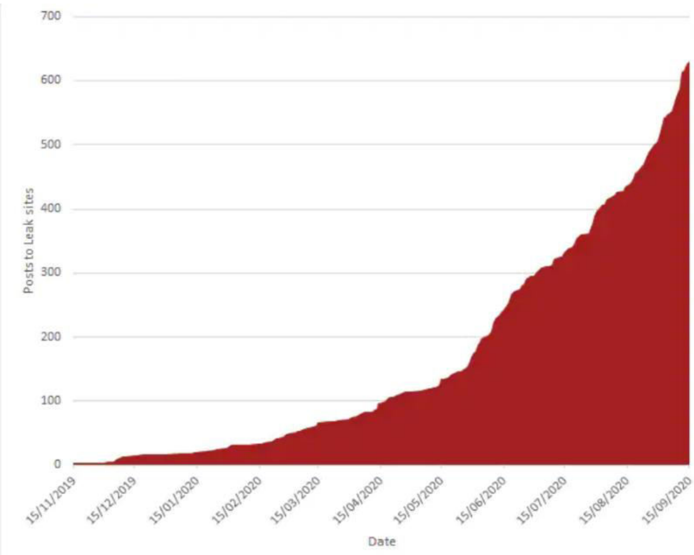
COVID-19 themed phishing emails attaching malicious Microsoft documents which are used to exploit a Microsoft vulnerability to execute malicious code

Multiple Phishing emails leading target users to fraud Centre For Disease Control (CDC) website which steal user credentials and passwords.

Phishing emails impersonating to come from various government Ministries of Health or World Health Organization conveying precautionary measures again by embedding malwares.

CYBERCRIME STATISTICS DURING PANDEMIC

The numbers are scary big. FBI recently reported that number of cyberattacks is many up to 4000 in a day. That represents a 400% increase since pre-covid-19. Interpol is also observing "alarming rate of cyber-attacks" specifically aimed at governments, military organizations and corporate businesses.



“A sudden explosion of Ransomware attacks during pandemic”

With organizations around the globe affected down by the COvid-19, Ransomware attacks has never been a worse time to suffer. Generic Ransomware is rarely targeted individually, instead a approach where attackers use email lists or compromised websites which blast out ransomware.

Here are few ransomware attacks of 2020

1- Travelex, a major international foreign currency exchange, confirmed getting infected by ransomware and certain services has been suspended

2- Hackers asking Richmond community schools to pay amount $10,000 in bitcoins to cover the hacking incident

3- After a failed attempt to disable the company's services, the Maze ransomware group published medical details and records of thousands of patients of a medical research firm

4-Blackbaud hack: More than 15 colleges in the United Kingdom and Canada confirmed being victim of cyber attack

EMAIL SCAMS RELATED TO COVID-19ESCALATED 667% IN MARCH

Reports of Barracuda networks, number of phishing scams exploded in march - July period. These phishing emails all work the same way

Only thing different is the tactics used by attackers. Because of sudden increase in digital infrastructure, people are accepting mails without verifying its legitimacy.

Cybersecurity Techniques

1.Access control

If threat inducing users cannot get into your network the amount of damage they can do will be minimum. It should also be observed that people who have access to internal networks are authorized and trusted because even authorized users can be potential threats as the are aware of the internal working of the system. Access control can be defined as giving access and resources to the user which is only required only for that individual’s responsibilities.

2.Anti Malware software

Malwares are malicious softwares which can be in the form of viruses, trojans, keyloggers, etc. These are designed to infect your system and cause damage. Anti-malware tools help us to identify these types of threats and quarantine or remove them. Although Anti-malware softwares are good to detect these threats but they can only do up to a certain point. There exist many viruses which bypass these softwares. Antimalware softwares are good but they should not be your only point of defense against threats.

3.Firewalls

Firewalls act as a network security device which monitors the incoming packets into your network. They can be software or hardware based and be configured with our own criteria to prevent or allow certain type of traffic. Web Applications use WAF'S (web application firewalls) for monitoring their traffic. Firewalls play an important role during an DOS (Denial of service) attack by detecting the manner of traffic and then preventing them from coming into the network

4.Intrusion prevention systems (IPS)

Intrusion Prevention systems constantly monitor traffic coming from outside your network(internet) and can detect any type of brute force attacks, SQL injection attacks etc. If the incoming network packet is identified as malicious it blocks the packet's ip address and prevents it from sending any further packets

5.Virtual Private Networks (VPN)

A virtual private network acts as a secure channel between 1 or more computers and the internet. All your data is Encrypted and sent via a virtual tunnel. Generally Remote access VPN use IPsec or secure socket layer (SSL) for authentication and encryptions. VPN's are used because they are secure against attacks and provide end to end encryption.

CONCLUSION

Cybersecurity is a vast Domain which is becoming more important day by day due to increased amount and widespread usage of internet. Huge number of online transactions are carried out everyday and we have to ensure smooth flow persists which requires immense amount of technical skills and knowledge for building robust and secure infrastructure. Cybercrime continues do diverge into different paths every day. It is important that we educate ourselves with the latest trends of cyberattacks and security to keep ourselves safe. In an organization a good cybersecurity team is ineffective if the company's employees are unaware of the common strategies and techniques used by criminals to infiltrate their network. In today's digital era there is no 100% secure method to protect ourselves from cyberattacks. The only thing we can do to prevent cyberattacks is to be as aware as possible and conduct educational programs and spread awareness among the people.

References

A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES ----- G. NIKHITA REDDY1 G.J.UGANDER REDDY2

CYBER CRIME AND CYBER SECURITY Soumya-SatishRevankar

https://www.buguroo.com/en/blog/covid-19-and-cybercrime

http://f3magazine.unicri.it/?p=2085