IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Challenges in the Post-Pandemic Digital Landscape

[1]Ramkumar Komakula, Assistant Professor, [2]Konala Uma Devi, Assistant Professor, [3]Vundamatla Guru kumar Assistant Professor,
Department of Computer Science and Engineering, BVC College of Engineering.

Abstract:- The world has started using more online activities like Bank transactions, social profiles etc after covid-19 pandemic, at the same time cyber security attacks have started trying to stealing the data and money from the users by using different methods. In this view the attacker has focused on social engineering attacks like phone call, messages ,Dumpster diving, shoulder surfing, emails, ads, pop-ups, and phishing etc, in obtaining the users critical data and trying to be more effective in their attacks. Accordingly many people have turned on to online work at the time of pandemic (covid-19).

The cyber security agencies like CERT-In i.e., Indian computer emergency response team has issued warnings that the cyber threat attackers are increasing and that they are improving in terms of stealing money, personal information and intellectual property.

The number of attacks has increased significantly during pandemic to more than 35% and also there has been an increasing vulnerability in cyber security among the government sector, businesses and individuals worldwide.

Keywords: Pandemic, security, sensitive information, warnings, attacks, significantly, concerns, online, Dumpster diving, shoulder surfing.

Introduction

Cyber Security is one of the application technologies, which is a practice of defending computers, servers, networks, mobile-devices, and data from malicious attacks i.e., unauthorized access or illegal usage. Now a day's cyber security is important for securing sensitive information from the security threats and cyber attacks. Some companies like Microsoft, McAfee, Avast... etc develop their own software's to protect their information. Cyber security includes a wide range of activities, form illegally downloading music files to stealing money from bank accounts.

Cyber attacks are not always towards financial scams and also non-monetary offences like job related, matrimonial frauds, stealing and misusing sensitive information (Debit/credit card details, bank account credentials, aadhaar details…etc), distribution of computer viruses, defamation of an individual on social media. Cybercrimes are also lead to sexual and physical abuse. India has highest number of internet users, after U.S.A. and China.

Cyber threats are classified into two types:

1. Cyber warfare
2. Cybercrime

1. Cyber warfare

In future wars will not be in traditional way, which means war will not be on land, water and air. When any state initiates the use of internet based invisible force as an instrument of state policy too fight against, another nation, called "cyber war", it includes websites, strategic controls, and intelligence.

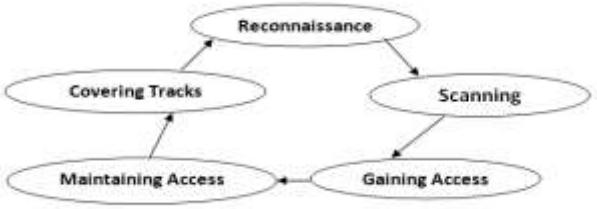
In 2008 attacks breached the US central command in Afghanistan. Flash drives with malicious code were inserted into military computers. In 2014, a cyber attack was done on German parliament for which the sofacy group is suspected. In 2020, December the USA discovered that Russian government hackers had infiltrated the networks of at least a dozen federal agencies in what become known as the S**olar Winds** hack.

2. Cyber Crime

Cyber Crime is an attack that can happen to a person or a business, which will be done on a computer or any electronic devices, like mobile phones. The cyber attackers use different software's and codes in cyber space to perform cyber attacks. They find vulnerabilities in the design of software or hardware, through injecting malicious malware like viruses, Trojans, worms etc.

By injecting these malware into the target system the attackers will try to gain the access to collect sensitive information. To inject malware in the target system, attackers use different techniques like sending phishing mails, or messages to the target.

Life cycle of Hacking:



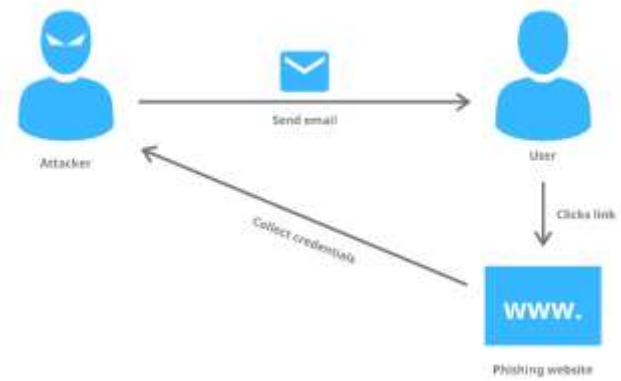
First of all, attacker gathers the information about the target and it can be done actively or passively, it makes the attacker closer to the target. Attacker scans the ports to identify the vulnerabilities or perform various assessments in order to get sensitive information. Using this scan result, i.e., information or vulnerability, attacker takes an advantage and perform exploit to gain access. Attacker injects the malware into the victim system to get sensitive information. Finally the attacker removes all the activity logs and session details in order to not get caught.

Here we are going to gain knowledge about the attacks which are performing after covid-19 pandemic. After covid-19 pandemic in India huge percentage of works are based online process, at the same time cyber crime rate was also increased.

Cyber security attacks were take place in each and every aspect of daily activities. The major cyber security attacks are listed below:

- Phishing attacks
- Social Engineering attacks
- Injecting malicious data
- Password cracking etc.

➢ In **phishing** attackers may refers to attempt to steal sensitive information in the form of username, passwords, credit cards, bank information etc.



For example a friend or a well known person will communicate with you through email and in that email there will be a malicious virus or a malicious file to download when you click on download your system may hack so that you have to take care about this type of fraud by communicating with them and knowing that the email was fake or real.

➢ In **social engineering** is not an attack, it is all about the psychology of persuasion. The target of this technique is to gain trust of targets and make them to perform unsafe actions. This technique maybe human based or tool based.

In this technique the attackers identify the target, gather the background information and select the attack method. Then engage the target, taking control of the interaction, then execute the attack finally remove all traces of malwares.

➢ **Injecting malicious** data is the top OWASP(Open Web Application Security Project) API security vulnerability and ranks high among common vulnerabilities and exposes that modern enterprises face. It also currently rank 6th in the top 25 common weakness enumeration of risks and common misconfiguration in distributed computing systems.

Mainly the attacker follows four ways in injecting malicious code, 1. Establish and maintain control over inputs, 2. Establish and maintain control over outputs, 3. Lockdown your environment, and 4. Assume external components can be subverted.

- **Password cracking** refers the process of identifying the weak passwords also to help the administrator for recovering the forgotten passwords, but more often it is used by bad actors to gain unauthorized access to systems and resources.

Prevention

To prevent these attacks we can take the following measures.

We have to give proper training to the employees in an organization, and also make awareness to the people like verifying the links, files before clicking and downloading. Verify the email address when we get the mails and we have to use common sense before sharing sensitive information.

We have to make our systems and software's up to date and the devices like mobile, laptop, tablets etc which are connected to corporate networks may give paths to security threats. These paths need to be protected with specific end point protection software. Using firewall is one of the way to protect our network from the attacks. We have to maintain data backup to avoid serious downtime. One of the attacks that you can receive on your system can be physical, having control over who can access the network. Secure your wifi networks and hiding them is one of the most safest things you can do for your systems.

Every organization should provide unique logins to employees for application and programs. And maintain admin rights to block installing unsafe software in the employee systems. Having different passwords setup for every application it may add real benefit to your security.

For complaint

You can complaint that the fraud like unauthorized access, investment fraud, OTP fraud, debit card credit card or any other type of cards frauds, dating apps, fake social media handling, E-Commerce fraud, honey trap, trading frauds etc. When you require to complaint against cyber crime you can approach the state cyber cell, if the fraud is done you can complaint to nearby police station along with fraud related documents.

Conclusion: Cyber Security is not just a technical challenge but a critical component of modern life, touching every aspect of society from personal privacy to national security. As technology advances, the threats evolve in sophistication and scale, making robust cyber security measures more vital ever.

To conclude, a comprehensive approach to cyber security is essential, incorporating technical solutions, user education, legal frameworks, and International Corporation. It's not merely about protecting data or systems, but safeguarding the very fabric of our digital existence. Only through continuous vigilance, innovation, and collaboration we can navigate the ever-changing landscape of cyber threats and ensure a safer, more resilient digital future.

References

1. © IEEE 2020. This article is free to access and download, along with rights for full text and data mining, re-use and analysis Authorized licensed use limited to: IEEE Xplore. Downloaded on March 19,2024 a t 07:14:22 UTC from IEEE Xplore. Restrictions apply.
2. Defense networks vulnerable to cyberattack: Expert https://www.cnbc.com/2013/10/11/department-of-defense-networks-vulnerable-to-cyberattack.html
3. By MAGGIE MILLER and LARA SELIGMAN 09/12/2023 10:32 AM EDT https://www.politico.com/news/2023/09/12/pentagon-cyber-command-private-companies-00115206#:~:text=In%20December%202020%2C%20the%20U.S.,known%20as%20the%20solarwinds%20hack.