Chapter 16
Emerging Cyber Security Threats During the COVID-19 Pandemic and Possible Countermeasures

Hepi Suthar
Rashtriya Raksha University, Gandhinagar, India & Vishwakarma University, Pune, India

ABSTRACT

The world suffering from COVID-19. In this situation, people are focusing on virtual or online modes of working, which can be done from home or anywhere. Cybersecurity has become the priority for all of us to protect data. This chapter mentions the most used cyber-attack techniques for stolen money and data from different sectors.

INTRODUCTION

A hostile Act as if aims to destroy data, steal data, or otherwise interfere with digital life is referred to as a cyber or cybersecurity threat. Cyber-threats include dangers like computer viruses, data breaches, and Denial of Service (DoS) attacks (D'Arcy J, 2020). Cyber threats and cyber-attacks are most visible in this situation because all activity takes place online, such as gaming, online certification or online course websites, payment applications, and many others. During COVID-19 situation, people want to make social distance and, because of that, only a few people move to the online platform, (Radanliev, 2020). Based on statistics, if compared to its increased usage of virtual and online application modes frequently used, the term "cybersecurity" describes a group of techniques, procedures, and procedures used to safeguard networks, devices, programs, and data from assault, deterioration, and unwanted access. Information technology security is another name for cybersecurity, (Khan, 2020). A hostile Act as if aims to destroy data, steal data, or otherwise interfere with digital life is referred to as a cyber or cybersecurity threat. Threats like computer viruses, data breaches, phishing, spamming, etc. are examples of cyber-attacks, (Partala, 2013).

DOI: 10.4018/978-1-6684-5250-9.ch016

Cyber-attacks are emerging due to more users using online platform for their work; likewise, professional meetings, online classes, online transactions, social media usage, online gaming, and many more, (Radanliev, 2020). Because of a lack of cybersecurity knowledge, cybersecurity is critical in taking lead in informing public during this pandemic situation. Using various cyber-attack techniques, data is stolen by hacker and breaches privacy policy of any company. A feature of such attacks will be that suppliers of security systems for companies, as well as organizations involved in development of control modules, will be under attack. Dozens of organizations working together can suffer at once. Another important trend in field of information security will be an increase in number of attacks on medical systems of clinics and hospitals, (Mastaneh Z, 2020). For example, in 2021, cybercriminals attacked systems that bill medical institutions and information databases containing customer medical records, (Rubí JN, 2020).

BACKGROUND

Provide In 2021, a large number of leaks of corporate data and user data were recorded. Among participants in high-profile incidents are well-known companies, and volume of lost user data is in hundreds of billions. There are different reasons, which include errors in operation of applications and protection tools, internal intruders, and actions of ransomware programs. In general, trend towards an increase in number of data leaks will continue since large amounts of corporate or personal data are always of interest to attackers due to their high cost, (Evans M, 2016). Separately, it is worth paying attention to a relatively new vector of attack propagation, namely attacks on supply chain or attacks by a third party. After attack on Solar-Winds and compromise of its Orion software, there were no less high-profile incidents, such as compromise of ASUS Live service or CCleaner program. The number of such attacks is predicted to increase in future, as corporate or private users do not expect to be attacked by trusted software or services. In same class of attacks, hacking networks of outsourcing companies and further attacks on infrastructure of their customers, as well as attacks on corporate resources through home computers of users transferred to remote work, remain relevant, (Ahmed N, 2020).

Of course, one of the most relevant cyber threats in 2022 will remain phishing attacks, in which victim receives a fake email from, for example, a search service or an online store with an offer to go to a fake website or open an email attachment that contains hidden ransomware code. According to Kaspersky Lab experts, in 2021, up to 350,000 new malware patterns were registered per day, most of which belong to ransomware class, as well as tens of millions of phishing emails. This growth is explained by fact that cyber fraud is actively developing as a separate industry, in which there are services for creating ransomware programs, distributing them, and collecting money. In addition, now, before encrypting data, ransomware will first try to find credentials to access victim's crypto wallets or other sensitive data.

Another emerging threat in 2022 will be attacks on IoT devices and process control systems. The former are usually poorly protected, latter often run on outdated operating systems and do not allow use of modern security tools. As a result, attackers have opportunity to mine cryptocurrency on any device that runs on Linux. For example, the Mirai botnet started using a Trojan for mining on video cameras back in 2017. Despite ridiculous hash rate (the computing power of farms for mining cryptocurrency), in this case, number of infected devices wins. Process control systems remain vulnerable: last spring, an attack on one of largest suppliers of gas and oil in West stopped all of its pipelines for five days.

In addition, in 2022, due to transition of many companies to remote modes of operation, personal safety of staff will decrease, (Burrell DN, 2020). Employees do not have a clearly defined motivation to