IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 4, March 2024

Cyber Crimes during COVID-19 Pandemic

Mr. Thakur Sadgurusingh Nareshsingh[1] and Prof. Sonali Doifode[2]
FYMSc CS, Department of Computer Science[1],
Research Scholar, Department of Computer Science, Shri JJT University, Rajasthan
Sarhad College of Arts, Commerce and Science, Katraj, Pune, India[2]
Savitribai Phule Pune University, Pune, Maharashtra
Corresponding Author: Thakur Sadgurusingh Nareshsingh
sadgurusinghthakur@gmail.com

Abstract*: The COVID-19 pandemic has accelerated the use of digital technologies online website causing significant changes in the way we live and work. While these developments provide the necessary tools for remote working, education and communication, theyalso create new opportunities for cybercriminals. This content explores the emergence and evolution of cybercrime in the context of the COVID-19 pandemic Examines increasingly common types of cybercrimes, including phishing attacks, ransomware, and online fraud. The details also reveal the motivation behind these cybercrimes, fromfinancial gain to exploiting fear and uncertainty. It also emphasizes the importance of cybersecurity knowledge and measures to protect people, organizations and critical system in the digital age. Has the world's grapple with the ongoing pandemic combating cybercrimes has become important parts of our response to this crisis.*

Keywords: COVID 19 pandemic, Digital transformation, Online platforms, Vulnerability, Cyber threats, Cyberattacks, Phishing, Ransomware, Online fraud, Disinformation campaigns

I. INTRODUCTION

The rise of technology in our increasingly interconnected and digitalize world has brought many benefits and conveniences however it has also led to the emergence of the virtual environment with the intension of damaging, controlling or using digital system, information and people.

Cybercrime has become a major challenge for law enforcement, government and individuals. These crimes know no boundaries and can affect anyone online. Motivation behind cybercrime can be from Financial gain to political or ideological gain.

The Covid19 pandemic has caused unprecedented changes in the world's behavior,education, communication and daily life as people and organizations rapidly use

technology in their work. While this digital transformation is essential for continuity,

it also creates a suitable environment for cybercrime. Cyber criminals took advantages of the anxiety and uncertainty created by the epidemic, leading to many cyber-attacks.

Examining cybercrime during the pandemic is important for the following reasons:

- Digital addiction is increasing
- Progress in cybercrime
- Public Security
- Global Security
- Assess the impact of cybercrime
- Describe cybercrime types and tactics
- Investigate the motivations and knowledge of cybercriminals
- Identify vulnerabilities and inconsistencies in cybersecurity

DOI: 10.48175/IJARSCT-15980

II. DIGITAL TRANSFORMATION DURING COVID-19

The COVID-19 pandemic has led to a massive and rapid digital transformation worldwide. As governments close their doors, businesses close their doors andschools close their campuses, people and organizations are turning to technology to manage simple tasks and connect.

The rapid use of digital technology and remote working during the COVID-19 pandemic is a response to the unprecedented challenges posed by healthcare worldwide. It bring benefits and challenges by changing the way people and organization work.

Digital platforms are playing an important role in maintaining essential services during the COVID-19 pandemic. In situations where physical interaction is limited, digital technologies and platforms play a key role in ensuring the continuity of basic services. Here are some important aspects of their role.

1. Remote working and collaboration
2. Telemedicine and Healthcare
3. Online education and e-learning
4. Digital payment and commerce
5. Banking and financial services
6. Digital communication and information sharing
7. Virtual events and meetings
8. Social services and support networks

The rapid adoption of digital technologies and remote working during the COVID-19 pandemic has led to increased digitization, expanding the stoppingpoint for cybercrimes.

III. TYPES OF CYBERCRIME DURING THE PANDEMIC

1. Phishing Attacks
2. Ransomware incidents
3. Internet fraud
4. Spread of fake news and fake news
5. Telemedicine and Fraud in Healthcare
6. Fake COVID-19 Tracking Apps

Due to increased stress, rapid changes in digital technology and increased productivity, individuals and organizations are becoming more vulnerable to cyber-attacks. Online games. Cybersecurity awareness and precautions are critical in combating these emerging threats.

IV. MOTIVATIONS BEHIND THE CYBERCRIME EPIDEMIC

1. Making Money:
2. Using Fear and Uncertainty:
3. Cyber state support:
4. Misinformation
5. Vaccine chain Attack

These incentives highlight the complexity of the cyber threat landscape duringa pandemic. Cybercriminals and threat actors use specific crisis situations to achieve their goals, highlighting the importance of security measures in cybersecurity and international cooperation in countering cyber threats.

V. IMPACT OF CYBERCRIME

1. Financial losses:
2. Impact on essential services:
3. Privacy and Personal Protection:
4. Loss of trust and reputation:
5. Health benefits:

DOI: 10.48175/IJARSCT-15980

6. Impact on education

VI. VULNERABILITIES AND CHALLENGES

1. Digital footprints:
2. Human error:
3. Law and international cooperation:
4. Public Awareness:

VII. CYBERSECURITY AWARENESS AND PREPAREDNESS

1. Education and Training:
2. Strong passwords and authentication:
3. Data Protection:

VIII. CASE STUDIES

Of course, here are some real-life example of significant cybercrimesoccurring during the COVID-19 pandemic:

SolarWinds Cyber Attack:

SolarWinds cyberattack discovered in late 2020 attack is a sophisticated supply chain attack that disrupted software updates for IT management software SolarWinds. Cybercriminals inserted malicious code into software updates, allowing them to a agencies and large corporations. The attack, for which actors in the country are blamed, shows the fragility of thesoftware.

Ransomware Attacks in Healthcare:

Healthcare organizations have been the target of ransomware attacks throughout the pandemic. In one case, the University of Vermont HealthNetwork suffered a ransomware attack that disrupted patient care and caused significant financial losses.

Vaccines related to COVID-19 cyberattacks:

Various cyberattacks have targeted organizations involved in the researchand distribution of vaccines against COVID-19.

COVID-19 Misinformation

The pandemic has witnessed a rise in misinformation on social media platform.

Legal and Regulatory Responses:

The government of India has implemented various laws and regulation to combat cybercrime and improve cybersecurity. These measures aim to strengthen the country's ability to prevent, investigate and prosecutecybercrime. Some important law and regulations in India are:

- Information Technology Act, 2000 (IT Act):
- Cyber Crime Cell:
- National Cyber Security Policy (2013):
- Data Protection Act:
- Information Technology Laws (Amendment) Bill, 2021:
- Social Media Mediation Guidelines:
- Cooperation with international partners:
- Cyber Security Awareness Activities

India's legal and regulatory framework continues to evolve to keep up withthe ever-changing cyber threat landscape. These measures are designed toincrease cybersecurity, protect critical systems and create a safer environment forpeople and organizations in the country.

IX. MITIGATION STRATEGIES

1. User Education and Awareness
2. Strong passwords and multi-factor authentication (MFA)

DOI: 10.48175/IJARSCT-15980

3. Regular software updates and patch management
4. Network security
5. Data encryption
6. Access Control
7. Endpoint Security
8. Crisis Response Plan
9. Security Information and Systems Management (SIEM)
10. Backup and disaster recovery

X. FUTURE TRENDS AND CHALLENGES

Due to technological changes and changes in the digital environment, thecybercrime landscape is constantly evolving. Looking ahead, some challenges and challenges will impact the world of cybercrime.

1) Evolution of Ransomware:

Ransomware attacks will continue; cybercriminals will use more sophisticated methods and target a variety of victims, including critical systems and mental chain organizations.

2) Internet of Things (IoT) Vulnerabilities:

As the number of IoT devices increases, attacks against cyber criminals also increase Vulnerabilities in IoT devices can be exploited to carry out a variety of cybercrimes, including botnets and data theft.

3) Artificial Intelligence and Machine Learning in Cybercrime:

Cybercriminals will use artificial intelligence and machine learning to automate attacks, improve evasion techniques, and optimize social engineering plans.

4) Deepfake Threats:

Deepfake technology can create fake content, including video and audio recordings. This increases the risk of misinformation, identity theft and fraud.

5) Insider Threats:

Insider threats, whether intentional or unintentional, can be very difficult. Organizations need to strengthen monitoring and analysis of user behavior to detect and prevent insider attacks.

6) Cybersecurity Skills Shortage:

The shortage of cybersecurity professionals will continue, making it difficult for organizations to build and manage security teams.

7) Cloud Security Issues:

As more and more information and services are moved to the cloud, cloud security is gaining importance. Improper installation and poor practices can result in the disclosure of sensitive information.

8) Digital Theft:

With the increasing use of identity and biometric technologies cybercriminals will target personal information and digital credentials. As cybercrime becomes more sophisticated and pervasive, organizations governments and individuals must adapt to these challenges. This includes strengthening cybersecurity measures, promoting awareness and education, and promoting international cooperation to effectively respond to cross-border threats.

In summary, the changing cybercrime landscape creates ongoing challenges for individuals, organizations, and governments around the world. The COVID-19 pandemic has further emphasized the importance's of cybersecurity measures and international cooperation in combating these threats.

Cyber criminals are equipped with advanced tools and equipment and looking for opportunities to exploit, steal data and disrupt critical processes. The rise of ransomware attacks, state-sponsored cyber campaigns, and new technologies such as deepfakes and policymakers. While the future promises hope in terms of innovation and digital trans formation, it also brings with it many negativities and risks. To protect against the changing cybercrime landscape, it is important to remain vigilant, adapt to new threats, and implement a good cybersecurity strategy. These strategies should include prevention, detection, intervention and recovery measures. In a world dependent on digital technology, the fight against cybercrime continues. Although the task may seem daunting, it is a shared responsibility to protect our digital future

DOI: 10.48175/IJARSCT-15980

and protect the integrity, privacy and security of people and organizations. With measures, tools and commitments, we can prevent cyber threats and reduce their impact on the world networks.

REFERENCES

[1]. Impact of Covid 19 on cybercrime: https://fully-verified.com/the-impact-of-covid-19-on-cybercrime/

[2]. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

[3]. https://doi.org/10.1016/j.cose.2021.102248https://www.researchgate.net/publication/349845621_Cyber_Security_in_the_Age_of_COVID-19_A_Timeline_and_Analysis_of_Cyber-Crime_and_Cyber-Attacks_during_the_Pandemic

[4]. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world

[5]. https://www.cbsnews.com/news/ransomware-phishing- cybercrime-pandemic/

DOI: 10.48175/IJARSCT-15980