International Journal of Advanced Technology in Engineering and Science
Vol. No. 10, Issue No. 01, January 2022
www.ijates.com
ijates
ISSN 2348 - 7550

CYBERSECURITY DURING COVID - A REVIEW

Vimalraj.M[1], Keerthivarman.N[2], Kavishankari.S.P[3], Vidhya.[4]

[1]*Third year CSE, Department of CSE, Builders Engineering College, Tirupur, India.*

[2]*Third year CSE, of CSE, Builders Engineering College, Tirupur, India.*

[3]*Third year CSE, Department of CSE, Builders Engineering College, Tirupur, India.*

[4] *Assistant Professor, Department of CSE, Builders Engineering College, Tirupur, India.*

ABSTRACT

COVID 19 has made a serious impact on the cyber world as it has made on the life of human beings. The covid has paved a way for the cyber criminals to exploit organisations and people in order to do what they want to do to get paid. It has put forward new challenges for cyber security to solve. It first gives a detailed view on the breaches and exploits happening in the last few years and gives a brief suggestion on how to prevent these attacks before happening.

Keywords - Botnet, COVID 19, Cyber Security, Phishing, Ransomware.

1. INTRODUCTION

Cyber security is one of the key components for the daily internet to work properly. During covid 19 the organisations changed their traditional method of working from an office to work from home method. This caused too many security loopholes for a threat actors to work with. The workers without adequate knowledge on security are easy prey to the hackers to get into the company's infrastructures. From DDOS assaults to cybersecurity exploits that result in a data breach, cyber-attacks present a growing threat to businesses, governments, and individuals. Whether they come from so-called hacktivist groups or state-sponsored cyber warfare units, this type of attack is increasingly giving cause for concern. The Zero days exploits that are exploited in the wild are a major concern for an organisation.

2. TYPES OF ATTACKS

There are different ways to attack an organisation or an individual, some of the major ways are mentioned below:

1 .DDOS

2. Ransomware

3. Malware

4. MITM

5. Phishing

6. ZERO DAY

2.1 DDOS

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices on the internet to launch this attack . This is known as a distributed-denial-of-service (DDoS) attack.

2.2 Ransomware

Ransomware is a type of malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them . Recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies that are used for the ransoms, making tracing and prosecuting the perpetrators difficult . Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, travelled automatically between computers without user interaction.

2.3 Malware

Malware, short for “malicious software”, refers to any intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

2.4 MITM

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

2.5 Phishing

Chances are you wouldn't just open a random attachment or click on a link in any email that comes your way is low. Attackers know this, too. When an attacker wants you to install malware or divulge sensitive information, they often turn to phishing tactics, or pretending to be someone or something else to get you to take an action you normally wouldn’t . Since they rely on human curiosity and impulses, phishing attacks can be difficult to stop . In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with . The email will seem legitimate, and it will have some urgency to it . In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, you’ll thereby install malware in your computer . If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file except the website is actually a trap used to capture your credentials when you try to log in.

2.6 Zero Day

Zero-day vulnerabilities are the hardest kind of vulnerability to protect against because no security company and very few, if any, anti-virus software packages are prepared to handle them or the malware that attempts to exploit them. There are no patches available to solve the issue and no other mitigation strategies because everyone just found out about the darn thing! Unfortunately, it is often easier and faster for cybercriminals to take advantage of these vulnerabilities than it is for the good guys to shore up defenses and prevent the vulnerability from being exploited.

3. STATISTICS ON ATTACKS DURING COVID-19

Figure 1 gives a detailed view of the percentage of organizations compromised by at least one successful attack.

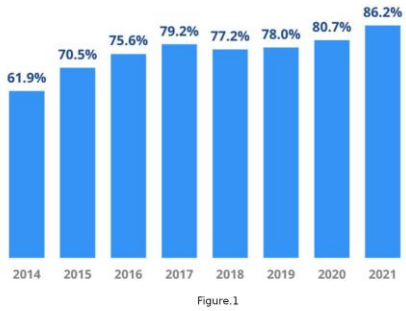


Figure.1

Successful attack compared to years before covid the rates of attacks have increased significantly.

4. ATTACKS ON ORGANISATIONS

April 03, 2021 Facebook was associated with large data breaches more than a few times in the past. Being one of the largest social media platforms, the data breaches happening for Facebook have always proved critical. The most recent data breach of Facebook has exposed the personal data of 533 Million users. The data exposed included phone numbers, DOB, locations, past locations, full name, and in some cases, email addresses.

June 29, 2020 Online learning platforms have become increasingly popular targets for data breaches over the past few months as the education world has gone digital. Unfortunately, OneClass is no exception and left the data of over a million North American students (many of them minors) exposed on an unsecured Elastic search server. The data exposed included students' full names, email addresses, schools/universities, phone numbers, account details and school enrollment details.

June 19, 2020 US tech giant Oracle owns BlueKai, a company very few have heard of outside of marketing circles but it possesses one of the largest banks of web tracking data outside of the federal government. The company uses website cookies, and other tracking technology, to follow your activities on the web then sells that data to companies and marketing firms. For an unknown period of time, all of that web tracking data was left exposed on a server without a password. Billions of records were unsecured for anyone to find. The data exposed included names, home addresses, email addresses and other identifiable data including web browsing

activity. The details are still fuzzy. Oracle says that they have taken care of the problem but haven't offered up any information as to how this happened and who was affected.

June 14, 2020 The Postbank in South Africa has had to replace over 12 million bank cards after an unencrypted master key was stolen by employees. The master key granted anyone complete access to the bank's systems and the ability to change information on any of the bank's 12 million cards. The breach specifically affected between 8 and 10 million beneficiaries who receive social grants every month. It's still unclear if any funds were stolen, and exactly what data was exposed.

June 9, 2020 Keepnet Labs is a UK security company that initially experienced a breach back in March 2020 when a database was exposed containing data that had been previously been exposed in other data breaches. After being notified, Keepnet Labs quickly took the data down but refused to acknowledge the breach. They even went as far as to pursue legal action against at least one tech reporter who had written about the breach.The breach was finally acknowledged this month when Keepnet Labs issued a statement saying that they were not directly responsible, but rather a third party provider was. Although no new data was exposed, it's ironic that a security company would experience a data breach.

June 4, 2020 Chartered Professional Accountants of Canada (CPA) experienced a cyberattack early in the month that allowed unauthorised third parties to gain access to the personal information of over 3,29,000 members and stakeholders. The stolen information was mostly related to the distribution of the CPA Canada magazine and included personal data such as names, addresses, email addresses, and employer information. Passwords and credit card numbers were also exposed, but CPA Canada says they were all protected by encryption. Anyone affected by the breach has been notified by the company, and CPA Canada notified the relevant authorities.

May 27, 2020 The personal data of 47.5 million Indians was found for sale on the dark web for $1,000, and is claimed to have originated from the popular caller ID and spam blocking app Truecaller. Personal information such as phone numbers, service providers, names, genders, and more was made available.However, Truecaller denies there was a breach at all. Truecaller suffered a previous data breach in May 2019, and the company suggests that it is the same data set that is for sale. If Truecaller has suffered a breach this month, then it's a case of gross negligence, or it could just be criminals trying to make a quick buck.

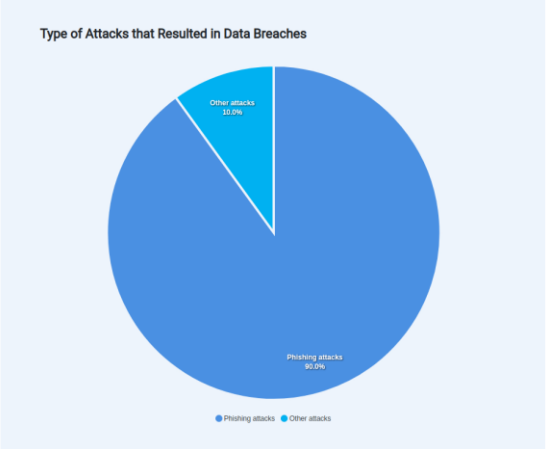
December 30, 2019 The smart camera provider Wyze suffered two breaches at the end of December when databases were left exposed for over two weeks. So far, it appears that only email addresses were leaked. Smart cameras are starting to become a popular target for hacks.

December 17, 2019 In what is believed to be the largest breach in Canadian history, medical testing company LifeLabs suffered a hack in October that left 15 million records of patient data exposed. The breach wasn't announced until December, and the company is now facing a billion dollar class action.

November 22, 2019 T-Mobile, the multi-national wireless network operator, suffered a major data breach, reportedly affecting over 1 million customers. The exposed data includes phone numbers, billing addresses, T-Mobile account numbers, names, and details about rates and plans.The news comes at a particularly bad time, as customers suffer a heightened risk of identity fraud during the holidays, while T-Mobile's attempted merger with Sprint may now face more intense scrutiny.

5. MOST SUCCESSFUL ATTACK VECTOR

The 2020 State of Phish Annual Report states that 65% of organizations in the United States fell victim to a phishing attack that year . The preponderance of social engineering methods suggests that cybercriminals take advantage of the emotions or negligence of human beings more often than they target system vulnerabilities.



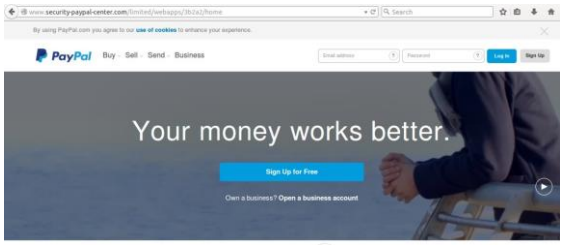
5.1 Email phishing

An email used as a tool to carry out fraudulent activities like stealing and misusing personal information is called a phishing email.

#	Email subject	Category
1	Microsoft account password reset	Legitimate
2	Your Mailbox Will Shotdown Verify Your Account	Common Phishing
3	Fw: DHL World Wide Delivery/Parcel Arrival	Common Phishing
4	Employee Starter Kit	COVID-19 Phishing
5	COVID-19 Travel Guideline	Legitimate
6	Verify your email address	Legitimate
7	RE: [HSBC] Important Message Alert !!!!.. REF ID 233455	Common Phishing
8	I highly recommend you analyze and abide by the instructions attached	COVID-19 Phishing
9	Critical security alert	Legitimate
10	Important Coronavirus (COVID-19) Safety Measures	COVID-19 Phishing
11	Did You Just Sign In?	Common Phishing
12	Genuine Details Concerning COVID-19	COVID-19 Phishing
13	Microsoft account security alert	Legitimate
14	Increased Coronavirus Cases in your Area	COVID-19 Phishing
15	Important Information Regarding Your Account	Common Phishing

5.2 Cloned website

During adversarial attack simulations harvesting credentials through phishing are typically performed through cloned websites. A cloned website works by essentially copying the front-end and hosting it on a domain designed to mimic the real domain.



6. PREVENTION

6.1 Steps for employers to adopt to mitigate risks

1.Engaging a team of experts to not only assist with the remediation, restoration and recovery of IT system and business operation but to head off any downstream risks which include regulatory scrutiny and litigation risks.

2. Often an HR policy will simply state that "information is to be kept confidential" but when informing employees of a cyber breach that has affected the company, it is important to emphasise the confidentiality of the details of such an incident to prevent rumour-mongering and unwanted public scrutiny.

3.Consider the flow of information within the organisation. Is it important to be completely transparent with staff, or is it more important to stop any flow of misinformation and therefore ensure that communications are kept to as small a group as possible? Both options likely have their advantages and it will depend on the specific facts of the security event as to the best approach to take. It is worth bearing in mind that employees may well be anxious and concerned about what has happened to their data, who has access to it, whether there will be any impact on their day to day activities and whether they will continue to be paid.

4.Employees should be on board to manage any client expectations and to provide the necessary assurance to clients that the incident is being handled competently.

5.It is key that all employees should be vigilant against any further attacks and must know what to look out for and how to go about reporting any suspicions. Training is key.

6.2 Cybersecurity tips for individuals

1.The first and most basic step in maintaining cybersecurity is to create a unique and original password for each account. Users should also remember to update passwords every three months.

2.Keeping up with software updates is important, as cybercriminals often target known flaws in software to access a user's system.

3.Cybercriminals may comb through social media posts in search of information commonly used in security questions, such as a pet's name or mother's maiden name. To combat this risk, social media users should set their account to private or avoid revealing sensitive information in posts.

4.A virtual private network (VPN) is a great way to protect sensitive data, especially when accessing a public Wi-Fi network. A VPN encrypts all information transmitted by your device and helps prevent many types of cyberattacks.

5.And finally, teachers and parents should educate children about proper internet usage. Children and teens should know what the rules and guidelines are for surfing the internet and using social media.

7. CONCLUSION

The increased usage of online services during the COVID19 pandemic, coupled with users' fear, has resulted in a spike of Cyber attacks.To gain insight into how the pandemic changed trends in phishing and scams and how attackers took advantage of this situation. Everyone deserves a right to live in a secure environment on the Internet. However,When online business activities are disrupted, its leads to great inconvenience for customers and companies.With technology being such a big part of our lifestyles today, cyber-crime has no place in it.

REFERENCE

[1]Top 10 Most Common Types of Cyber Attacks, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks.
[2]All Data Breaches in 2019 – 2021 – An Alarming Timeline, https://selfkey.org/data-breaches-in-2019/
[3]MarziehBitaab, Haehyun Cho, Adam Oest, Penghui Zhang, Zhibo Sun, Rana Pourmohamad,Doowon Kim, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupe and Gail-Joon Ahn,*ScamPandemic:How Attackers Exploit Public Fear through Phishing*,2021
[4]Top 10 Ways to Prevent Cyber Attacks https://www.cloudwards.net/cyber-security-statistics.
[5]Ways to Prevent Cyber Attacks https://www.datamation.com/security/cyber-attack-prevention.