Cyber Threats Landscape Overview Under the New Normal

Indraneel Mukhopadhyay

Abstract During the time of this pandemic, the dependency on Internet has increased manifolds. Employees are doing Work from Home, Students are Studying from Home, Teachers are teaching from Home, Everyone is shopping from Home and the list continues. All this has given rise to Cyber Security Vulnerability attacks like phishing attacks, malware attacks, ransomware attacks, social engineering attacks, identity theft, and a denial-of-service attack. This paper discusses the basic concept of cybersecurity and with a detailed review of recent cybersecurity attacks from January 2020 to March 2021 with a detailed analysis of motivation behind such attacks, attack techniques used, and targets of the attacks. This paper will also discuss cloud breaches, data breaches, and leaky buckets which have increased from 2021. The paper will discuss the types of cyber attacks, attack types, and targets of those attacks.

Keywords Cyber-attack · Cyber security · Data breaches · Leaky bucket

1 Introduction

Cybersecurity threats and breaches are taking away the sleep of Security Officers of the companies. They are not sure what kinds of attack, when and where will strike their network. Whenever we think of cyber attacks we can broadly classify it into three factors the spectacularity factor, the vulnerability factor and the fear factor. The spectacularity factor can be related to the impact factor of the attack that has been achieved on the targeted system. The impact can be financial loss, publicity loss for an individual or for the whole organization. An example of this impact factor is a Denial of Service (DoS) attack against any online service delivery platform business, which will result in stoppage of online service delivery and in turn lead to loss of substantial income. The vulnerability factor on the other hand is related to attacks on security system and security infrastructure. The fear factor plays on the attacker

I. Mukhopadhyay (✉)
Institute of Engineering & Management, Kolkata, India
e-mail: imukhopadhyay@iemcal.com

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_70

intention to create a sense of fear to its victim. Ransomware attacks have been one of the best methods to play fear factor on the government, organization or individual. Once the ransom has been paid the attackers decide whether to release the system or keep on going. The fear is always there with the victim. Nowadays all ransomware attacker uses cryptocurrency so that it becomes hard to trace.

Due to pandemic scenario change in working environment has seen increase in the motivation of cyber attack and also the target of the attack like government, healthcare facility and even pandemic research institutes [1]. If we take a survey 80% of the organizations do not spend enough budget on Threat Analysis and Prevention hence an overview threat landscape should give them the wake up call to do so. Though there was a 8% decline in global IT spending, the global spending for cybersecurity was increased to around 54.7 Billion US Dollar and its estimated that the spending will go up to 60.2 Billion US dollar compared to mere 40.8 Billion dollars I 2018 [2].

In this paper, we will compare the cyber security landscape of past few years and then we will compare it with pandemic scenario. We will also see how the motivation of a cyber security attacks' and its target have impacted our economy. We will also see major breaches that have happened in the Q1 2021 and its impact [3].

2 Comparison of Cyber Attack

As per a study conducted by AT&T most IT companies spend up to 10% of their IT budget on Cybersecurity [4]. This attracts hackers to attack the system. With the pandemic in employees working from home and login in to the company secure server it became a lucrative offer for all the hackers. What came was the never before seen threats to different sectors. If we compare the attack scenario of last three years, the per month attack has risen in 2020 and it is still on the rise. Figure 1 graphically shows the cyber attacks per month per year.

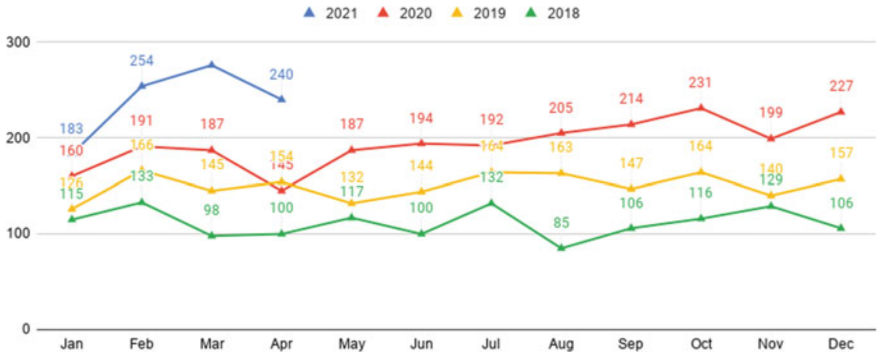

Fig. 1 Comparison of Cyber Attacks 2018–2021

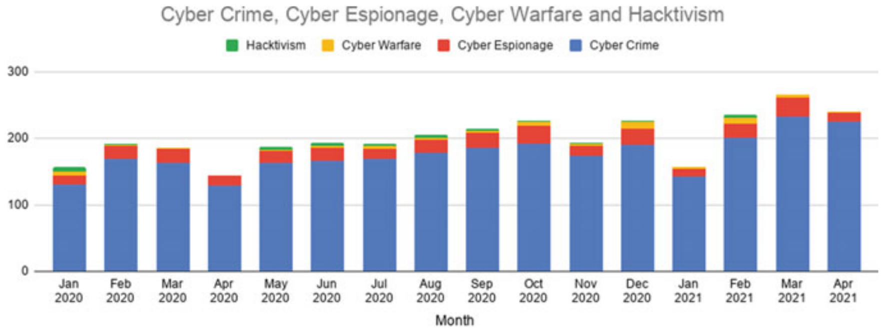

Fig. 2 What Motivates Hackers (2020–21)

Questions arises here that what is the motivation behind these attacks. As we have discussed in the earlier section the motivation behind cyber attack can be classified under spectacularity factor, the vulnerability factor and the fear factor. The other factors are cyber espionage, cyber warfare and Hacktivism.

Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property data. The reason behind such a cyber attack is to make sure the victim which can be an organization or government entity losses their advantage. This data can then be sold to the highest bidder in the dark web. Cyber warfare uses current computer technology to disrupt the digital or online activities of the state or organization, especially when there is a deliberate attack on computer system for government, energy, strategic and military purposes. If strategic and military systems are compromised it can lead to the death of large number of people hence they are called Cyber Warfare. Hacktivism on the other hand is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes. Example of Hacktivism in recent times are the operation #OpGeorgeFloyd, born after George Floyd was killed by police in Minneapolis in May 2020, amassed 8535 tweets in just three weeks. Some major hacks and cyber espionage of 2020 were like on July 15, 2020, more than a dozen high-profile Twitter accounts were commandeered by hackers who sent out tweets from the accounts of now President-Elect Joe Biden, Elon Musk, Bill Gates, Michael Bloomberg, Jeff Bezos, and others [5].

3 Comparisons of Cyber Attack Types and Target Industries

Before the Covid19 turned our life upside down the Industry was looking for an increase of cyber attack in the factor of 5 to 10% from the year 2019 to 2020 but little did we know the Covid19 scenario will create a tsunami of cyber attacks which took the advantage of the Work from the Home scenario. As the organizations were not ready with the new normal the organizations were forced to adapt protection protocol, but not giving away precious data. In this paper we have taken into account the Top 10 attack types used by hackers and also its intended industry target of attacks. The following section graphically represents the same.

If we compare the different attack type's attacks that was used to compromise the system in the year 2020 and 2021 (Till April 2021) as shown in Fig. 3, we will see Malware was the highest followed by account hijacking, targeted attack, and vulnerabilities and so on. But if you look at 2021 vulnerability attack is on the rise. This is due to the fact the attackers are trying to access the vulnerability not only at organizational level but also at individual level via which they can get access to organization.

As we have seen the amount of cyber attack is on the rise we have to also see which are the different industries affected the most. Figure 4 shows the various targeted area of attacks. As clear from the graphical representation Individual have been attacked considerable compared to other heads like Public Administration, Education, Financial, Social Welfare.

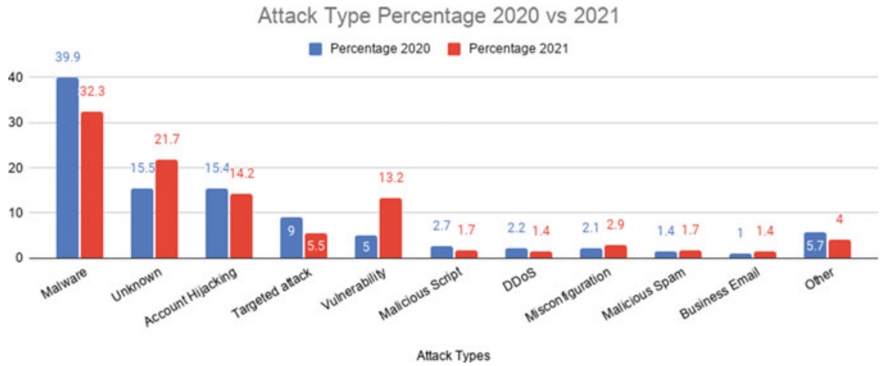

Fig. 3 Different Attack Type used

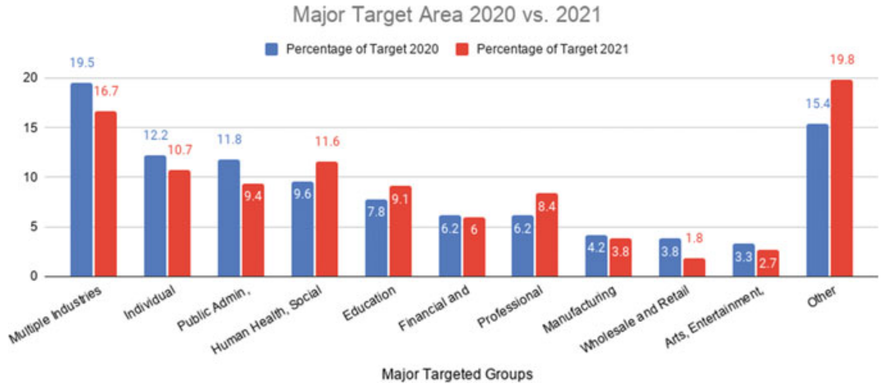

Fig. 4 Major Targets of Attacks

4 New Types of Threats in 2021

Threats are there but now the hackers have turned their attention to new types of attacks all due to the new normal. Due to the Work from Home scenario most of the organizations are trying to upload the data to the cloud so that the employees can login from anywhere and work. They do keep sensitive data on private network but the growth of cloud storage and work has risen considerably in the past one year. Due to this two major types of threats have become real. Cloud Misconfiguration threats.

4.1 Cloud-Native Threats

Cloud-native threats are action taken by malicious node via "Land" mechanism where attack is done taking into account the vulnerabilities in the cloud deployment by the organizations, without using an malware, Another mechanism is "Expand" where attacking of victim is achieved through the weakly or misconfigured or unprotected interfaces to locate classified and valuable data. Another method of attack is "Exfiltrate" where attack is done at data own storage location and is mostly done with the help of disgruntled employees. This is what is called an 'on-premises' attacks. Other methods by which a victim machine can be compromised is infecting the victim's machine with malware and then infecting in the network. These threats happen due to the prevalence of operating systems with well-documented vulnerabilities. In the cloud, there may not be a Windows, macOS, Linux, or even Android operating system to compromise. Attackers go after errors in configuration of the cloud and use stolen credentials for direct access for further increasing the severity of the cyber attacks [6].

The cloud native threats can be classified in four categories:

1. Delivery and Exploitation is the cloud service is exploited to deliver a malware strain or a phishing page e.g. Abuse Google Apps Script to steal credit cards from websites.
2. Actions on Objective is the cloud service is exploited to steal data, or launch other attacks e.g. ShinyHunters leaks personal information of over 20 million BigBasket user records,
3. Command and Control is the cloud service exploits attack the command and control infrastructure of the organization e.g. 30,000 MacOS endpoints New Silver Sparrow adware targeting Apple M1 Processors Exploited Service: AWS S3, and
4. Data Exfiltration is the cloud service is used as a drop zone for the exfiltrated data e.g. Multiple Targets Cybercriminals Target QuickBooks Databases Exploited service: Google Cloud Storage

Table 1 shows the different categories and percentage of attack. Figure 5 shows the graphical representation.

Table 1 Cloud Native threats and Percentage

Cloud Threat Categories	Percentage
Delivery and Exploitation	52.6
Action on Objectives	26.3
Command and Control	10.5
Delivery and Exploitation/Command and Control	5.3
Data Exfiltration	3.5
Delivery and Exploitation/Action on Objectives	1.8

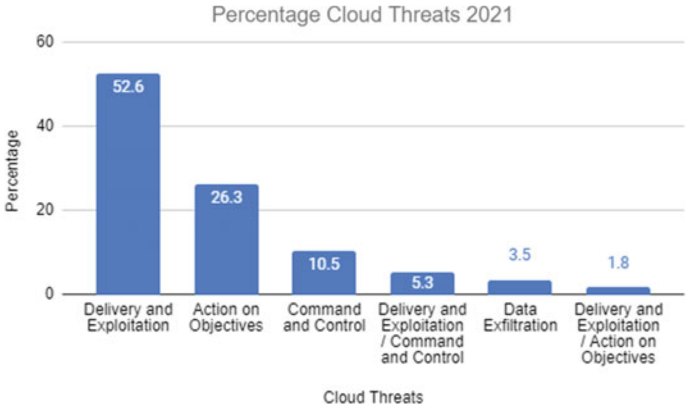

Fig. 5 Cloud threat Exploitation Categories

4.2 *Leaky Buckets: A List of Cloud Misconfiguration Threats*

Companies have been storing various types of data on the cloud, Over the last few years there have been multiple examples of leaky cloud services, exposing million of user records. This has been possible due to the victims are unaware, with can compromise the privacy of, or even lead to different kinds of attacks on the cloud infrastructure. For example two Magecart campaigns carried out compromising the AWS S3 buckets hosting the targeted sites' configuration files. And despite AWS S3 is the most common service to leak data, yet we use it [7, 8]. Figure 6 shows the leaky configurations percentage which leads to threats.

5 Data Breaches in Reported from India

Keeping the above number of threats that are looming above us, The Biggest Data Breaches that was there in India for the last 6 months is shown in Table 2:

The details of some of the major breaches in India in past 6 months:

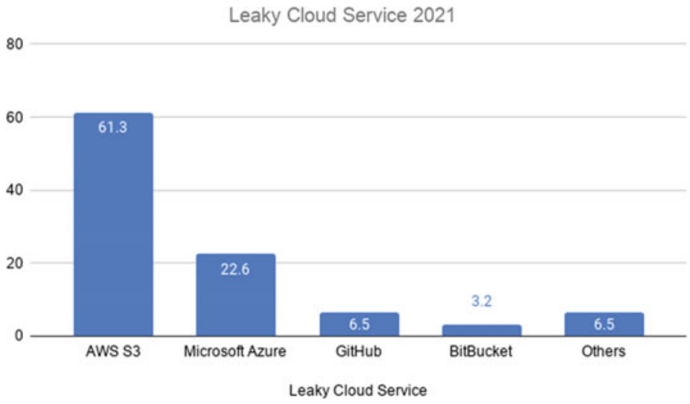

Fig. 6 Leaky Cloud Services

Table 2 Data Breaches from India

Date Reported	Date Discovered	Target	Target Class
25/04/2021	08/11/2020	BigBasket	Wholesale and retail trade
11/04/2021	–	Upstox	Financial and insurance
27/02/2021	Last week of February 2021	Zee5	Information and communication
02/02/2021	–	Airtel	Information and communication
29/01/2021	29/1/2021	(BPSSC)	Public administration and defence, compulsory social security

1. ShinyHunters leaked approximately 20 million BigBasket user records containing personal information and hashed passwords on a popular hacking forum.
2. Indian stock trading firm Upstox (Indian Stock Trading Firm) revealed that they might have given access to millions of customers' personal information due to Misconfiguration in their Server.
3. Zee5, an Indian OTT platform with over 150 million users data due to a security breach 9 million records have been leaked.
4. Personal details of 2.5 million Airtel customers were leaked by a hacker group 'Red Rabbit Team'
5. Database of 500,000 Indian citizens applied for Bihar Police Subordinate Services Commission (BPSSC) exam were discovered by CloudSEK.
6. The data of 35 million users from Juspay goes on sales in the dark web due to Cloud Misconfiguration

It is very clear from the description of the above breaches nothing is safe. In the last 6 months there have been around 46 major breaches, out of which 6 are from India amounting to **13%** of all breaches [9].

6 Conclusions

The 'New Normal' has made us think of security of digital devices that we thought we would never do. People have moved from free anti-virus software to anti-virus from McAfee or Norton for individual machines to security software's for organization. Software Vulnerability auditors are auditing the implementation to make sure it has been done correctly. But the hackers are always in the lookout to find the vulnerabilities. This paper gave a overview of type of vulnerabilities that have attacked the system in the last one and half year. In the interim, 15% may be "rubbed" with total data loss, resulting in a complete system reinstallation. To conclude, 5% of the devices will result in inoperability [10]. According to Data Breach Investigations Report, 60% of ransomware attacks are due to shareware software, which has been common in the new normal.

References

1. https://www.modernhealthcare.com/cybersecurity/hackers-taking-advantage-covid-19-spread-malware
2. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/
3. M. Singh, I. Mukhopadhyay, Cyber Security Issues in the COVID-19 Times. Lecture Notes on Data Engineering and Communications Technologies **62**, 671–680 (2021)
4. Kim Crawley, Cybersecurity budgets explained: how much do companies spend on cybersecurity? May 2020
5. Michael Castellucio, 2020 Major Hacks and Syber Espionage. January 13, 2021
6. What Is a Cloud-Native Breach? mcafee.com/enterprise/en-in/security-awareness/cloud/what-is-cloud-native-breach.html#:~:text=Cloud-native%20breaches%20are%20a,and%20"Exfiltrate"%20that%20data%20to
7. Paolo Passeri, https://www.hackmageddon.com/about/ 2021
8. Top cybersecurity facts, figures and statistics for 2020 by Josh Fruhlinger, March 2020
9. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
10. https://cio.economictimes.indiatimes.com/news/digital-security/cyber-security-amidst-thecovid-19-outbreak/75172086