Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

Cyber Attack-COVID Stress (Cyber Higiene "Wash Your Cyber Data Regularly")

Megha Raghav
Computer Science & Engineering
Swift College
Rajasthan, Bhilwara India

***Abstract*— We will be identifying cyber threats prevailing massively across the country during Pandemic Covid19 era. Aspire to create valuable research on this subject area as this has became the major concern not only if we look towards the current scenerio but affecting many breadwinners in our country struggling for security of their hard earnings throughout.We will have a look upon various security methods used to prevent such crimes spreading at a rapid rate .**

I. INTRODUCTION

Cyber Attack: **An malicious act of intruding inside the computer system of the user and stealing information /data,modifiy the confidential details ,alter , remove them without prior permission of the concerned authroized user ,or using a breached computer as a launch pad for future attacks .**

Types:

1.**Malacious Domains:**

There are several registered Domains on the internet containing terms related to pandemic – "Coronavirus","Corona-Virus","Covid19"and "Covid-19".

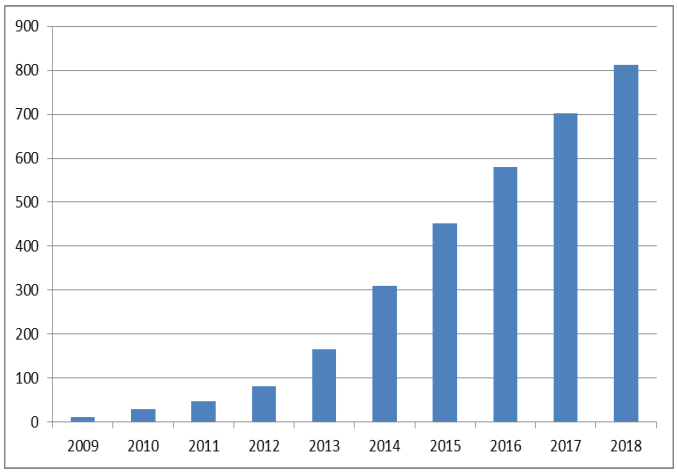
Though some are legitimate websites but still cyber hackers are creating thousands of new websites everyday to do spam phising or to spread malware.

2.Malware Attack:-

A malacious software perform unauthorized actions on the system without prior permission of the user,it is specifically injected into the victim's device .Some of the malware reported :-Bots & Botnets,Trojan Horses,Ransomware,Adware &Scams,Viruses,Worms,Spyware,Spam and phishing.

Year	Malware Infection Rate
	In Million
2009	12.4
2010	29.7
2011	48.17
2012	82.62
2013	165.81
2014	308.96
2015	452.93
2016	580.4
2017	702.06
2018	812.67

Total Malware infection growth Rate(Last 10 years):-



The Most shocking Malware attack occurred in 2020 :-

When on one hand country is devasted with COVID-19 pandemic all around at the same time for multinational corporations,buisnesses have became easy target for online crimes.

Online hackers are gaining access to the system to gain access to your network and developing a malacious software for either stealing sensitive information or causing data breach in the respective system .

The Seyfarth Shaw Malware Attack –one of the recent attack 2020.

It is one of the leading international legal company in Chicago that became victim of malware attack in month of October 2020, it has been later recognized as Ransomware attack .According to the resources of the company it targetted specifically the Email System of the company .

Quick review of the matter and approaching the Law Enforcement on right time the company get rid of this attack at earlier stage .

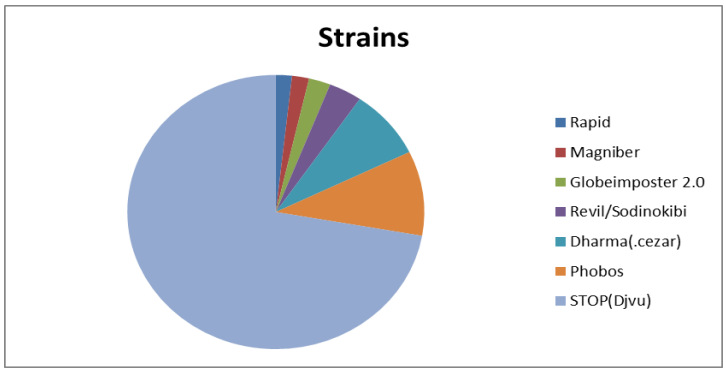
3.Ransomeware attack:-

An basically Bribe Software generally lock your system and demand a ransom for its release.

Firstly try to gain access to the computer system by injecting malware then encode the files or the complete operating system ..

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

Ransomware types	Strains
Rapid	**1.70%**
Magniber	**1.80%**
Globeimposter 2.0	**2.30%**
Revil/Sodinokibi	**3.50%**
Dharma(.cezar)	**8.00%**
Phobos	**9.70%**
STOP(Djvu)	**70.20%**



Most commonly reported ransomware strains of Q1 2020

The Software AG Ransomware Attack

Recently its been noted that the second biggest company in Germany /7th largest in Europe name '**Software AG'** experienced cyber threat in month of october 2020.

The attackers developed Clop ransomware in return demanded 20 million dollar in exchange .

Luckily the services which they are providing their customers remain unaffected .

The Sopra Steria Ransomware attack

The french based IT Company name Sopra Steria became another victim of ransomware attack name '**Ryuk'** after being identified by Sopra Banking software .

Review of Literals

Monthly count for COVID-19 related email threats during year 2020

Total:- 8,091,193

As we can easily see April Month was the peak month for email based COVID19 threats ...

Findings

As per World Health Organization(WHO) :-

They reported that in year 2020 we have fivefold increase in cybercrimes in late APRIL 2020.

"As the first case reported on 30 january 2020 in INDIA originated from China ,WHO has observed rapid increase in the number of cyber hacking , malacious activities informed by staff ,email phising targetting public at larger rate.

Around 450 active WHO email addresses and passwords were leaked online and along with this thousands of related to working on the novel coronavirus .

An old extranet system gets impacted higly as compared to new ones .

Video Conferencing services Breach:-

In between February 2020 and May 2020 about half of million people reported breach of personal data like username, passwords ,email addresses used by video conferencing was stolen and probably sold out on the Dark Web , as most user uses same username/password combinations from multiple accounts.

Analysis

One of the Common reasons I find out to be spike in cyber attack during COVID19 outbreak is Using your own devices approach(UOD) by corporate environment which means employees can use their own devices (phones, tablets,laptops)to access secured corporate information .

Home Wifi are a bit easy target ,person may have not installed Anti-virus /Anti –Malware Scan regularly ,home network does not have sufficient preventive measures to work upon .

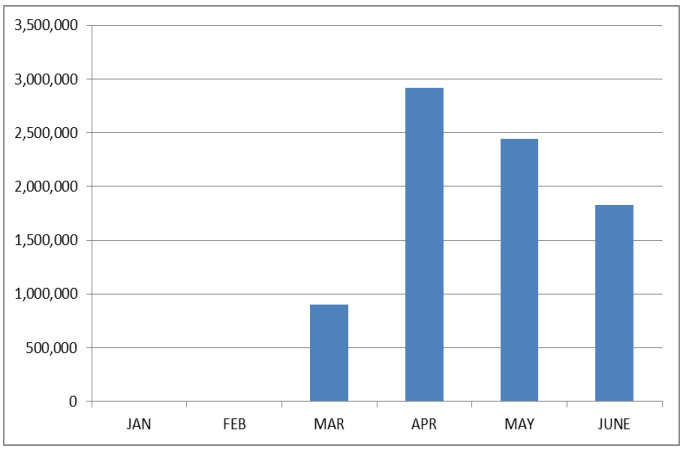
Human Error is one of my biggest concern also as prior to pandemic also we were facing several issues related to "Cyber insecurity" like ATM Skimming TRAP ,spam email response victim,sharing financial details on phone etc.

Discussion

Each and every person should be vigilant while talking to their family including childrens about how to properly operate net devices and e commerce websites .

We should regularly check our privacy and security settings of our phone ,laptop majorly using these days.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021



Monthly count for COVID-19 related email threats
During year 2020

Password need to be strong (mix of Uppercase,lowercase,numbers and special characters) always whether its your home Wifi password or laptop ,phone ..etc

Avoid clicking on links /open attachements in emails which is not of your knowledge or from an unknown sender .

'A Good Cyber Hygeine is Always Wash Your Cyber Data'

After completing work always ensure to wash all data shared ,saved (Do not save).

With the increase in development of modern technology all around bring countless advantages to millions of people sitting in their home availing the facilities effectively ,on the other side brings disadvantages too ,the best thing we can do for our company is to priotrising your safety and relying on cyber threat intelligence for proper protection .

Adhere to Cyber Hygeine Policy as you are protecting yourself from corona virus similarly:-

1.Regular Passoword Change .

2.Update your software you use ,getting better versions should be your regular hygeine review .

3.Hardwares(Old Computer ,smartphones needs to be updated inorder to maintain performance and prevent issues.

4.Limit your users :-Especially for MNCs limit access to admin –level only inorder to access programs .

5.Back up data regularly on some secondary sources(hard drive,cloud storage ensuring safety in times of breach or malfunctioning.

6.Develop a Cyber Security Framework (NIST Framework)to ensure security.

Once the policy is created routine need to be ensured for example after every 20 days changing passwords or check for updated atleast one per week .

Limitations

Employees working from Home during this outbreak in completely digitized world now ,so they must be using their own personal devices and even those using a corporate owned device should follow certain mandatory protocols :-

1.**Antivirus Protection:-**

All employees/ working professional from home should be equipped with a license of Antivirus and malware software while using their own personal devices .

2.**Cyber Awareness Programs needs to be initiated online to each employee (Trainee/Experienced staff):-**

Training part should start cyber awareness programs assessments by defining procedures of sending emails ,login information,not to reveal credential informations on video/audio conferences ,regulating them to use files and folders or any content to personal email addresses/cloud storage.

3.**Home Wifi Protection –**

Employee must ensure their home Wifi network is secured with a strong password protection especially .

.

4.**Regular weekly review sessions:-**

Weekends should only be having cyber security awareness tips sessions to all working staff working from their Home Network.

5.**CISCO devices should not be trusted as this may have Access granted fault error .**

6.Encoded voice software can be installed :-

Software encoding voice sessions by respective software so that only the authorized team discussing work can understand each other .

7.**Self Prepared for Illegal Intrusions,Data Leaking activities** :-

Organisations should ensure some simulation exercises programs to be alert of how to act /steps to be taken at random ,once get attacked by cyber criminals .

NOTE:-8. Application Download Avoidance:-

Apps such as measuring your BP/Antibodies test /**Sugar/OXYGEN COUNT level check** should never be used as hackers are creating such apps to engage.

ACKNOWLEDGMENT

The COVID-19 pandemic has given golden opportunity to various cyber criminals despite of having that before pandemic.

In addition to this rate of unemployment has also increased at rapid rate as most of the people half of the population is sitting at home and working on their respective systems/devices not much focussed on results of cyber interactions via Video conferencings apps like ZOOM ,Google Meet applications sharing sensitive data of companies .

Distraction among the minds of people these days due to pandemic stress stops them of thinking towards cyber concerns on regular basis their "Work needs to be

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

completed as targetted for the day that's it" this has became the major priority resulting in sharing data openly via emails etc.

In this Paper I tried highlighting all the aspects prevailing during COVID-19 period in a summarized way which needs to be looked upon seriously at present for secure future of youths.

My short research provides opportunity for further research related to POST COVID-19 situations facts and analysis to be considered .

REFERENCES

[1] https://www.google.com/search?q=ransomware+attack+percentage+in+2020&source=lmns&hl=en&sa=X&ved=2ahUKEwibnNn6yYPxAhVFhP0HHfbuBe4Q_AUoAHoECAEQAA.
[2] https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-#:~:text=The%20line%20between%20ransomware%20attacks,non%2Dpaying%20victims%2C%20according%20to.
[3] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
[4] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.
[5] https://fraudwatchinternational.com/all/the-most-shocking-malware-attacks-that-happened-in-2020/