Impact Of COVID-19 On Cyber World

written by Mirza Aslam Beg | April 15, 2020

The Unforeseen Effect of COVID On Cyber Sector - The Outline

At the time of writing this article, almost 210 countries and territories around the world have reported approximately 16,50,000 COVID-19 positive cases and the death toll has also touched the figure of one lakh. Various international medical & research organizations and governments that used to claim to have the world's best medical facilities are helplessly looking for solutions to control this global pandemic.

As of now, the only effective remedy to control the pandemic is a complete worldwide lockdown. Almost all affected countries are undergoing a lockdown. Therefore, most companies/firms/financial institutes are compelled to allow their employees to “work from home” for maintaining business continuity. Many business-related activities have been shifted to the internet, ranging from online meetings, online coordination with clients and customers, financing, email, WhatsApp communication, etc.

Due to the ramifications of work from home, proprietary data of large and small organisations is being accessed from laptops and home PCs that are not equipped with the latest security updates and the same level of firewall and security as in office setups. It has been observed that the home Wi-Fi systems of employees have a very low level of security standard and the same is an open invitation to the Cyber Hackers to get access to the laptop & home PCs and the data stored in it.

On the other end, Cyber Hackers are already knocking on virtual gateways, looking for a new entry point to access the personal details. I believe this is exactly the time when Cyber Hackers get creative with their malafide intentions of hacking the devices and stealing data and confidential personal details.

A rise in the registration of fake domains and cyber-attack

In the last three months, almost 51,000 coronavirus-related domains have been registered among which 30,000 new coronavirus-related domains were registered only in the last month of March, out of which 0.4 percent i.e. 131 were identified as malicious and 9% i.e. 2,777 are suspicious and same are under investigation. The below graph is clearly reflecting the sharp increase in coronavirus domains registration:

Lt. Gen. Rajesh Pant who is associated with India’s National Cyber Security Coordinator has reported that almost 4,000 fraud portals related

to coronavirus have been registered globally by the Cyber Criminals in the last two months only.

Since mid-February, an escalation in the number of coronavirus-related cyber-attacks is being noticed and in the last 20 days, the number of cyber-attack has increased drastically from a few hundred to as high as over 5,000 on 28th March 2020. The below graph is clearly reflecting the escalation in the number of coronavirus cyber-attack.

It is also identified in a study that the video meeting application zoom which is widely being used nowadays is vulnerable and employees who are using zoom may be targeted by the Cyber Hackers easily, therefore, experts are advising to either use the alternate video meeting application or use the zoom application in a browser.

Similarly, in the last few weeks, some business email interruption frauds have come to notice where Office 365 or Gmail accounts are being hacked through a phishing email. Thereafter, hackers send fraudulent invoice emails purporting to be from legitimate vendors and claiming that the business's banking details have changed for transferring the money to the hacker’s account.

Cyber Hackers are easily getting access to the systems [laptops and personal PCs] which are not equipped with the security software and the latest firewall or are not being operated in cyber hygienic conditions. Thereafter, Cyber Hackers demand the ransom to release the sensitive data of the organisations. If the ransom is denied, paying the ransom, they may sell the data, and in addition to that, may notify the customers/clients of the Enterprises/Companies that their data has been compromised.

How to stay safe from Cyberattacks?

- The employers need to prepare the employees who are unaccustomed to remote working which can be done through online training to teach the employees how to identify and avoid the risk, and also suggest to them the procedures to follow in case of any threat of cyberattack for stealing the login credentials or sensitive data.
- In order to reduce the risk of cyberattacks or to protect sensitive data, the access of sensitive systems and data should be given to the concerned employee and team only.
- Companies should provide the laptop to their employee, which is installed with VPN software and endpoint threat prevention. Use of personal devices [laptop or PCs] to access the data during work from home increases the risk and vulnerability and makes it easily accessible to the cyber hackers. In addition, the software powering the personal devices can be months or even years out of date.
- Employees must be adequately educated about phishing emails, and the risks related to spam. They must be asked to ensure that the programs or applications they install are the original versions from a trusted source.
- Employees should be made cautious to look for misspellings in URLs of the websites and always try to learn how fake websites are used to lure people into sharing their personal information. All the latest security patches and updates must be installed on devices to avoid any risk of the loss of data and unauthorized access and control of the system.
- There must be a long, complex router password for home Wi-Fi and system firewalls should be active on the Wi-Fi router. Also, reusing the passwords

across the web should be avoided.

- Companies must have an alternate way to contact their employees like secure texting applications "Signal", which should be outside of company systems. In case, a company falls victim to a cyber-attack, it would still be able to communicate with its employees.

Conclusion

There is a big issue of jurisdiction in the era of the internet and the medium of the internet does not recognize the sovereignty and territorial limitations. It is always difficult to send a cybercriminal behind the bars, who is sitting across the border and territorial jurisdiction of the state because of a lack of uniform international jurisdictional law. It is believed that cybercriminals are 10 steps ahead in cyber technology from law enforcement agencies and India IT Act 2000, which was last amended in 2008, does not have clarity on some new and technical aspects of cybercrime. Therefore, it is advisable that prevention is the best cure rather than investigation and subsequent prosecution of offences.

Contributed By - Mirza Aslam Beg
Designation - Partner
King Stubb & Kasiva,
Advocates & Attorneys
Click Here to Get in Touch
New Delhi | Mumbai | Bangalore | Chennai | Hyderabad | Kochi
Tel: +91 11 41032969 | Email: info@ksandk.com