Printed from
THE TIMES OF INDIA

As more people work from home, cases of cyber attacks rise

TNN | Apr 10, 2020, 02.34 AM IST

NEW DELHI: A senior corporate executive was on a video conference call with his top management using the popular Zoom app while working from home due to the coronavirus lockdown. Minutes after the meeting started, the screen was hacked, and pornographic content started playing across the screens of those who were on the call, prompting them to abruptly terminate the call.

Coronavirus outbreak: Live updates

Similarly, as PM Narendra Modi sought donations under the PM-CARES fund, more than a dozen similar-sounding UPI IDs cropped up, luring people to donate there. The fake IDs included pmcares@pnb, pmcares@hdfcbank, pmcare@yesbank, pmcare@ybl, pmcare@upi, pmcare@sbi and pmcare@icici. The issue was sorted out, but not before the intervention of the home ministry, CERT-in — the country's security watchdog, and private experts.

HACKING BIDS

- After PM-CARES fund was set up, several **similar-sounding fake UPI IDs** came up

- Several messages & websites are promising to inform about those infected 'near your location', or provide 'Covid-19 heatmaps'. Many promise to help one avail of unemployment funds. Most of these end up **hacking smartphones & laptops**

This is not all. Messages and websites are coming up by the dozens, promising to inform people about those suffering from coronavirus “near your location”, or providing “Covid-19 heatmaps”. Also, many are promising to help one avail unemployment funds. Sent from seemingly authorised sources, most of these fakes end up hacking, and even taking control of, smartphones and laptops that download them, leading to cyberattacks.

Home networks very vulnerable to cyberattacks

As people work from home during the lockdown, cases of cyberattacks, hacking and even ransomware have been on the rise, posing a serious challenge to the new economic realities where digital networks are increasingly fuelling GDP, businesses, government machinery, and even school & college classes.

Against the relatively secured networks at offices and workplaces, home networks are highly vulnerable, especially when many teammates are logging in through their personal devices under “bring your own device (BYOD)” practices.

“With most of the companies not having systems and protocols to work remotely, hackers and malware makers are having a field day,” says Gowree Gokhale, a partner at law firm Nishith Desai Associates, which has been advising firms on how to work securely, and what precautions they need to undertake to stay safe.

Shree Parthasarathy, the leader of Cyber Risk Services at Deloitte South Asia, says that against an average of 25,000-30,000 cases of spam emails that were originating in Europe and North America in a fortnight, the spam sent between March 13 and March 26 was as high as 4 lakh.

“BYOD is increasingly turning into Bring Your Own Disaster. If I look at the Indian market, some of the most targeted categories that we found were life sciences and healthcare companies, manufacturing sector, and financial services. These are being hunted to steal patents, processes, passwords, and other critical information.”

It is estimated that nearly 60% of the global workforce is working from home and remote locations.

GV Anand Bhushan, partner at leading law firm Shardul Amarchand Mangaldas, says that enterprises cannot afford to have a lackadaisical attitude at this point in time. “Apart from external attacks, there are also instances where employees may also be violating the privacy codes as they start using their own devices. For example, when using personal devices to access company networks, people may be engaging in sharing of passwords across project teams; or making backups in violation of client contracts.”

Prashant Choudhary, partner for risk advisory services at Ernst & Young, says “multiple vulnerabilities” have been detected in companies where employees are using personal devices. “Companies may be advising employees to install anti- virus and anti-malware. But does the employee want to spend for that, or does s/he understand its importance, or can s/he manage the installation process?”

Also, Choudhary says that many of the proprietary company applications that are being offered to employees to access from home were not originally designed for the internet. “Many of them never had security features. They were for internal intra-net corporate purpose.”

The experts also said that there have been cases on Zoom app where hackers have not only gained entry into private meetings, but have also recorded personal conversations as well as the information being shared on the screens. “There had been issues around data breach with Zoom where malicious hackers had even taken the recordings of the meetings, and these were made available over the internet,” Ernst & Young’s Choudhary says, hinting that corporate espionage may also be carried out in such nefarious activities.

Most of the experts were of the unanimous opinion that an individual or a corporate, whose computer or organisation was compromised, should “immediately inform their internal IT teams as well as the government’s cyber security department.”

Supratim Chakraborty, a partner at Khaitan & Co, says that instead of sharing screens to discuss sensitive work, companies and employees should use official emails for critical matters. “We have become quite vulnerable, both enterprises and individuals. Hackers and fraudsters are hyper active and sensitisation is the only recourse.”

Shivpriya Nanda, partner at law firm J Sagar Associates, says that while laws are there to take action against data thefts and cyber frauds, the penalties may not be commensurate to the scale of crimes. “The new data protection law is yet to become a reality.”