Na Vijayashankar

Chinese Checkers

Even as the CERT-In Advisory warns of a cyber attack through a massive phishing exercise, the fact is that our neighbour has penetrated the entire Indian IT environment and a "cyber nuclear attack" is a possibility

Amitava Sen

AS the country grapples with border clashes with China, Indian IT users have been given a notice by the Computer Emergency Response Team (CERT-In) of a possible cyber war attack.

CERT-In is a quasi-judicial authority having enormous powers under the Information Technology Act, 2000. It is perhaps time for it to realise its powers as well as responsibilities and grow beyond issuing advisories to initiating specific actions to secure Cyber India.

The notification of June 21, 2020, for the first time named China for planning a cyber attack through a massive phishing exercise under the guise of Covid-related information. CERT-In even identified one of the e-mail addresses that may be used—*ncov2019@gov.in*—for sending such phishing mails. It is expected that several government identities may be used to send phishing e-mails which may contain malicious virus attachments that can plant Trojans, key loggers or even launch a ransomware attack. The advisory suggests the usual precautionary measures that need to be taken.

It is well-known for quite some time that China has been building its cyber

war capabilities not only against large countries such as Russia and the US but India too which is its traditional enemy. Though experts have warned the government for a long time, its advisers have ignored the warnings that China has been penetrating the Indian systems by various means and keeping in readiness for any attack.

Technically, Chinese companies such as Huawei as well as others have taken a firm grip over the Indian telecom network system. Today, almost all network routers in the country and all telecom operators in the country use telecom equipment supplied from China. These are known to come with backdoors that steal data.

In the past, Chinese credit card swiping machines have been found to be embedded with additional chips. It is referred to as the Manchurian Chip Attack in cyber crime circles and it sends copies of data to China. Scotland Yard reportedly discovered this in the UK and identified such rogue POS machines by weighing them.

Even in India, the telecom industry had raised a flag and at one point of time, a system for "Certifying Telecom Equipment" was suggested. Those were the days of Chinese friendship and India constituted a committee for such certification with some known experts. The purpose of the committee was defeated the very moment Huawei was to fund the project, indicating the complete absence of security by the expert committee. The committee is now defunct, though some of its members are still active in the design of a cyber security framework in India.

A few years back, there was even a suspicion that the Chinese could have planted bugs in CERT-In. The issue was not made public in view of the national interest. The Chinese had even planted their nationals in some organisations and one of the Indian companies handling a project for World Bank found that data was being diverted to China and attributed it to some malicious Chinese employees.

Chinese companies such as Huawei and others have a firm grip over the Indian telecom network system. Almost all telecom operators in the country use equipment supplied from China.

Many Indian companies in the IT sector have been funded by Chinese agencies and they have access to the systems and are fully aware of the technical architecture of the companies. It is no surprise that some of these companies are getting attacked today with ransomware.

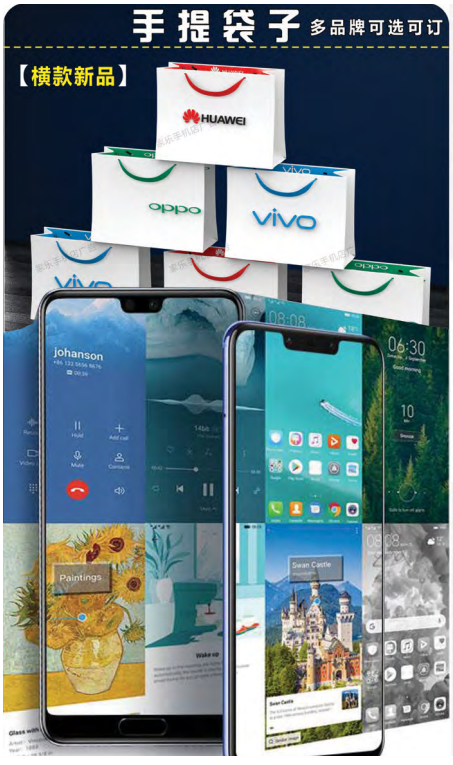
China even has good control over crypto-currency holdings and has mined and reserved a large stock of Bitcoins which could be unleashed as a weapon in India if the government allows them to be legitimised. Chinese manufacturers of mobiles and laptops have long been suspected to have planted malicious codes to steal data and even take over control of the devices through a secret switch.

Indian software companies have transferred valuable technology to China by opening offices in that country and employing the Chinese workforce. These companies have sold the interests of India for a few dollars and it allegedly includes all big IT companies.

Thus, China has systematically penetrated the entire Indian IT environment and is suspected to have a much larger control on the Indian network than a "phishing attack". At best, a phishing attack may only be a "diversion" and a major attack like a "cyber nuclear attack" is a possibility. Unfortunately, CERT-In has not been vocal about such threats. Its advisory that phishing will increase is welcome but falls woefully short of expectations of the security market.

What we need now is an advisory to telecom companies to identify their reliance on Chinese equipment and do a source code audit on all software and hardware supplies from China. We need to filter all IP addresses leading to China and authenticate the destination.

We must note that Russia has set up a completely isolated internet network ▶



Gird up for cyber attacks

Taking advantage of Covid-19, cyber criminals have been regularly launching new attacks. There have already been successful phishing attacks and users' data and login credentials being compromised. These criminals have also successfully distributed malware, Trojans and back-door entry for larger attacks, leading to ransomware.

To combat these threats, organisations have not only made required changes in the way they work, but also taken due precautions and measures. This may have helped them manage the initial phase of the crisis. But unfortunately, this is a prime time for cyber criminals and fraudsters to thrive and launch newer attacks and people must stay continuously vigilant.

The major impact areas have been– proliferation of fraudulent domains, newer mode of transaction and collaboration, privacy and security of data. Another critical threat is from human-related threats—remote work force in an insecure and uncontrolled working environment. So the tough times are not over yet.

Newer fraudulent domains are getting registered in unimaginable numbers to take advantage of the pandemic situation. Post-lockdown, the unprecedented increase in online shopping and deliveries, digital and contactless payments, remote working, distance learning, tele-health, online entertainment and use of IOT and drones are a clear indication that digital transformation is happening fast. Along with it, there are more threats necessitating the need for robust security processes and measures.

Remote work fundamentally changes the dynamics, especially for teams habituated to working together in a controlled and monitored environment. Unexpected changes can seed and drive new security risks. In contrast, cyber security has always been working to embrace zero trust. This is centred on the belief that users should not automatically trust anything inside or outside the trusted perimeter and instead, verify everything that is trying to connect to the organisation.

Further, most organisations have been forced to allow employees to work from home. In fact, some have modified their policy around safe/secure remote/home working and even adopted new technology to take care of privacy concerns. But some bypassed these protocols and many are wondering what

and exercises a far greater control on information flow out of the country. We in India need to move in this direction and create a nationwide information gateway infrastructure so that any data moving out can be monitored so that one knows its final destination.

While this may entail a privacy threat, it is a national security requirement. Just as we cannot allow free movement of people across the borders from Pakistan or China, we need to be able to monitor data traffic from India to China and vice-versa. We may, therefore, consider that the CERT-In advisory is only the bare minimum and has to be supplemented with more security vision.

CERT-In also came up with an advisory—"Zoom is a Security Threat". It ignored the fact that Zoom was a US company and not a Chinese one. It appears that the advisory was released to indirectly benefit some of the business competitors of Zoom. These include MNCs who have their own lobbying power with the decision-makers.

Given the expertise of China in espionage capabilities, the possibility of the Chinese penetrating the government machinery also cannot be ruled out. If part of our political leadership can be seen as openly supporting China, the possibility of some bureaucrats having a soft corner for the country cannot be ruled out. The government has to, therefore, start an operation to clean up its internal systems and people to identify the dependence of our systems on China. Any laptop or mobile with Chinese origin used by government employees, including secretaries, needs to be checked.

Despite the anti-China sentiments, it was recently reported that the sale of a new model of mobile from a Chinese manufacturer was sold out in a few hours, indicating that the penetration of Chinese IT equipment is continuing. Whenever such sales take place, apart from prior licence to sell, the government has to acquire a few random samples of the items being sold and subject them to a

to do. And very few have adequate insurance cover to take care of any resultant penalties.

The current situation is such that just reviewing the key controls is not sufficient. Instead, there is a need for a different level of preparedness to address these increased attacks. There is a need for re-calibrating hygiene requirements, with more investment in automation and orchestration. One needs to have a new value chain for security which requires adoption of newer technology such as AI/ML, blockchain, embedded security, zero-trust, threat intelligence, digital identity, etc. There is also a requirement for more cloud adaptation, with improved response and re-mediation through API-driven automation and actionable intelligence.

Threat hunting also requires a new approach and AI-based threat management. With these technological advancements and innovations along with the proliferation of cloud, pay per use model and outcome-based services are pushing growth in threat monitoring and management.

So, businesses are transforming to the no-touch model and technology to the "anywhere, anytime" working model. While these threats continue to appear, it has become important for organisations to take these security concerns head-on. They should review their business contingency and crisis management plans to effectively include and prioritise protecting remote workforces from attacks.

In effect, the future of crisis and crisis management has already arrived. The current crisis has given us an opportunity to change not only the state of preparedness, but also our mindsets. The crisis will be more complex and harder to contain. Quite contrary to what we have been seeing for decades, most of the crises stem from day-to-day operations, disruption, supply chain, product failure, technology failure, etc. But today, cyber crime constitutes one of the biggest causes of modern-age crisis. This seems natural with the increasing dependency on technology and its availability. In future, stakeholders will demand hyper-transparency and expect swifter reaction to crisis triggers.

—By Rajesh Kumar, Director, Cybersecurity, Netrika Consulting India Pvt. Ltd.

INCREASING DIGITALISATION
Apps like Zoom have gained popularity with more and more people working from home

security scrutiny.

When we introduce such tough measures, there could be charges of violation of free trade principles. This should not be applicable in the current war-like situation.

Recently, CERT-In came up with an unwarranted advisory on Zoom. But it did not find it necessary to come up with an advisory on the following:

- "Chinese mobiles" using their own OS systems and pre-installed apps
- "Chinese made laptops" where the OS and pre-installed apps could have been tampered with
- POS machines used universally for card payments and biometrics which may steal critical data
- Internet routers and set-top boxes which can be used to control communication channels to ordinary citizens, including the possibility of a denial of service attack across the country.

This needs to be corrected. If China has access to computers and mobiles sold in India, they do not need a cyber attack through phishing which any script kiddie can do.

Now that CERT-In has come up with this public announcement on China, we must move this intelligence finding to its logical end. Such an activity falls under Section 66F of the Information Technology Act and can be considered as "Cyber Terrorism". CERT-In indirectly declared China as a "rogue nation" indulging in cyber terrorism and cyber warfare. Hence, there is no reason why international trade agreements for free trade are to be considered as not applicable in the current situation.

It is time that the CERT-In goes beyond issuing advisories and initiates concrete action to assess and mitigate the China risk in Indian IT infrastructure. ■

—The writer is a cyber law and techno-legal information security consultant based in Bengaluru