Source : www.thehindu.com Date : 2021-03-15

FORESTALLING A CYBER PEARL HARBOUR

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

The threat posed to key Indian entities by antagonistic forces such as China is beginning to merit critical attention in all the right quarters. This follows revelations by the U.S.-based cyber security firm, Recorded Future, which were carried by the media in the United States.

According to a despatch by *The New York Times*, in the lead-up to the India-China border clashes, Recorded Future had found an increase in malware attacks targeting the Indian government, defence organisations and the public sector. Also that, coinciding with Chinese incursions in Eastern Ladakh, certain Indian power facilities had been targets of a cyber attack. Furthermore, that there was still some evidence of ongoing intrusions, though the intensity of the activity appeared to have ceased by mid-February 2021.

Explained | Red Echo, ShadowPad, and the targeting of India's power grid

A needless controversy did erupt in the wake of these disclosures, as to whether the October 2020 blackout in Mumbai was directly linked to this cyber attack. State authorities in Maharashtra attributed the blackout to the attack by the Chinese cyber group, but authorities in Delhi blamed it on human error. Far more crucial than merely assigning blame, and what should have been of real concern, is that key infrastructure facilities, such as the power sector, were now in the crosshairs of a hostile China, which appeared intent on deploying cyber weapons to target India. China's intention evidently is to keep India in thrall, while outwardly demonstrating a conciliatory posture, such as vacating some of the areas in Eastern Ladakh that it had occupied post April 2020.

The reported events are a wake-up call for India, and it would be a grievous error if India were to underestimate the extent of the cyber threat posed to it by China. Indian government agencies, such as the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In) may have more information on China's aggressive cyber campaign, but if what Recorded Future has indicated is true, *viz.*, 'that since early 2020, there has been an observation of a large increase in suspected targeted intrusion activity against Indian organisations from Chinese state-sponsored groups' concentrating on infrastructure targets, including the power sector and ports, then India needs to be on its guard.

At least 10 Indian distinct power sector organisations are said to have been targeted, in addition to two Indian ports. What adds verisimilitude to these revelations is the identification of the network infrastructure *viz.*, AXIOMATICASYMPTOTE, whose servers are known to be used by RedEcho, a China-linked activity group, that targets India's power sector, and facilitates the employment of a malware known as ShadowPad. ShadowPad is a network intrusion malware affiliated to both the Chinese Ministry of State Security and the People's Liberation Army. ShadowPad is depicted as a "back-door 'Trojan' malware which creates a secret path from a targeted system to a command and control server to extract information". If indeed the future is digital, and if China has indeed embarked on an all-out offensive of this nature, India needs to adopt comprehensive measures to forestall a potential 'Cyber Pearl Harbour', as far as India is concerned.

Also read | Chinese cyber attack foiled: Power Ministry

Across the world, Beijing does appear to be engaged in a major cyber offensive, directed not only against countries like India but against many advanced nations as well. In attempting this,

what China is doing is essentially exploiting to perfection the many vulnerabilities that software companies (essentially those in the West), have deliberately left open (for offensive purposes at an opportune time). Exploiting this loophole, and also turning matters on its head, it is companies in the western world that are now at the receiving end of such antics, having ‘left vulnerabilities for future exploitation’.

Chinese cyber espionage sets no limitations on targets. Towards the end of 2020, and as the world prepared for large-scale deployment of COVID-19 vaccines, their attention was directed to vaccine distribution supply chains around the world. A global ‘spearphishing campaign’ targeting organisations responsible for vaccine storage and transportation was reportedly unleashed, and while concrete evidence as to which country was indeed responsible for this is not available, the shadow of suspicion has fallen mainly on Chinese hackers. Their objective seems to have been targeting vaccine research, gaining future access to corporate networks, and seeking sensitive information relating to COVID-19 vaccine distribution.

Comment | Patching the gaps in India’s cybersecurity

Very recently in 2021, several thousands of U.S. organisations were hacked in an unusually aggressive Chinese espionage campaign. The Chinese group, Hafnium, which has been identified as being responsible for this breach, exploited a series of flaws in the Microsoft software, enabling attackers to gain total remote control over affected systems. Each hour of the day, thousands of Microsoft servers were compromised as a result, till the breach was discovered.

While Chinese cyber espionage may be the flavour of the month, what must be recognised is that many other countries, including the U.S. and Russia, do engage in the same kind of cyber warfare. Little is publicised about western cyber espionage, and while these may not match that of either China or Russia, it does happen. The U.S. has extensively publicised Russia’s cyber antics from time to time. Best known are accusations of Russia’s cyber interference in the U.S. presidential elections in 2016, which approached the level of a major scandal. Russia is currently the prime suspect in one of the greatest data breaches concerning the U.S. Federal government, involving the Departments of Defence, Energy, State, Homeland Security, Treasury, etc. Headlined SolarWinds, the late 2020 breach is a prime example of the damage that can be caused by a cyber attack.

Also read | Only 20% of Indians are not confident in their ability to prevent a cyber attack

Cyber attacks and cyber espionage could rewrite the history of our times. We are witnessing only the tip of the iceberg at present and most nations are truly unaware of the extent to which breaches are taking place. Nations should beware and be warned about how cyber attacks can bring a nation to its knees. This was well demonstrated way back in 2016, when a major attack on Ukraine’s power grid took place and set an ominous precedent in this respect. The attacks were carried out by skilled cyber security professionals, who had planned their assaults over many months, testing the quality of the malware, carrying out detailed logistics planning, and conducting a very sophisticated operation. The Ukraine example should be a wake-up call for India and the world, as in the intervening five years, the sophistication of cyber attacks and the kind of malware available have become more advanced. India, could well be blindsided by Chinese cyber attacks on critical infrastructure if the latter sets out to do so, unless prophylactic measures are taken in time.

There are no readymade solutions to counter the cyber offensive emanating from different quarters. No nation can hope, or can claim, to be insulated from such attacks. The U.S. seemed to fully wake up to the cyber threat only in 2017 when U.S. security tools were hacked, having

preferred for long to indulge in a kind of ‘active defence’ by seeking to hack enemy networks. U.S. President Joe Biden is now understood to have included a sum of over $10 billion for cyber security in his COVID-19 Relief Bill, which is clearly intended to improve U.S. ‘readiness and resilience in cyber space’.

Also read | Over 2.9 lakh cyber security incidents related to digital banking reported in 2020, Rajya Sabha told

From an Indian perspective, the Chinese cyber threat could prove to be truly daunting. The reasons for this are many. China’s analysis of the state of current relations between China and India is that they remain antagonistic to the point of ‘de-coupling’, and the confrontation between Chinese President Xi Jinping’s ‘Community with shared future for mankind’ and India’s current posture could lead to a ‘long period of volatility’. As India grows closer to the U.S., this gap between the two key Asian nations can be expected to become still wider.

Under Mr. Xi, China has forged a firm nexus between authoritarianism, global ambitions and technology, and is determined to transform the global order to advance its interests. ‘Cyber’ could well be one of China’s main threat vectors employed against countries that do not fall in line with China’s world view. China’s 2021 Defence Budget (amounting to $209 billion) gives special weightage to the Strategic Support Force (SSF), which embraces cyber warfare — an ominous portent that bodes little good for countries that posit a challenge to China’s ambitions, such as India. Drawing up a comprehensive cyber strategy, one that fully acknowledges the extent of the cyber threat from China, has thus become an imperative and immediate necessity.

M.K. Narayanan, a former National Security Adviser and a former Governor of West Bengal, is currently Executive Chairman of CyQureX Pvt. Ltd., a U.K.-U.S.A. cyber security joint venture

a request for those who can afford to subscribe: please do. As we fight disinformation and misinformation, and keep apace with the happenings, we need to commit greater resources to news gathering operations. We promise to deliver quality journalism that stays away from vested interest and political propaganda.

Dear subscriber,

Thank you!

Your support for our journalism is invaluable. It's a support for truth and fairness in journalism. It has helped us keep apace with events and happenings.

The Hindu has always stood for journalism that is in the public interest. At this difficult time, it becomes even more important that we have access to information that has a bearing on our health and well-being, our lives, and livelihoods. As a subscriber, you are not only a beneficiary of our work but also its enabler.

We also reiterate here the promise that our team of reporters, copy editors, fact-checkers, designers, and photographers will deliver quality journalism that stays away from vested interest and political propaganda.

Suresh Nambath

Please enter a valid email address.

You can support quality journalism by turning off ad blocker or purchase a subscription for unlimited access to The Hindu.

Sign up for a 30 day free trial.

END