MANOHAR PARRIKAR

idsa

MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

March 2021

- Indian Critical infrastructure networks penetrated
- Hackers try to poison drinking water in Florida City
- Government to update policy on cryptocurrencies
- China blocks access to social media app Clubhouse
- RBI takes measures following Juspay data breach
- U.S. semiconductor industry calls for government support
- Government notifies rules for intermediaries
- SWIFT sets up JV with China's central bank

Prepared by: Ms. Debopama Bhattacharya

Indian Critical infrastructure networks penetrated

The New York Times reported that a US cybersecurity company, Recorded Futures, had issued a detailed report showing the presence of malware of Chinese origin in various parts of the National Electricity Grid and seaports.[1] The penetration was observed over a period of time and the Indian authorities had been informed after which they took action to remove the malware and shut down communication paths between the malware and its Command and Control servers located in China. In a statement, the Power ministry also confirmed that it had been intimated of these threats by the Computer Emergency Response Team- (India) (CERT-in) and the National Critical Information Infrastructure Protection Centre (NCIIPC). It listed a number of actions it had taken in response, including blocking of IPs and domains.[2] The New York Times report had gone further and speculated that a major power outage in October 2020 could have been the result of this malware but the Ministry reiterated that the functioning of the power grid had not been affected by the malware which had since been removed.

As the recent Solarwinds breach in the US shows, such breaches are not unique to India. The Power Ministry has also been upfront in confirming that a state-sponsored non-state actor was behind the breach and that it was under investigation. Any report on the investigation, or relevant parts, should be made public not only to name and shame the perpetrators, but also to facilitate the sharing of lessons learnt from the episode amongst all stakeholders.

Hackers try to poison drinking water in Florida City

An attempt was made to tamper the chemical levels in the drinking water supply of Florida City in the US on February 5th by hacking the control system of a water treatment plant.[3] The hacker tried to tamper with the levels of sodium hydroxide, also known as Lye, which is used to treat water acidity, from 100 parts per million to a dangerous level of 11,100 parts per million.

The hacker had gained unauthorized entry to the system controlling the water treatment plant using a remote access program. This was detected by a supervisor monitoring the computer system who saw sudden changes in his computer window. The intruder was active for three to five minutes. The levels of Lye were reversed as soon the hack was detected, averting a crisis.

Responding to this incident, Microsoft and other industry professionals have strongly recommend upgrading computer systems, especially in critical infrastructures to an actively supported operating system in order to avoid easy remote accessibility. The water treatment plant was using an outdated Windows 7 which is more susceptible to exploitation since Microsoft no longer supports it with security updates.[4]

Government to update policy on cryptocurrencies

The government of India plans to introduce a bill to regulate cryptocurrencies in the country. The bill named ‘Cryptocurrency and Regulation of Official Digital Currency Bill’ aims to create a framework for the creation of an official digital currency in the country and impose a ban on private cryptocurrencies.[5]

A high-level Inter-Ministerial Committee (IMC) was constituted under the Chairmanship of Secretary, Economic Affairs to study the issues related to cryptocurrencies and propose necessary actions that need to be taken with respect to private cryptocurrencies. It has come out with a report, in which it stated that all private cryptocurrencies, except virtual currencies issued by state, would be prohibited in India.[6]

Earlier in 2018, processing of transactions involving cryptocurrencies by various banks were banned by the Reserve Bank of India. In March 2020, the Supreme Court had overturned the ban.

The finance minister, Nirmala Sitharaman has reiterated the government stance on cryptocurrencies announced in the Budget Speech for 2018-19 that the government does not consider cryptocurrencies a legal tender. RBI and SEBI also do not have a legal framework to directly regulate cryptocurrencies as of now as they are neither currencies nor assets or securities or commodities issued by an identifiable user.

However, the underlying technology of cryptocurrencies, the block chain technology will be allowed to be explored by the Government under certain exceptions since the technology is an emerging technology which can boost the digital economy.

China blocks access to social media app Clubhouse

The audio-only US social media platform Clubhouse was blocked by China for domestic access on February 8 after it gained massive popularity in mainland China due to the uncensored, free speech discussions it provided to users.

The move was taken after thousands had freely discussed sensitive topics like Xinjiang and the Tiananmen Square massacre on the platform. Some students and activists had also described their experiences of surveillance by Chinese authorities.[7]

Clubhouse is an invitation-only US app, which was launched in April 2020 and works on iPhones. It allows users to listen to and speak to others in random chat rooms on a wide range of topics, without the option of sending or receiving messages. A Clubhouse user, ones creates an account on the app, can further send invites to two more people. Reportedly, the app’s invitation codes were also sold on Chinese e-commerce sites, for as much as 400 yuan ($62).

According to data from Sensor Tower, Clubhouse has reached 3.6 million users globally.[8] The sudden increase in the number of users in recent weeks happened after Elon Musk, the chief executive officer of Tesla and SpaceX appeared on the platform and even invited Russian President Vladimir Putin to a Clubhouse Chat.

In China, users now would need to use virtual private networks to access Clubhouse. In addition, a report by the Stanford Internet Observatory has said that there were certain security flaws in the app due to which users' data had become vulnerable to access by the Chinese government. Clubhouse in response to the incident has stated that it is reviewing its data protection and security features.

RBI takes measures following Juspay data breach

The Reserve Bank of India (RBI) has taken steps to look into matters related to enforcement of new payment aggregator licensing norms, following cyberattacks on Indian payments companies like Juspay. A team from the RBI has enquired into the matter and reached out to key stakeholders including the Payment Council of India.[9]

A cybersecurity researcher on January 3 discovered that data of around 10 crore cardholders was being sold on the dark web for an undisclosed amount. It involved sensitive information of customers like email ids and mobile numbers and card transaction details apparently from the data breach of Juspay that took place in August 2020. [10]

Juspay had confirmed the August 2020 data breach after an investigation revealed unauthorized access by hackers on a server that formed part of its payment system. The data breach affected 35 million customer accounts with masked card data and card fingerprints.

Even though the card data remains masked, the fingerprint of the card number gets stored which, according to cybersecurity researchers, is a hash value of the card number and any hacker who can figure out its algorithm can unmask all digits. Juspay processes over 4 million transactions everyday across e-commerce platforms such as Amazon, Swiggy, and others.

U.S. semiconductor industry calls for government support

The Semiconductor industry in the US has called for support from the Biden administration. In a letter to the US President Joe Biden, the Semiconductor Industry Association (SIA) has asked for substantial funding for incentives like grants and tax credits for semiconductor manufacturing.[11]

The chief executive officers of companies including Intel Corp., Qualcomm Inc. and Advanced Micro Devices Inc. have urged the President to support domestic manufacturing of semiconductors since they presently outsource most of the production to Taiwan Semiconductor Manufacturing Co. and South Korea's Samsung Electronics Co. This has also become a national security issue as tensions rise between the U.S. and China, which is investing heavily to expand its own chip industry.

The country's share of chip manufacturing has dropped to 12% from 37% in 1990 according to the SIA. Also government incentives in other countries have unfairly disadvantaged the U.S. chip manufacturing companies. The letter also mentioned that the U.S. is lagging behind in terms of incentives for research and development too.

In response to the issue, the Biden administration has decided to discuss a comprehensive strategy with businesses and trading partners to identify and address the supply chain bottlenecks and other problems like chip shortage faced by the semiconductor industries. Long term strategies would involve broader supply chain assessments focused on technology and infrastructure.[12]

Government notifies rules for intermediaries

The Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (Rules). These rules cover social media platforms, messaging services, OTT platforms and news portals.[13]

The immediate impeus for the promulgation of the rules was the refusal of social media platform Twitter to accede to government instructions to block certain accounts. The Ministry of Electronics and Information Technology (MeitY) had asked Twitter to block around 257 URLs, one hashtag and around 1,178 accounts under section 69A of the Information Technology

Act for allegedly spreading misinformation on farmers' protest.[14]

But Twitter instead only withheld several accounts, which meant that these accounts became inaccessible only in India and could be accessed from outside India. Twitter had also restored these accounts within hours. A non-compliance notice was issued to Twitter by the government soon after.

Subsequently, a virtual meeting was held between Twitter executives and the Government. The MeitY in the meeting referred to the toolkit shared by Swedish climate activist Greta Thunberg. It also stated that freedom of speech and expression in the country is not absolute and subject to reasonable restrictions.[15]

India's information technology minister, Ravi Shankar Prasad in response to the Twitter row stated (in Parliament) that 'action' would be taken against social media platforms if they were misused to spread fake news and violence. They were free to do business and make money, but only in accordance with the Indian Constitution, irrespective of their own rules and guidelines.[16]

Amid the Twitter clash with the government, the Koo app, which is an Indian alternative for Twitter has seen a surge in users. The Koo app was launched last year and had won the government's Aatmanirbhar App Challenge in August 2020.

SWIFT sets up JV with China's central bank

SWIFT, the global system for financial messaging and cross-border payments, has set up a joint venture with payment market participants and infrastructure providers to comply with China's regulatory requirements.

The need for the joint venture is mainly to be able to obtain necessary licences for local network management activities, according to SWIFT. The move indicates a sign that China wants to promote the global usage of its planned digital yuan. It would also support the nation's push to compete with the US as a global economic power and reduce its reliance on the US Dollar.

The participants in the joint venture with SWIFT are Chinese central bank's digital currency research institute, the China National Clearing Centre, China's Cross-border Interbank Payment System and the Payment & Clearing Association of China all supervised by the People's Bank of China (PBOC).[17]

In a global race to launch central bank digital currencies, China has already launched trials in major cities like Shenzhen, Chengdu and Hangzhou. The Digital yuan would help in increasing the efficiency of cross-border payments.

[1] China Appears to Warn India: Push Too Hard and the Lights Could Go Out at https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

[2] Chinese cyber attack foiled: Power Ministry at https://www.thehindu.com/news/national/attacks-by-chinese-groups-thwarted-power-ministry/article33965683.ece

[3] Hackers try to contaminate Florida town's water supply through computer breach at https://www.reuters.com/article/usa-cyber-florida/update-1-hackers-broke-into-florida-towns-water-treatment-plant-attempted-poisoning-sheriff-says-idUSL1N2KE2UE

[4] Turns out that Florida water treatment facility left the doors wide open for hackers https://www.theverge.com/2021/2/10/22277300/florida-water-treatment-chemical-tamper-teamviewer-shared-password

[5] Draft Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019 at https://www.prsindia.org/billtrack/draft-banning-cryptocurrency-regulation-official-digital-currency-bill-2019

[6]Govt committee recommends ban all cryptocurrencies, except those issued by state: FM at https://www.livemint.com/market/cryptocurrency/govt-committee-says-ban-all-cryptocurrencies-except-those-issued-by-state-fm-11612866715432.html

[7]China bans Clubhouse app at

https://www.abc.net.au/news/2021-02-10/china-bans-clubhouse-app-as-netizens-stand-with-uyghurs/13136624

[8] Elon Musk wants to host a Clubhouse session with Vladimir Putin at https://tech.hindustantimes.com/tech/news/elon-musk-wants-to-host-a-clubhouse-session-with-vladimir-putin-71613283774938.html

[9] Juspay Data Leak fallout at https://economictimes.indiatimes.com/tech/technology/juspay-data-leak-fallout-rbi-swings-into-action-to-curb-cyberattacks/articleshow/80125430.cms?from=mdr

[10] Juspay data breach could have far-reaching consequences at https://www.csoonline.com/article/3603473/juspay-data-breach-could-have-far-reaching-consequences.html

[11]U.S. Chip Industry Urges Biden to Support Domestic Production at https://www.bloombergquint.com/onweb/u-s-chip-industry-urges-biden-to-support-domestic-production

[12] Biden Team Pledges Aggressive Steps to Address Chip Shortage at https://www.bloomberg.com/news/articles/2021-02-11/biden-team-pledges-aggressive-steps-to-address-chip-shortage

[13]Government Notifies New Rules For Social Media, Digital News And OTT Platforms at https://www.bloombergquint.com/law-and-policy/government-notifies-new-rules-for-social-media-digital-news-and-ott-platforms

[14] Twitter sets record straight on suspended, withheld accounts over farmers' protest, Govt calls it unusual: story in 10 points at https://www.financialexpress.com/industry/technology/twitter-sets-record-straight-on-suspended-withheld-accounts-over-farmers-protest-govt-calls-it-unusual-story-in-10-points/2192047/

[15] In meeting with Twitter, ministry mentions Greta's toolkit, US Capitol violence at https://www.hindustantimes.com/india-news/in-meeting-with-twitter-ministry-mentions-greta-s-toolkit-us-capitol-violence-101613008794798.html

[16] The Indian government's war with Twitter at https://www.bbc.com/news/world-asia-india-56007451

[17] SWIFT sets up JV with China's central bank at https://www.nasdaq.com/articles/swift-sets-up-jv-with-chinas-central-bank-2021-02-04-0