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

CYBER *Digest*

June 2021

- **Companies comply with new IT Rules 2021**
- **Cryptocurrencies in deep flux**
- **Ransom paid for Colonial Pipeline Hack**
- **Reported data breaches at Air India and Domino's**
- **Facebook lifts ban on Covid lab-leak theory posts**
- **Crippling ransomware attack on Irish health service**

Companies comply with new IT Rules 2021

The Ministry of Electronics and Information Technology (MeitY) had released the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 in February and had given the Social Media platforms a three month period to comply with the rules.[1] The government on May 26, at the end of the three month period, issued a notice to all social media intermediaries seeking the details on the status of compliance with the new rules, which led to a strong backlash from some of the social media companies.

The new IT Rules aim to empower ordinary users of social media and over-the-top (OTT) platforms, with a mechanism for redressal and timely resolution of their grievance. A Grievance Officer has to be appointed according to the new rules in order to deal with such complaints. Special emphasis has been given for the protection of women and children from sexual offences, fake news and other misuse of the social media. Identification of the first originator of the information would be required in case of an offence related to sovereignty and integrity of India. A Chief Compliance Officer, a resident of India, needs to be appointed who shall be responsible for ensuring compliance with the Act and Rules. Also, a monthly compliance report mentioning the details of complaints received and action taken on the complaints would be necessary.

Companies like Google, Facebook, WhatsApp, Telegram, Koo, Sharechat, and LinkedIn, have shared details with the ministry as per the requirement of the new norms. Twitter sought an extension of the compliance window[2] while WhatsApp has filed a case in the Delhi High Court against traceability of messages.[3]

The rules have endeavoured to maintain a delicate balance between freedom of speech and expression and reasonable restrictions that uphold national sovereignty and security considerations.

Cryptocurrencies in deep flux

The cryptocurrency market stood at a market capitalization of around $1 trillion on May 23, with all major cryptocurrencies trading at levels far lower than the previous week ($2.2 trillion). The market crash was reported following Tesla Founder Elon Musk's statement that Tesla will not be accepting Bitcoin payments for cars due to the high energy consumption during the mining process of these currencies.[4]

Bitcoin fell around 29.5 percent (at $34,000), Ethereum around 45 percent (at $2,000), Dogecoin slipped 40.93 percent to trade below $1. Elon Musk subsequently tweeted that he had reversed his company's position following talks with North American Bitcoin miners on cryptocurrency mining energy conservation efforts.[5] Bitcoin again reached nearly $40,000 following his latest tweet.

Elon Musk's tweets on cryptocurrencies have influenced the crypto market for a while now. Some cryptocurrency enthusiasts have formed a group called "stop Elon" to stop him from tweeting on the subject and even developed a coin called $STOPELON[6] since they believe

him to be a 'market manipulator 'of cryptocurrency.

As per latest reports, Indian banks are still reluctant regarding use of cryptocurrencies since the 2018 Reserve Bank of India (RBI)'s ban of crypto-transactions. Though the Supreme Court of India overturned the ban in 2020, but yet there is no legal framework in the country to directly regulate cryptocurrencies. The government is on its way to regulating cryptocurrencies in India.[7] The National Payment Corporation of India, although has asked banks to develop their own guidelines for transactions involving cryptocurrencies. The Paytm Payments Bank announced that it has stopped providing banking support to cryptocurrency exchanges, such as WazirX, ZebPay, and CoinSwitch Kuber.[8]

Ransom paid for Colonial Pipeline Hack

The US fuel pipeline operator, Colonial Pipeline, was hit by a cyber-attack on May 9. This led to the shutdown of supplies of gasoline, diesel and jet fuel, in important cities of the US. The company took parts of its systems offline soon after the attack to contain the threat. The cyber-attack on the Colonial Pipeline network involved ransomware and the 'DarkSide' group of hackers was responsible for the attack as confirmed by The Federal Bureau of Investigation (FBI).[9]

Shutdown of operations of the pipeline led to shortage of supplies of around 2.5 million barrels per day. Oil prices rose with the price of Brent crude rising to $69 per barrel the following week, a 1.5 per cent rise.[10] On May 15, Colonial Pipeline announced that it had returned to its normal operations. As per reports, Colonial Pipelines paid a ransom amount of nearly $5 million to the hackers in cryptocurrency.[11]

The DarkSide group has repetitively attacked organisations in the past using the same modus operandi of ransomware. Reports note that at least 90 utilities were impacted in the past, including companies like Brookfield, OneDigital and Gyrodata, among others.[12] DarkSide has openly published a list of all the companies it has hacked and the information on the data it has stolen on its website on the dark web. The hackers work with 'access brokers' – cyber-criminal gangs who steal and sell personal data to the highest bidders on the dark web.[13]

Following the cyber-attack, US president Joe Biden, signed an executive order (EO) on May 13 to encourage improvements in digital security standards across the private sector and better equip federal agencies with cybersecurity tools.[14] The EO focusses on the steps to prevent, detect, assess, and remedy cyber incidents that would help ensure national and economic security. It also calls for Public Private Partnership to adapt to the continuously changing cyber threat environment.

Reported data breaches at Air India and Domino's

Two high profile hacks reported this month are of Air India and Domino's India. The attack on Air India, which saw the personal data of around 4.5 million passengers being leaked was directed at SITA, the Geneva based the passenger service system data

processor, responsible for storing and processing of personal information of the passengers.[15] The compromised servers were later secured, Air India stated.

The breach involved name, contact information, passport information, Star Alliance and Air India frequent flyer data, etc., however no passwords or CVV/CVC numbers were affected according to the airline. The breach included the data of passengers who had registered during a ten year period- August 2011 to February 2021. SITA had notified other airlines of a breach earlier this year.[16]

Domino's India, also had a similar data breach in April that involved sensitive information such as phone numbers, names, and payment information including credit cards. A massive amount of around 18 crore orders' data from the breach has been put up on the dark web for sale as a searchable database. Alon Gal, the CTO of Hudson Rock, a cybersecurity firm confirmed that this data was sold for around Rs 4.5 crore in bitcoins.

The repeated data breach incidents indicate an urgent need to regulate upon the amount of personal data collection by companies and their automatic deletion after a stipulated time period. This could prevent such incidents to a large extent.

Facebook lifts ban on Covid lab-leak theory posts

Facebook has decided to no longer restrict posts involving the origin theory of the coronavirus that claims it to be lab-made. The move comes after consultation with public health experts and in light of the ongoing investigations regarding the origin theory of Covid-19.[17]

Earlier, in February 2021, Facebook had explicitly banned posts related to covid-19 misinformation including the lab-leak theory of the virus, that Covid-19 was 'man-made or manufactured' and classified it under false claims regarding Covid-19. Accounts that posted such claims saw their posts removed or restricted and repeated sharing of such posts also could have led to a ban from the site altogether.

A Wall Street Journal report recently stated that that US intelligence sources believe that there is evidence to the "lab leak" theory based on the November 2019 incident where three staff members at the Wuhan Institute for Virology sought hospital treatment for flu-like symptoms.[18]

Facebook however maintains strict restrictions on other misleading content about Covid-19 and vaccines. It has also come up with new rules in which users who repeatedly share false content would have all their posts suppressed. Also a pop-up notice warning users of the posting history of page that repeatedly shares false information would be given to users who "like" such pages.

Crippling ransomware attack on Irish health service

The Irish Department of Health was hit by a major cyber-attack on May 20. A similar attack also took place on May 14 on the centralized Health Service Executive (HSE) which is responsible for managing healthcare for the Irish population.[19] The HSE attack involved the 'Conti-ransomware' developed by a cybercriminal

gang that habitually releases stolen information as a double-extortion strategy.

The attack inserted malware across the HSE healthcare system network in multiple locations thereby disrupting all outpatient services and shutting down the IT systems. The cyber-attack also forced the Covid-19 vaccine portal to close temporarily causing a major disruption to the on-going vaccine programme. However authorities have stated that the programme will continue as planned with the same amount of doses expected to be given to the population in the following weeks.

The National Cyber Security Centre of Ireland has shared information about the incident with the European Union and other international partners to ensure that the HSE has the necessary cyber support.[20] The assessment and restoration work of the IT network continues by the health department. Irish Foreign Minister Simon Coveney has stated that it is going to take quite some time to backup and protect as much of the data as possible.[21]

[1] Government notifies IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, at https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1700749

[2] Twitter defaming India, defying laws, says government, at https://www.thehindu.com/news/national/twitters-statement-an-attempt-to-dictate-its-terms-to-india-government/article34659934.ece

[3] WhatsApp moves Delhi High Court against India's new IT Rules, at https://www.thehindu.com/sci-tech/technology/internet/whatsapp-sues-govt-says-new-media-rules-mean-end-to-privacy/article34646518.ece

[4] Bitcoin carnage | Everything that happened in the cryptocurrency world this week, at https://www.moneycontrol.com/news/business/cryptocurrency/bitcoin-carnage-everything-that-happened-in-the-cryptocurrency-world-this-week-6928011.html

[5] Bitcoin jumps 12% as Elon Musk hints change in position on environment impact of Bitcoin mining, at https://www.moneycontrol.com/news/business/cryptocurrency/bitcoin-jumps-12-as-elon-musk-hints-change-in-position-on-environment-impact-of-bitcoin-mining-asks-for-ideas-to-develop-dogecoin-6934081.html

[6] $STOPELON: Investors Accuse Musk Of 'Manipulating' Crypto Market, Form New Meme Currency at https://gadgets.ndtv.com/internet/news/stopelon-investors-form-meme-currency-start-group-to-stop-musk-from-tweeting-on-cryptocurrencies-2448940

[7] https://prsindia.org/billtrack/draft-banning-of-cryptocurrency-regulation-of-official-digital-currency-bill-2019

[8] Paytm closes account with crypto exchanges, at https://www.livemint.com/market/cryptocurrency/crypto-exchanges-scramble-to-add-partners-as-paytm-suspends-banking-support-11621599374656.html

[9] FBI Statement on Network Disruption at Colonial Pipeline, at https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline

[10] Oil rises 1% after cyber attack forces closure of US fuel 'jugular' pipeline, at https://www.livemint.com/market/commodities/oil-rises-1-after-cyber-attack-forces-closure-of-us-fuel-jugular-pipeline-11620610154131.html

[11] Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom, at https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

[12] What We Know About the DarkSide Ransomware and the US Pipeline Attack https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

[13] US fuel pipeline hackers 'didn't mean to create problems', at https://www.bbc.com/news/business-57050690
[14] Executive Order on Improving the Nation's Cybersecurity, at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[15] Notification, http://www.airindia.in/images/pdf/Data-Breach-Notification.pdf
[16] Air India passenger data breach reveals SITA hack worse than first thought, at Air India passenger data breach reveals SITA hack worse than first thought | TechCrunch
[17] Facebook lifts ban on posts claiming Covid-19 was man-made, at https://www.theguardian.com/technology/2021/may/27/facebook-lifts-ban-on-posts-claiming-covid-19-was-man-made
[18]Intelligence on Sick Staff at Wuhan Lab Fuels Debate on Covid-19 Origin, at https://www.wsj.com/articles/intelligence-on-sick-staff-at-wuhan-lab-fuels-debate-on-covid-19-origin-11621796228
[19]Cyber-attack on Irish health service 'catastrophic', at https://www.bbc.com/news/world-europe-57184977
[20]Irish Health Care System Suffers New Cyber Attack, RTE Reports, at https://www.bnnbloomberg.ca/irish-health-care-system-suffers-new-cyber-attack-rte-reports-1.1604461
[21] Cyber-crime: Irish health system targeted twice by hackers, at https://www.bbc.com/news/world-europe-57134916