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

CYBER *Digest*

March 2024

- Cyber incidents in Canada
- Malawi government network hit by cyberattack
- Ransomware attack on Romanian health-care facilities
- Australian telecom service provider reports data breach
- LockBit infrastructure taken down in coordinated effort
- Deepfake employed for million-dollar fraud
- US Executive Order on Sensitive Personal Data
- India File

Cyber incidents in Canada

Reports indicate that the Royal Canadian Mounted Police (RCMP) has confirmed the initiation of a criminal investigation in response to a cybersecurity attack against its networks. The RCMP further stated its ongoing efforts to ascertain the scope of the security breach and emphasized that there have been no noticeable impacts on foreign police and intelligence services.[1] In a separate incident within Canada, Hamilton City fell victim to a ransomware attack, resulting in significant disruptions to city services persisting for over a week.[2] This incident has resulted in the shutdown of nearly all city phone lines, interrupted city council operations, and affected numerous services, including the bus schedule app, library Wi-Fi access, and permit application processes.

Malawi government network hit by cyberattack

According to reports, the government of Malawi has halted the issuance of passports in response to a cyber-attack on the immigration service's computer network.[3] President Lazarus Chakwera informed Members of Parliament that this attack on the department constituted a significant breach of national security. He elaborated that the hackers had demanded a ransom. However, the president affirmed that the government would not yield to their demands and was actively engaged in resolving the issue. No additional details regarding the cyber-attack were disclosed publicly, including potential implications for personal data security.

Ransomware impact on health-care facilities in Romania

Over 100 healthcare facilities in Romania were rendered offline following a ransomware attack targeting at least 25 hospitals, as reported by the country's cybersecurity agency.[4] The Romanian National Cyber Security Directorate also stated that the attack originated at Pitesti Paediatric Hospital and subsequently affected other institutions. Additionally, 79 healthcare facilities have opted to disconnect from the internet in an attempt to evade the hackers. The identities of the hackers remain undisclosed to the public. Still, according to the Romanian agency, they employed a strain of ransomware known as Phobos, which is attributed to Russian-speaking hackers. This particular strain has been leaked and is accessible for use by any criminal hacker.

Australian telecom service provider reports data breach

Australian telecommunications provider Tangerine has announced that the personal information of 230,000 individuals was compromised in a recent cyberattack.[5] According to Tangerine, the attackers gained unauthorized access to a legacy customer database containing the details of approximately 230,000 current and former customer accounts. The compromised personal information encompasses names, addresses, dates of birth, email addresses, mobile phone numbers, and Tangerine account numbers. According to Tangerine, the attackers seem to have gained access to the database using the login credentials of a contractor. The company clarified that the incident did not affect its services or customer accounts, as they are safeguarded with multi-factor authentication (MFA).

LockBit infrastructure taken down in coordinated global effort

February proved to be the worst month for the Lockbit cybercriminal gang. In a widely reported joint operation, global law enforcement authorities, including the FBI, have disrupted the activities of the formidable LockBit ransomware gang.[6] Most recently, they had claimed responsibility for hacking one of India's leading brokerage firms, Motilal Oswal.[7]

According to reports, the authorities have taken control of its platform and seized data associated with its global ransomware-as-a-service (RaaS) operation. Information obtained through the operation, dubbed Operation Cronos, includes source code, details of ransomware victims, stolen data, decryption keys, and the amount of money extorted by LockBit and its affiliates. In what appears to be a coordinated effort, the United States has charged two Russian nationals with deploying Lockbit ransomware against companies and groups globally. Furthermore, police in Poland and Ukraine have made two arrests in connection with the case.

The UK's National Crime Agency, the U.S. Department of Justice, the FBI, and Europol convened in London to announce the disruption of the gang, which has targeted over 2,000 victims worldwide.[8] The gang has received more than $120 million in ransom payments and demanded hundreds of millions of dollars. However, it was reported that in a surprising turn of events, the LockBit RaaS operation has relaunched its leak site.[9] This rebound may be attributed to the fact that its backup systems remained untouched, allowing the operation to quickly rebound.

Deepfake employed for million-dollar fraud

The Hong Kong police reported that a finance worker at a multinational firm was deceived into transferring $25 million to fraudsters who used deepfake technology to impersonate the company's chief financial officer during a video conference call.[10] The case is one of several recent episodes in which fraudsters are suspected to have employed deepfake technology to alter publicly available video and other footage as a means to deceive individuals into parting with their money.

US Executive Order on Sensitive Personal Data

President Biden issued an Executive Order with the objective of safeguarding Americans' sensitive personal data from exploitation by countries of concern.[11] The order focuses on protecting Americans' most personal and sensitive information, which encompasses genomic data, biometric data, personal health data, geolocation data, financial data, and certain types of personally identifiable information. In the order, the president directed The Departments of Justice and Homeland Security to collaborate in establishing stringent security standards. These standards are aimed at preventing access by countries of concern to Americans' data through other commercial avenues, such as data accessible via investment, vendor, and employment relationships. President Biden also directed the Committee for the Assessment of

Foreign Participation in the United States Telecommunications Services Sector, commonly referred to as "Team Telecom," to take into account the threats posed to Americans' sensitive personal data during its reviews of submarine cable licenses.

India File

- The Seventh and concluding Session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 29 January 2024 to 9 February 2024 in Hybrid mode. The Indian delegation led by the Ministry of Home Affairs participated in the negotiations.

- The 12th ASEAN Regional Forum (ARF) Open-Ended Study Group (OESG) on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the use of Information and Communications Technologies in the field of Security of and in the use of ICTs' was held on 26 February 2024 in virtual mode. Shri Ravi Shanker Goel, Director (CD), attended the event.

- The IT ministry decided to issue an order to block the end-to-end encrypted email service Proton Mail following a request from the Tamil Nadu police.[12] This request stemmed from a hoax bomb threat sent to at least thirteen private schools in Chennai in February. The decision was made during a meeting of the 69A blocking committee. Under Section 69A of the IT Act, the designated officer, with approval from the IT Secretary and upon recommendation of the 69A blocking committee, has the authority to issue orders to any intermediary or government agency to block content for reasons related to national security, public order, and related concerns.

- The ransomware gang LockBit has claimed responsibility for hacking one of India's leading brokerage firms, Motilal Oswal. Indian authorities have stated that they are aware of the incident and are currently investigating it. LockBit asserts that they have gained access to "confidential company data." The company's shares fell by 2% following the incident.[13]

- In response to the increasing number of cyber incidents, particularly financial fraud, the Secretary of the Department of Financial Services (DFS) under the Ministry of Finance chaired a meeting. The meeting aimed to address pressing concerns raised during a previous meeting held in November regarding cybersecurity in the financial services sector and to devise comprehensive strategies to mitigate such threats. One of the key highlights of the meeting was the action taken by the Department of Telecom in blocking approximately 1.4 lakh mobile handsets associated with financial fraud.[14]

- In the 2024 interim budget, the Indian government nearly doubled the allocation for cybersecurity projects, increasing it from Rs 400 crore in 2023-2024 to Rs 759 crore in 2024-2025. The majority of these projects are undertaken by the Ministry of Electronics and Information Technology (MeitY).[15]

[1] CBC News, RCMP networks targeted by cyberattack, 23 February 2024, https://www.cbc.ca/news/politics/cybersecurity-breach-rcmp-1.7123787

[2] CBC News, Hamilton hit by ransomware attack, city says for 1st time since incident paralyzes services, 4 March 2024, https://www.cbc.ca/news/canada/hamilton/ransomware-attack-1.7133457

[3] BBC News, Cyber-attack hits Malawi's immigration service, 22 February 2024, https://www.bbc.com/news/world-africa-68366749

[4] NBC News, More than 100 Romanian health care facilities taken offline after cyber attacks target hospitals, 13 February 2024, https://www.nbcnews.com/tech/security/romania-hospital-hack-ransomware-russia-cyber-rcna138607

[5] Security Week, 230k Individuals Impacted by Data Breach at Australian Telco Tangerine, 23 February 2024, https://www.securityweek.com/230k-individuals-impacted-by-data-breach-at-australian-telco-tangerine/

[6] Dark Reading, Global Law Enforcement Disrupts LockBit Ransomware Gang, 20 February 2024, https://www.darkreading.com/cybersecurity-operations/global-law-enforcement-disrupts-lockbit-ransomware-gang

[7] Techcrunch, LockBit claims cyberattack on Indian broker Motilal Oswal, 15 February, https://techcrunch.com/2024/02/15/lockbit-ransomware-cyberattack-india-brokerage-firm-motilal-oswal/

[8] Reuters, Lockbit cybercrime gang faces global takedown with indictments and arrests, 20 February 2024, https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/

[9] Dark Reading, LockBit's Leak Site Reemerges, a Week After 'Complete Compromise', 27 February 2024, https://www.darkreading.com/threat-intelligence/lockbit-leak-site-reemerges-week-after-complete-compromise-

[10] CNN, Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’, 4 February 2024, https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

[11] The White House, FACT SHEET: President Biden Issues Executive Order to Protect Americans’ Sensitive Personal Data, 28 February 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/

[12] Hindustan Times, IT ministry looks to block Proton Mail on request of Tamil Nadu police, 15 February 2024, https://www.hindustantimes.com/india-news/it-ministry-looks-to-block-proton-mail-on-request-of-tamil-nadu-police-101707938167006.html

[13] Moneycontrol, Motilal Oswal falls prey to cyber-attack by ransomware group Lockbit, shares fall two percent, https://www.moneycontrol.com/news/business/markets/motilal-oswal-falls-prey-to-cyber-attack-by-ransomware-group-lockbit-shares-in-focus-12300291.html

[14] CNBCTV18, India tackles financial cyber threats, DFS Secretary leads action meeting, 9 February 2024, https://www.cnbctv18.com/economy/india-tackles-financial-cyber-threats-dfs-secretary-leads-action-meeting-19020411.htm

[15] Moneycontrol, Govt nearly doubles allocation for cybersecurity projects in Budget 2024, 1 February 2024, https://www.moneycontrol.com/news/business/budget/govt-nearly-doubles-allocation-for-cybersecurity-projects-in-budget-2024-12170711.html