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

CYBER *Digest*

February 2024

- Ukraine-Russia Cyber conflict
- Beirut Airport hack displays anti-Hezbollah message
- Paraguay military issues alert over Ransomware attack
- Israeli movie theatre targeted by hackers
- Cyber-focused FBI agents to join US embassies worldwide
- Australia sanctions individuals behind a major hack
- India File

Ukraine-Russia Cyber conflict

Following the revelation of a major cyber attack on Ukrainian telecom provider Kyivstar in December 2023, the Ukrainian Blackjack hacker group executed a cyberattack targeting the Moscow-based Internet provider M9 Telecom. The attack resulted in the destruction of the provider's servers, leading to the deletion of approximately 20 terabytes of data. As reported, the affected data included the company's official website, branch websites, mail server, and cyber protection services.[1] The group has also previously targeted Russia's infrastructure, including a water utility company.

In a separate incident, massive waves of denial-of-service (DDoS) attacks were executed against Monobank, Ukraine's largest mobile-only bank.[2] Authorities reported that Monobank faced a targeted attack involving 580 million service requests in a single incident.

Beirut Airport hack displays anti-Hezbollah message

Rafic Hariri International Airport in Beirut experienced an electronic hacking attack in early January.[3] While this resulted in temporary hindrance, the airport maintained regular operations, and scheduled flights proceeded as planned. Texts appeared on departure and arrival screens at the airport, addressing Hezbollah and its security chief, Hassan Nasrallah, and replacing the usual landing and departure timetables. At the same time, the baggage system encountered a technical malfunction. Since the commencement of hostilities on the southern Lebanese front involving Hezbollah and the Israel Defense Forces, Rafik Hariri International Airport has experienced disruptions to its air and sea navigation systems.

Paraguay military issues alert over Ransomware attack

In the first week of January, the Paraguayan military issued a cautionary notice highlighting the risks of ransomware following a cyberattack that significantly impacted one of the nation's leading internet service providers.[4] The General Directorate of Information and Communication Technologies, an agency within the armed forces commonly referred to by its acronym *Digetic*, officially released an alert detailing the detrimental effects of ransomware within the country. Over the past few years, numerous nations in Latin America and the Caribbean have experienced such attacks.

Israeli movie theatre targeted by hackers

In another significant cyber event in Israel, threatening messages and images from the October 7 Hamas attack were displayed on the screens of the Lev Cinema chain in Tel Aviv.[5] The threat actors, reportedly of Turkish origin, infiltrated the computer system of the movie theaters' advertising screens. They displayed images from the October 7 Hamas attack alongside threatening messages written in broken Hebrew. After the attack, it was reported that the screens displaying the slides were promptly turned off, and an investigation was initiated.

Cyber-focused FBI agents to join US embassies worldwide

According to reports, the FBI is expanding its deployment of agents to American embassies abroad, specifically emphasizing the investigation of cyber-related crimes.[6] The addition of six new positions marks an almost 40% increase in the FBI's cyber assistant legal attachés (ALATs). These new roles will include New Delhi, Rome, and Brasilia postings. With this expansion, the total number of FBI agents specializing in cyber-related issues deployed to U.S. embassies will reach 22. The FBI initiated the placement of cyber-focused agents in U.S. embassies in 2011.

Australia sanctions individuals behind a major hack

Australia has publicly identified and enforced cyber sanctions on a Russian individual for his purported involvement in a ransomware attack in 2022.[7] This marks the country's first application of such penalties. The attack targeted Medibank, one of Australia's major private health insurers, and resulted in the theft of sensitive personal data from 9.7 million customers. The compromised information included names, dates of birth, medical details, and Medicare numbers. Australian authorities further noted that some of these records were subsequently published on the dark web.

As per reports, the sanctions entail that providing assets to Ermakov or engaging in any use or dealings with his assets is now a criminal offense. This prohibition extends to various forms, including cryptocurrency wallets and ransomware payments. Subsequently, the United States and the United Kingdom joined Australia in solidarity by jointly implementing trilateral sanctions against the Russian threat actor.[8]

India File

- According to a threat assessment report, Pakistan-based threat actors have been targeting Indians with fake loan android applications.[9] The fraudulent loan application purports to offer instant loans to users. Upon installation, the app presents reasons for seeking permissions. Subsequently, victims are prompted to log in and provide their details for Know Your Customer (KYC) purposes, including the submission of a selfie. Later, the threat actor manipulates the selfie to create a nude image to extort money by threatening to distribute it to their contact list.
- According to a threat intelligence report, personal data of nearly 75 Crore Indians, including Aadhar details and phone numbers, has been put up for sale online.[10] The threat actor named CyboDevil posted in an underground forum promoting the sale of the consumer database. The report also sounded alarms regarding the substantial risks associated with such leaks, emphasizing the potential for deployment in sophisticated ransomware attacks or data exfiltration.
- It was reported that in a massive security breach, the System for Pension Administration Raksha (SPARSH) portal, India's central web-based system for automating pension processes for defense personnel, including Army, Navy, Air Force, and civilian defense staff, has experienced a significant data leak.[11]The dtat leak of the portal, developed by Tata Consultancy Services (TCS), includes sensitive information such as usernames, passwords, URLs, and pension numbers posing serious threat

to the the privacy and financial security of affected pensioners.

- The Indian Army has developed an end-to-end secure mobile ecosystem known as SAMBHAV (Secure Army Mobile Bharat Version).[12] This mobile ecosystem is designed to provide secure communication with instant connectivity, especially while on the move, representing a noteworthy advancement in India's defense capabilities. SAMBHAV has been developed through collaboration between the Indian Army and prominent academic and industry experts.

- According to data from the National Cybercrime Reporting Portal (NCRP), the instances of financial cybercrime fraud in Kerala more than doubled in 2023 compared to 2022.[13] The recorded cases rose from 9,518 in 2022 to 20,569 in 2023. In the same year, the cumulative amount of money lost due to cybercrime in Kerala reached a new record. Ernakulam Rural Police Station recorded the highest number of cybercrime cases in 2023, with 1,947 reported incidents. Following closely, Palakkad Police Station reported 1,900 cases, and Ernakulam City Police Station documented 1,712 cases during the same period.

- Experts believe that Indonesian hackers may have been behind the latest hack of multiple Indian websites, including those run by the Indian army, the Census of India, and institutions like Banaras Hindu University, as part of hacktivist campaigns.[14] India's stance in the present war between Israel and Hamas is believed to be the reason for these attacks.

- 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 commenced in New York on 29 January 2024 for 12 days in Hybrid mode. The Indian delegation is actively participating in the negotiations.

[1] The Kyiv Independent, Ukrainian hackers hit Russian internet provider, claim they are preparing 'revenge for Kyivstar', 9 January 2024, https://kyivindependent.com/media-ukrainian-hackers-hit-russian-internet-provider-claim-they-are-preparing-revenge-for-kyivstar.

[2] The Kyiv Independent, Massive cyberattack targets Ukrainian online bank, 22 January 2024, https://kyivindependent.com/massive-cyberattack-targets-ukrainian-online-bank/

[3] Arab News, Screens at Beirut airport hacked with anti-Hezbollah message, 7 January 2024, https://www.arabnews.com/node/2437611/middle-east

[4] The Record, Paraguay military warns of 'significant impact' of ransomware after attack on internet provider, 9 January 2024, https://therecord.media/paraguay-military-warns-of-ransomware

[5] Ynetnews, Hackers broke into Tel Aviv movie theater system and screened October 7 images, 23 January 2024, https://www.ynetnews.com/article/bygmwdtft

[6] Cyberscoop, The FBI is adding more cyber-focused agents to U.S. embassies, 3 January 2024, https://cyberscoop.com/the-fbi-is-adding-more-cyber-focused-agents-to-u-s-embassies/

[7] CNN, Australia sanctions Russian national accused of hacking in Medibank data leak, 24 January 2024, https://edition.cnn.com/2024/01/23/tech/medibank-attack-australia-sanction-revil-intl-hnk/index.html.

[8] U.S. Department of the Treasury, United States, Australia, and the United Kingdom Sanction Russian Cyber Actor Responsible for the Medibank Hack, 23 January 2024, https://home.treasury.gov/news/press-releases/jy2041

[9] Cyfirma, Pakistan-based Threat Actor Targets Indians with Fake Loan Android Application, 22 January 2024, https://www.cyfirma.com/outofband/pakistan-based-threat-actor-targets-indians-with-fake-loan-android-applications.

[10] Scroll, Aadhaar details, phone numbers of nearly 75 crore Indians put up for sale, claims cybersecurity firm, 25 January 2024, https://scroll.in/latest/1062708/aadhaar-details-phone-numbers-of-nearly-75-crore-indians-put-up-for-sale-says-cybersecurity-firm

[11] The Cyber Express, TCE Exclusive: Massive Data Leak at India's SPARSH Pension Portal Puts Defense Personnel at Risk, 8 January 2024, https://thecyberexpress.com/sparsh-portal-data-leak-exposes-sensitive-info/

[12] The Times of India, Indian Army develops end-to-end encrypted mobile ecosystem SAMBHAV: How it will work and more, 14 January 2024, https://timesofindia.indiatimes.com/gadgets-news/indian-army-develops-end-to-end-encrypted-mobile-ecosystem-sambhav-how-it-will-work-and-more/articleshow/106810294.cms

[13] The News Minute, RTI reply shows Kerala lost Rs 200 crore to cyber fraudsters in 2023, 14 January 2024, https://www.thenewsminute.com/kerala/rti-reply-shows-kerala-lost-rs-200-crore-to-cyber-fraudsters-in-2023.

[14] The Economic Times, Alarm bells go off as Indonesian hacktivists breach government websites, 30 January 2024, https://economictimes.indiatimes.com/tech/technology/indonesian-hackers-behind-breach-of-indian-websites-this-month-experts/articleshow/107239316.cms