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

CYBER *Digest*

December 2024

- **Increasing Incidents Linked to Cyber-Scam Compounds**
- **China Linked Actor Targets Telecommunication Sector**
- **Undersea Cable Linking Finland to Central Europe Damaged**
- **Pro-Russia Groups Linked to Cyberattacks on South Korea**
- **Cyberattack Disrupts Credit Card Readers in Israel**
- **Hungary Confirms Cyberattack on Defence Procurement Agency**
- **Pakistani Religious Body Declares VPN Use Un-Islamic**
- **Indians lose $1.3 billion to Cyber Fraud in 2024**
- **Pakistan-Linked Hackers Target India via Applications**
- **India File**

Increasing Incidents Linked to Cyber-Scam Compounds

Amid the rising number of cyber scam cases, Cambodia's Ministry of Interior has reaffirmed its stance against the operation of online scam centres within the country.[1] The ministry emphasized the need for strengthened international collaboration to combat these transnational crimes. In a recent raid in Phnom Penh, authorities uncovered illegal online gambling activities involving nearly 200 individuals, primarily Chinese and Pakistani nationals.

Meta reported that, so far this year, it has removed over two million accounts associated with scam operations in Myanmar, Laos, Cambodia, the United Arab Emirates, and the Philippines.[2] Initially focusing on scam centres in Cambodia, the company has since expanded its efforts to address the growing presence of these networks in countries like Laos, Myanmar, and, more recently, the United Arab Emirates.

China Linked Actor Targets Telecommunication Sector

A Chinese state-sponsored hacking group, Salt Typhoon, has been accused of breaching major U.S. telecommunications providers, including T-Mobile, Verizon, AT&T, and Lumen Technologies.[3] The hackers reportedly infiltrated critical systems used for law enforcement surveillance, exploiting vulnerabilities in Cisco routers to gain unauthorized access to sensitive communications, potentially including unencrypted messages. While there is no evidence of significant customer data compromise, the breach is described as extensive and sophisticated, raising serious national security concerns about the potential exposure of sensitive information to foreign adversaries.

Undersea Cable Linking Finland to Central Europe Damaged

Finnish authorities are investigating a disruption in the C-Lion1 undersea cable, which links Finland to Germany via the Baltic Sea. The 1,200-kilometer cable, commissioned in 2016, is Finland's sole submarine communication link to Central Europe. State-owned service provider Cinia detected a fault that has interrupted data transmission and is working to determine the cause of the damage.

Pro-Russia Groups Linked to Cyberattacks on South Korea

South Korea's presidential office reported that pro-Russia hacking groups launched cyberattacks following North Korea's deployment of troops to Russia in support of its war in Ukraine.[4] An emergency inter-agency meeting was convened after recent denial-of-service attacks (DDoS) targeted government and private websites, causing temporary outages but no significant damage. The government pledged to enhance its cybersecurity measures, noting that such attacks, previously sporadic, have increased in frequency since North Korea's involvement in the conflict.

Cyberattack Disrupts Credit Card Readers in Israel

Reports indicate that a suspected cyberattack caused a malfunction in devices used across Israel to read credit cards, disrupting communication services. As a result, customers at supermarkets and gas stations were unable to process payments for about an hour. The attack, identified as a distributed denial-of-service (DDoS)

assault, targeted the payment gateway company Hyp's CreditGuard product. While the attack disrupted communication between card terminals and the payment system, it did not compromise payment information or lead to theft.[5]

Hungary Confirms Cyberattack on Defence Procurement Agency

Hungarian officials confirmed that the country's defines procurement agency (VBÜ) was attacked by an "international group of hackers."[6] The cybercrime group, known as INC Ransomware or INC Ransom, claimed responsibility for the breach and posted sample screenshots of the agency's data on its dark web portal. The group, which emerged last year, has primarily targeted healthcare, education, and government sectors, though the identities of its operators remain unknown. In response to media inquiries, the Hungarian Ministry of National Defence refrained from commenting on any potential data leaks, citing an ongoing investigation. The ministry also stated that VBÜ does not handle sensitive military data.

Pakistani Religious Body Declares VPN Use Un-Islamic

Pakistan's top religious advisory body, the Council of Islamic Ideology, has declared that using virtual private networks (VPNs) to access blocked content is against Shariah law.[7] The ruling comes as the Pakistani government enforces a nationwide firewall and urges users to register VPNs with the state media regulator, citing the need for enhanced cybersecurity and terrorism prevention. However, critics argue that these actions increase online surveillance, restrict freedom of expression, and harm e-commerce. VPNs are commonly used to conceal user identities, ensuring privacy, and allowing access to restricted content. The council stated that VPNs are being used to access illegal or immoral content, including pornography and disinformation, and emphasized that such actions violate Islamic and social norms.

Indians lose $1.3 billion to Cyber Fraud in 2024

India suffered cyber fraud losses of approximately Rs. 11,333 crores in the first nine months of 2024, according to data from the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs.[8] Stock trading scams caused the highest losses, totalling Rs. 4,636 crores from 2,28,094 complaints. Investment scams followed, with ₹3,216 crore lost from 1,00,360 complaints, while "digital arrest" frauds accounted for Rs. 1,616 crores across 63,481 complaints. Data from the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) revealed nearly 12 lakh complaints in 2024, with 45% traced to Southeast Asian nations, including Cambodia, Myanmar, and Laos.

Pakistan-Linked Hackers Target India via Applications

A Pakistan-linked hacking group, Transparent Tribe (APT36), is actively targeting Indian entities with advanced malware called ElizaRAT.[9] First detected in September 2023, ElizaRAT has since been upgraded with more sophisticated techniques and enhanced command-and-control capabilities. A report details three distinct campaigns conducted between late 2023 and early 2024, each using different versions of ElizaRAT to steal data from target systems. Notably, all versions of the

malware are set to Indian Standard Time (IST), suggesting that it is specifically designed to target India.

India File

- The Army is intensifying efforts on 16 specific technology clusters and plans to induct domain specialists to transform itself into a future-ready force equipped with the necessary offensive capabilities for increasingly digitized battlefields.[10] The Indian armed forces are focusing on these technologies to strengthen their position and catch up in the evolving strategic competition.
- As part of its modernization efforts, the Indian Army is launching an internship program to attract young, tech-savvy individuals to explore the integration of new technologies into military operations.[11] This initiative is aimed at ensuring the Army stays ahead in fields such as cybersecurity, information technology (IT), and information warfare. With warfare shifting towards non-kinetic strategies, the Army is focused on preparing the next generation of leaders to navigate this evolving domain.
- The Bharat National Cyber Security Exercise (Bharat NCX 2024), a major initiative to enhance India's cybersecurity resilience, was launched by the National Security Council Secretariat (NSCS) in partnership with Rashtriya Raksha University (RRU).[12] This 12-day exercise aims to equip cybersecurity professionals and leaders with advanced skills in cyber defence, incident response, and strategic decision-making to address evolving threats.
- The Bengaluru Metro Rail Corporation Limited (BMRCL) is set to establish a dedicated Security Operations Centre (SOC) to counter cyber threats, becoming the first metro operator in India to do so.[13] The SOC aims to enhance preparedness against potential cyberattacks, leveraging AI and machine learning to tackle automated threats. According to a senior BMRCL official, it will provide comprehensive network visibility by collecting logs from all devices.
- A critical defence unit was targeted in a ransomware attack in 2023, as revealed in the 2023-24 annual report of the Department of Personnel and Training (DoPT) released in November.[14] The report highlights vital cybercrime cases investigated by the Central Bureau of Investigation (CBI), including the ransomware attack, a data breach affecting millions of Indian users, a malware incident in a Ministry, and a large-scale DDoS attack on critical infrastructure and airports.
- The Telecom Cyber Security Rules, 2024, enforced by the Department of Telecommunications in November, require telecom entities to report cybersecurity incidents to the central government within six hours of detection.[15] This aligns with the six-hour timeline specified in the 2022 CERT-In directions. Entities must also provide details of the affected system and a description of the incident within this period. Released for public consultation on August 29, the rules mandate telecom operators to adopt measures to prevent and address cyber threats.

[1] The Phnom Penh Post, Ministry clarifies no tolerance for scam centres, calls for international cooperation, 7 November 2024, https://www.phnompenhpost.com/national/ministry-clarifies-no-tolerance-for-scam-centres-calls-for-international-cooperation

[2] Meta, Cracking Down On Organized Crime Behind Scam Centers, 21 November 2024, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers

[3] Infosecurity Magazine, T-Mobile Breached in Major Chinese Cyber-Attack on Telecoms, 19 November 2024, https://www.infosecurity-magazine.com/news/tmobile-breached-chinese/

[4] Reuters, South Korea says pro-Russia groups responsible for cyberattacks after North's troop dispatch, 8 November 2024, https://www.reuters.com/world/south-korea-says-pro-russia-groups-responsible-cyberattacks-after-norths-troop-2024-11-08/

[5] The Record, Cyberattack causes credit card readers to malfunction in Israel, 11 November 2024, https://therecord.media/cyberattack-causes-credit-card-readers-in-israel-to-malfunction

[6] The Record, Hungary confirms hack of defense procurement agency, 14 November 2024, https://therecord.media/hungary-defense-procurement-agency-hacked

[7] Voa News, Pakistani religious body declares using VPN is against Islamic law, 15 November 2024, https://www.voanews.com/a/pakistani-religious-body-declares-using-vpn-is-against-islamic-law-/7865991.html

[8] The Indian Express, Rs 11,333 crore lost in just 9 months: A look at the cyber scams that have hit India the worst, 27 November 2024, https://indianexpress.com/article/india/cyber-scams-india-pm-modi-9692771/

[9] Money Control, Pakistan-linked hackers are using Google Drive, Telegram and Slack to target Indian entities, claims report, 5 November 2024, https://www.moneycontrol.com/technology/pakistan-linked-hackers-are-using-google-drive-telegram-and-slack-to-target-indian-entities-claims-report-article-12858567.html

[10] The Times of India, Army steps on the gas for high-tech infusion for futuristic warfare, plans to induct 'domain specialists', 22 November 2024, https://timesofindia.indiatimes.com/india/army-steps-on-the-gas-for-high-tech-infusion-for-futuristic-warfare-plans-to-induct-domain-specialists/articleshow/115574996.cms

[11] Financial Express, Indian Army Launches Internship Program to Engage Young Talent in Emerging Technologies, 22 November 2024, https://www.financialexpress.com/jobs-career/indian-army-launches-internship-program-to-engage-young-talent-in-emerging-technologies-3674057.

[12] Press Information Bureau (PIB), Bharat NCX 2024 Officially Inaugurated: Strengthening Cyber Defense and Strategic Decision-Making Across India, 18 November 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2074256

[13] Money Control, In a first, Bengaluru Metro to set up Security Operations Centre to tackle cyber threats, 5 November 2024, https://www.moneycontrol.com/technology/in-a-first-bengaluru-metro-to-set-up-security-operations-centre-to-tackle-cyber-threats-article-12858477.html

[14] The Hindu, Crucial defence unit was hit by ransomware attack in 2023: DoPT report, 10 November 2024, https://www.thehindu.com/news/national/crucial-defence-unit-was-hit-by-ransomware-attack-in-2023-dopt-report/article68849536.ece.

[15] Hindustan Times, Report cybersecurity cases within 6 hrs: DoT notifies rules, 22 November 2024, https://www.hindustantimes.com/india-news/report-cybersecurity-cases-within-6-hrs-dot-notifies-rules-101732214667359.html