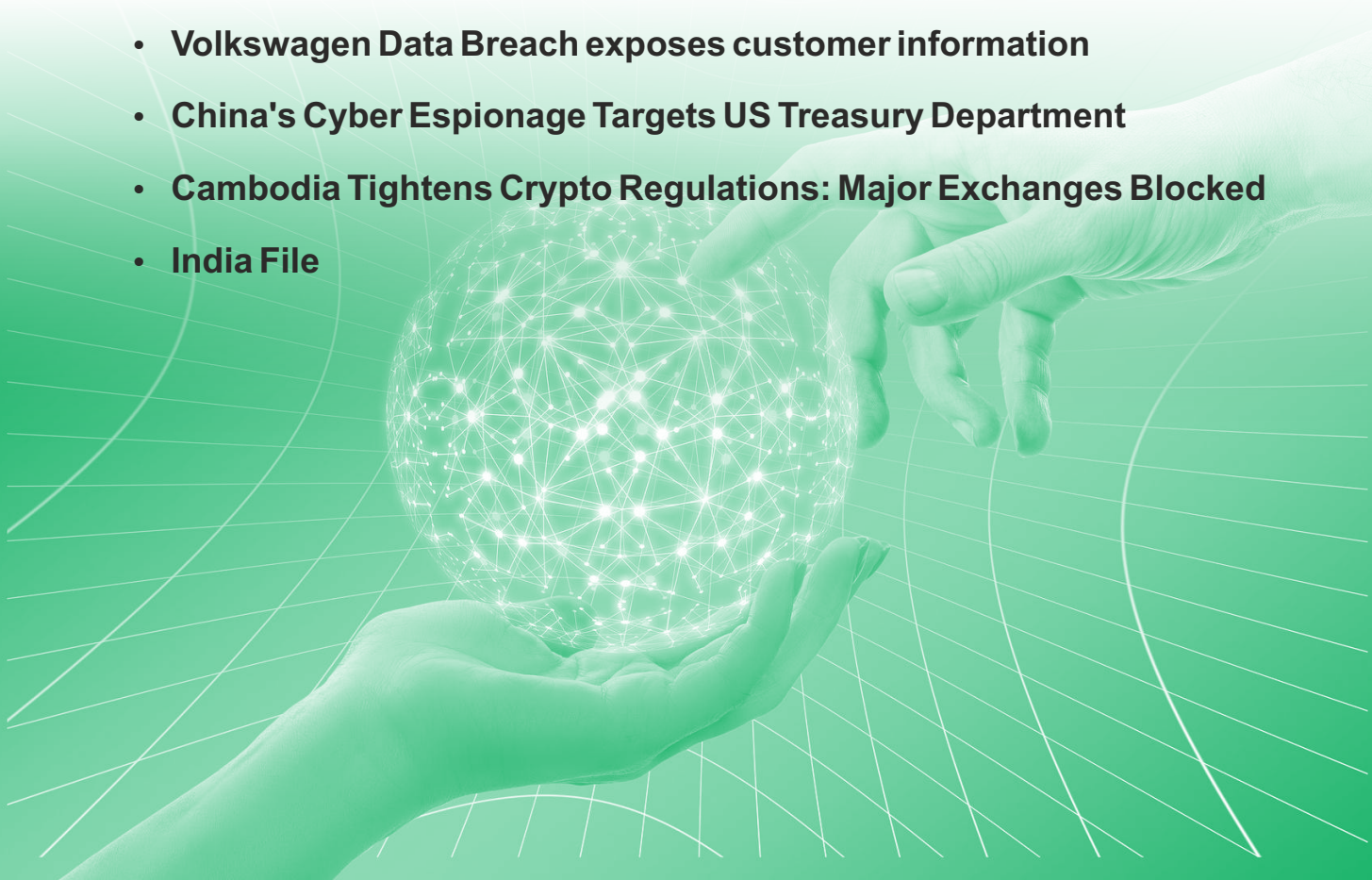
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

January 2025

- December sees uptick in Ransomware attacks
- One of Russia's largest banks taken offline by Ukraine
- Government Agencies and Infrastructure targeted in Italy
- Volkswagen Data Breach exposes customer information
- China's Cyber Espionage Targets US Treasury Department
- Cambodia Tightens Crypto Regulations: Major Exchanges Blocked
- India File



December sees uptick in Ransomware attacks

In early December, it was reported that multinational telecommunications giant BT Group (formerly British Telecom) confirmed a ransomware attack by the Black Basta group targeting its BT Conferencing division.[1] As a result, some servers were taken offline. However, the incident reportedly did not affect BT Group's overall operations or BT Conferencing services. The cybercrime group supported their claims by publishing folder listings and screenshots of documents requested during the company's hiring process. They also added a countdown on their dark web leak site, threatening to release the allegedly stolen data the following week.

In another incident, Electrica Group, a major provider in Romania's electricity distribution and supply sector, recently reported a ransomware attack.[2] Serving over 3.8 million users across the country with electricity supply, maintenance, and energy services, the company confirmed that its SCADA systems, responsible for monitoring and controlling its distribution network, were not affected, according to a statement from the Ministry of Energy.

Namibia's state-owned telecoms company also suffered a ransomware attack, leading to the leak of sensitive customer data, including information reportedly linked to top government officials.[3] Telecom Namibia confirmed that the data was released after it refused to negotiate with a hacker group called Hunters International. The company is now investigating the cause of this significant system breach.

The government of Rhode Island also reported that hackers responsible for a recent ransomware attack on several of the state's digital platforms have begun leaking data stolen during the breach last month.[4]

One of Russia's largest banks taken offline by Ukraine

In early December, Russian users reported difficulties accessing services at Gazprombank, one of the country's largest privately-owned banks, following an alleged cyberattack by Ukraine's military intelligence agency.[5] Website outage tracking data revealed customer complaints about being unable to complete transactions or pay bills via the bank's app or website. Reports indicate that cyber specialists from Ukraine's military intelligence (HUR) successfully launched a powerful distributed denial-of-service (DDoS) attack on Gazprombank's systems.[6] The assault disrupted the bank's online and mobile banking services, causing significant service outages.

Government Agencies and Infrastructure targeted in Italy

Hackers targeted around ten official websites in Italy, including those of the Foreign Ministry and Milan's two airports, temporarily disrupting their operations, according to Italy's cybersecurity agency.[7] The pro-Russian hacker group Noname057 (16) claimed responsibility for the attack on Telegram. A spokesperson for the agency noted that the DDoS attack was likely linked to the pro-Russian group. The spokesperson also stated that the agency promptly assisted the targeted institutions and companies, ensuring the attack's impact was swiftly mitigated.

Volkswagen Data Breach exposes customer information

Volkswagen Group experienced a data breach that exposed the sensitive personal information of approximately 800,000 electric vehicle owners across its brands, including Volkswagen, Audi, Seat, and Skoda.[8] The breach was attributed to a misconfiguration in an Amazon cloud storage system managed by its software subsidiary, Cariad. As a result, personal and location data were left publicly accessible online for several months, leading to the breach. The exposed data from the breach includes vehicle location details, such as when electric vehicles (EVs) were turned on and off, as well as location data, email addresses, phone numbers, and home addresses of car owners.

China's Cyber Espionage Targets US Treasury Department

Chinese hackers remotely accessed several U.S. Treasury Department workstations and unclassified documents after compromising a third-party software service provider.[9] In a letter to lawmakers, the agency revealed that the hackers gained access to a key used by the vendor to secure a cloud-based service that provided remote technical support for Treasury Department Offices (DO) end users. With the stolen key, the attackers bypassed the service's security, gaining remote access to particular Treasury DO user workstations and unclassified documents maintained by those users.[10]

Cambodia Tightens Crypto Regulations: Major Exchanges Blocked

Cambodia has blocked web access to 16 major cryptocurrency exchanges, including Binance, OKX, and Coinbase, in an effort to combat crypto-related crimes.[11] The move is part of the country's strategy to regulate the crypto market. Reports indicate that these exchanges failed to secure the necessary licenses from Cambodia's Securities and Exchange Regulator, which are required for operating within the country.

However, in another significant development, the National Bank of Cambodia (NBC) has issued a directive allowing commercial banks and payment institutions to offer services related to Category 1 crypto assets, such as backed or stable cryptocurrencies.[12] However, unbacked cryptocurrencies like Bitcoin remain prohibited. The directive is part of the country's effort to regulate digital currency operations and businesses, aligning with global financial innovations.

India File

- Ride-hailing platform Rapido has resolved a security vulnerability that exposed the personal information of its auto-rickshaw users and drivers.[13] The flaw could have allowed hackers to access full names, email addresses, and phone numbers via a website form intended for collecting feedback from drivers and users. The issue was linked to one of Rapido's APIs, which was used to retrieve data from the feedback form through a third-party service, leaving the information exposed.
- Thomas Cook India experienced a cyberattack that disrupted its IT systems, prompting the company to shut down the affected infrastructure, according to an exchange filing. The company stated that it immediately took steps to investigate and respond to

the incident, including shutting down compromised systems.[14]

- The Delhi Police's X handle was hacked, marking the sixth cyberattack on the unit's website or social media handles in the past 15 months.[15] However, the breach was short-lived, and the account was restored within an hour. In the latest incident, hackers changed the name, profile photo, and biography of the Delhi Police's X account.

[1] Bleeping Computer, BT unit took servers offline after Black Basta ransomware breach, 4 December 2024, https://www.bleepingcomputer.com/news/security/bt-conferencing-division-took-servers-offline-after-black-basta-ransomware-attack/

[2] Bleeping Computer, Romanian energy supplier Electrica hit by ransomware attack, 9 December 2024, https://www.bleepingcomputer.com/news/security/romanian-energy-supplier-electrica-hit-by-ransomware-attack/

[3] BBC, Sensitive data leaked after Namibia ransomware hack, 17 December 2024, https://www.bbc.com/news/articles/ce3l509e6x7o

[4] The Record, Rhode Island warns of cybercriminals leaking stolen state files as Deloitte works to restore system, 3 January 2025, https://therecord.media/rhode-island-data-breach-deloitte

[5] The Record, Russian users report Gazprombank outages amid alleged Ukrainian cyberattack, 6 December 2024 , https://therecord.media/gazprombank-outages-russia-ukraine-claims-cyberattack

[6] The Kyiv Independent, Ukrainian intelligence hackers disrupt Russia's Gazprombank, source says, 5 December 2024, https://kyivindependent.com/hur-gazprombank-cyberattack/

[7] Reuters, Cyber attack on Italy's Foreign Ministry, airports claimed by pro-Russian hacker group, 28 December 2024, https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/

[8] Dark Reading, Volkswagen Breach Exposes Data of 800K EV Customers, 2 January 2025, https://www.darkreading.com/cyberattacks-data-breaches/volkswagen-breach-exposes-data-of-800k-customers

[9] NPR, Treasury says Chinese hackers remotely accessed documents in 'major' cyber incident, 31 December 2024, https://www.npr.org/2024/12/31/nx-s1-5243850/china-hacking-treasury-cyber-security

[10] Reuters, US Treasury says Chinese hackers stole documents in 'major incident', 1 January 2025, https://www.reuters.com/technology/cybersecurity/us-treasurys-workstations-hacked-cyberattack-by-china-afp-reports-2024-12-30/

[11] Binance, Cambodia Bans 16 Major Exchanges Including Binance, OKX and Coinbase, 3 December 2024, https://www.binance.com/en-KZ/square/post/17060445719561

[12] The Phnom Penh Post, Regulated cryptocurrency assets approved for operation in Cambodia, 27 December 2024, https://www.phnompenhpost.com/business/regulated-cryptocurrency-assets-approved-for-operation-in-cambodia#.

[13] The Indian Express, Rapido fixes security flaw that exposed data of users and drivers, 20 December 2024, https://indianexpress.com/article/technology/tech-news-technology/rapido-security-flaw-exposed-personal-data-9736077/

[14] Business Standard, Thomas Cook hit by cyberattack, temporarily shuts down affected IT systems, 31 December 2024, https://www.business-standard.com/companies/news/thomas-cook-shut-down-cyber-attack-it-infrastructure-bse-124123100576_1.html

[15] Hindustan Times, Delhi Police suffers sixth cyber attack in 15 months, 12 December 2024, https://www.hindustantimes.com/cities/delhi-news/delhi-police-suffers-sixth-cyber-attack-in-15-months-101733940285185.html