MANOHAR PARRIKAR

idsa

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

CYBER *Digest*

October 2024

- Takeaways from Prime Minister Modi's visit to US
- Transport for London Hit by Major Cyber Attack
- New Advisory Unveils Russian Military Cyber Tactics
- Stolen Campaign Data Sent to Political Rivals by Iranian Hackers
- Cyber Attack Hits Kuwait's Health Infrastructure
- Cyber Attack Targeting AFP's IT Systems
- DDoS Attacks against Austrian and Taiwan's websites
- India File

Takeaways from Prime Minister Modi's visit to US

During his visit to the U.S., Prime Minister Modi and President Biden endorsed several new initiatives, including mechanisms to strengthen cyberspace cooperation through the bilateral cybersecurity dialogue.[1] The leaders praised ongoing efforts to enhance cooperation in advanced domains, including space and cyber, and expressed optimism that the November 2024 bilateral cyber engagement will further strengthen the U.S.-India cyber cooperation framework. New areas of collaboration will focus on threat information sharing, cybersecurity training, and joint efforts to mitigate vulnerabilities in energy and telecommunications networks.

Transport for London Hit by Major Cyber Attack

Transport for London (TfL) first detected issues with its cybersecurity in the first week of September.[2] It later confirmed that certain customer data had been compromised, including names, addresses, contact information, and bank details. The organization reported that it took immediate action, including restricting access to some live travel information services on its apps and website.[3] It also temporarily disabled the option for passengers to view their journey history for trips paid with contactless cards.

New Advisory Unveils Russian Military Cyber Tactics

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) have determined that cyber actors linked to the Russian General Staff's Main Intelligence Directorate (GRU), specifically the 161st Specialist Training Center (Unit 29155), have been conducting computer network operations targeting global entities for espionage, sabotage, and reputational damage since at least 2020.[4] GRU Unit 29155 cyber actors initiated the deployment of the destructive WhisperGate malware against several Ukrainian organizations as early as January 13, 2022.

Stolen Campaign Data Sent to Political Rivals by Iranian Hackers

According to the FBI and two other government agencies, Iranians sent "unsolicited emails" containing stolen, non-public material from former President Donald Trump campaign to individuals connected with the Biden campaign.[5] The FBI, along with officials from the Office of the Director of National Intelligence (ODNI) and the Cybersecurity and Infrastructure Security Agency (CISA), reported that there is no evidence suggesting that recipients associated with President Joe Biden's campaign responded to the emails. Government officials condemned these actions as part of an effort to sow discord and undermine confidence in the electoral process.

Cyber Attack Hits Kuwait's Health Infrastructure

Kuwait's Health Ministry experienced a cyberattack that disrupted systems at several hospitals and affected the Sahel healthcare app.[6] Following the attack, the Ministry of Health's website also went down. The government utilized backup systems to restore operations at the Kuwait Cancer Control Center, as well as in the offices managing the national health insurance and expatriate check-up systems. The ministry confirmed that the hackers were prevented from accessing essential databases. However, it stated that certain systems had to be shut down to implement necessary updates.

Cyber Attack Targeting AFP's IT Systems

AFP confirmed that its IT systems were targeted in a cyberattack during the last week of September.[7] The agency stated that the attack impacted a portion of its delivery service to clients. The identity of the attackers and the motives behind the incident remain unclear. AFP's technical teams are addressing the situation with assistance from the French National Agency for IT Systems Security (ANSSI). No group has claimed responsibility for the incident.

DDoS Attacks against Austrian and Taiwan's websites

Pro-Russia hacker groups have claimed responsibility for disrupting numerous Austrian websites ahead of the country's general election later this month.[8] The groups, identified as NoName057(16) and OverFlame, announced that they launched distributed denial-of-service (DDoS) attacks targeting websites belonging to the Austrian government, airports, financial services, and a stock exchange. Two of Austria's political parties, the OVP and SPO, also reported that their websites experienced temporary outages recently due to DDoS attacks.

In a separate incident, NoName057 launched a DDoS attack on the Taiwanese government in retaliation for President William Lai's remarks suggesting that China should engage in a territorial dispute with Russia.[9] Reports indicate that NoName057 typically targets countries that support Ukraine, focusing on their financial sectors, public infrastructure, communication services, and media outlets.

India File

- The Tamil Nadu government recently unveiled its Cyber Security Policy 2.0, outlining measures to safeguard government assets.[10] The policy includes guidelines and Standard Operating Procedures (SOPs) for auditing, compliance, and monitoring cyber threats and attacks. The Cyber Security Policy 2.0, issued on August 23 this year, is set to replace the Tamil Nadu Cyber Security Policy 2020, which was introduced in September 2020. The updated policy includes contributions from the Centre for Development of Advanced Computing (C-DAC), Indian Institute of Technology Madras (IIT-M), and the Tamil Nadu e-Governance Agency, among others.

- In a significant move to strengthen cybersecurity, the Ministry of Home Affairs has announced several new initiatives.[11] These include the training of 5,000 'cyber commandos,' the establishment of a web-based data registry, a portal for sharing cybercrime information, and the creation of a national registry of suspects to help prevent future crimes. The Minister of Home Affairs also announced the establishment of a Cyber Fraud

Mitigation Centre (CFMC), which will include representatives from major banks, financial intermediaries, payment aggregators, telecom service providers, IT intermediaries, and law enforcement agencies from states and Union Territories.

- The Central Bureau of Investigation (CBI) has arrested 26 individuals in Pune, Hyderabad, and Visakhapatnam as part of a major operation against a tech-enabled crime syndicate.[12] The crackdown spanned 32 locations and uncovered a network that targeted victims overseas. In the process, the CBI identified 170 suspects believed to be involved in illegal online activities through four call centres. The investigation into the cybercrime network is being carried out in close coordination with the United States' Homeland Security Investigations and other international law enforcement agencies.

- The Minister of Home Affairs has launched an online 'suspect registry' containing data on 1.4 million cybercriminals involved in financial fraud and various cybercrimes.[13] Developed by the Indian Cyber Crime Coordination Centre (I4C), the registry is accessible to states, Union Territories, and central investigation and intelligence agencies. The collaboration with banks and financial intermediaries, aims to strengthen fraud risk management within the country's financial system.

- The National e-Governance Division (NeGD), under the Ministry of Electronics and Information Technology (MeitY), Government of India, organized a 'Chief Information Security Officer (CISO) Workshop on Cyber Security' in New Delhi on September 18, 2024. As part of the "Cyber Surakshit Bharat" initiative, the workshop saw the participation of over 250 CISOs, Deputy CISOs, frontline IT officers, and senior officials from various Ministries and State Departments.[14]

- In a major hacking incident, Star Health, one of India's largest health insurance providers, has suffered a breach compromising the personal details of over 31 million customers, including sensitive medical records.[15] The stolen data has been made publicly accessible through chatbots on the Telegram messaging app. Star Health has confirmed the data breach and is working with law enforcement authorities to investigate the incident.

- An assessment revealed that citizens in India are losing between ₹1.3 lakh and ₹1.5 lakh to cybercriminals every minute.[16] These estimates were shared by the Deputy Secretary of the Telangana IT and Electronics Department during the ISACA Annual Cyber Security Conference held in Madhapur, Hyderabad. The conference brought together industry leaders, including bureaucrats, bankers, consultants, and technology experts, who shared insights on the future of cybersecurity in the age of AI and strategies for managing and protecting data privacy.

- According to reports, an investigation into an online gaming app has led the Enforcement Directorate (ED) to uncover a Rs. 400-crore fraud involving Chinese nationals.[17] The ED has frozen the accounts of several Chinese individuals connected to the online gaming app Fiewin, with approximately Rs. 25 crore now frozen. The investigation revealed that the Chinese nationals were orchestrating this fraud with assistance from local connections in India.

- The government has designated the National Security Council Secretariat (NSCS) as the nodal agency for addressing the rising cyber security threats.[18] According to the notification, specific responsibilities have been assigned to various ministries for enhanced clarity. The telecom department will oversee telecom network security, the IT department will handle cyber security, and the home ministry will focus on combating cybercrime.

[1] US Embassy and Consulates in India, Joint Fact Sheet: The United States and India Continue to Expand Comprehensive and Global Strategic Partnership, https://in.usembassy.gov/joint-fact-sheet-the-united-states-and-india-continue-to-expand-comprehensive-and-global-strategic-partnership/

[2] BBC, TfL cyber attack: What you need to know, 28 September 2024, https://www.bbc.com/news/articles/ceqn7xng7lpo

[3] BBC, TfL still affected by 'ongoing cyber incident', 6 September 2024, https://www.bbc.com/news/articles/cwyjezrne3go

[4] Australian Signals Directorate, Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, 6 September 2024, https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/russian-military-cyber-actors-target-us-and-global-critical-infrastructure

[5] *NBC News,* Iranian hackers sent stolen Trump campaign info to Biden campaign associates, FBI says, 19 September 2024, https://www.nbcnews.com/politics/politics-news/fbi-says-iranian-hackers-sent-stolen-trump-campaign-info-biden-campaig-rcna171759

[6] The Record, Kuwait Health Ministry restoring systems after cyberattack takes down hospitals, healthcare app, 27 September 2024, https://therecord.media/kuwait-ministry-restoring-systems-cyberattack

[7] The Record, Agence France-Presse says cyberattack targeted IT systems, 30 September 2024, https://therecord.media/afp-cyberattack-targeted-it-systems

[8] The Record, Pro-Russia hackers aim DDoS campaign at Austrian websites ahead of elections, 24 September 2024, https://therecord.media/austria-websites-ddos-incidents-pro-russia-hacktivists

[9] Taipei Times, Pro-Russian hackers launch DDoS attack over Lai comments: cybersecurity firm, 10 September 2024, https://www.taipeitimes.com/News/taiwan/archives/2024/09/10/2003823576

[10] *The Hindu,* Tamil Nadu unveils its Cyber Security Policy 2.0, 7 September 2024, https://www.thehindu.com/news/national/tamil-nadu/tamil-nadu-unveils-its-cyber-security-policy-20/article68613913.ece

[11] *NDTV,* 5,000 'Cyber Commandos', Online Registry: Centre's Steps To Curb Cybercrime, https://www.ndtv.com/india-news/5-000-cyber-commandos-online-registry-centres-steps-to-curb-cybercrime-6533702.

[12] *The Hindu*, Operation Chakra-III: CBI arrests 26 more ‘cybercriminals’, 30 September 2024, https://www.thehindu.com/news/national/operation-chakra-iii-cbi-arrests-26-more-cybercriminals/article68700515.ece.

[13] *Business Standard,* India launches online 'suspect registry', 1.4 mn listed for financial fraud, 12 September 2024, https://www.business-standard.com/india-news/india-launches-online-suspect-registry-1-4-mn-listed-for-financial-fraud-124091200207_1.html

[14] PIB, Ministry of Electronics and Information Technology (MeitY) organizes 'CISO workshop on Cyber Security' as part of “Cyber Surakshit Bharat” initiative, 18 September 2024, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2056193

[15] The 420, CEO Must Be Held Accountable: Star Health Insurance Hacked, 3.1 Crore Sensitive Customer Records for Sale on Telegram, 20 September 2024, https://www.the420.in/ceo-must-be-held-accountable-star-health-insurance-hacked-3-1-crore-sensitive-customer-records-for-sale-on-telegram

[16] *The Hindu,* Indians lose ₹1.5 lakh to cyber criminals every minute: official, 28 September 2024, https://www.thehindu.com/news/cities/Hyderabad/indians-lose-15-lakh-to-cyber-criminals-every-minute-official/article68693674.ece.

[17] *NDTV,* An Online Gaming App, Promise Of Big Prizes And A ₹ 400-Crore Fraud, 26 September 2024, https://www.ndtv.com/india-news/fiewin-enforcement-directorate-how-gaming-app-linked-to-chinese-nationals-was-used-for-rs-400-crore-fraud-6652673#pfrom=home-ndtv_topscroll

[18] *The Times of India,* NSCS takes charge of cybersecurity oversight in India, 29 September 2024, https://timesofindia.indiatimes.com/india/nscs-takes-charge-of-cybersecurity-oversight-in-india/articleshow/113773830.cms.