MANOHAR PARRIKAR idsa

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

CYBER *Digest*

November 2024

- Counter Ransomware Initiative issues joint statement
- Internet Archive hit by cyberattack
- Canada issues statement warning Chinese-linked reconnaissance
- US charges threat actors amidst increasing cybersecurity incidents
- Cyberattacks targeting Iran and Israel amidst escalation
- Prime Minister cautions citizens about “digital arrest”
- INTERPOL operation targets cybercriminals in West Africa
- Cyprus government portal foils cyberattack
- India File

Counter Ransomware Initiative issues joint statement

The 68 members of the International Counter Ransomware Initiative (CRI) convened in Washington, D.C., for the Fourth CRI gathering.[1] Members reaffirmed their commitment to strengthening collective resilience against ransomware, supporting affected members, holding perpetrators accountable, preventing safe havens for ransomware actors, countering the use of virtual assets in ransomware schemes, partnering with the private sector for guidance, and building international alliances to more effectively combat ransomware globally.

The CRI also released guidance for organisations on handling ransomware incidents.[2] While non-binding and not superseding any specific laws within CRI member jurisdictions, this guidance aims to reduce the overall impact of ransomware attacks on organisations by minimising disruption and costs to businesses, reducing the number of ransoms paid by victims, and lowering the ransom amounts where victims opt to pay.

Internet Archive hit by cyberattack

The Internet Archive experienced a significant data breach that exposed the personal information of 31 million users, including email addresses, screen names, and encrypted passwords. Cybersecurity experts are advising users to change their passwords immediately.[3] This breach has sparked concerns over data privacy and the security of the popular digital library, widely recognized for its Wayback Machine. The founder of the Internet Archive acknowledged the data breach and the Distributed Denial-of-Service (DDoS) attacks impacting the platform.

Canada issues statement warning Chinese-linked reconnaissance

The Canadian Centre for Cyber Security, part of the Communications Security Establishment Canada (CSE), has urged Canadian organizations to stay vigilant and strengthen their defenses against reconnaissance scanning, a persistent low-level cyber threat in Canada.[4] The Cyber Centre warned that a sophisticated, state-sponsored actor from the People's Republic of China has conducted extensive reconnaissance scanning throughout 2024, targeting numerous Canadian domains. Most affected organizations include Government of Canada departments and agencies, federal political parties, and the House of Commons and Senate.

US charges threat actors amidst increasing cybersecurity incidents

A federal grand jury in the US has indicted two Sudanese brothers, Ahmed and Alaa Salah Yousif Omer, for allegedly operating Anonymous Sudan, a major cyberattack-for-hire group.[5] They are accused of conducting around 35,000 denial-of-service attacks in a year, targeting high-profile organisations worldwide, including Microsoft, PayPal, the Pentagon, and a hospital, as part of an ideologically driven extortion campaign.

In another incident, American Water Works, a provider of water and wastewater services to over 14 million people, reported a breach of its computer networks.[6] This attack forced the company to suspend customer billing, and its customer portal, MyWater, was taken offline.

Georgia's Secretary of State office was targeted in an attempted cyberattack aimed at crashing the absentee voting website.[7] Officials detected the attack after noticing a surge of over 420,000 access attempts from around the world in a coordinated effort to overload the site. Security experts successfully thwarted the attack.

Cyberattacks targeting Iran and Israel amidst escalation

Reports indicate that Iran faced a massive cyberattack, disrupting operations across all three branches of government- the judiciary, legislature, and executive, as well as targeting nuclear facilities.[8] Firouzabadi, the former secretary of Iran's Supreme Council of Cyberspace, confirmed the attacks.

In a separate incident, just before Israel launched a retaliatory strike on Iran, Iranian defense radar systems were reportedly breached, causing their screens to freeze, according to reports.[9] This breach is said to have limited Iran's ability to intercept targets, enabling the Israeli air force to penetrate Iranian airspace. Israel also reportedly carried out a preliminary strike on radar installations in Syria to disable Iran's defenses ahead of an attack.

Unknown hackers have also reportedly attempted to infect Israeli organizations with Wiper malware distributed through phishing emails impersonating the cybersecurity firm ESET.[10] The malicious emails, appearing to be from ESET, claimed that the recipient's device was targeted by a state-sponsored threat actor and included a link to a ZIP file allegedly hosted on ESET's servers that promised recovery tools.

Prime Minister cautions citizens about "digital arrest"

According to projections from the Indian Cyber Crime Coordination Centre (I4C) under the Union Ministry of Home Affairs (MHA), Indians are expected to lose more than Rs 1.2 lakh crore to cyber fraud in the coming year.[11] Reports indicates that mule bank accounts, which are used to facilitate illegal transactions and money laundering, are a major factor in online financial scams that could potentially drain 0.7% of the country's GDP. Also, according to reports, Indians have lost Rs. 120.30 crore to "digital arrest" frauds in the first quarter of 2024.[12] Many perpetrators of these frauds operate from three neighbouring Southeast Asian countries: Myanmar, Laos, and Cambodia. In a recent episode of his radio program Mann Ki Baat, Prime Minister Narendra Modi also highlighted the issue of "digital arrests" and cautioned the public about this scam.

INTERPOL operation targets cybercriminals in West Africa

INTERPOL has announced the arrest of eight individuals in a major crackdown on cybercrime, disrupting criminal operations in Côte d'Ivoire and Nigeria.[13] The arrests were part of INTERPOL's Operation Contender 2.0, an initiative focused on combating cyber-enabled crime in West Africa through enhanced international intelligence sharing. Operation Contender 2.0 marks the latest phase of ongoing efforts under INTERPOL's African Joint Operation against Cybercrime (AFJOC). Launched in 2021, AFJOC was created in response to intelligence from authorities and private partners on cybercriminal syndicates in Africa, especially in West

Africa. The initiative targets various cyber threats, including business email compromise (BEC) schemes, a form of phishing where criminals exploit trust to deceive executives into transferring funds or revealing sensitive information.

Cyprus government portal foils cyberattack

Cyprus has confirmed thwarting a cyberattack aimed at disrupting access to the government's central online portal, following similar attacks targeting state-run utilities and the Cypriot subsidiary of a Greek energy company.[14] The Deputy Ministry of Research, Innovation, and Digital Policy stated that a swift, coordinated response by authorities prevented major disruption. The distributed denial-of-service (DDoS) attack briefly affected the main government portal, gov.cy, for only a few minutes without impacting ministry or service websites.

India File

- Uttarakhand faced a significant cyberattack that disabled its essential IT infrastructure, rendering over 90 government websites, including the Chief Minister's helpline, entirely inaccessible.[15] This disruption impacted the state's entire IT system, affecting both public services and internal government functions. The attack also disrupted critical e-office systems across various districts, bringing government operations to a complete standstill. A case was subsequently filed against an unidentified individual at the state cyber police station in Dehradun.[16] The suspect allegedly hacked into the Information Technology Development Agency (ITDA) server and demanded a ransom.
- According to reports, the Indian government is collaborating with around 20 countries interested in adopting India's digital public infrastructure (DPI), which was developed specifically for Indian citizens. Nations implementing this infrastructure for public services include Nepal, Sri Lanka, Singapore, the Maldives, France, and Bhutan.
- In Tamil Nadu, cyber financial frauds led to substantial losses of Rs 1,116 crore between January and September 2024, as reported by the state's cyber crime police.[17] This alarming amount underscores the rising cybercrime threat in the region and highlights the need for heightened awareness and quick reporting. The cybercrime wing also reported that it successfully froze Rs 526 crore through both automated and manual interventions.
- Star Health, India's largest health insurer, reported receiving a $68,000 ransom demand from a hacker following a breach involving customer data and medical records.[18] Star Health Insurance suffered a significant data breach, which the company has confirmed and is actively investigating.[19] Reports indicate that this breach may have compromised the personal information of 31 million customers.
- India has emerged as one of the top ransomware targets in the Asia-Pacific region, ranking second in successful attacks, according to a Threat

Intelligence Report.[20] Covering trends from April 2023 to April 2024, the report reveals a global increase in ransomware incidents, underscoring the growing risk to critical sectors. The report also highlighted that as AI-driven attacks increase, vulnerabilities in India's digital defenses are widening, leading to calls for stronger cybersecurity measures.

- To enhance India's cybersecurity capabilities, the Indian Computer Emergency Response Team (CERT-In) and the Information Sharing and Analysis Center (ISAC) have partnered to issue joint certifications for Cohort 6 of the National Cyber Security Scholar Program (NCSSP).[21] This program aims to cultivate credible and ethical cybersecurity leaders who prioritize national cybersecurity in their careers.

- The Ministry of Defence has designated a senior army officer, the Additional Directorate General (ADG) of Strategic Communication in the Indian Army, as the "nodal officer" authorized to issue notices, including takedown requests, to social media platforms regarding illegal content related to the Indian Army.[22] This authority is granted under Section 79(3)(b) of the Information Technology Act. Previously, the Indian Army depended on the Ministry of Electronics and Information Technology (MeitY) to have unlawful content related to the army removed or blocked.

- The inaugural ASEAN-India Track 1 Cyber Policy Dialogue took place on October 16, 2024, in Singapore. It was co-chaired by Mr. Amit A. Shukla, Joint Secretary of the Cyber Diplomacy Division, Ministry of External Affairs, and Mr. Jeffrey Ian Dy, Undersecretary for Infrastructure Management, Cybersecurity, and Upskilling from the Philippines.[23] During the dialogue, participants shared insights on the cyber threat landscape, national cybersecurity policies, threat assessments, and recent ICT developments at the United Nations. They also discussed cooperation in capacity building and training to pinpoint specific areas for collaborative action.

- India and Singapore held their first Cyber Policy Dialogue on October 17, 2024, in Singapore, co-chaired by Mr. Amit A. Shukla and Mr. David Koh, Chief Executive of Singapore's Cyber Security Agency.[24] The dialogue covered the cyber threat landscape, national cybersecurity strategies, and global cyber governance developments under the UN. They also explored bilateral cooperation in cyber threat response, critical infrastructure protection, and joint capacity-building initiatives.

- During the first India-Italy Bilateral Cyber Dialogue, both sides shared perspectives on the cyber threat landscape and national cybersecurity strategies.[25] They discussed critical infrastructure protection, capacity-building initiatives, and collaboration in multilateral forums, particularly on recent UN developments in cybersecurity. Both countries agreed to strengthen cooperation between their agencies to promote a safe and resilient cyberspace.

[1] The White House, International Counter Ransomware Initiative 2024 Joint Statement, 2 October 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/02/international-counter-ransomware-initiative-2024-joint-statement/

[2] Gov.uk, CRI guidance for organisations during ransomware incidents, 2 October 2024, https://www.gov.uk/government/publications/cri-guidance-for-organisations-during-ransomware-incidents/cri-guidance-for-organisations-during-ransomware-incidents

[3] NDTV, Internet Archive Hit By "Catastrophic" Attack, 31 Million Passwords Stolen, 11 October 2024, https://www.ndtv.com/world-news/internet-archive-hit-by-catastrophic-attack-31-million-passwords-stolen-6763970

[4] Government of Canada, Statement on People's Republic of China reconnaissance of Canadian systems, 25 October 2024, https://www.cyber.gc.ca/en/news-events/statement-peoples-republic-china-reconnaissance-canadian-systems

[5] CBS News, 2 Sudanese brothers charged with running cyberattack-for-hire gang, 16 October 2024, https://www.cbsnews.com/news/2-sudanese-nationals-charged-cyber-attack-for-hire-gang/

[6] CBS News, Water supplier American Water Works says systems hacked, 8 October 2024, https://www.cbsnews.com/news/security-hack-breach-american-water-works.

[7] CBS News, Georgia secretary of state's office says it repelled cyberattack, 23 October 2024, https://www.cbsnews.com/news/georgia-secretary-of-state-office-cyberattack/

[8] News18, Iran Hit By 'Heavy Cyberattacks' Targeting Its Nuclear Facilities Amid Middle East Tensions, 12 October 2024, https://www.news18.com/world/iran-hit-by-heavy-cyberattacks-targeting-its-nuclear-facilities-amid-middle-east-tensions-9083699.html

[9] The Jerusalem Post, Radar systems in Iran breached prior to Israel's Saturday counter-strike – report, 28 October 2024, https://www.jpost.com/breaking-news/article-826414

[10] The Record, Hackers reportedly impersonate cyber firm ESET to target organizations in Israel, 18 October 2024, https://therecord.media/hackers-impersonate-eset-wiper-malware

[11] The Hindu, Cyberfraud losses could amount to 0.7% of GDP, projects Ministry’s study, 24 October 2024, https://www.thehindu.com/sci-tech/technology/cyber-fraud-losses-could-amount-to-07-of-gdp-mha-study-projects/article68788093.ece#:~:text=Indians%20are%20likely%20to%20lose,of%20Home%20Affairs%20(MHA)

[12] The Indian Express, Indians lost Rs 120 crore in digital arrest frauds in January-April 2024, 28 October 2024, https://indianexpress.com/article/india/indians-lost-rs-120-crore-in-digital-arrest-frauds-in-january-april-2024-9641952/

[13] INTERPOL, Arrests in international operation targeting cybercriminals in West Africa, 1 October 2024, https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa.

[14] AP, Cyprus thwarted a digital attack against the government’s main online portal, 21 October 2024, https://apnews.com/article/cyprus-cyber-digital-attack-a5971b2387269a8c154a09998e3697f5

[15] The 420, Cyber Attack Cripples Uttarakhand Government IT System, Halts Entire Digital Operations, 4 October 2024, https://www.the420.in/uttarakhand-cyber-attack-90-govt-websites-down-cm-helpline-crisis/

[16] The Times of India, Malware attack: Case against unidentified person for ‘hacking ITDA server to lock files, demad ransom’, 8 October 2024, https://timesofindia.indiatimes.com/city/dehradun/ransomware-attack-on-itda-server-cybercriminals-demand-payment-after-breaching-186-government-websites/articleshow/114056563.cms

[17] India Today, Tamil Nadu cyber scam victims lose over Rs 1000 crore from January to September, 11 October 2024, https://www.indiatoday.in/india/tamil-nadu/story/cyber-financial-crime-frauds-1116-crore-loss-tamil-nadu-january-september-2024-2615454-2024-10-11

[18] Reuters, India's Star Health says it received $68,000 ransom demand after data leak, 12 October 2024, https://www.reuters.com/world/india/indias-star-health-says-it-received-68k-ransom-demand-after-data-leak-2024-10-12.

[19] India Today, Star Health insurance hack led to personal data of 31 million customers being compromised: Story in 5 points, 11 October 2024, https://www.indiatoday.in/technology/features/story/star-health-insurance-hack-led-to-personal-data-of-31-million-customers-being-compromised-story-in-5-points-2615354-2024-10-11

[20] Business Standard, India second highest target for ransomware attacks in Asia Pacific: Report, 15 October 2024, https://www.business-standard.com/india-news/india-second-highest-target-for-ransomware-attacks-in-asia-pacific-report-124101500791_1.html

[21] The Print, CERT-In and ISAC Collaborate to Develop focussed pool of Cybersecurity Leaders through the National Cyber Security Scholar Program (NCSSP), 18 October 2024, https://theprint.in/ani-press-releases/cert-in-and-isac-collaborate-to-develop-focussed-pool-of-cybersecurity-leaders-through-the-national-cyber-security-scholar-program-ncssp/2318021/

[22] Hindustan Times, Army can now directly issue notices to remove online posts, 31 October 2024, https://www.hindustantimes.com/india-news/army-can-now-directly-issue-notices-to-remove-online-posts-101730313177838.html

[23] Government of India (GoI), Ministry of External Affairs (MEA), First ASEAN-India Track 1 Cyber Policy Dialogue, 16 October 2024, https://www.mea.gov.in/press-releases.htm?dtl/38428/First+ASEANIndia+Track+1+Cyber+Policy+Dialogue

[24] GoI, MEA, First Cyber Policy Dialogue between India and Singapore, 18 October 2024, https://www.mea.gov.in/press-releases.htm?dtl/38435/First+Cyber+Policy+Dialogue+between+India+and+Singapore.

[25] GoI, MEA, First India-Italy Bilateral Cyber Dialogue, 25 October 2024, https://www.mea.gov.in/press-releases.htm?dtl/38468/First+IndiaItaly+Bilateral+Cyber+Dialogue.