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

CYBER *Digest*

September 2024

- Chinese Hackers Breach Internet Firms in US and India
- New appointments in US Cybersecurity Leadership
- Olympic venue stuck by Ransomware
- FBI ramps up efforts to combat election interference
- UN Cybercrime Convention Set for Adoption by General Assembly
- CCP-Backed Sources Push Pro-China Content on TikTok
- Malaysia Introduces Data Breach Notification System
- Ukrainian hackers breach servers of Russian TV channels
- India File

Chinese Hackers Breach Internet Firms in US and India

According to reports, the state-sponsored Chinese hacking group Volt Typhoon is exploiting a vulnerability in a California-based startup's product to hack American and Indian internet companies.[1] Volt Typhoon has breached four U.S. firms, including internet service providers, and one Indian company through a flaw in a Versa Networks server product. Versa, which develops software for managing network configurations, recently announced the bug and provided a patch along with other mitigations. This revelation heightens concerns about the vulnerability of U.S. critical infrastructure to cyberattacks.

New appointments in US Cybersecurity Leadership

The Cybersecurity and Infrastructure Security Agency (CISA) has appointed Lisa Einstein as its first Chief Artificial Intelligence Officer.[2] Since 2023, Einstein has been leading CISA's AI initiatives as the Senior Advisor for AI, and since 2022, she has also served as the Executive Director of the CISA Cybersecurity Advisory Committee. CISA, which operates under the Department of Homeland Security, created this new role in response to White House directives requiring all government agencies to designate a senior official to oversee their AI systems.[3]

In a related development, the Senate has confirmed Michael Sulmeyer as the Assistant Secretary of Defense for Cyber Policy at the Pentagon, marking the first time this position has been filled. Sulmeyer previously served as the principal cyber advisor to the Secretary of the Army, where he was involved in cyber readiness and strategic initiatives. His extensive background includes roles in the Office of the Secretary of Defense, the National Security Council, and Cyber Command.[4] Outside of his government roles, Sulmeyer led the Cybersecurity Project at the Belfer Center for Science and International Affairs at Harvard Kennedy School.[5]

Olympic venue stuck by Ransomware

Cybercriminals targeted the system used to centralize financial data for brands at various institutions in first week of August, demanding a ransom and threatening to leak financial information, according to sources.[6] France's national cybersecurity agency, ANSSI, confirmed it had been alerted to the incident, noting that the compromised systems were not related to the Olympic games.

The Grand Palais, which was an Olympic venue for fencing and martial arts, acknowledged it had been hit by the cyberattack but declined to provide further details. The Grand Palais attack was part of a broader campaign targeting around 40 museums by an unnamed organized gang.[7] The group also threatened to release financial data if their ransom demands are not met within 48 hours, according to reports. Recent developments reveal that the Brain Cipher ransomware group has claimed responsibility for the incident, threatening to release 300 GB of data.[8]

FBI ramps up efforts to combat election interference

The FBI has announced an investigation into hacking attempts targeting both the Trump and Biden-Harris campaigns.[9] The

probe includes efforts to breach the accounts of Biden-Harris campaign staffers and a former advisor to former President Donald Trump. According to reports, it remains unclear whether the attempts to hack Biden's staff were successful.

In a separate operation, the FBI has dismantled the globally active hacking group Radar/Dispossessor.[10] The takedown involved seizing servers in the US, UK, and Germany, effectively crippling the group's ability to carry out attacks. This criminal ransomware group is reported to have targeted 43 companies, including those in India, across sectors such as healthcare and transport.

UN Cybercrime Convention Set for Adoption by General Assembly

On August 8, 2024, after more than three years of negotiations, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (aka the Ad Hoc Committee on Cybercrime) approved a draft Convention. Marked a significant step in establishing a global legal framework for combating cybercrime.[11] The Committee, proposed by the Russian Federation, was established by the UN General Assembly through Resolution 74/247, which was adopted in December 2019. It held its first meeting only in May 2021 after a delay caused by the Covid pandemic.

The decision to establish the Ad Hoc committee was undertaken amidst rising cybercrime cases, to enhance coordination and cooperation among states in combating the use of ICTs for criminal purposes, including by providing technical assistance to developing countries. The negotiations covered a wide range of issues, including human rights provisions, criminalisation of various cyber offenses, procedural measures, law enforcement, preventive measures, and technical assistance.

Human Rights organisations and tech companies have expressed their concerns that, in its current form, the provisions of the treaty could be misused as a tool for state surveillance and could severely undermine human rights protections and compromise privacy.

The Convention will now proceed to the General Assembly for further consideration and adoption.

CCP-Backed Sources Push Pro-China Content on TikTok

A recent report reveals that TikTok has been promoting pro-China content to influence public opinion in the U.S.[12] The report highlights a link between the platform's usage and the development of pro-Chinese Communist Party (CCP) attitudes among users. It also claims that TikTok's algorithms consistently amplify pro-CCP content while suppressing anti-CCP narratives. User data in the report further suggests that TikTok is intentionally limiting the reach of content critical of the CCP.

Malaysia Introduces Data Breach Notification System

Malaysia has launched a Data Breach Notification system designed to ensure prompt reporting and mitigation of data leaks, aiming to protect citizens from becoming victims of fraud, according to Deputy Communications Minister Teo Nie.[13] Data users will now have to report

any personal data breaches, including hacking threats. The minister also added that law enforcement agencies, regulatory bodies, and other organizations in Malaysia are collaborating to increase public awareness of the system, enforce stricter regulations, and enhance protection against scams.

Ukrainian hackers breach servers of Russian TV channels

Hackers associated with Ukraine's military intelligence agency (HUR) have reportedly breached the servers of several Russian television channels, broadcasting "objective videos about the war in Ukraine."[14] According to reports, HUR's footage was shown three times on prime-time channels including Pervouralsk TV, Eurasia 360, and Eurasia Pervyi Kanal, among others. The affected channels were forced to suspend their broadcasts due to the hack. Both sides have extensively employed cyberattacks throughout the full-scale conflict.

India File

- Researchers have found that a ransomware attack on a digital payment system used by many Indian banks originated from a vulnerability in Jenkins, a popular open-source automation tool for developers.[15] The study, analyzed how attackers exploited CVE-2024-23897, a flaw in the Jenkins Command Line Interface. On July 31, the National Payments Corporation of India (NPCI), which oversees retail payment systems in India, reported that it was addressing a disruption caused by a ransomware attack on a third-party tech provider.
- To address the growing issue of spam calls affecting Indian consumers, the Telecom Regulatory Authority of India (TRAI) has mandated an immediate halt to all voice promotional calls from unregistered senders or telemarketers.[16] Announced in August, this directive seeks to provide much-needed relief to mobile phone users nationwide. The directive requires all access service providers, including telecom operators, to immediately cease facilitating pre-recorded or computer-generated promotional voice calls from unregistered sources.
- Durex India has exposed customers' personal information, including full names, phone numbers, email addresses, shipping addresses, product details, and payment amounts.[17] The breach occurred due to inadequate authentication on its order confirmation page. While the exact number of affected customers is not known, evidence indicates that hundreds of individuals had their information compromised.
- The Karnataka government has unveiled its Cybersecurity Policy 2024, allocating Rs 104 crore to tackle online crime and enhance cybersecurity awareness over the next five years.[18] The policy, which is divided into two parts, aims to bolster cybersecurity across various sectors—including the public, academia, industry, startups, and government—and improve the state's IT infrastructure. Key focus areas of the awareness program include education, skill-building, industry and startup

promotion, and capacity-building partnerships.

- Officials have rescued at least 47 Indians who were being held against their will in Laos and forced to carry out online scams targeting people back home.[19] The Indian government has been warning citizens about fake job offers in Laos and Cambodia, which are often traps to exploit individuals as cyber slaves. To date, the Indian mission has rescued 635 Indians from these situations and facilitated their return to India. Victims are lured to Laos with job offers, only to have their passports seized, preventing them from leaving. They are then coerced into creating fake social media profiles, given daily targets, and subjected to punishment for failing to meet them.

- The Union Ministry of Electronics and Information Technology (MeitY) plans to assign trained data experts and analysts to various central government ministries and departments, according to reports.[20] These specialized analysts will focus on streamlining the internal datasets managed by different ministries, improving data handling and analysis across the government.

- The government has partnered with IITs and IIITs to train the first batch of cyber commandos, with the special unit set to be commissioned in coming months.[21] Nearly 350 personnel, selected from various state police forces, will be trained to handle and counter cyberattacks. The training program includes investigation officers and senior police officers, who will be equipped to respond to and manage cyber threats, officials noted.

---

[1] The Hindu Business Line, Chinese hackers breach US, India internet firms, Lumen says, 28 August 2024, https://www.thehindubusinessline.com/info-tech/chinese-hackers-breach-us-india-internet-firms-lumen-says/article68575478.ece

[2] CISA, CISA Names First Chief Artificial Intelligence Officer, 1 August 2024, https://www.cisa.gov/news-events/news/cisa-names-first-chief-artificial-intelligence-officer.

[3] The Indian Express, Who is Lisa Einstein, chief AI officer appointed by US cybersecurity watchdog?, 3 August 2024, https://indianexpress.com/article/technology/artificial-intelligence/us-cybersecurity-watchdog-names-chief-ai-officer-9490702/

[4] NextGov, Senate confirms first-ever Pentagon cyber policy chief, 2 August 2024, https://www.nextgov.com/cybersecurity/2024/08/senate-confirms-first-ever-pentagon-cyber-policy-chief/398537/

[5] The Record, Senate confirms first DOD cyber policy chief, 2 August 2024, https://therecord.media/senate-confirms-first-dod-cyber-policy-chief

[6] France 24, Olympic venue among 40 museums hit by ransomware attack: French police source, 6 August 2024, https://www.france24.com/en/live-news/20240806-olympic-venue-among-40-museums-hit-by-ransomware-attack-french-police-source

[7] Cybernews, Paris Olympics ransomware attack hits famed Grand Palais venue, 6 August 2024, https://cybernews.com/security/paris-olympics-ransomware-attack-grand-palais-venue/

[8] The Register, Brain Cipher claims attack on Olympic venue, promises 300 GB data leak, 29 August 2024, https://www.theregister.com/2024/08/29/brain_cipher_olympic_attack/

[9] NBC News, FBI says it's investigating efforts to hack Trump and Biden-Harris campaigns, 13 August 2024, https://www.nbcnews.com/tech/security/fbi-says-s-investigating-trump-campaign-claim-hacked-files-rcna166197

[10] The Times of India, FBI shuts down 'dangerous' global hacking group that targeted over 40 companies in 13 countries, including India, 14 August 2024, https://timesofindia.indiatimes.com/technology/tech-news/fbi-shuts-down-dangerous-global-hacking-group-that-targeted-over-40-companies-in-13-countries-including-india/articleshow/112504440.cms.

[11] The Record, UN cybercrime treaty passes in unanimous vote, 9 August 2024, https://therecord.media/un-cybercrime-treaty-passes-unanimous

[12] ANI, CCP-backed sources promote Pro China content on social media platforms: Report, 14 August 2024, https://www.aninews.in/news/world/asia/ccp-backed-sources-promote-pro-china-content-on-social-media-platforms-report20240814153317/

[13] The Malaysian Reserve, Malaysia introduces data breach notification system to combat scams, 1 August 2024, https://themalaysianreserve.com/2024/08/01/malaysia-introduces-data-breach-notification-system-to-combat-scams/

[14] The Kyiv Independent, Ukrainian hackers show war footage on Russian TV, source says, 22 August 2024, https://kyivindependent.com/ukrainian-hackers-show-war-footage-on-russian-tv/

[15] The Record, Ransomware attack on Indian payment system traced back to Jenkins bug, 16 August 2024, https://therecord.media/jenkins-vulnerability-india-npci-ransomware-attack

[16] Business Today, India cracks down on spam calls: TRAI orders immediate halt to unregistered promotional calls, 14 August 2024, https://www.businesstoday.in/technology/news/story/india-cracks-down-on-spam-calls-trai-orders-immediate-halt-to-unregistered-promotional-calls-441454-2024-08-14

[17] Tech Crunch, Durex India spilled customers' private order data, 28 August 2024, https://techcrunch.com/2024/08/28/durex-india-spilled-customers-private-order-data/

[18] The Hindu Business Line, Karnataka launches cybersecurity policy, 1 August 2024, https://www.thehindubusinessline.com/news/karnataka-launches-cybersecurity-policy/article68473395.ece

[19] NDTV, 47 Indian 'Cyber Slaves' In Laos, Forced To Run Dating Apps Scam, Rescued, 31 August 2024, https://www.ndtv.com/indians-abroad/47-indian-cyber-slaves-in-laos-forced-to-run-dating-apps-scam-rescued-6459872

[20] Business Standard, Meity plans to deploy experts for streamlining internal govt data use, 26 August 2024, https://www.business-standard.com/industry/news/meity-plans-to-deploy-data-experts-for-streamlining-internal-govt-data-use-124082600678_1.html

[21] The New Indian Express, MHA ropes in IITs, IIITs, other top institutes to train first batch of cyber commandos, 29 August 2024, https://www.newindianexpress.com/nation/2024/Aug/29/mha-ropes-in-iits-iiits-other-top-institutes-to-train-first-batch-of-cyber-commandos.