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

CYBER *Digest*

July 2024

- US bans Kaspersky software sales
- Japanese Prime Minister calls for cyber defence legislation
- Cyberattack Targeting Swiss Government
- Breach reported in Pakistani UN mission
- Vietnam Post Faces Ransomware Attack
- Bangladeshi police officials accused of selling classified data
- Indonesian authorities arrest foreign nationals for cybercrime
- Ransomware Attacks: Governments Resist, Corporations Comply
- Cyber Defence budgets rise across Europe
- India File

US bans Kaspersky software sales

The Biden administration has announced plans to prohibit the sale of antivirus software developed by Russia's Kaspersky Lab in the United States, citing significant security risks due to Russia's influence over the company.[1] Kaspersky's customer base includes critical infrastructure providers and state and local governments, raising concerns about the software's potential misuse. The administration warned that the software's privileged access to computer systems could be exploited to steal sensitive information from American computers, install malware, and withhold critical updates, thereby increasing the threat. Kaspersky has responded, stating that the U.S. decision is driven by the current geopolitical climate and theoretical concerns rather than a thorough evaluation of the integrity of Kaspersky's products and services.

Japanese Prime Minister calls for cyber defence legislation

Prime Minister Fumio Kishida has instructed his government to draft potential legislation to introduce an active cyber defense system.[2] This system would enable preemptive actions against cyberattacks, marking a significant step in Japan's cybersecurity strategy. The government aims to submit this legislation in the next parliamentary session, which is expected to begin in autumn. During a meeting, Digital Transformation Minister Taro Kono identified three key issues: strengthening information sharing between the public and private sectors, identifying servers behind cyberattacks, and determining the extent of authority to be granted to the government. He requested that the panel report progress on these issues within the next few months.

These developments come amidst reports of a cybersecurity incident affecting Niconico, a popular Japanese video-sharing platform, which forced the company to suspend its services.[3] The Tokyo-based company has temporarily shut down its live-streaming platform and user channels to minimize the impact of the incident.

Cyberattack Targeting Swiss Government

Switzerland's government websites experienced a wave of cyberattacks ahead of a summit on peace in Ukraine, hosted in Bern.[4] The National Cyber Security Centre (NCSC) reported that distributed denial-of-service (DDoS) attacks, which overwhelm websites or network resources with malicious traffic, caused minor outages. The NCSC reported that various federal government websites and organizations involved in the upcoming summit on peace in Ukraine experienced a first wave of DDoS attacks. These attacks, expected and presumed to be connected to the summit, caused minor outages but did not significantly impact the operation of the affected units. The NCSC stated it would provide regular updates on the situation.

Breach reported in Pakistani UN mission

Pakistan's Permanent Mission to the United Nations has been targeted by a cyberattack that has infiltrated its official email account and YouTube channel, according to media reports.[5] The breach targeted the email ID used by the Permanent Mission's information wing. The mission's YouTube

channel was compromised, with attackers altering its name, banners, and content. The Pakistani UN mission has requested that all emails and videos posted on its channels be ignored until they regain control of their accounts. No group or entity claimed responsibility for the cyberattack.

Vietnam Post Faces Ransomware Attack

Vietnam Post, the government-owned postal service, was recently hit by a ransomware attack that disrupted its postal and delivery services.[6] Initially, the company reported that its financial, administrative, and goods distribution services were unaffected by the attack. However, the cyberattack forced the shutdown of several services for days. The Vietnamese postal service has now successfully restored its operations. This is not the first time the postal service has experienced a digital intrusion. Last November, researchers discovered that the company had left its security logs and employee email addresses accessible to external users, highlighting ongoing vulnerabilities in its cybersecurity infrastructure.

Bangladeshi police officials accused of selling classified data

Two senior officials working for the anti-terror police in Bangladesh have allegedly collected and sold classified and personal information of citizens to criminals on Telegram, according to reports.[7] The data reportedly sold included national identity details of citizens, cell phone call records, and other classified secret information. These allegations are based on a letter signed by a senior Bangladeshi intelligence official. According to a letter signed by a senior Bangladeshi intelligence official, the police agents were caught after investigators analyzed logs of the National Telecommunication Monitoring Centre's (NTMC) systems and monitored how frequently the two accessed them.

Indonesian authorities arrest foreign nationals for cybercrime

Indonesian immigration authorities have arrested over a hundred foreign nationals suspected of committing cybercrimes.[8] During the operation, law enforcement seized several computers and mobile phones reportedly used to carry out the illicit activities. According to Indonesia's immigration authorities, 14 of the 103 arrested individuals were identified as Taiwanese citizens. The identities of the remaining detainees are unknown, although all were in possession of Taiwan passports. The suspects were accused of misusing their visas and residence permits in addition to participating in cybercrime.

Ransomware Attacks: Governments Resist, Corporations Comply

In a significant development, Indonesia's national data center has been compromised by a hacking group that has demanded an $8 million ransom.[9] The government has stated its refusal to pay the ransom. In another incident, a group claiming to have hacked CDK Global, a major software provider for numerous car dealerships across North America, has demanded tens of millions of dollars in ransom, as reported by sources familiar with the situation. According to reports, CDK Global is planning to make the ransom payment. The hacking group responsible for the attack is

believed to be based in Eastern Europe, raising concerns about cybersecurity vulnerabilities and international cyber threats.[10]

Cyber Defence budgets rise across Europe

Ukraine's Defense Ministry announced that the IT Coalition for Ukraine, consisting of 12 European nations, has collectively raised 58 million euros ($62.9 million) to bolster Ukraine's IT and cybersecurity defense capabilities.[11] During recent meetings, Luxembourg, Iceland, Estonia, and Belgium additionally pledged 22 million euros ($23.8 million) in funding contributions, highlighting a concerted effort among European countries to support Ukraine's cybersecurity resilience amidst ongoing challenges. Established in September 2023, the coalition pledged to support Ukraine's Defense Ministry and Armed Forces' information technology (IT) infrastructure over the next six years under a cooperation agreement.

Poland has announced plans to allocate nearly $760 million to bolster its defenses against ongoing cyberattacks attributed to Russia, according to the country's digital minister.[12] The decision follows an incident where hackers, believed to be Russia-sponsored, published a false article about military mobilization on Poland's state news agency, PAP.

India File

- India's Chief of Defence Staff (CDS), General Anil Chauhan, unveiled the country's first joint doctrine for cyberspace operations during a meeting of the Chiefs of Staff Committee.[13] The doctrine recognizes cyberspace as a critical and complex domain in modern warfare. According to the Defence Ministry, the joint doctrine serves as a foundational document to guide armed forces commanders in conducting cyberspace operations amidst today's intricate military environments. In May, CDS Gen Anil Chauhan had emphasised the significance of enhancing India's cyber defense capabilities during his participation in 'Exercise Cyber Suraksha – 2024'.[14] He stressed the essential requirement for collaboration among all stakeholders in the cyber domain. The CDS commended the initiative for fostering a collaborative environment aimed at addressing emerging cyber threats effectively.
- According to reports, Mumbai has recorded the highest number of cybercrime complaints in the state, with 70,904 complaints filed via the helpline 1930 and the national crime reporting portal over last three years.[15] Prompt action by cyber police following these complaints resulted in savings of Rs 223 crore overall. Of this amount, at least Rs 60 crore was recovered from cybercrime cases reported in Mumbai alone.
- According to reports, there was a breach in the Telangana State (TS) COP app, occurring shortly after reports of the department's HawkEye system being hacked.[16] Data from the Telangana police SMS service portal has reportedly been leaked. Launched in 2018, the app is touted as the first-of-its-kind crime detection tool in

India. It features a face recognition system (FRS) to enhance its capabilities in identifying and addressing criminal activities.

- The Computer Emergency Response Team (CERT-In) is collaborating with Mastercard to enhance cooperation and information sharing in cybersecurity within the financial sector.[17] Under a Memorandum of Understanding (MoU), the two organizations will leverage their expertise to focus on cybersecurity incident response, capacity building, and sharing cyber threat intelligence specific to the financial sector. This partnership also includes advanced malware analysis initiatives.
- The Reserve Bank of India (RBI) has proposed the establishment of a Digital Payments Intelligence Platform aimed at leveraging advanced technologies to mitigate payment fraud risks.[18] To advance this initiative, the RBI has formed a committee chaired by A.P. Hota, former MD & CEO of NPCI. The committee's mandate is to assess various aspects related to setting up a digital public infrastructure for the platform. The committee is expected to deliver recommendations within two months.

---

[1] Reuters, Biden bans US sales of Kaspersky software over Russia ties, 21 June 2024, https://www.reuters.com/technology/biden-ban-us-sales-kaspersky-software-over-ties-russia-source-says-2024-06-20.

[2] The Japan Times, Kishida wants active cyberdefense bill to be drawn up swiftly, 7 June 2024, https://www.japantimes.co.jp/news/2024/06/07/japan/cyber-defense-panel.

[3] The Record, Japanese video-sharing website Niconico suspends services following cyberattack, 10 June 2024, https://therecord.media/niconico-japan-video-streaming-site-cyberattack

[4] Space War, Swiss govt hit by cyberattack ahead of Ukraine peace summit, 13 June 2024, https://www.spacewar.com/reports/Swiss_govt_hit_by_cyberattack_ahead_of_Ukraine_peace_summit_999.html

[5] The Print, Cyber attack on Pakistani UN Mission; account, email, YouTube channel breached, 15 June 2024, https://theprint.in/world/cyber-attack-on-pakistani-un-mission-account-email-youtube-channel-breached/2132974/

[6] The Record, Vietnam's state postal service claims to restore its systems after cyberattack, 10 June 2024, https://therecord.media/vietnam-claims-restore-services-cyberattack

[7] Techcrunch, Bangladeshi police agents accused of selling citizens' personal information on Telegram, 6 June 2024, https://techcrunch.com/2024/06/06/bangladeshi-police-agents-accused-of-selling-citizens-personal-information-on-telegram/

[8] The Record, Indonesia arrests over 100 foreigners in Bali suspected of participating in cybercrime, 28 June 2024, https://therecord.media/indonesia-bali-arrests-foreigners-cybercrime

[9] NBC News, Indonesia won't pay an $8 million ransom after a cyberattack compromised its national data center, 25 June 2024, https://www.nbcnews.com/news/world/indonesia-wont-pay-8-million-ransom-cyberattack-compromised-national-d-rcna158747

[10] Fortune, Software company plans to pay tens of millions in ransom to hackers who crippled car dealerships across North America, 22 June 2024, https://fortune.com/2024/06/22/cdk-ransomware-attack-payment-hackers-tens-millions-car-dealerships/

[11] The Kyiv Independent, European IT Coalition raises 58 million euros for Ukraine's IT, cybersecurity defense capabilities, 1 June 2024, https://kyivindependent.com/european-led-it-coalition-raises-58-million-euros-for-ukraines-it-cybersecurity-defense-capabilities/

[12] The Record, Poland to invest $760 million in cyberdefense as Russian pressure mounts, 5 June 2024, https://therecord.media/poland-cyberdefense-spending-russian-attacks

[13] The Hindu, In a first, CDS releases its blueprint for warfare in cyberspace, 18 June 2024, https://www.thehindu.com/news/national/in-a-first-cds-releases-its-blueprint-for-warfare-in-cyberspace/article68303975.ece

[14] Press Information Bureau (PIB), CDS Gen Anil Chauhan attends Exercise Cyber Suraksha – 2024, 22 May 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2021343

[15] The Times of India, 71,000 cybercrime complaints in Mumbai in 3 years, but 1,500 FIRs, 11 June 2024, https://timesofindia.indiatimes.com/city/mumbai/mumbai-records-71k-cybercrime-complaints-in-3-years-with-15k-firs/articleshow/110885605.cms.

[16] The New Indian Express, Second major data breach hits Telangana police as TSCOP app hacked, 8 June 2024, https://www.newindianexpress.com/states/telangana/2024/Jun/08/second-major-data-breach-hits-telangana-police-as-tscop-app-hacked

[17] PIB, CERT-In and Mastercard India sign MoU for collaboration in cyber security to enhance India's cyber-resilience in Financial Sector, 19 June 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2026677

[18] The Indian Express, RBI plans new digital platform to check payment fraud risks, 8 June 2024, https://indianexpress.com/article/business/banking-and-finance/rbi-plans-new-digital-platform-to-check-payment-fraud-risks-9379018.