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

CYBER *Digest*

November 2023

- Cyber attacks amidst Israel-Hamas conflict
- ICRC releases guidelines for hactivists
- Hack of Russia's largest private bank attributed to Ukraine
- Five Eyes intelligence summit on securing innovation
- Chinese hackers target semiconductor companies
- Biden's Executive Order on safe and secure AI
- Cyberattack disables Guatemalan government websites
- Cybersecurity developments in the Philippines
- India File

Cyber attacks amidst Israel-Hamas conflict

The Israel-Hamas conflict has been accompanied by a noticeable uptick in cyber attacks as well. Hamas is believed to have only rudimentary cyber capabilities and the bulk of the attacks have been carried out by foreign hacktivist groups on either side. In a recent attack, a group known as AnonGhost reportedly leveraged a vulnerability in the application programming interface (API) of Israel's real-time rocket alert app.[1] The attackers shared details about the alleged attack on their official Telegram channel. Due to the increasing frequency of such incidents, the Israeli National Cyber Directorate has recently warned Israeli citizens to exercise caution regarding the security of their home surveillance cameras, given concerns about potential hacking attempts by hostile entities.[2] Israeli websites have also been heavily targetted by DDoS attacks, with newspaper and media sites being the most affected, followed by IT and banking companies.[3]

ICRC releases guidelines for hactivists

The International Committee of the Red Cross (ICRC) has been active in formulating rules of the road for cyberspace. Most recently, its global advisory board released a report on Protecting Civilians Against Digital Threats During Armed Conflict. The report contains "4 guiding principles and a set of 25 concrete recommendations addressed to belligerents, states, tech companies, and humanitarian organizations to prevent or mitigate digital threats to civilian populations."[4] The ICRC also brought out ethical guidelines for hactivists during wartime in a blogpost. These guidelines were distilled into 8 "humanitarian law-based rules" and 4 obligations for states.[5] There was a mixed response from hacking groups to these guidelines, with some rejecting them outright while others were more receptive to the idea. [6]

Hack of Russia's largest private bank attributed to Ukraine

According to reports, Ukrainian hackers reportedly worked in collaboration with Ukraine's security services, the SBU, to breach Russia's largest private bank.[7] Two groups of pro-Ukrainian hackers, known as KibOrg and NLB, successfully infiltrated Alfa-Bank and have claimed to have acquired data from over 30 million customers. This data includes their names, dates of birth, account numbers, and phone numbers, as indicated in a post on their official website. This is not the first collaboration between Ukraine's intelligence agencies and hacktivists. The Head of Cybersecurity at the Security Service of Ukraine, Illia Vitiuk, has previously noted that documents leaked by Ukrainian hackers substantially impact the nation's cyber intelligence activities.

Five Eyes intelligence summit on securing innovation

The leaders of the Five Eyes intelligence alliance, comprising the United States, the United Kingdom, Canada, Australia, and New Zealand, met at the launch of the first Emerging Technology and Securing Innovation Security Summit in Palo Alto, California.[8] The summit also convened a gathering of business leaders, entrepreneurs, government officials, and academics. They engaged in discussions about challenges facing innovation and upcoming trends in the potential misuse of emerging technologies. They explored avenues for collaborative efforts to enhance economic security and public safety. The purpose of the gathering was also to raise

awareness of the risks presented by China in high-tech domains, including quantum computing, artificial intelligence (AI), and synthetic biology.[9]

Chinese hackers target semiconductor companies

According to assessments, state-sponsored Chinese hackers have launched a new espionage campaign targeting the semiconductor industry in East Asia.[10] In this recent campaign directed at semiconductor companies, the group impersonated the Taiwan Semiconductor Manufacturing Company (TSMC) to deceive victims into clicking on malicious links. TSMC is a significant player in the industry, producing microchips for prominent companies like Apple and Nvidia. The threat actors are employing software commonly used as a penetration testing tool by cybersecurity professionals. This tool is typically used to simulate cyberattacks and evaluate the security of computer systems. However, in this case, criminals have misused it to issue commands and steal information from their victims remotely.

Biden's Executive Order on safe and secure AI

The U.S. President issued an Executive Order focused on Safe, Secure, and Trustworthy AI, with the aim of enabling America to take the lead in harnessing the potential and effectively managing the risks associated with artificial intelligence.[11] The order is aimed at safeguarding American citizens from the potential risks associated with AI. The order establishes new standards for AI safety and security, emphasizing protecting American citizens' privacy. It also highlights concerns about how irresponsible AI usage can exacerbate issues such as discrimination, bias, and other abuses within the realms of justice, healthcare, and housing. It is designed to maintain the United States' leadership in innovation and competitiveness through a range of actions. It also calls for producing a report on the potential labor-market impacts of AI and exploring options to enhance federal support for workers who may face job disruptions, including those resulting from AI.

Cyberattack disables Guatemalan government websites

As reported, hackers associated with the activist group Anonymous launched coordinated cyberattacks that disabled multiple Guatemalan government websites.[12] These attacks appeared to be in solidarity with demonstrations led by Indigenous organizations in the country. The hackers used distributed denial-of-service attacks to target government web pages. Guatemalan authorities have categorized the hacking incidents as a "national security" concern and have initiated responses to address the situation.

Cybersecurity developments in the Philippines

In a recent turn of events, a massive amount of personal data was leaked by hackers from the Philippine Health Insurance Corporation (PhilHealth) servers. This occurred when the state insurer declined to make a payment of $300,000 in response to a ransom demand.[13] The report indicated that the breach had a far-reaching impact, affecting millions of individuals, including residents within the Philippines and overseas Filipino workers in locations like Hong Kong. The attack was attributed to a hacker self-identifying as DiabloX Phantom, although government agencies have not yet confirmed the authenticity of this claim.

In another development, the Philippine defense chief has issued an order instructing all defense personnel and the 163,000-strong military force to abstain from using digital applications that utilize artificial intelligence for generating personal portraits.[14] This measure is being taken due to concerns over potential security risks associated with such applications.

Furthermore, the Chief of the Armed Forces has also announced the establishment of a dedicated cyber command within the military.[15] This move aims to enhance the defense capabilities against the frequent cyber attacks the military faces almost daily. Moreover, the military plans to revise recruitment rules in order to attract and enlist cybersecurity experts who can bolster their cybersecurity efforts.

India File

- As per reports, a substantial data breach has occurred, revealing personal information from 81.5 Crore Indian citizens.[16] This data includes COVID-19 test records, Aadhaar, and passport details. The leaked data of Indian citizens were with the Indian Council of Medical Research (ICMR). However, the claims are yet to be verified by an authorized agency.
- The Bharat National Cyber Security Exercise (NCX) 2023 was organised in New Delhi.[17] The event brought together a wide range of government agencies, public organizations, and the private sector, all displaying a strong dedication to the protection of critical information infrastructure.
- Tata Tele Business Services, a subsidiary of the Tata Group, has reportedly experienced a data breach orchestrated by the LockBit ransomware group.[18] The threat actor has claimed responsibility for the and listed the company on its dark web portal.
- The Central Bureau of Investigation (CBI) announced that it conducted a series of criminal raids in multiple cities across India.[19] This operation was facilitated by a joint referral made by both Microsoft and Amazon. This collaborative referral allowed for sharing of actionable intelligence and insights between the CBI and other international law enforcement agencies, enabling them to take comprehensive actions. The illegal call centers raided by CBI were set up to impersonate Microsoft and Amazon customer support.
- The Seventh India-EU Cyber Dialogue was held on 05 October 2023 in Brussels. The respective principals from the MEA and the European External Action Service expressed appreciation for the Cyber Dialogue mechanism as it provides a platform to discuss a wide range of issues related to cyberspace. Both sides exchanged views on cyber policies, strategies, and areas of mutual interest. They discussed cyber cooperation in multilateral forums, including at the United Nations, and in regional settings, including at OSCE, ARF, and G20. They also discussed cooperation in promoting capacity building in cyberspace and combating the criminal use of ICTs. Both sides agreed to hold the next India-EU Cyber Dialogue on a mutually convenient date.

[1] Cybernews, Red Alert, Israel's rocket alert app, breached by hacktivists, 23 October 2023, https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/

[2] Calcalist Tech, Israel's cyber authorities warn home-camera owners against potential hacking by terrorists, 15 October 2023, https://www.calcalistech.com/ctechnews/article/syjznmfzt

[3] Cloudflare blog, Cyber attacks in the Israel-Hamas war, https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/

[4] ICRC, Protecting Civilians Against Digital Threats During Armed Conflict, https://www.icrc.org/en/document/protecting-civilians-against-digital-threats-during-armed-conflict

[5] ICRC blog, 8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them , https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them

[6] BBC, Rules of engagement issued to hacktivists after chaos , https://www.bbc.co.uk/news/technology-66998064

[7] The Record, Ukraine security services involved in hack of Russia's largest private bank, 23 October 2023, https://therecord.media/sbu-involved-in-alfa-bank-hack

[8] FBI, FBI Hosts Five Eyes Summit to Launch Drive to Secure Innovation in Response to Intelligence Threats, 16 October 2023, https://www.fbi.gov/news/press-releases/fbi-hosts-five-eyes-summit-to-launch-drive-to-secure-innovation-in-response-to-intelligence-threats

[9] Financial Times, Five Eyes spy chiefs warn Silicon Valley over Chinese threat, 18 October 2023, https://www.ft.com/content/0a37da0a-ad06-43d0-b069-bfafa0ff35a4

[10] The Record, China-based spies are hacking East Asian semiconductor companies, report says, 6 October 2023, https://therecord.media/china-budworm-apt27-east-asia-semiconductor-companies

[11] The White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, 30 October 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

[12] AP News, Hackers attack Guatemalan government webpages in support of pro-democracy protests, 15 October 2023, https://apnews.com/article/guatemala-porras-anonymous-hack-protest-democracy-ae14b4ca19a834a242d5843fa0ab3c89

[13] SCMP, Philippines' cybersecurity failures exposed as hackers leak state secrets, people's data, 22 October 2023, https://www.scmp.com/week-asia/politics/article/3238687/philippines-cybersecurity-failures-display-hackers-expose-state-secrets-peoples-data

[14] AP News, Philippine military ordered to stop using artificial intelligence apps due to security risks, 20 October 2023, https://apnews.com/article/philippines-artificial-intelligence-defense-secretary-gilberto-teodoro-jr-b682e926a5247621befc208b3584f887

[15] Reuters, Philippines to recruit 'cyber warriors' for online defence, 19 October 2023, https://www.reuters.com/world/asia-pacific/philippines-recruit-cyber-warriors-online-defence-2023-10-19/

[16] The Economic Times CISO, Data of 81.5 crore Indians dumped on dark web, 31 October 2023, https://ciso.economictimes.indiatimes.com/news/data-breaches/boeing-assessing-lockbit-hacking-gang-threat-of-sensitive-data-leak/104771554

[17] Business World, Bharat National Cyber Security Exercise Focuses On Elevating India's Cybersecurity Preparedness, 24 October 2023, https://www.businessworld.in/article/Bharat-National-Cyber-Security-Exercise-Focuses-On-Elevating-India-s-Cybersecurity-Preparedness/24-10-2023-496144/

[18] The Cyber Express, LockBit Claims Tata Tele Business Services Data Breach, Sets Data Release Deadline, 6 October 2023, https://thecyberexpress.com/tata-tele-business-services-data-breach/

[19] Microsoft, Microsoft, Amazon, and international law enforcement join forces to fight tech support fraud, 19 October 2023, https://blogs.microsoft.com/on-the-issues/2023/10/19/microsoft-amazon-tech-support-fraud-india/