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

CYBER *Digest*

June 2023

- Tech Initiatives at Quad Leaders' Summit
- India targeted in Cyber-espionage campaigns
- Wave of Ransomware Attacks sweeps across India
- US Justice Department takes down “Snake” malware network
- Increase in Iranian cyber influence operations reported
- EU and US voice security concerns over Huawei to Malaysia
- Chinese Hackers target Kenyan Government
- European Parliament spyware inquiry committee releases final report
- Threat actors exploiting AI-based voice technology
- India File

Tech Initiatives at Quad Leaders' Summit

On May 20, 2023, the Quad Leaders' Summit convened in Hiroshima, bringing together Prime Minister Narendra Modi, President Biden of the US, Prime Minister Anthony Albanese of Australia and Prime Minister Kishida Fumio of Japan.[1] During the meeting, the discussion encompassed various significant initiatives, including critical and emerging technologies. The announcement of "The Quad Partnership for Cable Connectivity and Resilience" signifies recognition of the crucial role played by undersea cables in communication infrastructure. The partnership intends to facilitate access to develop trusted and secure cable systems and establish better internet connectivity and resiliency in the Indo-Pacific.

The Quad's commitment to share the benefits of new and emerging technologies throughout the region was demonstrated by its announcement of partnering with the Government of Palau and the Palau National Communication Corporation (PNCC) to design, implement and operationalize the deployment of Open RAN capabilities.

India targeted in Cyber-espionage campaigns

Meta's quarterly Adversarial Threat Report has detailed how a Pakistan-based state-linked actor is spying on military personnel in India and the Pakistan Air Force using fake apps and websites to compromise their personal devices.[2] However, the report did not give the Pakistan-based group a name. According to the report, the Pakistan-based group used traditional tricks to lure victims like impersonating journalists, women seeking romantic connections and even military personnel. The traditional social engineering method used for the operations, the report states, have allowed the Pakistan-based actor to avoid investing in developing sophisticated malware.

In another report, Ukraine's Computer Emergency Response Team, CERT-UA, has identified a cyber-espionage campaign against countries including India and Israel.[3]

Wave of Ransomware Attacks sweeps across India

After a brief lull, ransomware actors are back, with a series of ransomware attacks reported across multiple locations in India. In the first incident, over 600 GB of Fullerton India's data was released on the dark web. The Fullerton India Credit Company Limited is registered as a Non-Bank Financial Company (NBFC) with the Reserve Bank of India. The released data include loan agreements with individuals and legal entities, agreements with banks and other financial institutions, data on international transfers, and personal information of the company's customers such as Aadhaar card numbers, residential addresses, phone numbers, and other sensitive data. Fullerton India had first acknowledged the 'malware' incident in a press release in April 2023, assuring its customers that steps had been taken to mitigate the fallout. In another incident, an Ahmedabad-based hospital was attacked by ransomware actors, demanding USD 70 000 to restore data. The police reported that the hackers demanded the amount through an email and also offered a discount if the hospital agreed to pay the amount.

Insurance Information Bureau of India (IIB), an independent body, reported that

Russian hackers had encrypted their data through a ransomware attack and demanded bitcoins worth $25,000 undo the damage. According to police, some encrypted data included confidential information, and the damage's extent is still being assessed. The police also reported that IIB has a backup of sensitive data, which is helping in continuing daily operations.

Similarly, a ransomware attack hit Madhya Pradesh Power Management Company Limited (MPPMC) and crippled its internal information technology system used for communication among different functionaries of the state-run entity. The Chief General Manager (IT) of MPPMC said that the attackers had not sought money as yet but had provided email IDs to contact them. Following the complaint, the state cyber cell initiated an investigation into the ransomware attack on the company's IT system.

US Justice Department takes down "Snake" malware network

The Justice Department announced the completion of the court-authorized operation, code-named MEDUSA targeting a global peer-to-peer network of computers compromised by "Snake" malware.[4] The US government attributes the malware to a unit within the Federal Security Service of the Russian Federation (FSB). The operation disabled malware on compromised computers by using an FBI-created tool named PERSEUS, which issued commands that caused the Snake malware to overwrite its key components. The US government has reportedly investigated Snake and Snake-related malware tools for nearly 20 years. The US agencies have identified Snake infrastructure in over 50 countries across the globe, which was being used to collect sensitive intelligence from government networks, research facilities, and journalists.[5]

Increase in Iranian cyber influence operations reported

Iran has reportedly been leveraging cyber-enabled influence operations to achieve its geopolitical objectives. According to Microsoft, the Iran efforts have been accelerating since June 2022, and most of these operations are being run by Emennet Pasargad, which is tracked as Cotton Sandstorm (formerly NEPTUNIUM).[6] The same Iranian state actor is also sanctioned by the US Treasury Department for their attempts to undermine the integrity of the 2020 US Presidential elections. The operation of the threat actor remains focused on Israel, Iranian opposition figures and groups, and Gulf countries.

Iran has also been at the receiving end of threat actors in cyberspace. A hacktivists group named "Uprising Till Overthrow" hacked the server infrastructure of Iran's Ministry of Foreign Affairs, disabling 210 sites and online services and leaking a large batch of documents.[7] The hacktivists group is linked to Albania-based opposition Mujahideen-e Khalq (MEK) group. The leaked documents include identification documents, minutes of meetings, phone numbers of ministry officials, and the name of 11,000 foreign ministry employees. This is not the first time that the hacktivists group is targeting the Iranian regime. Previously, the group has hacked into and deactivated over 5,000 surveillance cameras and 150 websites and online services of Tehran Municipality.[8]

EU and US voice security concerns over Huawei to Malaysia

The EU and US have warned Malaysia over risks to national security as the government finalizes a review of its 5G rollout.[9] The concerns revolve around Huawei's potential role in the country's telecoms infrastructure. The envoys to Malaysia from the US and EU wrote letters to the Malaysian government sharing their concerns in April. Huawei, the Chinese equipment maker, which is blacklisted by the US, has reportedly lobbied heavily for another chance at a role in building Malaysia's network.

Chinese Hackers target Kenyan Government

According to reports, the Chinese hackers targeted Kenya's government in a widespread cyber intrusion against key ministries and state institutions.[10] The hacking campaign illustrates China's willingness to use espionage to monitor and protect economic and strategic interests abroad. Reports also said that these hacks were aimed, at least in part, at gaining information on debt owed to Beijing by the East African nation, which is also a strategic link in the Belt and Road Initiative. The Chinese hackers also subjected the office of Kenya's president, its defense, information, health, land, interior ministries, and other institutions to persistent and prolonged hacking activity.

European Parliament spyware inquiry committee releases final report

The European Parliament's Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware (PEGA) has called on EU officials to create an EU Tech Lab in its final report.[11] The new institution would provide independent research with powers to investigate surveillance, provide legal and technological support, including device screening, and perform forensic research. The final report also condemned the spyware abuses in several EU countries as it pointed out systemic issues in Poland and Hungary. To remedy the situation, the European Parliament members called on the two countries to comply with European Court of Human Rights judgements and restore judicial independence and oversight bodies. The members also encouraged an in-depth investigation of spyware export licences, stronger enforcement of the EU's export control rules alongside a joint EU-US spyware strategy and ensuring EU's development aid does not support acquisition and use of spyware.

Threat actors exploiting AI-based voice technology

A recent study indicates that India has the highest number of victims, with 83% of Indians losing their money by cyberattacks exploiting AI-based voice technology.[12] According to the report, scammers are taking advantage of AI to mimic the voices of distressed family members, and many Indians are becoming victims of such scams. The study also reveals that almost 47% of Indian adults have either been a victim of or know someone who has been scammed using voice technology. AI-generated News websites have also been proliferating online globally with a report identifying 49 sites using AI tools to generate unreliable news and content.[13] These websites failed to disclose ownership or control while ensuring a high volume of content on a variety of topics, including politics, health, entertainment, finance, and technology.

India File

- The European Union and India held their first ministerial meeting of the Trade and Technology Council (TTC) focusing on deepening strategic engagement on trade and technology.[14] The EU-India Trade and Technology Council is the second bilateral forum for the EU and the first one established with any partner for India. The EU and India has decided to work on quantum and High-Performance Computing research and development projects to help address challenges such as climate change and healthcare.

- India's national security agencies, in collaboration with tri-services conducted a cyber defence exercise to test the resilience of critical civilian and military infrastructure amid escalating cyber threats, particularly from China.[15] The cyber defence exercise was led by the Cyber Defence Agency (DCyA) and it involved the participation of various branches of national security. The exercise has been initiated in response to the discovery of Chinese sleeper malware in Australian and Japanese networks, which according to assessments was implanted within critical networks and remained dormant for extended periods.

- The Indian government has blocked 14 mobile messenger applications used by terrorists to receive texts from Pakistan.[16] According to reports, terrorists used these mobile messenger apps to spread and receive messages from Pakistan.

- A cyberattack on Suzuki's India plant halted the production of motorbikes and scooters for more than a week.[17] The incident occurred on 10th May, and it is estimated that the company has lost production of over 20,000 vehicles since then. The Suzuki Motorcycle India spokesperson has confirmed the incident and has reported the same to the concerned government department.

- The AI Supercomputer 'AIRAWAT' installed at C-DAC, Pune, has placed India among the top supercomputing list.[18] The system is installed under National Program on AI by the Government of India. The declaration was made in the 61st edition of the Top 500 Global Supercomputing List at the International Supercomputing Conference (ISC 2023) in Germany.

- The 9th Meeting of the BRICS Working Group on Security in the use of ICTs was held in Johannesburg, South Africa from 16-19 May 2023. Shri Ravi Shanker Goel, Director (CD) represented India in the meeting.

[1] The White House, Quad Leaders' Summit Fact Sheet, 20 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/

[2] The Record, Cyber-espionage campaigns targeting military personnel in South Asia, Meta warns, 3 May 2023, https://therecord.media/pakistan-india-cyber-espionage-meta-bahamut-patchwork

[3] The Record, Spying campaign targets Ukraine, Israel, India, Kazakhstan and others, cyber agency says, 23 May 2023, https://therecord.media/cyber-espionage-ukraine-uac-0063-cert-ua

[4] The United States Department of Justice, Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service, 9 May 2023, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled

[5] Cybersecurity & Infrastructure Security Agency (CISA), Hunting Russian Intelligence "Snake" Malware, 9 May 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

[6] Microsoft, Rinse and repeat: Iran accelerates its cyber influence operations worldwide, 2 May 2023, https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/

[7] Iran International, Hacktivists Target Iran's Foreign Ministry, Leak Trove Of Data, 7 May 2023, https://www.iranintl.com/en/202305079860

[8] Iran International, Tehran's 5,000 Surveillance Cameras, 150 Sites Hacked, 2 June 2022, https://www.iranintl.com/en/202206025165

[9] Financial Times, EU and US warn Malaysia of 'national security' risk in Huawei's bid for 5G role, 2 May 2023, https://www.ft.com/content/3da9a1bd-a49c-46f4-acc2-60333e55eaaa

[10] Reuters, Exclusive: Chinese hackers attacked Kenyan government as debt strains grew, 24 May 2023, https://www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24/

[11] European Parliament News, Spyware: MEPs sound alarm on threat to democracy and demand reforms, 8 May 2023, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms

[12] Livemint, India tops the list for victims of AI-powered voice scams with 83% losing money, report reveals, 3 May 2023, https://www.livemint.com/technology/tech-news/india-tops-the-list-for-victims-of-ai-powered-voice-scams-with-83-losing-money-new-report-reveals-11683096941884.html

[13] The Verge, AI is being used to generate whole spam sites, 2 May 2023, https://www.theverge.com/2023/5/2/23707788/ai-spam-content-farm-misinformation-reports-newsguard

[14] European Union, First EU-India Trade and Technology Council focused on deepening strategic engagement on trade and technology, 17 May 2023, https://www.eeas.europa.eu/delegations/india/first-eu-india-trade-and-technology-council-focused-deepening-strategic_en?s=167

[15] Livemint, India conducts national cyber defence exercise to safeguard critical infrastructure amid escalating threats, 28 May 2023, https://www.livemint.com/news/india-conducts-national-cyber-defence-exercise-to-safeguard-critical-infrastructure-amid-escalating-threats-11685248974907.html

[16] Livemint, India blocks 14 mobile messenger apps used by terrorists to receive texts from Pakistan, 1 May 2023, https://www.livemint.com/news/india/india-blocks-14-mobile-messenger-apps-used-by-terrorists-to-receive-texts-from-pakistan-11682913456963.html

[17] The Economic Times, Suzuki Motorcycle India halts operations due to cyberattack, 19 May 2023, https://auto.economictimes.indiatimes.com/news/two-wheelers/cyberattack-brings-suzuki-motorcycle-india-operations-to-a-halt-since-may-10/100361726

[18] Press Information Bureau, AI Supercomputer 'AIRAWAT' puts India among top supercomputing league, 24 May 2023, https://pib.gov.in/PressReleasePage.aspx?PRID=1926942