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

CYBER *Digest*

September 2022

- Meta disrupts cyberespionage operations in South Asia
- Turmoil in the crypto world
- Chinese Cyberattacks on Taiwan following Pelosi visit
- UK Cyber Vulnerabilities exposed
- Huawei radar on island nations
- Iranian Threat Actors target Albania and Israel
- Official use of spyware in the EU
- Bangladesh highly vulnerable to ransomware attacks
- Major data breaches in India
- Russia-Ukraine Cyber Conflict
- India File

Meta disrupts cyberespionage operations in South Asia

Meta, Facebook's parent company, reported that it took action earlier this year against two cross-platform cyberespionage operations that used various online services to distribute malware. Bitter APT (T-APT-17) is the first group of hackers that Meta disrupted during the second quarter. The group has been active since at least 2013, targeting entities in the energy, engineering, and government sectors in India, New Zealand, Pakistan, and the United Kingdom. The second group of hackers is APT36 is based in Pakistan. The group is believed to be connected to the Pakistani government. APT36 has been observed targeting government officials, human rights activists, military personnel, students, and non-profit organisations in Afghanistan, India, Saudi Arabia, and the United Arab Emirates.

Crypto world in turmoil

- A security flaw cost Nomad, a bridge protocol for transferring crypto tokens across different blockchains, nearly $200 million. Blockchain data showed that various accounts drained the software system of funds over hours and in small batches.
- Thousands of crypto wallets linked to the Solana ecosystem were emptied ($ 4million in total) by hackers who stole both Solana (SOL) and USD Coin using the owners' private keys (USDC). Solana linked the attack to Slope mobile wallet app accounts.
- Russian national Alexander Vinnik, the alleged operator of the illegal cryptocurrency exchange BTC-e, was extradited from Greece to the United States will face charges in the Northern District of California. BTC-e facilitated transactions for cybercriminals all over the world and received more than $4 billion in bitcoin during its operation.
- The United States sanctioned virtual currency mixer Tornado Cash and Blender.io, a North Korea-linked crypto mixing service, accusing them of helping hackers, including Lazarus Group from North Korea, in laundering proceeds from cybercrime. Tornado Cash, one of the largest mixers identified by the Treasury as problematic, has reportedly laundered more than $7 billion in virtual currency since its inception in 2019.
- Crypto bridges, which connect blockchain networks, have become major targets for cybercriminals. According to research from blockchain analytics company Chainalysis, breaches on cross-chain bridges have cost users a total of almost $1.4 billion this year. The largest incident involved the theft of a record $615 million from Ronin, a bridge that supported the well-known non fungible token game Axie Infinity.

Chinese Cyberattacks on Taiwan following Pelosi visit

The official website of Taiwan’s presidential office experienced an overseas cyberattack even before Speaker Nancy Pelosi landed in Taiwan. The Chinese also allegedly carried out a cyberattack on private organisations, including 7-ELEVEN unified supermarket, Taiwan Railway, Kaohsiung City Environmental Protection Bureau along with National Taiwan University. However, without directly blaming any state or non-state actor, Taipei stated that the attacks originated from addresses in China and Russia.

UK Cyber Vulnerabilities exposed

- Voting for the next UK prime minister was delayed after Government Communications Headquarters' National Cyber Security Centre warned that cyber hackers could change people’s ballots.

- A cyberattack caused a "major" system outage at the NHS 111 non-emergency medical help line, with hosting firm, *Advanced*, warning that patient scheduling services could be disrupted for at least several days. The details of the cyberattack are limited, but the National Crime Agency has confirmed that it was a malicious action carried out by a threat actor.
- South Staffordshire Plc, the parent company of Cambridge Water and South Staffordshire Water, has reassured its 1.6 million customers that their water supplies are safe following an apparent ransomware attack by the ransomware gang, Clop (aka Cl0p). It appears that the gang misidentified Cambridge Water as completely different organisation, Thames Water, which services properties in London and South East England.

Huawei radar on island nations

- Huawei has had a nearly two-decade presence in Mauritius, and the company states on its website that Huawei will play a key role in the development of an all-cloud Safe City based on the concept of 'one cloud and one pool,' harnessing centralised, mixed storage of videos, images, voice, and structured data gathered from multiple sources, including surveillance cameras.
- Huawei Marine Networks collaborated with E-marine, the leading provider of submarine cable solutions in West Asia, to complete the 260-kilometer Avassa Submarine Cable System marine installation in the Comoros Islands in 2016.
- In neighbouring Madagascar, a Smart City project was launched in 2015 in collaboration with the Huawei Group, and it has since gained momentum.
- The Solomon Islands government has secured a $66 million (A$96 million) loan from China to construct and supply 161 mobile communication towers. It is China's first loan to the Pacific country since it switched diplomatic allegiance from Taiwan to China in 2019.

Iranian threat actors target Albania and Israel

Iranian Threat Actors engaged in politically motivated disruptive activity against Albanian Government Organisations, according to Mandiant, a cybersecurity research firm. Mandiant identified the ROADSWEEP ransomware family and a Telegram persona targeting the Albanian government ahead of a conference hosted by an Iranian opposition organisation in late July 2022. This operation could indicate a greater willingness to take risks when using disruptive tools against countries perceived to be working against Iranian interests.

Official use of spyware in the EU

According to Microsoft, an Austrian firm, DSIRF GesmbH, created malicious software that was detected on the computer systems of some of its clients in at least three countries. DSIRF stated that its spying tool "Subzero" was only for official use in EU states. The spyware is capable of gaining access to confidential information such as passwords or login credentials at an unspecified number of banks, law firms, and strategic consultancies.

Bangladesh highly vulnerable to ransomware attacks

According to a recent Kaspersky survey, Bangladesh is at the top of the list of countries at risk of ransomware Trojan attacks. According to the survey, 3.69% of Kaspersky users in Bangladesh are victims of Trojan attacks, the highest rate in the world. Bangladesh ranked 83rd in the National Cyber Security Index (NCSI) published by Estonia in 2019, but advanced to 33rd in 2022. Following Bangladesh, the highest percentages of Trojan-affected users were reported in Haiti (1.79%), Sudan (1.69%), Turkmenistan (1.41%), Palestine (1.33%), Yemen (1.10%), Tajikistan

(1.03%), China (1.01%), Ethiopia (1%), and Pakistan (0.87%).

Major data breaches in India

- Akasa Air admitted to a data breach that allowed unauthorised individuals to view data from some of its customers. The incident was "self-reported" to CERT-In by Akasa Air.
- According to cyber security firm CyberX9, Vi (formerly Vodafone Idea) has exposed its users' data, which includes the records of more than 20 million postpaid customers, to possible breach. Phone numbers, addresses, call logs, SMS records, and mobile Internet usage information for approximately 301 million customers, including all postpaid users, were discovered to have been leaked online. Vodafone Idea denied the data breach, calling the report false and malicious.
- Hackers were discovered to have leaked Provident Fund (PF) data for approximately 28 crore Indians. A cybersecurity researcher from Ukraine discovered that details such as Universal Account Numbers (UANs), names, marital status, Aadhaar details, gender, and bank account details were exposed online.

Russia-Ukraine Cyber Conflict updates

Researchers have observed activities from a variety of threat actors, including hacktivists, nation-state APTs, and cyber criminals, since Russia began its military operations in Ukraine from February 2022. Following are major cyber-related activities in the region for the month of August:

- Meta released their in-depth threat research into a Russian troll farm that targeted numerous apps across the internet in an unsuccessful attempt to create the ‘false impression’ of widespread support for Russian military operations in Ukraine.
- Pro-Russian hacktivist group Killnet was accused of being involved in many cyberattacks this month. Killnet hackers launched a cyberattack on the website of Lockheed Martin, a weapons manufacturer, which manufactures the M142 High Mobility Artillery Rocket System (HIMARS) that the US has supplied to Ukraine. It also launched a large distributed denial-of-service (DDoS) attack in retaliation for Estonia's removal of a Soviet-era war memorial. Finally, websites belonging to Latvia's parliament were allegedly subjected to a distributed denial-of-service (DDoS) attack by Killnet.
- The ALPHV ransomware gang, also known as BlackCat, claimed responsibility for a cyberattack on Creos Luxembourg, a natural gas pipeline and electricity network operator in the country's central Europe.
- According to Spain's science ministry, the National Research Council, its leading scientific research body, was targeted by a ransomware attack that national authorities suspect originated in Russia.
- The Ukrainian Security Service (SSU) announced the dismantlement of a large Russian botnet operation used to spread Russian propaganda and disinformation.
- The Russian government named the Anonymous collective as one of the top four active hacking groups defending Ukraine, along with Squad303, American Ghostclan (USA), Ukraine's IT Army, and Georgian GNG.
- The Microsoft Threat Intelligence Center (MSTIC) took action to disrupt campaigns launched by SEABORGIUM, a Russian threat actor. Its campaigns include ongoing phishing and credential theft campaigns that result in intrusions and data theft.

- Russia was accused of launching a distributed denial-of-service (DD0S) attack on the website of Energoatom, the Ukrainian state corporation in charge of the country's four nuclear power plants.
- Roskomnadzor, Russia's internet watchdog, is developing Oculus, an automatic scanner that will use artificial intelligence to scan websites for prohibited information.
- According to the Montenegrin Agency for National Security, Russian services staged coordinated attacks on government servers, but the authorities were able to prevent any damage. However, the Cuba ransomware gang, a for-profit criminal enterprise claimed responsibility for the attack on the darkweb.
- NATO is assessing the impact of a data breach involving classified military documents sold online by a hacker group. MBDA Missile Systems confirmed that its data was among the stash, but claimed that none of the classified files that were released belonged to the company.

India File

- **India seizes $46m from crypto exchange Vauld**

  The local entity of Vauld, Flipvolt Technologies, has had assets worth $46.4 million frozen by India's anti-money laundering agency for facilitating "crime-derived" proceeds from predatory lending firms, in the latest setback for the crypto exchange, which filed for creditor protection. According to the Enforcement Directorate, Vauld's India entity failed to provide the agency with a complete trail of crypto transactions made by Yellow Tune, as well as KYC details for the wallets.

- **India signs 6 pacts with the Maldives including cybersecurity**

  The six agreements signed by India and the Maldives during Maldivian President Ibrahim Solih's visit to India include MOUs on cyber-security cooperation, training of Maldivian local government officials, data sharing and marine research collaboration for forecasting potential fishing zones, and disaster management cooperation.

- **India and Thailand agree to boost cooperation in cybersecurity**

  India and Thailand agreed to strengthen defence and security cooperation, including cybersecurity. Dr S Jaishankar and his Thai counterpart Don Pramudwinai, stated to the media that they had agreed to strengthen cooperation in defence and security, including cyber-security and the exchange of personnel and expertise. According to Dr S Jaishankar, the decision was made to increase joint training and exercises in defence and security, as well as recognise the importance of further cooperation in ICT.

- **United Nations *Ad hoc* Committee on Cybercrime holds 3rd session**

  The Third Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes is being held in New York from 29 August 2022 to 09 September 2022 in Hybrid mode. Smt. Muanpuii Saiawi, Joint Secretary (CD) is leading the Indian delegation to New York.

- **Government pulls data bill to make way for wider law**

  Based on the recommendations of a parliamentary panel, the government withdrew the draft personal data protection (PDP) bill introduced in 2019 in order to replace it with a broader legal framework on the digital ecosystem. The move comes after a joint Parliamentary panel requested 81 amendments to a bill with 99 sections. The bill had proposed to create three categories of personal data, sensitive personal data and critical personal data.

- **Hackers backed by the Chinese government targeted NIC**

  According to a report released by cybersecurity firm Recorded Future, Chinese government-backed hackers allegedly targeted India's National Informatics Centre (NIC) in a cyberattack. RedAlpha has also repeatedly spoofed login pages for India's NIC, which manages the Indian government's overall IT infrastructure and services.

- **Australia to unveil Centre of Excellence for Critical Technology**

  Australia intends to strengthen its alliance with India in critical technology areas and cybersecurity, and will soon open a Center of Excellence for Critical and Emerging Technology Policy in Bengaluru as part of a joint initiative with India. The centre would draw on critical technology policy expertise from academia, civil society, and government thought leaders in Australia and India to shape norms, policy frameworks, and standards.

- **India participates in CICA workshop hosted by Russia**

  The Conference on Interaction and Confidence Building Measures in Asia (CICA) held a workshop on Secure and sustainable development of the Internet on 24 August 2022 in virtual mode. Shri Ravi Shanker Goel, Deputy Secretary (Cyber Diplomacy) participated in the event.