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

CYBER *Digest*

May 2022

- **Update on Russia-Ukraine Cyber Conflict**
- **Ransomware attack on Oil India**
- **Chinese Hacking attempt on Ladakh's Power Grid**
- **US State Department launches Cyber Bureau**
- **UN Panel Coordinator endorses stricter sanctions on North Korea**
- **NATO conducts annual Locked Shields exercise**
- **Colombo Conclave holds Virtual Meet on Terrorism Investigation**
- **India File**

Update on Russia-Ukraine Cyber Conflict

Although a full-scale cyber campaign continues as part of the Ukraine -Russia conflict, these cyberattacks have not been on the scale envisaged prior to the conflict. Between the two, the cyberattacks on Russia appear more devastating while Ukraine seems to have been able to defend its networks better.[1] Among the more notable attacks:

- On the Ukrainian side, Viasat (used by Ukraine's military) modems were infected with Russian wiper malware. It is considered the most serious cyberattack in the conflict so far, with the GRU's Sandworm APT being considered the most likely suspect.[2]
- Sandworm was behind another attack that shut down substations at one of the Ukraine's main energy companies, resulting in blackouts for two million people. The malicious software employed in the attack was identical to that utilised by Russian hackers in earlier attacks on Kyiv that resulted in power outages.[3]
- Anonymous, the hacktivist collective that has come out in support of Ukraine uploaded 446 GB of data to the DDoSecrets dump site. Anonymous claimed to have targeted many Russian organisations ranging from private enterprises to the Tver Governor's office, the Blagoveshchensk City Administration, the Russian Federation's Ministry of Culture, and the Russian Orthodox Church's Department for Church Charity and Social Service.[4]
- The Ukrainian Ministry of Defenses' Main Intelligence Directorate doxed personal information on 620 people it alleges are FSB officials involved in Russia's conflict in Ukraine.[5]
- Influence networks operating on behalf of the Russian and Belarusian governments have been disrupted by Facebook's corporate parent Meta.[6]
- The Chinese government threat group "Bronze President" (also known as Mustang Panda, RedDelta, and TA416) has been seen conducting espionage activities against Russia in an effort to get a better understanding of the current status of the conflict.[7]

Ransomware attack on Oil India

Oil India, a public sector unit's operation in Assam was disrupted by a cyberattack on April 10 at their Geological and Reservoir department workstations. They received a ransom demand of USD 75,00,000 (about Rs 57 crore) from the attacker. A case has been registered under various sections of the Indian Penal Code and the Information Technology Act, 2000, after the company lodged a complaint with the police.[8]

The Intelligence Bureau has joined the investigation into the ransomware attack, as have the two national cyber security agencies – Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC). A senior police investigator stated that it was Russian malware planted from a server in Nigeria.[9]

On a related note, the REvil' ransomware group's new data leak site showed a data dump of OIL India though it is not clear if that is reason enough to attribute this attack to REvil or a group impersonating the group.[10] REvil was dismantled by the Russian authorities in January this year at the request of US government agencies.

Chinese Hacking attempt on Ladakh's Power Grid

Recorded Future, a US-based cyber security firm, said that Chinese government-linked cyber groups targeted at least seven Indian State Load Dispatch Centers (SLDCs) in northern India in a large cyber-espionage campaign. These centres are in charge of conducting real-time grid control and electricity dispatch operations in northern India. Shadowpad, one of the backdoor tools used in the operation, is thought to have come from Chinese Ministry of State Security contractors (MSS).

Internet Protocol (IP) cameras, which are often used in Closed-Circuit Television (CCTV) networks, and internet-operated Digital Video Recording (DVR) devices were most likely compromised in the Chinese operation.[11] However, according to Union Power Minister R K Singh, China has attempted three "probing cyberattacks" on India's power infrastructure in strategically positioned Ladakh since December 2021, but has been unsuccessful due to measures in place to prevent such incursions.[12]

US State Department launches Cyber Bureau

The United States State Department has established the Bureau of Cyberspace and Digital Policy, which is part of a long-term attempt to integrate international diplomacy into federal efforts to combat the rise of malicious nation-state cyberattacks and the spread of criminal ransomware. International Cyberspace Security, International Information and Communications Policy, and Digital Freedom will be the three policy units of the new government entity. The State Department is also working to create an Office of Special Envoy for Critical and Emerging Technology.[13]

UN Panel Coordinator advocates stricter sanctions on North Korea

Despite the most severe sanctions regime ever imposed by the United Nations on a nation state, North Korea has significantly increased its missile testing, notably in the last six months, according to Eric Penton-Voak of the United Nations Security Council's Panel of Experts on North Korea. The coordinator said that a stepped up focus was needed on cybercrime, which had become fundamental to Pyongyang's ability to finance its banned weapons programs. Penton-Voak claimed cyber activity has become "absolutely fundamental" to North Korea's ability to avoid UN sanctions and collect money for its nuclear and missile programmes, but the experts' panel biannual reports have not reflected this since member states have been hesitant to report breaches.

The recent theft of the Axie Infinity video game demonstrated that North Korean hackers were on the cutting edge of cyber technology. The theft of hundreds of millions of dollars' worth of bitcoin linked to Axie Infinity was linked to North Korean hackers in March, according to the US. On March 23, digital cash worth about $615 million was stolen, according to Ronin, a blockchain network that allows users to transfer crypto in and out of the game. According to a post on the official Ronin blog, the FBI has linked the hack to the Lazarus Group, a hacker group run by North Korea's Reconnaissance General Bureau. North Korea has also been accused of being involved in the "WannaCry" ransomware attacks, hacking of international banks and consumer accounts, and the Sony Pictures Entertainment cyberattacks in 2014.[14]

NATO conducts annual Locked Shields exercise

The annual NATO Locked Shields cyber exercise took place with simulated attacks on power grids and financial-messaging systems. Conducted by the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence, participants from NATO countries as well as allies including South Korea, Brazil, Finland, and Sweden undertook simulation exercises modelled on real-life attacks. Ukraianian experts also took part this year.

The simulations included attacks on a power grid for the first time. The Financial Services Information Sharing and Analysis Center, an industry group that aims to mitigate cyber threats in the sector, along with some top global firms, helped plan the financial part of Locked Shields exercises. Participants had to defend against mock cyberattacks on their reserve management and financial-messaging systems. Experts were drilled not only on how to defend technical networks, but also on other aspects of cyberattack, such as how to deal with legal disputes and how to notify the media about events.[15]

Colombo Conclave holds Virtual Meet on Terrorism Investigation

The National Investigation Agency of India hosted a one-day Colombo Security Conclave Virtual Conference on sharing experiences in Terrorism Case Investigation on April 19, 2022. The virtual conference drew panellists and participants from India, the Maldives, Mauritius, Sri Lanka, and Bangladesh. Participants reviewed the numerous issues associated with terrorism in their individual nations, as well as their experiences with terrorist prosecution, foreign fighter strategies, and combatting the misuse of the internet and social media. For successful investigation and prosecution of terrorism and radicalisation-related crimes, panellists emphasised the necessity for increased cooperation and coordination among member and observer countries of the Colombo Security Conclave.

India File

- **Meity Directions on Mandatory Reporting of Cyber Incidents**

The Ministry of Electronics and Information Technology emphasised in its "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet"[16] that service providers, intermediaries, data centres, body corporates, and government organisations are required to notify any breaches or leaks within six hours of their detection. This direction will come into effect within 60 days. It will have far-reaching ramifications as to how the entities mentioned above collect and store, the period for which it will be stored and the mandatory need to share it with the government in case of a breach.[17]

Furthermore, companies offering virtual private network (VPN) or cloud services in India may be required to collect, as well as maintain, extensive and accurate data of their consumers for five years under the direction. The failure to furnish the information or non-compliance with the directions, may invite punitive action.[18]

- **70% rise in Ransomware attacks on Critical Infrastructure**

According to a new analysis by cybersecurity firm Trellix, cyber-attacks on critical infrastructure by nation-state threat actors have escalated considerably, with

India seeing a 70% spike in ransomware activity in the fourth quarter (Q4) of 2021. Over half of adversarial advanced persistent threat actor activity originated from Russian and Chinese backed groups and Russian-backed groups like APT29 have continued to greatly increase their activity in 2022.

The report found a significant 73 per cent increase in cyber incidents targeting individuals and positioned people as the top attack sector in Q4 2021. Individual consumers are the top target of cybercriminals, closely followed by the healthcare vertical. Additionally, the transportation, shipping, manufacturing and information technology industries showed a sharp increase in threats. Malware was the technique used most often, accounting for 46 per cent of total cyber incidents.[19]

- **National Cyber Security Incident Response Exercise**

To bolster India's cyber posture, the National Security Council Secretariat organised the National Cyber Security Incident Response Exercise (NCX India) for government officials and critical sector organisations. National Security Advisor Ajit Doval inaugurated the National Cyber Security Incident Response Exercise, and the exercise was held from 18-29 April. The platform for training was provided by Cybexer Technologies, an Estonian cybersecurity company accredited for globally conducting several large cyber exercises.[20]

More than 140 officials were trained through training sessions, Live Fire and Strategic exercises. The participants were trained on various key cyber security areas such as Intrusion Detection Techniques, Malware Information Sharing Platform (MISP), Vulnerability Handling & Penetration Testing, Network Protocols & Data Flows, Digital Forensics, among others.[21]

- **Government initiatives to address cybercrime**

In response to a question in the Rajya Sabha, the Minister of State for Home Affairs gave a detailed reply on the various initiatives undertaken by the Central government to supplement the initiatives of the State Governments for the capacity building of their LEAs to combat cybercrime. Among those listed were

- Establishment of the National Cyber Forensic Laboratory in New Delhi to provide early stage cyber forensic assistance
- The National Cyber Crime Reporting Portal (www.cybercrime.gov.in) has been launched to enable the public to report incidents pertaining to all types of cybercrimes, with special focus on cyber-crimes against women and children.
- The Citizen Financial Cyber Fraud Reporting and Management System has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters.
- Seven Joint Cyber Coordination Teams have been constituted covering the whole country based upon cybercrime hotspots/ areas having multi-jurisdictional issues by onboarding States/UTs to enhance the coordination framework among the LEAs of the States/UTs.[22]

- **Cyber Diplomacy updates**

India and the United States held their fourth '2+2' dialogue with the Ministers of Defence and External Affairs meeting with their counterparts in Washington., D.C. on 11th April. The joint statement issued at the end of the Dialogue emphasised the considerable attention paid to cybersecurity. Considering growing national security threats from both state and non-state malicious cyber actors, the Ministers recognized the importance of an open, interoperable, secure, and reliable Internet and stable cyberspace. Both sides reaffirmed the 2021 reports of the UN Open Ended Working Group (OEWG) and the UN Group of Governmental Experts (UNGGE), which articulate a framework of responsible state behaviour in cyberspace and committed to work together in future multilateral negotiations to encourage States to implement the framework. They confirmed their intent to work closely as part of ongoing efforts to counter the use of information communications technologies for criminal purposes. The Ministers applauded the recent and upcoming meetings of the India-U.S. Cyber Dialogue and the Information and Communication Technology (ICT) Working Group to deepen cybersecurity cooperation. They strongly condemned ransomware and other cyber-related crimes and recognized the need to bolster protection of critical networks and infrastructure.[23]

- **Sixth India-Germany Cyber Dialogue**

India and Germany held their Sixth Cyber Dialogue in Berlin during 7- 8 April 2022. A five member Indian delegation was led by Ms. Muanpuii Saiawi, Joint Secretary (Cyber Diplomacy Division, Ministry of External Affairs). The German delegation was led by Ms.Regine Grienberger, Cyber Ambassador from Ministry of Foreign Affairs (MFA). The Dialogue began with a field visit to Germany's cyber facilities in the city of Bonn on 7 April 2022 followed by formal discussions in Berlin on 8 April 2022. Both sides exchanged views on national cyber policies, international developments in cyber domain and various other areas related to cyber space.

- **Fifth India-UK Bilateral Cyber Dialogue**

India and the UK held their Annual Cyber Dialogue in London on 11-12 April 2022. The Indian delegation was led by Ms. Muanpuii Saiawi, Joint Secretary Cyber Diplomacy Division, MEA. The UK delegation was led by Mr. Will Middleton (Cyber Director, Foreign, Commonwealth and Development Office). The meeting was attended by senior officials from several government ministries. Both sides welcomed the substantial bilateral engagement which covered cyber governance, deterrence and mutual resilience. They reiterated their commitment to a joint programme of action and next steps in implementing the Enhanced Cyber Security Partnership agreed upon by the two Prime Ministers in May 2021.[24]

[1] British intelligence. Report on the situation in Ukraine on the 69th day of the war at

https://thetimeshub.in/british-intelligence-report-on-the-situation-in-ukraine-on-the-69th-day-of-the-war/833/

[2] Satellite Modems Nexus of Worst Cyberattack of Ukraine War at

https://www.securityweek.com/viasat-satellite-modems-nexus-worst-cyberattack-ukraine-war

[3] Ukrainian power grid 'lucky' to withstand Russian cyber-attack at

https://www.bbc.com/news/technology-61085480

[4] Anonymous Hits Russian Ministry of Culture- Leaks 446GB of Data at https://www.hackread.com/anonymous-hits-russian-ministry-of-culture-leaks-446gb-of-data/

[5] Employees of the FSB of Russia involved in the criminal activities of the aggressor country in Europe at https://gur.gov.ua/content/sotrudnyky-fsb-rossyy-uchastvuiushchye-v-prestupnoi-deiatelnosty-stranyahressora-na-terrytoryy-evropy.html

[6] Facebook cracks down on covert influence networks targeting Ukraine at https://www.washingtonpost.com/technology/2022/04/07/facebook-covert-influence-ukraine/

[7] BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX at

https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx

[8] Oil India suffers cyber attack, receives Rs 57 crore ransom demand at

https://www.business-standard.com/article/companies/oil-india-suffers-cyber-attack-receives-rs-57-crore-ransom-demand-122041301002_1.html

[9] Oil India cyber attack: Russian malware planted from Nigeria at https://economictimes.indiatimes.com/news/india/oil-india-cyber-attack-russian-malware-planted-from-nigeria/articleshow/91010072.cms

[10] REvil reborn? Notorious gang's dark web site redirects to new ransomware operation at https://www.tripwire.com/state-of-security/security-data-protection/revil-dark-web-site-redirects-new-ransomware-operation/

[11] China used compromised cameras to snoop into India's power grids, says US-based group at https://www.indiatoday.in/india/story/china-used-compromised-cameras-snoop-india-power-grids-says-us-based-cyber-security-group-1934613-2022-04-07

[12] China tried to hack Power Grid systems in Ladakh thrice: R K Singh at

https://www.business-standard.com/article/current-affairs/china-tried-to-hack-power-grid-systems-in-ladakh-thrice-r-k-singh-122040701313_1.html

[13] State Department launches cyber bureau amid rising global tensions at

https://www.cybersecuritydive.com/news/state-department-bureau-cyberspace-digital-policy/621588/

[14] U.N. panel coordinator urges stepped up focus on North Korea cyber crime at

https://www.reuters.com/world/un-panel-coordinator-urges-stepped-up-focus-north-korea-cyber-crime-2022-04-20/

[15] NATO Cyber Exercise Proceeds Against Backdrop of Ukraine War at https://www.wsj.com/articles/nato-cyber-exercise-proceeds-against-backdrop-of-ukraine-war-11650480793

[16] No. 20(3)/2022-CERT-In at https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[17] Report breach within six hours: Govt frames cybersecurity norms at

https://www.hindustantimes.com/india-news/report-breach-within-six-hours-govt-frames-cybersecurity-norms-101651171521206.html

[18] Centre asks VPN services to log, hand over customer data at

https://www.hindustantimes.com/india-news/centre-asks-vpn-services-to-log-hand-over-customer-data-101651689707080-amp.html

[19] India sees 70% spike in ransomware attacks on critical infrastructure at

https://www.business-standard.com/article/technology/india-sees-70-spike-in-ransomware-attacks-on-critical-infrastructure-122042700442_1.html

[20] National Security Council Secretariat organises National Cyber Security Incident Response Exercise (NCX India) for Government officials and Critical Sector Organisations to strengthen India's Cyber posture at https://pib.gov.in/PressReleasePage.aspx?PRID=1817745

[21] National cyber exercise underway to train govt officials on cyber threat at

https://www.livemint.com/news/india/national-cyber-exercise-underway-to-train-govt-officials-on-cyber-threat-11650301347390.html

[22] Advanced Centre For Cyber Security at https://pib.gov.in/PressReleasePage.aspx?PRID=1814119

[23] Joint Statement on the Fourth India-U.S. 2+2 Ministerial Dialogue at https://www.mea.gov.in/bilateral-documents.htm?dtl/35184/Joint+Statement+on+the+Fourth+IndiaUS+22+Ministerial+Dialogue

[24] Fifth India-UK Bilateral Cyber Dialogue at https://www.mea.gov.in/press-releases.htm?dtl/35189/Fifth_IndiaUK_Bilateral_Cyber_Dialogue