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

CYBER *Digest*

February 2023

- **Lazarus group linked with attacks on Indian organisations**
- **UK's Royal Mail international services down after ransomware attack**
- **Russia accuses Western countries of being behind cyberattacks**
- **Nordic states agree to develop common cybersecurity strategy**
- **Iran faces cyber-attacks following support to Russia**
- **India File**

Lazarus group linked with attacks on Indian organisations

North Korean APT actor Lazarus Group has been linked to attacks on Indian public and private sector research organizations, including companies carrying out "health care research, a manufacturer of technology used in energy, research, defense, and health care verticals, as well as the chemical engineering department of a leading research university."[1] Finland based cybersecurity company, Withsecure, (formerly F-Secure Business) noted that the attackers had used two vulnerabilities to gain access to a Zimbra mail server to steal over 100 GB of data. Vulnerabilities in the same software were reportedly used to hack into the All India Institute of Medical Sciences towards the latter part of 2022.[2] Whilst the US Cybersecurity and Infrastructure Security Agency had put out an advisory in August 2022on the Zimbra vulnerability, the India Computer Emergency Response team (CERT-IN) had put out a similar advisory in October 2022.[3]

UK's Royal Mail international services down after ransomware attack

The UK's Royal Mail postal and courier service became the victim of a ransomware attack by actors using Lockbit ransomware software on January 11. The ransomware attack encrypted devices used for international shipping and caused ransom notes to be printed on printers used for customs dockets. [4] The postal service was still struggling to restore full services almost a month after the attack.[5]

Lockbit is a prolific ransomware gang, accounting for over 25% of 2903 ransomware attacks recorded in 2022.[6] The same group had targeted the Port of Lisbon towards the end of December 2022 and the California Finance department the previous month, exfiltrating over 75GB of data. Attacks using Lockbit first began in September 2019.[7]

Russia accuses Western countries of being behind cyberattacks

In the first comments by a Russian government official about cyber-attacks in the Russia-Ukraine conflict, Russian Deputy Foreign Minister Oleg Syromolotov, in an interview to the TASS news agency, accused the United States and the Western allies of "digital sabotage' using all the possible tools to carry out attacks against the country's critical infrastructure. Portraying Russia as the victim, he said that it had become the target of "coordinated aggression involving intelligence agencies, transnational IT corporations and hacker activists from the collective West and its puppets." Describing Ukraine being used as a springboard for cyberattacks on Russia and its partners, he said the attacks had increased in frequency and complexity over the year. This could be discerned from significant funds being pumped by Western countries "into personnel training and technical assistance in the Kiev regime's attempts to increase its offensive capabilities in terms of information and communication technologies" as well as the contributions by Microsoft and Amazon.[8]

For its part, the State Cyber Protection Centre of Ukraine (SSSCIP), the main government agency responsible for the protection of critical information infrastructure has been coming out with regular reports detailing Russian-linked cyber activities in Ukraine. A report published in January 2023, brought out in collaboration with the Economic Security Council of Ukraine, lays out a number of recommendations to secure global cyberspace, including the use of sanctions against aggressor countries, and updating international legal regimes to equate cyber attacks to war crimes. [9]

Nordic states agree to develop common cybersecurity strategy

Member states of the Nordic Council, including Denmark, Finland, Iceland, Norway, and Sweden, have agreed to develop a common cybersecurity strategy. Norway currently holds the 12-month rotating presidency of the Council. While the Nordic Council has been exploring the idea since 2016, the Russia-Ukraine conflict which has also resulted in cyber attacks on both Nordic and Baltic states, accelerated the process. Whilst Sweden is investing an additional $130 million in its military budget for 2023-2024 to bolster cyber capabilities, Finland's cybersecurity budget during the same period is being doubled to $80 million. Norway has also allocated 21 million euros for cyber defence. The implementing agency, Nordic Defense Cooperation group, is expected to be tasked with improving intelligence sharing between the militaries and civilian agencies across the Nordic countries.[10]

Iran faces cyber-attacks following support to Russia

Iran has become a target of cyber attacks following its support of Russia as supply of drones to the Russian war effort. Targets have included the Central Bank of Iran, the website of Iran's supreme leader Ali Khamenei, and the National Iranian Oil Company (NIOC).[11] DDOS attacks and website defacements have formed most of the incidents and though the identity of the attackers is unclear, they are believed to be pro-Ukraine activists. The internet in Iran has faced a turbulent year with stringent censorship following antigovernment protests coupled with cyber-attacks by hacktivists against Iranian government sites and critical infrastructure.[12] On the 25th of January, there was a nation-wide drop in internet traffic for ten minutes which the authorities blamed on a cyber attack though the perpetrators were not identified.[13]

India File

- Following the AIIMS cyber attack, the Union Ministry of Home Affairs (MHA) is creating a new wing of “special commandos” who will be based at the district headquarters across the country. [14] Personnel would be specially recruited and trained to be able to respond quickly to cyber incidents. The states have also been brought on board to provide unhindered legal and administrative support.[15]

- The CEO of the UK National Cyber Security Centre, Lindy Cameron, held meetings with National Cyber Security Coordinator, Lt. Gen. (Dr.) Rajesh Pant, the Director General of CERT-IN, Dr Sanjay Bahl, as well as the Secretary of the Ministry of Electronics and Information Technology (MEITY), Shri Alkesh Sharma, during her visit to India. This is the first visit since the India-UK cyber statement was agreed to in 2022, reaffirming the countries' shared commitment to promoting an open, secure, stable, accessible and peaceful cyberspace.[16]

- The Quad Senior Cyber Group Principals, Deputy National Security Advisers of Japan and US respectively, Masataka Okano, and Anne Neuberger, Michael Pezzullo, Secretary, Department of Home Affairs, Australia, and Lt Gen. Rajesh Pant, National Cyber Security Coordinator, India, along with their inter-agency delegations, met in New Delhi on 30-31 January 2023. During the meeting, participants discussed sharing threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security requirements to improve the broader software development ecosystem for the benefit of the Indo-Pacific region.[17]

- The second edition of the 4-month long hackathon, Sainya Ranakshetram 2.0, organised under the Army Training Command (ARTRAC), ended on January 17th.[18] The event was aimed at identifying indigenous talent in niche domains of Cyber Deterrence, Security Software Coding, Electromagnetic Spectrum Operations (EMSO) and Artificial Intelligence / Machine Learning (AI/ ML). The prize winners of the event were felicitated by Army Chief General Manoj Pande.[19]

[1] *The Record*, Hackers linked to North Korea targeted Indian medical org, energy sector - https://therecord.media/hackers-linked-to-north-korea-targeted-indian-medical-org-energy-sector/

[2] *The Hindu* , Investigators asking E&Y about its audit of hospital's cyber systems - https://www.thehindu.com/news/national/aiims-cyber-attack-investigators-asking-ey-about-its-audit-of-hospitals-cyber-systems/article66218762.ece

[3] *CERT-In*, CERT-In Vulnerability Note CIVN-2022-0401 Multiple Vulnerabilities in Zimbra Original Issue October 20, 2022 https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2022-0401

[4] *BBC News*, Royal Mail hit by Russia-linked ransomware attack https://www.bbc.com/news/business-64244121

[5] *Computer Weekly*, Post Office branches struggling after Royal Mail cyber attack https://www.computerweekly.com/news/365530230/Royal-Mail-branches-still-struggling-after-cyber-attack

[6] *Financial Times*, How Royal Mail's hacker became the world's most prolific ransomware group, https://www.ft.com/content/5d53c9fe-ce36-444b-bcf0-f55f81cff93d

[7] *Kaspersky*, LockBit ransomware — What You Need to Know, https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

[8] *TASS*, Russia becomes target of West's coordinated aggression in cyberspace https://tass.com/russia/1568405

[9] *SSSCIP Ukraine*, Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression

https://cip.gov.ua/en/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi

[10] *C4ISR*, Nordic states to develop common cybersecurity strategy https://www.c4isrnet.com/global/europe/2023/01/17/nordic-states-to-develop-common-cybersecurity-strategy/

[11] *Reuters*, Iran says it foiled cyberattack on central bank https://www.reuters.com/world/middle-east/iran-says-it-foiled-cyberattack-central-bank-2023-01-06/

[12] *The Record*, Iran's support of Russia draws attention of pro-Ukraine hackers https://therecord.media/irans-support-of-russia-draws-attention-of-pro-ukraine-hackers/

[13] *Al Arabiya English*, Iran blames cyberattack for internet disruption: Report https://english.alarabiya.net/News/middle-east/2023/02/02/Iran-blames-cyberattack-for-internet-disruption-Report

[14] *The Tribune India*, Soon, cyber commandos to battle growing online threat https://www.tribuneindia.com/news/nation/soon-cyber-commandos-to-battle-growing-online-threat-474442

[15] Deccan Chronicle, MHA plans to create a specialised cyber wing in each district, https://www.deccanchronicle.com/nation/crime/300123/mha-plans-to-create-a-specialised-cyber-wing-in-each-district.html

[16] *High Commission of India, UK*, India-United Kingdom Cyber Statement https://www.hcilondon.gov.in/news_letter_detail/?id=46

[17] *Press Information Bureau, India*, Quad Senior Cyber Group Meets in New Delhi to Strengthen Cybersecurity Cooperation, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1895073

[18] *Sainya Ranakshetram* website, https://www.sainya-ranakshetram.in/

[19] *Indian Express*, Amid increasing cyberattacks, Army organises event to seek innovative solutions to cyber challenges, https://indianexpress.com/article/cities/delhi/cyberattacks-army-event-innovative-solutions-cyber-challenges-8391805/