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

# CYBER *Digest*

October 2022

- Iran-Albania cyber conflict intensifies
- Australia to modify privacy laws after Optus breach
- China accuses the US of cyberspying on universities
- Cyber Espionage around South China Sea
- Worok APT activities in Central Asia & Middle East
- Microsoft discloses TikTok cybersecurity vulnerabilities
- Lazarus Group cyberattacks on energy companies
- Uber data breach
- Bangladeshi Hacktivists launched cyberattacks on GOI websites
- Chinese cyber criminals steal $529m from Indian citizens
- Quad moves to counter cyberattacks from the China
- Russia-Ukraine cyber conflict
- India File

## Iran-Albania cyber conflict intensifies

Albania severed diplomatic relations with Iran and expelled its diplomats following a cyberattack blamed on the Iranian government in July, a move supported by the US, which promised to take action in response to the attack on its NATO ally. Albania and Iran have had tense relations since 2014, when Albania accepted 3,000 members of the exiled opposition group People's Mujahideen Organization of Iran, also known as Mujahideen-e-Khalq in Farsi, who have settled in a camp near the country's main port of Durres. Furthermore, Albania reports that it has been subjected to additional cyberattacks from Iran, presumably in response to Tirana's split with Tehran over the July cyber incidents. Iran allegedly took down the Total Information Management System (TIMS) used in Albania for border control.

As the contours of Iranian cyberattacks on Albania's government networks became clearer, the US Treasury Department imposed sanctions on Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence, Esmail Khatib, for their role in the NATO country's cyberattacks. However, Iran condemned the US action, with the Foreign Ministry claiming that the Albanian government made a false accusation. The US Cybersecurity and Infrastructure Security Agency (CISA) has issued a joint warning with the FBI outlining Iran's cyber campaign against Albania. The warning includes suggested safeguards and mitigations in the event that the campaign spreads to targets outside of Albania. Due to shared experiences of being targeted by Iranian cyber operations, Israel has also offered cyber defence assistance to Albania.

## Australia to modify privacy laws after Optus breach

After hackers targeted Optus, Australia's second-largest telecommunications company, the country aims to alter its privacy laws so that banks can be notified more quickly when a company is the victim of a cyberattack. Optus, which is owned by Singapore Telecommunications Ltd, revealed that databases containing the home addresses, driver licence numbers, and passport numbers of up to 10 million customers - roughly 40 percent of Australia's population - were compromised in one of the country's largest data breaches. Australia has been working to strengthen its cyber defences, and in 2020 pledged to spend A$1.66 billion ($1.1 billion) over a decade to fortify company and household network infrastructure.

## China accuses the US of cyberspying on universities

China accused the US of hacking into computers at Northwestern Polytechnical University, which, according to US officials, conducts military research, adding to both states' complaints about rampant online spying on each other. The National Computer Virus Emergency Response Center reported computer break-ins at Northwestern Polytechnical University. It stated that the centre, in collaboration with a commercial security provider, Qihoo 360 Technology Co., traced the attacks back to the National Security Agency, but did not specify how. Northwestern Polytechnical University, located in the western city of Xi'an, is on a US government "entity list," which restricts its access to American technology. According to Washington, the university assists the PLA in the development of aerial and underwater drones, as well as missile technology.

## Cyber Espionage around South China Sea

A cyber espionage campaign delivered the ScanBox exploitation framework to targets who visit a malicious domain masquerading as an Australian news website, according to a report by the Proofpoint Threat Research Team that provides a moderate confidence assessment on recent campaigns targeting the federal government, energy, and manufacturing sectors globally may be recent efforts by TA423 / Red Ladon. In governmental indictments, activity that overlaps with this threat actor has been publicly referred to as "APT40" and "Leviathan." TA423 / Red Ladon is an espionage-motivated threat actor based in China that has been active since 2013, targeting a variety of organisations in response to political events in the Indo-Pacific region, with a focus on the South China Sea. Defence contractors, manufacturers, universities, government agencies, legal firms involved in diplomatic disputes, and foreign companies involved in Australasian policy or South China Sea operations are among the organisations targeted.

## Worok APT activities in Central Asia & Middle East

Researchers have discovered targeted attacks against various high-profile companies and local governments, mostly in Asia, Middle East, and Africa that used pirated tools. These attacks were carried out by Worok, a previously unknown espionage group that has been active since at least 2020. Worok's toolkit includes a C++ loader CLRLoad, a PowerShell backdoor PowHeartBeat, and a C# loader PNGLoad that extracts hidden malicious payloads from PNG files using steganography. It is unclear who Worok works for despite significant circumstantial overlap with other organisations, some of which are connected to Beijing.

## Microsoft discloses TikTok cybersecurity vulnerabilities

Microsoft disclosed a flaw in the TikTok Android app that threat actors could have used to hijack TikTok user accounts with a single click. Fortunately, TikTok patched the vulnerability before it was publicly disclosed in early 2022. However, shortly after Microsoft publicly disclosed the vulnerability, a Breach Forums user claimed to have access to a server containing 6.7TB of TikTok and WeChat data stolen. While TikTok appears to be investigating the matter, the company has denied any claims that it was the victim of a data breach.

## Lazarus Group cyberattacks on energy companies

A new cyber espionage campaign targeting US, Canadian, and Japanese energy providers has been linked to the North Korean state-sponsored Lazarus hacking group, according to security researchers. According to Cisco Talos research, the hackers exploited a year-old Log4j vulnerability known as Log4Shell to compromise internet-exposed VMware Horizon servers in order to gain an initial foothold on a victim's enterprise network before deploying bespoke malware known as "VSingle" and "YamaBot" to gain longterm persistent access. Japan's national cyber emergency response team, recently linked YamaBot to the Lazarus APT.

## Uber data breach

Uber discovered that its computer network had been hacked, prompting the company to shut down several internal communications and engineering systems while it investigated the extent of the breach. Uber believes the attackers are members of the Lapsus$ hacking group. This group typically employs similar techniques to target technology companies, and has breached Microsoft, Cisco, Samsung, Nvidia, and Okta, among others, in 2022 alone. It was also reported that the same actor breached the security of video game developer Rockstar Games. Uber is working closely with the FBI and the US Department of Justice on this matter.

## Bangladeshi Hacktivists launched cyberattacks on GOI websites

Mysterious Team Bangladesh (MT), a hacktivist group targeting Indian government websites and servers, has been discovered by CloudSEK, an AI-powered cyber intelligence and threat detection company. The attacks resemble those launched by DragonForce in early 2022. The threat actor is primarily motivated by hacktivism and has ties to the Indonesian hacktivist group "Hacktivist of Garuda." They have also been involved in mass reporting of content across public platforms such as YouTube, Facebook, and Linkedin. CloudSEK concluded that Mysterious Team used the Raven Storm tool for DDoS attacks. The tool employs multithreading to send multiple packets at the same time in order to bring the server down.

## Chinese cyber criminals steal $529m from Indian citizens

According to Uttar Pradesh's cybercrime unit, Chinese scammers stole $529 million from Indian residents using instant lending apps, part-time job offers, and bogus cryptocurrency trading schemes. The scammers advertised their scheme via bulk TXT messages, which the police traced to the Middle Kingdom, with some operators based in Nepal and directed by Chinese threat actors. Fake websites and cryptocurrency apps were set up to entice investors. Furthermore, so far, the Enforcement Directorate has conducted search operations on the 12 Chinese companies involved in the Part-Time Job Fraud case in Bengaluru, seizing Rs.5.85 crore under the Prevention of Money Laundering Act, 2002.

## Quad moves to counter cyberattacks from the China

The Foreign Ministers of the Quad grouping released a joint statement on ransomware — the first of its kind — proclaiming their resolve to take action against malicious cyber activities targeting key infrastructure and focusing on state-sponsored cybercrime coming from China, Russia, and Iran. The joint statement was released during a meeting between External Affairs Minister S Jaishankar and counterparts from the US, Australia, and Japan on the sidelines of the UN General Assembly session in New York. The Quad countries commit to further cooperation on capacity-building programmes and initiatives aimed at improving regional cybersecurity and resilience against ransomware attacks in the Indo-Pacific, according to the statement.

## Russia-Ukraine cyber conflict

In order to impede the Ukrainian military's offensive operations, Ukraine claimed that the Kremlin planned to launch cyberattacks against its energy sector. Following are major cyber-related activities in the region for the month of September:

- Officials in Montenegro and Bulgaria accused Russia of conducting cyber-attacks on their countries' infrastructures. The National Security Agency of Montenegro (ANB) reported that several Russian agencies were responsible for a hack on critical IT systems of state institutions. Bulgaria's former ruling Gerb party said it was attacked by Russian hackers who targeted three specific publications on its social media pages.

- Privateers of the BlackCat/ALPHV ransomware have claimed responsibility for an attack on the Italian renewable energy provider Gestore dei Servizi Energetici SpA (GSE). They had previously targeted Eni SpA, Italy's largest energy company, though with hardly any impact on the utility's operations, and have also claimed attacks against Creos Luxembourg S.A., a natural gas pipeline and electrical grid operator, and Oiltanking, a German oil supply company. BlackCat/ALPHV is a Russian gang that is widely assumed to be a rebranding of the BlackMatter/DarkSide gang.

- According to Google researchers, a growing body of evidence suggests that pro-Russian hackers and online activists are collaborating with the GRU, the country's military intelligence agency. The GRU organises the activities of purported hacktivist groups and provides them with GRU tools to attack Ukrainian networks. Killnet is one of the hacktivist front groups that is most likely associated with the GRU.

- The Void Balaur cyber mercenary group, which specialises in hack-for-hire operations and has been active in the criminal-to-criminal market since 2016, has expanded its operations. New targets include a wide range of industries, many of which have specific business or political ties to Russia.  A unique and short-lived connection links Void Balaur's infrastructure to the Russian Federal Protective Service (FSO), implying a low-confidence customer relationship or resource sharing between the two.

- Meta closed down two unconnected networks in China and Russia for violating their policy against coordinated inauthentic behaviour. The Russian network, which was the largest of its kind to be disrupted by Meta since the beginning of the Ukrainian war, primarily targeted Germany, France, Italy, Ukraine, and the United Kingdom with narratives focused on the war and its impact via a sprawling network of over 60 websites impersonating legitimate news organisations.

- The websites of the Tokyo Metro and Osaka Metro have been rendered inaccessible on the second day of cyberattacks on Japan, with a pro-Russia hacker group, Killnet, claiming responsibility for the attack on social media.

## India File

- **India and the UK conduct a 'Cyber Security Exercise' for 26 countries**

  A 'Cyber Security Exercise' for 26 countries was successfully designed and conducted by India's National Security Council Secretariat (NSCS) and the UK Government in collaboration with BAE Systems (British Aerospace). The goal of the virtual Cyber Exercise on Ransomware Resilience was to simulate a large, widespread cyber security incident affecting organisations throughout a country. The exercise was conducted as part of the International Counter Ransomware Initiative-Resilience Working Group, which is led by India and handled by the NCSC. There were over 26 invitees, from CRI Partner Nations and their respective organisations; including Cyber Security, National Crisis Management, National Security Policy, Critical National Infrastructure, and Law Enforcement Agencies.

- **Ad hoc Committee on Cybercrime**

  The Third Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 29 August 2022 to 09 September 2022 in Hybrid mode. Muanpuii Saiawi, Joint Secretary (NEST & CD) led the Indian delegation to New York. During the Session, provisions on International Cooperation, technical assistance, preventive measures and the mechanism of implementation were discussed.

- **SCO Expert Forum on Information Security**

  Shanghai Cooperation Organisation Expert Forum on Information Security was held on 6 September 2022 in virtual mode. During the Session, India spoke on 'Expanding access to information is an important factor in the development of modern society', 'Information and ideological threats and the development of effective response measures' and 'Protection of objects of critical information infrastructure in the conditions of dynamic development of ICT'.

- **India-US Bilateral Cyber Dialogue**

  The Deputy NSA, NSCS- led Fourth India-US Bilateral Cyber Dialogue was held in Washington DC, USA from 21-23 September 2022.

- **India, Vietnam decide to strengthen cyber security cooperation**

  The Second India-Vietnam Security Dialogue, held at the Deputy National Security Advisor and Deputy Minister levels, agreed to strengthen cyber and maritime security cooperation in the face of China's aggression in the Indo-Pacific region. On such capacity-building programmes, India will be guided by the Vietnamese side's requirements. India also offered to share its cyber security expertise and domain knowledge.