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

CYBER *Digest*

June 2024

- **2024 Cybersecurity Posture of the United States report released**
- **Kosovo government websites face cyberattacks**
- **Details of British soldiers leaked in a data breach**
- **Pakistan-based threat actors target Indian military officials**
- **Increasing cybercrimes in India from Southeast Asia**
- **Thailand to set up a cyber command center**
- **India File**

2024 *Cybersecurity Posture of the United States* report released

The Office of the National Cyber Director (ONCD) has released the 2024 Report on the Cybersecurity Posture of the United States.[1] The report offers crucial updates on the nation's efforts to tackle the challenges in cyberspace. This report highlights the cybersecurity threats and issues facing the United States, including new and emerging technologies that may impact national security, economic prosperity, and the rule of law. It also includes an assessment of the strategic environment and examines the landscape of emerging technologies and cyber risks, presenting both challenges and opportunities for U.S. cybersecurity policy and strategy. The document also covered the actions taken by the federal government during 2023.

Kosovo government websites face cyberattacks

According to reports, Russian hackers targeted government websites in Kosovo.[2] A government official confirmed that several websites were temporarily unavailable due to a distributed denial-of-service (DDoS) attack. It was also reported that the incident impacted the websites of the president and prime minister. Other government ministers suggested a possible Russian connection to the hack. The foreign minister of Kosovo asserted that Russia is targeting Kosovo in response to Kosovo's decision to supply military equipment to Ukraine

Details of British soldiers leaked in a data breach

According to reports, the data breach exposed the names and bank details of thousands of serving British soldiers, sailors, and air force members.[3] The breach is suspected to have involved state-sponsored actors. The breach affected a third-party payroll system that held bank details for up to 272,000 serving armed forces personnel and recent veterans. In some instances, addresses may have been exposed as well. The responsible threat actor and any potential state backing have not been officially confirmed.

Pakistan-based threat actors target Indian military officials

A threat intelligence firm recently intercepted Android malware believed to have been deployed by a Pakistan-based APT group targeting Indian defense personnel.[4] Surprisingly, this campaign has been active for over a year. The payload was likely generated by the Spynote Android remote administration tool or a modified version known as 'Craxs Rat'. Further investigation revealed that the delivered payload was part of a campaign that had been active for a year. It bears similarities to a payload flagged on VirusTotal, communicating with the same C2 server. The threat actor used social engineering by impersonating a senior officer and attempting to deliver the app directly via WhatsApp. They tried to make the files appear defense-related, but once installed, the app names differed from the names displayed when clicked.

In another incident, an assessment revealed that the Indian government, along with the defense and aerospace sectors, were allegedly targeted by a suspected Pakistan-based hacking group between late 2023 and April 2024.[5] It was also reported that the roots of the espionage campaign were

traced to Pakistani cities, specifically targeting three state-owned companies involved in aerospace and defense. According to the assessment, the group deployed a range of malicious tools similar to those used in previous campaigns conducted by Transparent Tribe. Transparent Tribe, also known as APT36, ProjectM, Mythic Leopard, and Earth Karkaddan, is a suspected Pakistan-based cyber espionage threat group, according to reports.

Increasing cybercrimes in India from Southeast Asia

According to reports, nearly half of the financial frauds targeting Indians originate from the three Southeast Asian countries of Myanmar, Cambodia, and Laos.[6] Many web applications used to commit these frauds are written in Chinese, suggesting a possible Chinese connection. In the first four months of the year, Indians lost over Rs. 1,776 crore in 89,054 cases of financial crimes, including digital arrest, stock market scams, investment scams, and romance or dating scams. There has been a notable increase in organized crime in Southeast Asia.

In response to the growing malicious activities, Indian authorities have arrested five people accused of trafficking unwitting job seekers into Southeast Asian scam compounds.[7] This action comes shortly after the repatriation of dozens of Indian nationals who had been lured into "fraud factories" in Cambodia and Laos. Southeast Asia's cyber fraud industry, primarily operated by Chinese organized crime groups with local connections, is fueled by a forced labor pool. People are lured into large scamming compounds with the promise of job opportunities.

To address this, the government has established an inter-ministerial committee comprising various law enforcement and intelligence agencies to address the recent surge in transnational organized cybercrimes targeting Indians from Southeast Asian countries such as Cambodia.[8] Rajesh Kumar, chief executive officer of the Indian Cybercrime Coordination Centre (I4C), announced at a press conference that the Ministry of Home Affairs (MHA) set up the committee on May 16, and it has held two meetings so far.

Thailand to set up a cyber command center

The Royal Thai Armed Forces (RTARF) have been directed to establish a Cyber Command Centre by October 1, aiming to increase military capability, enhance cybersecurity, and counter technological threats.[9]The order was issued by the Defence Minister during a Defence Council meeting in response to concerns over new forms of warfare and global threats, particularly the use of modern technology for attacks or espionage against national security agencies worldwide. The initiative aims to enhance Thailand's cyber capabilities by developing cyber personnel through collaboration with educational institutions, the private sector, and security agencies. The goal is to produce 300-500 skilled personnel annually, as reported.

India File

- Ransomware attacks against Indian organizations dropped to 64 percent this year from 73 percent last year,

according to an assessment.[10] However, while the number of targeted firms has decreased, the impact on victims has become more severe, with higher ransom demands and increased recovery costs compared to the previous year. It was also reported that Indian organizations were more inclined to recover data by paying the ransom (65 percent) rather than utilizing backups (52 percent). Around 44 percent of impacted computers were encrypted in attacks against Indian victims, and 34 percent of these attacks involved data theft in addition to encryption.

- According to reports, the Russian ransomware group LockBit has claimed to have successfully hacked the computer systems of two Kerala-based companies.[11] On its dark web portal, LockBit announced that it had targeted four Indian companies, including two in Kerala. It is also reported that, as part of its claim, LockBit has posted pictures of bank account details, invoices, purchase orders, supply details, content from computer drives, and employees' driving licenses on its dark web portal.

- According to reports, the Tamil Nadu police's Facial Recognition Portal, a software used to track criminals and missing persons, has been compromised.[12] Data samples from the portal have been made available for sale on the dark web. An analysis of the leaked samples indicates that 1.2 million lines of data, including names of police officers, phone numbers, and FIR details, have been accessed illegally. A group named 'Valerie' has claimed responsibility for the breach. They have compromised a file containing 55,000 lines of data on police officials, including IPS officers, another file with 890,000 lines of FIR data, and a third file with 2,700 lines of data on police stations (mostly available in the public domain).

- A threat intelligence report identified a spike in malicious cyber activity targeting the election in India.[13] This activity is reportedly supported by multiple independent hacktivist groups that coordinate cyber-attacks and publish stolen personally identifiable information (PII) of Indian citizens on the dark web. The report identified 16 groups involved in targeting multiple law enforcement, government, healthcare, financial, educational, and private sector organizations in India. These groups took advantage of geopolitical narratives before the recent elections.

- It was reported that a non-password-protected database containing over 1.6 million documents belonging to a leading Indian provider of biometric authentication solutions was exposed.[14] The records included the biometric identity information of police, army, teachers, and railway workers. The data might have been for sale on a dark web-related Telegram group.

[1] Office of the National Cyber Director, 2024 Report on the Cybersecurity Posture of the United States, May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

[2] The Record, Kosovo's government reportedly faces Kremlin-backed cyberattacks, 11 May 2024, https://therecord.media/russian-hackers-kosovo-ddos-pristina

[3] AP, The UK says a huge payroll data breach by a 'malign actor' has exposed details of military personnel, 7 May 2024, https://apnews.com/article/uk-defense-ministry-data-breach-china-49899b429f138bb2075d9fd6703ac7b0.

[4] Cyfirma, New Pakistan-based Cyber Espionage Group's Year-Long Campaign Targeting Indian Defense Forces with Android Malware, 3 May 2024, https://www.cyfirma.com/research/new-pakistan-based-cyber-espionage-groups-year-long-campaign-targeting-indian-defense-forces-with-android-malware.

[5] Business Standard, Pakistani hackers may have hit 3 major Indian defence firms. Find out which, 28 May 2024, https://www.business-standard.com/external-affairs-defence-security/news/pakistani-hackers-may-have-hit-3-major-indian-defence-firms-find-out-which-124052801049_1.html

[6] The Hindu, 'Cambodia, Myanmar, Laos emerge hub of organised financial crimes targeting Indians', 22 May 2024, https://www.thehindu.com/news/national/cambodia-myanmar-laos-emerge-hub-of-organised-financial-crimes-targeting-indians/article68204329.ece

[7] The Record, Indian police arrest five accused of trafficking people into scam compounds, 30 May 2024, https://therecord.media/india-arrests-human-trafficking-southeast-asia-scam-compounds?ref=news.risky.biz

[8] The Indian Express, MHA sets up high-powered committee to tackle increasing cybercrimes originating from SE Asian region, 22 May 2024, https://indianexpress.com/article/india/mha-high-powered-committee-cybercrimes-from-se-asia-9345843/

[9] The Nation, Military to set up Cyber Command Centre by October, 25 May 2024, https://www.nationthailand.com/news/general/40038311

[10] Business Standard, 64% firms report ransomware attacks in India; 65% opt to pay ransom: Report, 14 May 2024, https://www.business-standard.com/industry/news/64-firms-report-ransomware-attacks-in-india-65-opt-to-pay-ransom-report-124051400881_1.html

[11] The New Indian Express, LockBit ransomware group claims cyber attacks on two Kerala-based companies, 15 May 2024, https://www.newindianexpress.com/states/kerala/2024/May/15/lockbit-ransomware-group-claims-cyber-attacks-on-two-kerala-based-companies.

[12] The New Indian Express, Tamil Nadu police's face recognition portal hacked; FIR, personal information up for sale, 5 May 2024, https://www.newindianexpress.com/states/tamil-nadu/2024/May/05/tamil-nadu-polices-face-recognition-portal-hacked-fir-personal-information-up-for-sale

[13] Resecurity, Cybercriminals Are Targeting Elections In India With Influence Campaigns, 21 May 2024, https://www.resecurity.com/blog/article/cybercriminals-are-targeting-elections-in-india-with-influence-campaigns

[14] Websiteplanet, Indian Military & Police Biometrics Exposed in Data Breach, 23 May 2024, https://www.websiteplanet.com/news/india-biometric-breach-report.