INDIA FUTURE FOUNDATION

INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

IN THE SPOTLIGHT

INDIA'S NEW CYBER RULES FOR TELECOMS SPARK PRIVACY CONCERNS

The Department of Telecommunications (DoT), Government of India recently introduced stringent cybersecurity rules under the Telecom Act, 2023 to safeguard critical infrastructure networks. These rules came into force on 21 November 2024. However, privacy experts warn that these regulations could compromise the fundamental privacy rights of users'.

The new rules require telecom entities to report cybersecurity incidents within six hours, share user traffic data with cybersecurity authorities and implement comprehensive cybersecurity policies. While the regulations aim to protect telecom networks, they grant the government access to user metadata, raising significant privacy concerns.

IN THIS NEWSLETTER

The rules specify that the data collected should be only used for telecom cybersecurity. However, experts believe that the vague phrasing could allow misuse, leading to potential violations of citizens' digital rights.

Impact on the Telecom Industry

As per the rules, telecom companies must submit a detailed report on cybersecurity incidents within 24 hours of the initial six-hour notification, a timeline criticized as "unrealistic" by many experts. Global standards, such as the General Data Protection Regulation (GDPR), 2016, require incident reporting within 72 hours, offering a more feasible approach.

While experts have raised concerns about the new rules, another school of thought is of the view that compliance with these regulations is expected to increase operational costs, potentially resulting in higher consumer prices.

India's regulatory approach highlights the ongoing challenge of balancing security with privacy, underscoring the importance of revisiting these rules to ensure inclusivity and transparency.

CYBERSECURITY AND INTERNET TRENDS DURING THE 2024 US ELECTIONS

The 2024 U.S. election underscored the critical role of Internet security and traffic management in ensuring the integrity of democratic processes. Despite the high-stakes environment and potential cyber threats, Cloudflare's (one of the biggest networks operating on the Internet) analysis revealed a stable online infrastructure supporting campaigns, voter information portals and election-related activities.

Key Observations

- **Cybersecurity Resilience**
  - Between 31 October 2024 and 1 November 2024, over 6 billion malicious HTTP DDoS requests targeting U.S. election-related websites were mitigated.
  - Cyberattacks increased significantly as the elections neared, but Cloudflare ensured no major disruptions occurred to government or campaign websites.

- **Traffic Surges**
  - Traffic spikes were most notable in states like Maine, South Dakota, and Montana, reflecting heightened public engagement.

- **DNS Trends**
  - Websites of news outlet websites and polling services experienced dramatic traffic increases, with DNS requesting traffic to polling services up 756 per cent during poll closures.

- **Cyber Threats Analysis**
  - Notable DDoS attacks targeted campaign and state political party websites, peaking at rates exceeding 700,000 requests per second.
  - Such intense attacks were effectively neutralised through advanced defence mechanisms.

Cloudflare’s Role in Election Security

Cloudflare fortified the election ecosystem through its Athenian Project, Project Galileo and partnerships with organisations like CISA(America’s Cyber Defense Academy). Over 800 election-related websites benefited from tools designed to prevent service disruptions, ensuring voters and stakeholders had uninterrupted access to critical information.

Implications for Future Elections

The U.S. elections demonstrated that coordinated efforts between cybersecurity providers, government bodies and non-profit organisations can safeguard democratic processes. Continued investments in resilient digital infrastructure will be empowered to mitigate evolving cyber threats.

FAKE COPYRIGHT CLAIMS DELIVERING RHADAMANTHYS MALWARE

Cybercriminals are exploiting fake copyright claims in a phishing campaign to distribute a new variant of Rhadamanthys Stealer, CopyRh(ight)adamantys. These attacks target individuals and organisations globally, accusing them of copyright infringement to trick them into downloading malware.

Attackers, using Gmail accounts, impersonate legitimate companies to send fraudulent emails. These emails contain malicious links or files that, when accessed, install Rhadamanthys Stealer, enabling the theft of sensitive data such as credentials and financial information of individuals accessed the link.

The campaign, identified by Check Point researchers, mainly aimed at industries like media, technology, and software. It leverages artificial intelligence for automated phishing but shows occasional localisation errors. Despite its advanced approach, the operation is linked to financially motivated cybercrime groups rather than state-sponsored actors.

Businesses are thereby urged to implement robust email security measures to defend against sophisticated phishing campaigns and prevent data breaches.

ROCKSTAR 2FA PHISHING TOOLKIT TARGETS MICROSOFT 365 USERS

Trustwave (a leading cybersecurity and managed security services provider) reported that cybercriminals are exploiting a Phishing-as-a-Service (PhaaS) toolkit named Rockstar 2FA to steal Microsoft 365 account credentials through adversary-in-the-middle (AiTM) attacks. The AiTM mode enables attackers to intercept login credentials and session cookies, rendering even multi-factor authentication (MFA) ineffective.

The Rockstar 2FA toolkit, an upgraded version of the DadSec phishing kit, is marketed via platforms like ICQ and Telegram under a subscription model, starting at $200 for two weeks. It boasts of features like 2FA bypass, cookie harvesting, antibot protection and customisable phishing templates mimicking legitimate services like Microsoft.

Phishing campaigns using this toolkit deploy various vectors, including URLs, QR codes and document attachments, often leveraging trusted platforms like Google Docs Viewer, Atlassian Confluence and Microsoft Dynamics to host phishing links. These sophisticated attacks bypass spam detection systems and mimic legitimate login pages, harvesting credentials and session cookies upon user interaction.

Researchers also revealed related phishing campaigns, such as Beluga, which use .HTM attachments to steal Microsoft OneDrive credentials and deceptive betting game advertisements promoting fraudulent financial applications. These scams result in significant economic losses, with some victims reporting losses exceeding $10,000.

Organisations are urged to implement robust email security measures and educate users about phishing threats to mitigate the risks posed by such advanced attacks.

STARBUCKS AND MAJOR RETAILERS AFFECTED BY RANSOMWARE ATTACK

A ransomware attack targeting **Blue Yonder,** a leading AI-driven supply chain platform, has disrupted operations across multiple organisations, including Starbucks in the U.S.A and two major U.K. supermarket chains.

Blue Yonder confirmed the attack occurred on **21 November 2024,** affecting its managed services environment. The company is prioritising a secure recovery, but as of now, no timeline for full-service restoration has been provided.

The attack impacted back-end processes for Barista schedule management and Starbucks payroll systems. However, a Starbucks spokesperson assured that employee payments were processed without significant disruptions and that store operations and customer services remained unaffected.

Blue Yonder's platform plays a crucial role in supply chain logistics, and such incidents highlight the broader risks ransomware attacks pose to global supply chains. Security experts warn organisations to strengthen cybersecurity measures to mitigate widespread implications of such attacks.

CYBERSECURITY CONCERNS DOMINATE

Cybersecurity, once a peripheral issue handled by IT departments, has leapfrogged to the forefront of business discussions globally. With the surge in cyberattacks, the rise of generative AI-driven threats, and escalating costs of data breaches, cybersecurity is now a core concern that affects every aspect of modern operations. This has also to with the fact that the world at large is getting digitized at a very rapid pace. This rapid pace of digitization has enveloped not just governments but even organisations in the private sector.

The 2024 *Allianz Risk Barometer* identifies cyber events as the top global business risk, reinforcing that cybersecurity is not merely a technical challenge but is a strategic necessity, especially in the present day and more so going forward. As a result, organisations are ramping up investments. Attesting this fact, Gartner is predicting a 15 per cent growth in global information security spending by 2025.

From Afterthought to Boardroom Priority

Cyberattacks, including ransomware attacks, data breaches and phishing campaigns, have increased manifold in recent years. In 2023, over 72 per cent of businesses worldwide were victims of ransomware attacks. The financial toll of cybercrimes is staggering, and is projected to reach $10.5 trillion by 2025. IBM's 2024 data reports the average data breach cost at $4.88 million, marking a 10 per cent increase over the previous year.

Executives are increasingly getting aware that cybersecurity is not just a technical hurdle but is a crucial business issue. According to a 2024 KPMG survey, 40 per cent of C-suite leaders reported experiencing a cyberattack, and 76 per cent of security leaders are concerned about the growing sophistication of threats.

Small Businesses Under Attack

The expansion of remote work and cloud computing has increased the vulnerability of small businesses, which often lack the resources to deploy strong cybersecurity measures. According to the U.S. Chamber of Commerce survey, 60 per cent of small businesses cite cybersecurity risks, such as phishing and ransomware attacks, as their primary concerns. This trend highlights that cybersecurity is no longer solely a challenge for large corporations, as small businesses face increasing vulnerability and may struggle to recover from a significant breach.

Generative AI: A New Threat

Generative AI has added a new layer of complexity to cybersecurity threats. Cybercriminals are leveraging AI to conduct large-scale social engineering attacks. Gartner predicts that by 2027, 17 per cent of cyberattacks will involve generative AI. This shift is prompting organisations to invest in advanced security software to mitigate these new risks.

While AI poses significant challenges, it also offers opportunities to enhance cybersecurity. AI-driven technologies are integrated into security operations to improve threat detection, monitoring and incident response. According to KPMG, two-thirds of C-suite leaders believe that AI-based automation is essential for staying ahead of emerging threats.

The Global Response: Increased Investments in Cybersecurity

Organisations are ramping up their spending in cybersecurity to address the growing complexity and scale of risks. Gartner forecasts that global information security spending will reach $212 billion by 2025, driven by factors like the expanding threat landscape, the growing adoption of cloud technologies and the widening skills gap in the cybersecurity workforce. With cloud migration on the rise, the demand for robust cloud security solutions is expected to grow, with cloud-native security markets projected to reach $8.7 billion by 2025.

The shortage of skilled cybersecurity professionals fuels the demand for security services, such as consulting, managed and professional services.

As cyber threats evolve—ranging from ransomware to AI-driven attacks—cybersecurity will remain a key concern in the C-suite, among small business owners and at the national level. Organisations must remain proactive, investing in tools, talent and strategies to stay ahead in an ever-changing cybersecurity landscape.

TEAM EUROPE WINS THE INTERNATIONAL CYBERSECURITY CHALLENGE 2024!

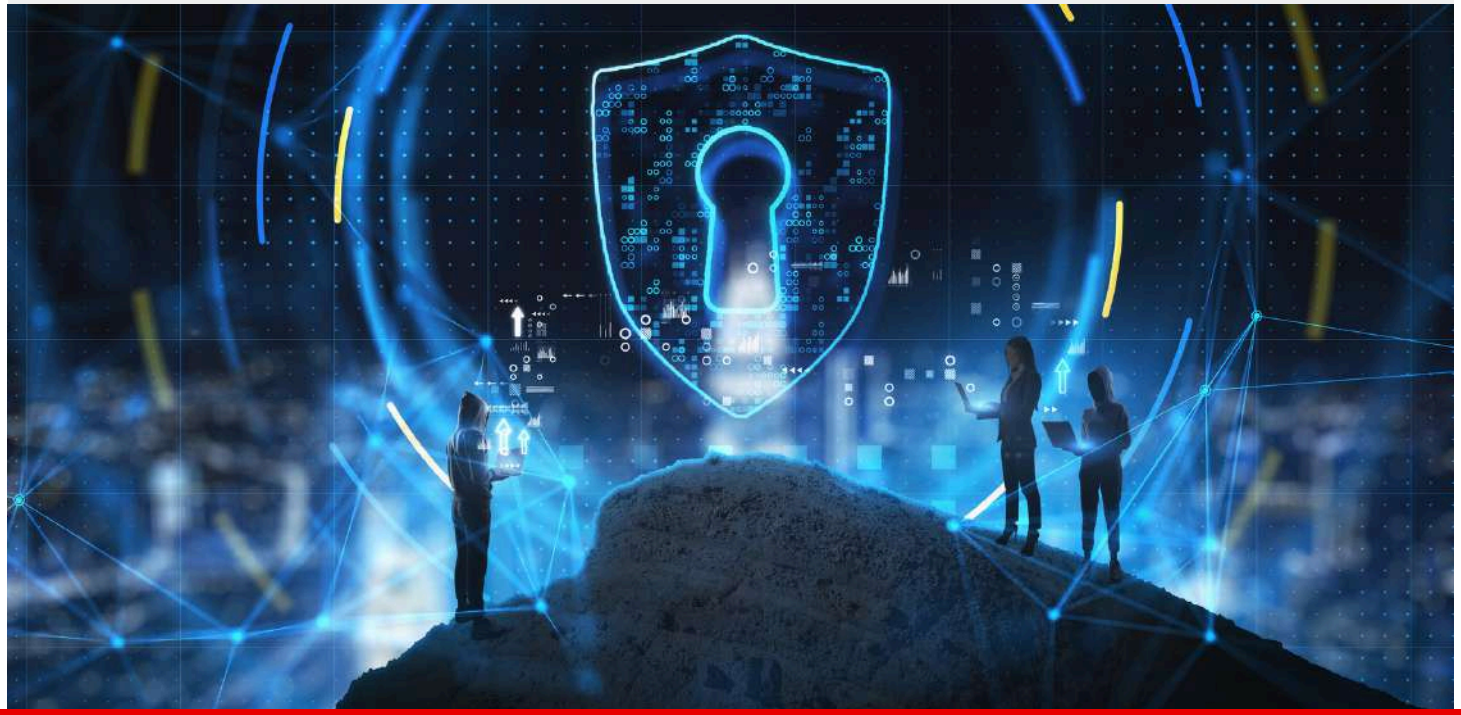
The European Union Agency for Cybersecurity (ENISA) announced that **Team Europe** has emerged victorious in the **International Cybersecurity Challenge (ICC) 2024** for the third consecutive year. The team topped the **Capture the Flag (CTF)** and **Attack/Defence** challenges, securing the highest scores and reaffirming its dominance. **Team Asia** claimed the second place, while **Team Oceania** took third place.

The winning team included participants from across Europe. The following members were part of team Europe:

- **Louis Dasnois** (Belgium), **Odysseas Stavrou** (Cyprus), **Alexander Skovsende** (Denmark), **Astrid Bek** (Denmark), **Stepan Fedotov** (Finland), **Jan-Niklas Sohn** (Germany), **Yannik Marchand** (Germany), **Nikolaos Mourousias** (Greece), **Cillian Collins** (Ireland), **Vincenzo Bonforte** (Italy), **Rick de Jager** (Netherlands), **Maja Kądziołka** (Poland), **Szymon Borecki** (Poland), **Mariana Rio Costa** (Portugal), **Dragoș Albăstroiu** (Romania), **Andraž Strgar** (Slovenia), and **Philippe Dourassov** (Switzerland).

ENISA Executive Director, Mr Juhan Lepassaar, highlighted the importance of nurturing the next generation of cybersecurity talent, stressing that initiatives like the ICC are key to addressing the global cybersecurity skills gap.

The **2024 ICC** took place in **Santiago, Chile,** from **October 28 to November 1,** bringing together top cybersecurity experts from across the globe. Teams from Africa, Asia, Canada, Europe, Latin America, Oceania and the United States pf America participated in solving complex cybersecurity challenges in various areas, including cryptography, reverse engineering, forensic analysis, web exploitation, cloud security, AI, OT environments, mobile apps and IoT.



The competition also featured an **Attack and Defence** segment, where teams defended vulnerable services while exploiting weaknesses in others' systems to score points. Team Europe's success has been attributed to their rigorous preparation, including **training boot camps,** a **qualifier** and **online sessions,** all coordinated by ENISA and led by a team of dedicated coaches: **Jan Gocník, Mario Polino, Sanne Maasakkers, Pedro Adao,** and **Carlos Polop Martin.**

Additionally, **50 volunteers** provided valuable training and authored challenges, contributing to the event's success. ENISA expressed its gratitude to the volunteers and partners, especially **Accenture** and **Ubitech,** for their support, for the event.

The ICC, launched in 2021, is the first global **Capture the Flag** event aimed at nurturing aspiring talent in the cybersecurity domain. It continues to grow as an incubator for excelling in the realm of cybersecurity, fostering the development of skills that are essential to combating evolving cyber threats worldwide.

NEW RULES TO BLOCK CHINA, RUSSIA, AND IRAN FROM ACCESSING BULK US DATA

The US Justice Department has proposed new rules to prevent foreign adversaries such as China, Russia, Iran and other nations like Venezuela, Cuba and North Korea from accessing bulk US data. These rules protect sensitive federal government data and personal information of American citizens from being exploited for cyberattacks, espionage, or blackmail.

This proposal follows an executive order issued by US President Joe Biden earlier in 2024, aiming to restrict foreign entities' use of American financial, genomic and health data. The new rules limit certain business transactions, particularly with data brokers, to prevent them from transferring information to these "countries of concern." This includes data related to US government employees, with the potential for criminal and civil penalties for non-compliance.

The specific restrictions outlined in the proposal include the following:

- Human genomic data on more than 100 Americans
- Personal health or financial data on more than 10,000 individuals
- Precise geolocation data on over 1,000 US devices

The proposal also suggests that Chinese applications like TikTok could violate the rules if they transfer sensitive US user data to Chinese parent companies. This is part of a broader effort by the US to curb the flow of American personal data to foreign governments, addressing long-standing national security concerns related to data privacy and cybersecurity.

CYBERCRIME EMERGES AS THE WORLD'S THIRD-LARGEST ECONOMY

On 6 November 2024, At the HACK 2.0 Summit, Shri C.V. Anand, Police Commissioner, Hyderabad revealed that cybercrime has rivalled the world's third-largest economy, marking an unprecedented rise in criminal profitability. Nationwide cybercrime incidents have surged by 24 per cent, though the actual figure could be closer to 50 per cent due to underreporting.

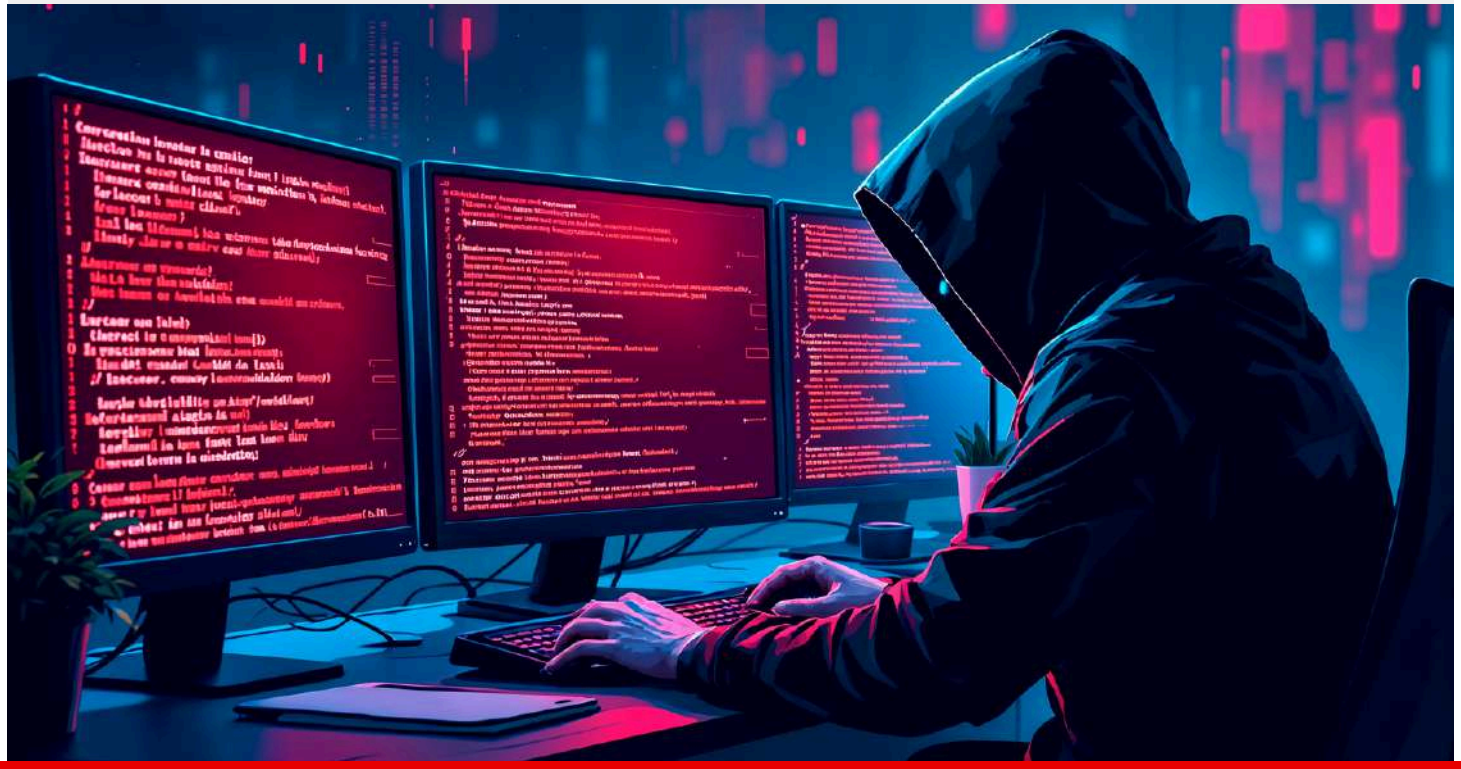
Telangana IT Minister Shri D. Sridhar Babu highlighted the dual nature of technology, emphasising that the state's vision of complete digitisation and its challenges. He stressed on the government's role in bridging gaps between industry and the academia to combat the growing menace cyber threats.

Shri Anand described cybercriminals' increasing sophistication, citing their global coordination and their ability to convert stolen funds into cryptocurrency, making recovery nearly impossible. Despite challenges, Hyderabad Police successfully froze ₹73 crore in fraudulent transactions.

With over 7,000 daily cybercrime cases reported in India, officials, at the summit, urged for having heightened awareness and stronger cybersecurity measures to protect individuals, businesses and governments.

Nearly 60% of Indian Enterprises Fall Below Cybersecurity Poverty Line

A recent study by global cybersecurity firm Sophos reveals that nearly 60 per cent of Indian enterprises operate below the "cybersecurity poverty line," leaving them vulnerable to cyberattacks. This term refers to organisations lacking the essential resources and tools that are necessary to safeguard against cyber threats, such as updated software, skilled personnels and advanced technologies.



The study also highlights that 65 per cent of Indian enterprises have paid ransom to recover data after cybersecurity breaches. The average ransom demand was $4.8 million (approximately. ₹ 40 crore), with the median payment around $2 million (approximately ₹ 17 crore). Recovering the data added an average of $1.35 million (approximately ₹ 11 crore). These figures emphasise on the importance of cybersecurity readiness gap in Indian businesses.

Experts attribute this issue to the reactive nature of cybersecurity efforts in India, with companies only responding after a breach occurs. Mr Chetan Jain, founder of Inspira Enterprise (a global Cybersecurity & Data Analytics & AI services provider), noted that only about 4 per cent of Indian enterprises have the necessary cybersecurity infrastructure to prevent attacks. The Reserve Bank of India's report also reveals that unauthorised network scans and vulnerabilities account for over 80 per cent of security incidents in India, with phishing being the most common form of attack.

While small and medium-sized enterprises (SMEs) are more likely to fall below the cybersecurity poverty line, larger firms are also at risk. Experts advocate for increased investment in cybersecurity, awareness campaigns, and organisational structural changes to address these challenges. Drawing inspiration from the European General Data Protection Regulation (GDPR), 2016 they suggest penalising lax cybersecurity practices and subsidising cybersecurity products and services. Additionally, a shift in mindset is required, viewing cybersecurity as an ongoing operational expense rather than a one-time capital investment.

This growing cybersecurity crisis underscores the urgent need for Indian businesses to invest proactively in cybersecurity to avoid severe financial losses and protect sensitive data.

CANADA LABELS INDIA AS A "CYBER ADVERSARY"

In a significant development, Canada has formally labelled India as a “cyber adversary” for the first time in an official government document. This assertion appears in the National Cyber Threat Assessment 2025-2026, released by the Canadian Centre for Cyber Security. The assessment categorises several countries, including China, Russia, Iran, North Korea and India, as state adversaries in cyber threats.

The report suggests that India’s state-sponsored cyber threat actors are likely conducting cyber activities aimed at Canadian government networks, particularly for espionage purposes. The report further highlights that India’s cyber programme is designed to advance its national security objectives, including espionage and counterterrorism and promote its global stature. The report also implies that India might utilise commercial cyber vendors to enhance its cyber operations.

This latest assessment comes amidst growing tensions between the two nations. In October 2024, India withdrew six diplomats from Canada following their designation as “persons of interest” in investigations related to violent criminal activities. In a reciprocal move, India expelled six Canadian diplomats. Justin Trudeau, Prime Minister, Canada had earlier accused India of violating Canadian sovereignty, specifically alleging India’s involvement in the killing of a pro-Khalistan figure in British Columbia. However, Canadian authorities have not released concrete evidence, on the matter.

The report reflects both countries' broader geopolitical tensions and cyber challenges, with India asserting that the accusations are “preposterous” and politically motivated.

ICEPEONY AND TRANSPARENT TRIBE TARGET INDIAN ENTITIES

India has become a key target for two cyber-espionage groups—Pakistan-based Transparent Tribe and a previously unknown China-nexus group, IcePeony. Both groups have exploited cloud-based tools and sophisticated malware for their malicious campaigns.

Transparent Tribe's Attack Methods

Transparent Tribe has been using the ElizaRAT malware, a Windows-based remote access tool (RAT), to infiltrate high-profile entities in India. The group has been active since 2013 and is known by multiple aliases such as APT36, Earth Karkaddan and Mythic Leopard. ElizaRAT is used to control compromised systems through cloud-based services like Telegram, Google Drive and Slack for command-and-control (C2) communications.

ElizaRAT's deployment is often triggered by spear-phishing attacks, with the malware providing complete control of the infected systems. A recent update to Transparent Tribe's tactics includes using ApoloStealer, a malware designed to collect and exfiltrate specific file types such as .DOC, .XLS, .PPT and images. Additionally, the group has introduced a new module, ConnectX, which targets external drives like USBs.

IcePeony's Campaigns

The IcePeony group, an advanced persistent threat (APT) actor linked to China, has been targeting government bodies, academic institutions, and political organisations in India, Mauritius and Vietnam since at least 2023. Their attack strategies often start with SQL injection, followed by exploiting web shells and backdoors to gain further access to systems. The group's primary goal is credential theft.

One of IcePeony's key tools is IceCache, an ELF binary that is designed to exploit Microsoft Internet Information Services (IIS) servers. This custom version of the reGeorg web shell facilitates file transmission and command execution. The group also uses a backdoor called IceEvent, which allows them to upload and download files and execute commands on compromised systems.

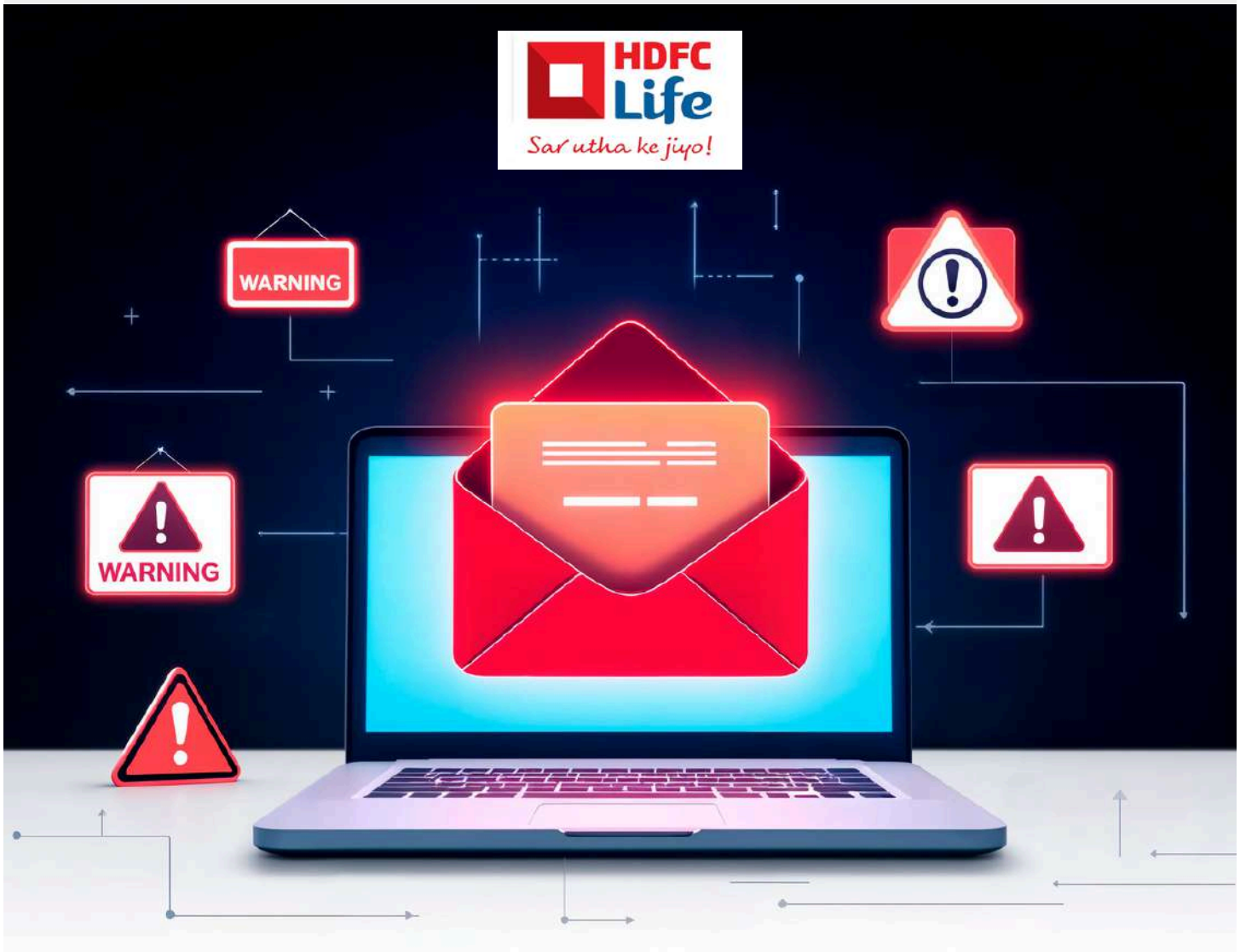
Both groups have leveraged cloud-based services to mask their activities, making detection more difficult. This trend highlights the increasing sophistication of cyber adversaries using legitimate services to blend in with normal enterprise activities. As these groups continue to expand their arsenals, they pose a significant threat to India's cybersecurity landscape.

HDFC LIFE REPORTS DATA LEAK, LAUNCHES INVESTIGATION

HDFC Life Insurance has reported a data leak and initiated a detailed investigation in consultation with cybersecurity experts to identify the cause and take appropriate remedial actions. The company disclosed that an unknown source had maliciously shared specific customer data fields, prompting the investigation to assess the potential impact. HDFC Life reassured customers that it would handle the situation carefully to protect their interests.

The leak follows similar incidents in the insurance sector, with Star Health and Allied Insurance also conducting forensic investigations after a cyberattack compromised the sensitive data of 31 million customers. Reports suggested that the breach involved the sale of 7.24 terabytes of personal and medical information on Telegram. Additionally, Tata AIG recently faced a data leak incident that raised concerns in the sector.

In response to these breaches, the Insurance Regulatory and Development Authority of India (IRDAI) has directed insurers to audit their IT systems to safeguard policyholder data. IRDAI emphasised its commitment to protecting customer interests and addressing data security issues in the industry.



NATIONAL CONFERENCE ON "NAVIGATING THE CLOUD: AN ESSENTIAL SECURITY ROADMAP"

India Future Foundation (IFF), in collaboration with AWS and Indian Institute of Public Administration (IIPA), New Delhi, hosted the conference—"National Conference on Navigating the Cloud: An Essential Security Roadmap" on 13 November 2024 at IIPA, New Delhi.

The event brought together eminent experts and policymakers to address the critical challenges of cloud security. With a focus on empowering government departments and public sector enterprises (PSEs) in their digital transformation journeys, this event showcased expert insights, hands-on simulations and collaborative discussions to chart a secure and resilient future for cloud adoption.

Highlights of the Event:

- **Keynote Address:**
  Lt Gen. MU Nair, PVSM, AVSM, SM (Retd.), National Cyber Security Coordinator stressed on the importance of a unified national cybersecurity strategy and collaboration between government and entities from the private sector to bolster cyber resilience.
- **Panel Discussion on Secure Cloud Adoption:**
  Experts who attended the consultation included Dr Yask Sharma (CISO, Indian Oil Corporation), Mr Akshaya Kumar Patel (GM-IT & CISO, National Thermal Power Corporation) and Dr Gaurav Gupta (Scientist F, Ministry of Electronics and Information Technology), highlighted the best practices for cloud migration, the adoption of Security, Risk, and Compliance (SRC) frameworks and the criticality of governance models in ensuring robust cloud security.
- **Interactive Executive Security Simulation:**
  Facilitated by AWS, the simulation provided hands-on experience in managing cloud security risks, encouraging participants to align security investments with organisational objectives while navigating real-world challenges.

Key Insights Shared:

Emerging Trends:
Discussions, at the consultation, highlighted the rise in sophisticated cyberattacks, the necessity of operational resilience and the integration of adaptive security measures to combat evolving threats.

Operational Resilience:
Strategies emphasised disaster recovery planning, resilience-by-design principles and ongoing compliance monitoring to ensure seamless operations amid disruptions.

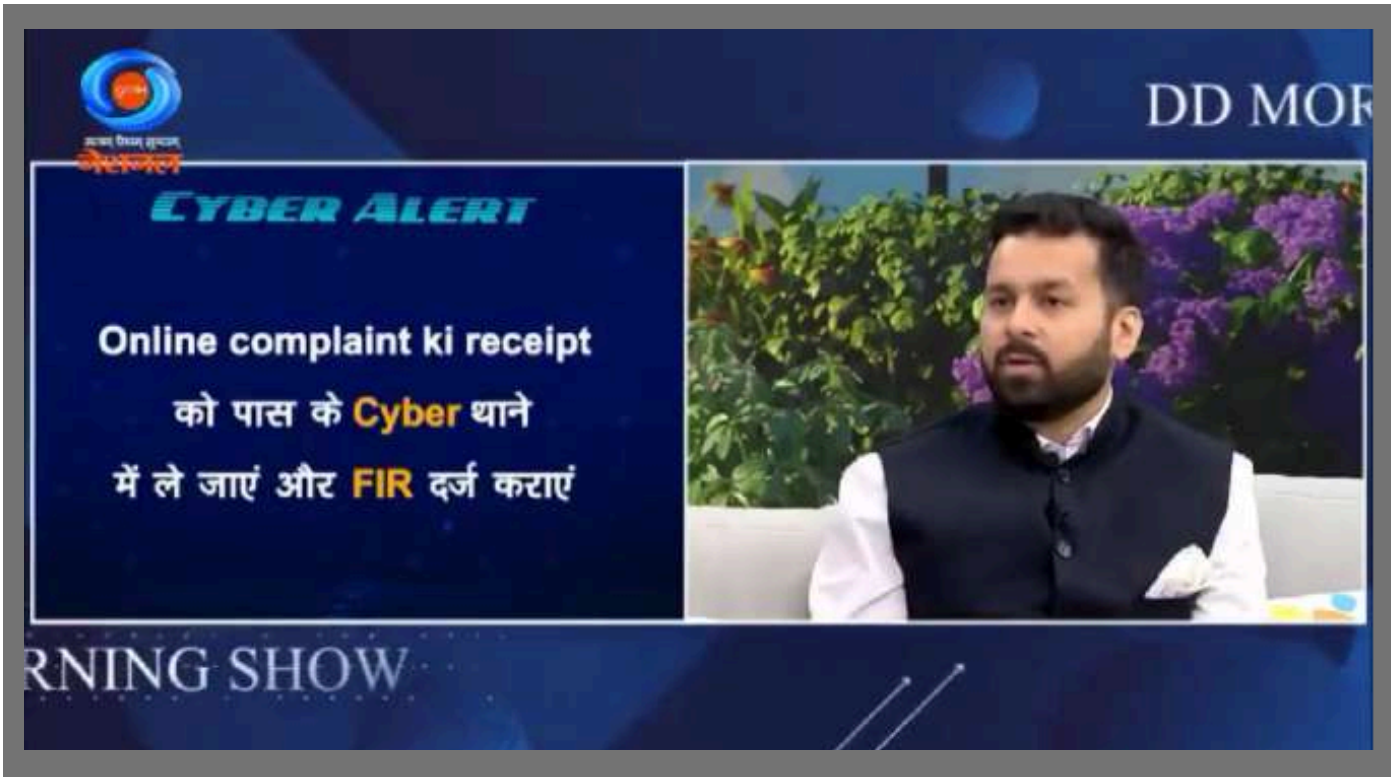
Governance Models:
The panellists stressed on the importance of defining roles in the shared responsibility model and aligning security protocols with global standards, such as ISO 27001.

Recommendations:

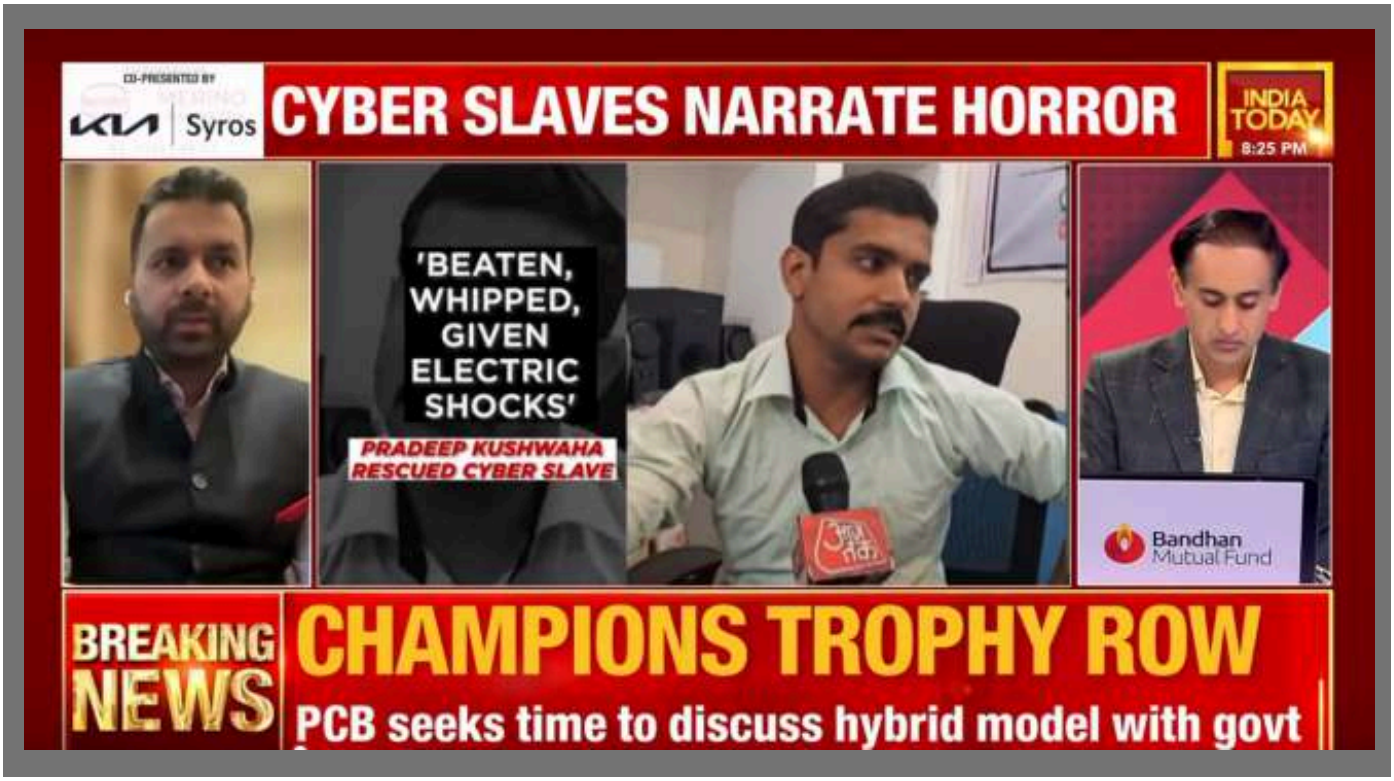
- Strengthen collaboration between government agencies and private entities to share expertise and resources.
- Establish robust governance frameworks for secure cloud adoption.
- Promote resilience by design and continuous compliance monitoring.
- Conduct regular training, awareness programs and hands-on exercises to build a culture of cybersecurity awareness.

The conference underscored the urgency of innovative and collaborative approaches to cloud security. Participants gained actionable strategies and tools to navigate the complexities of digital transformation while safeguarding critical infrastructure.

IFF IN THE MEDIA



Kanishk Gaur, Founder & CEO, IFF shared guidelines on reporting a cybercrime on *DD National*.



Kanishk Gaur, Founder & CEO, IFF shared his insights on Cyber Slavery on *India Today*.

INDIA FUTURE
FOUNDATION

Contact Us

+91-1244045954, +91-9312580816

Building no. 2731 EP, Sector 57, Golf Course
Ext. Road, Gurugram,
Haryana, India – 122003

helpline@indiafuturefoundation.com

www.indiafuturefoundation.com