INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

'MADE IN INDIA' CYBERSECURITY TECH

IN THIS NEWSLETTER

Shri Rajeev Chandrasekhar, Union Minister of State, Ministry of Electronics and Information Technology (MeitY), Government of India reiterated the government's unwavering commitment to fostering indigenous cybersecurity technology while participating in the Nasscom Future Forge 2023 event, in Bengaluru, on 7 November 2023. Predicting substantial transformation in the cybersecurity landscape within the forthcoming three to six months, Chandrasekhar highlighted the prospective benefits for developers in cultivating native technology. He emphasized on the government's objective to fortifying its digital infrastructure, expanding the market for indigenous cybersecurity technologies, products and platforms. Acknowledging the lack of cybersecurity awareness, particularly among Chief Information Security Officers (CISOs), the Minister identified this as a significant challenge. Addressing this concern, he outlined plans to enhance the competency and proficiency of CISOs by revamping the Information Security Awareness programme. The proposed strategy includes instituting a reskilling and upskilling framework mandating recurrent training for CISOs annually.

CERT-IN EXEMPTED UNDER RTI ACT 2005

On Friday, 24 November 2023, The Indian Computer Emergency Response Team (CERT-In) became the 27th organization to be exempted from the ambit of the Right to Information Act (RTI), 2005.

The Department of Personnel and Training (DoPT) issued the notification of the inclusion of CERT-In to the Second Schedule of the RTI Act, exempting it from public scrutiny.

The inclusion of CERT-In to the Second Schedule comes after inter-departmental consultations, previously acknowledged by MeitY.

Shri Rajeev Chandrasekhar, Union Minister of State, Ministry of Electronics and Information Technology (MeitY), Government of India, during discussions in the Rajya Sabha earlier this year, highlighted the ongoing deliberations among departments, including the Ministry of Law and Justice, regarding CERT-In's potential exemption from the RTI Act, 2005.

There are 26 other intelligence and security organizations established by the Central government, such as the Intelligence Bureau (IB), Research and Analysis Wing (RAW), Directorate of Enforcement (ED) and National Technical Research Organisation (NTRO), which are outside the purview of the RTI Act, 2005.

CERT-In's addition to the list of organisations that are outside the purview of the RTI Act, 2005 underscores the government's intent to fortify confidentiality in cyber security operations.

TAJ HOTEL GROUP PROBES ALLEGED BREACH

On 24 November 2023, a potential data breach at the Taj Hotels Group, New Delhi, raised concerns about exposing personal information belonging to an estimated 1.5 million individuals. The Tata-owned hotel chain is initiating an investigation following these alarming revelations.

Earlier this November, the Taj Hotels Group encountered a security incident that may have compromised sensitive data. In response to these claims, the hotel group stated that it has commenced an internal probe into the matter, affirming that there is no indication of an ongoing security threat.

However, there is a possible security breach involving someone called "Dnacookies" who claims to have personal information of customers of the Taj Hotel customers from 2014 to 2020. This includes addresses, IDs, phone numbers and more. According to media reports a ransom of USD 5,000 (around ₹4,16,549) was asked for not leaking this data.

The Indian Hotels Company (IHCL) on the other hand claimed that the perpetrators of this breach have some customer info but not sensitive information. The company also informed about this incident to the Indian Computer Emergency Response Team (CERT-In).

CYBERCRIMINALS EXTORT INR 3.7 CRORE

A senior executive at Infosys, Bengaluru, fell victim to cybercriminals masquerading as officials from the Telecom Regulatory Authority of India (TRAI), Central Bureau of Investigation (CBI) and the Mumbai Police, who extorted a staggering INR 3.7 crore from him.

The perpetrators of this crime, threatened the victim of imminent arrest for his alleged involvement in various crimes, including money laundering, which forced the victim into making the payments to his alleged blackmailers.

This Infosys employee from Whitefield, Bangalore, received a call on 21 November 2023 from someone pretending to be from the Vakola Police Station, in Mumbai. The person on the other side, informed the alleged victim that he had done something wrong and that he was involved in money laundering activities.

As he felt the heat from the cybercriminals, he made the transfer of INR 3.7 crore to the cybercriminals. Upon receiving the complaint, the Cyber Crime Police, at Bengaluru, promptly registered a case under the Information Technology Act, 2000 and IPC sections 419 and 420.

As the amount involved in the matter, exceeded INR 3 crore, the case would be escalated to the Criminal Investigation Department (CID). The efforts are also underway to collaborate with bank officials to freeze the accounts linked to the perpetrators.

First, the scam started with someone pretending to be an official from TRAI informed the victim of that his SIM card was used for illegal ads. Then, the other group claiming to be from the Mumbai police, threatened the victim to come to Mumbai and Delhi or face legal trouble.

Later, the scammers faked a police station on a video call, dressed like police officers with fake IDs and lodged a fake complaint against the victim. They forced the victim to transfer money to different accounts, promising to fix the case.

The victim only realized that he had been scammed on 25 November 2023 and reported the matter to the authorities.

UK'S CYBER THREATS DEMAND VIGILANCE

The National Cyber Security Centre (NCSC), an organization of the United Kingdom Government that provides advise and support for the public and private sector on how to avoid computer security threats, issued its seventh Annual Review on 14 November 2023, where it emphasized on the persistent and significant threats faced by the UK's critical infrastructure and urged increased resilience and collaborative efforts to counter the escalating cyber challenges.

The NCSC, part of Government Communications Headquarters (GCHQ), highlighted the precarious threat landscape in the wake of rising state-backed groups, aggressive cyber activities and ongoing geopolitical tensions, signalling enhanced measures to safeguard vital sectors. These sectors encompass fundamental areas such as water supply, electricity, communication networks, transportation, finance and Internet connectivity.

Over the past year, the NCSC witnessed the emergence of a new class of cyber adversaries linked to state interests, often sympathetic to Russia's actions in Ukraine. In a joint advisory issued in May 2023, the NCSC revealed insights into the 'Snake' malware, a core component employed by Russia's Federal Security Service (FSB) for espionage operations, for nearly two decades.

The Review underscores the continued, enduring threat from states and state-aligned groups to the UK's essential assets, calling for concerted efforts to protect the nation's critical infrastructure for daily societal operations.

Furthermore, the NCSC's Annual Review emphasizes the targeting of personal email accounts of high-profile individuals involved in politics, indicating a shift from mass campaigns to specifically targeting individuals holding sensitive information.

To counter this, the NCSC introduced an opt-in service alerting high-risk individuals about potential malicious activities detected on personal devices.

The Annual Review underscores the UK government's commitment to fortify democratic processes. Recent measures include implementing digital imprint rules, strengthening defenses against foreign interference and advancing online safety measures.

Moreover, the report points to the continuous threat from China-affiliated cyber actors, urging collaboration with allies and industry to understand and counter evolving cyber capabilities. Russia, despite being a significant actor in cyberspace, primarily targets Ukraine and operates cybercriminal networks responsible for high-profile ransomware attacks in the UK.

While less sophisticated, Iran uses digital intrusions for theft and sabotage and targeting vulnerabilities in critical national infrastructure sectors.

The NCSC's Annual Review serves as a clarion call for enhanced vigilance and collective action to combat the evolving cyber threat landscape, emphasizing the need for proactive measures and collaborative strategies to safeguard the UK's critical assets and democratic processes.

CHINA PROPOSES ENHANCED CYBER CHECKS FOR AUDITORS

China's finance ministry has proposed new regulations requiring auditors to undergo additional cybersecurity checks, particularly when their work intersects with national security concerns. The recently disclosed draft measures also outline stringent protocols for managing data related to Chinese firms.

Over the past few years, China's cybersecurity authority has been developing policies dictating cybersecurity protocols for businesses. These policies emphasize on the need for comprehensive security assessments and checks.

The proposed measures specifically target auditors engaged by domestic firms or those handling cross-border assignments. As per the draft rules, the chief partner of an auditing firm is responsible for ensuring data security.

Amid escalating concerns about data security, Chinese authorities are intensifying scrutiny on auditors. Earlier regulations, issued in May 2023, mandated state-owned companies and listed enterprises to reinforce assessments of accountants' capabilities in managing information security.

Additionally, reports surfaced earlier this year indicating Beijing's directives to certain state-owned entities to halt engagements with the four prominent global accounting firms. This directive aligns with China's efforts to reduce the influence of Western auditors.

INDIA FACES SURGE IN CYBERATTACKS

India's digital infrastructure vulnerabilities, propelled by its rapid deployment, have led to an upsurge in cyberattacks, in the country. Experts attribute the increasing number of attacks to the swift pace of digital transformation, which has created intricate technological systems harboring inherent weaknesses, making them prime targets for cyber threats.

The country experienced a substantial 70% rise in cyberattacks during the third quarter of this year, according to Indusface's State of Application Security Report. The report detailed that sectors like banking and insurance faced a staggering 90% surge in bot attacks. Moreover, the study highlighted a ten-fold increase in attacks on Software-as-a-Service (SaaS) and conglomerate companies compared to the previous quarter. Additionally, the healthcare domain encountered widespread bot attacks, affecting nearly every website within the sector.

The report flagged India, the US, the UK, Russia, and Singapore as significant sources of global cyberattacks, identifying approximately 46,000 vulnerabilities in Q3, with 32% remaining unaddressed for over 180 days, underscoring the urgency for immediate action.

Cybersecurity experts recommend harnessing the potential of AI, expansive language models and machine learning to create intelligent systems to tackle the growing threat scenario. These systems can independently recognize and counter cyber threats. Experts argue that these technologies, are flexible enough to adapt to changing data patterns and provide a responsive defence against cyberattacks.

ROLE OF AI IN CYBERSECURITY

In the ever-evolving cybersecurity landscape, artificial intelligence (AI) stands at the forefront, offering both promise and apprehension. AI brings both promise and worry in the realm of cybersecurity. There are concerns among countries and hacking groups using AI for quick/prompt cyberattacks. But at the same time, it's also seen as helpful tool for defenders to find weak spots and stop attackers, in an affective manner.

Cybersecurity firms explore integration of AI to bolster their cyber defences using accumulated data. Experts stress merging various data sources—network, cloud, and endpoints. AI's strength lies in analyzing large-scale patterns in daily threats.

Automated tools make it easier for early analysts to identify problems and determine their origins. This helps cybersecurity teams spend more time finding and stopping threats. They pay extra attention to managing data well to make good decisions.

The government's zero trust plan underscores the significance of continuously monitoring data access across various platforms within applications, devices, or cloud systems. This approach prioritizes a strong foundation that facilitates the optimal functioning of AI and ensures users have control over their data.

By leveraging AI in cybersecurity, the focus shifts from reactive to proactive and preventive approaches. This enables a more robust and anticipatory defence against evolving threats in the digital landscape.

INDIA'S FOCUS TO FORTIFY IT’S CYBERDEFENCES

On 27 November 2023, a Cyber Security and Digital Forensics workshop was held at JSS Science and Technology University in Mysuru, Karnataka. The spotlight, of the workshop, was on India's concerted efforts to fortify ity cyber defences within its technological landscape. The event showcased insights from Shri E. Sai Prasad Chunduru, former Assistant Director at the Central Forensic Science Laboratory, Hyderabad, who emphasized on the nation's strides toward establishing a resilient cybersecurity framework through technological advancements and policy directives.

At the workshop, the challenges in cybersecurity were discussed, touching upon administrative, legal, human resource and technical aspects. The significance of ongoing policies like the Indian Cybercrime Coordination Centre (I4C) and the Centre for Prevention of Cybercrime Against Women and Children (CCWC) were also emphasized, at the workshop.

This workshop was organised by the Department of Computer Applications to provide timely training to faculty members. It encompassed diverse aspects, including cutting-edge research guided by senior scientists from central research laboratories. It also incorporated industry insights and perspectives from experienced officers in the Criminal Investigation Department.

Industrial visits to observe ongoing cybersecurity projects, providing comprehensive insights into the subject, also formed part of the workshop.

Esteemed figures such as Dr A.N. Santosh Kumar, Vice-Chancellor of JSS STU, Dr C. Nataraju, Principal at SJCE, JSS STU, and Dr R.K. Bharathi, the workshop's organizer, graced the event.

FIVE TRENDS TO SHAPE CYBERSECURITY IN 2024

Nippon Telegraph and Telephone (NTT) Corporation, a pivotal player in the cybersecurity industry headquartered in Tokyo, Japan, has identified five critical trends that are projected to influence the cybersecurity landscape, in 2024 and beyond, in a major way.

NTT is a global technology leader providing mobile, infrastructure, network, application and consulting services. With a focus on innovation and sustainability, NTT's extensive offerings and global presence serve consumers, enterprises and governments across diverse industries, aiming to create a more secure and connected world.

As the world grapples with evolving digital transformations and escalating cybersecurity challenges, NTT highlights critical areas that will dictate the future of security strategies.

AI's Influence on Cybersecurity Dynamics

AI's role in driving cybercriminal activities and defensive strategies will expand in 2024. Malicious actors will harness the capabilities of AI to accelerate attacks, while cybersecurity strategies will leverage AI for enhanced detection and analysis, fostering more robust responses against threats.

Upholding Election Integrity Through Cybersecurity Measures

With upcoming presidential campaigns in various countries, safeguarding election integrity will rely on countering disinformation fueled by generative AI. This having in place, ensuring secure voting technology and implementing essential cybersecurity measures will be crucial.

Zero Trust Framework Implementation

Zero Trust will transition from being a mere trend to becoming a pivotal cybersecurity framework, addressing emerging threats and strengthening security defenses. It emphasizes risk-based management and continuous processes integrating various technologies.

Preparation for Impending Quantum Threats

While widespread adoption of quantum technology may not occur in 2024, readiness efforts will intensify. Given the substantial time required for migration, preparing systems and applications for quantum computing's arrival is critical.

Evolution in Cryptography and Encryption

Research into advanced encryption systems like Attribute-Based Encryption (ABE) will continue progressing. Privacy concerns in interactions with AI models will prompt explorations into enabling private engagements with these technologies.

PROBE INTO PHONE HACKING OF POLITICIANS

Shri Ashwini Vaishnaw, Union Minister, Minister of Electronics and Information Technology (MeitY), Government of India, confirmed an active investigation by the country's cybersecurity agency into complaints made by senior opposition politicians concerning mobile phone hacking incidents. These complaints were triggered by cautionary messages received from Apple, as disclosed by Vaishnaw to the media.

The Minister stated that CERT-In, headquartered in New Delhi, had launched the probe and verified Apple's acknowledgment of receiving the investigation notice. Both the Union Home Ministry and a political aide to Vaishnaw assured the public that all cybersecurity concerns raised by the politicians were undergoing a thorough examination.

The recent controversy arose after opposition leader Rahul Gandhi accused Prime Minister Narendra Modi's Administration of attempting to hack mobile phones of opposition politicians. Numerous lawmakers shared screenshots on social media displaying notifications allegedly from Apple, cautioning them about being targeted by state-sponsored attackers aiming to compromise their iPhones remotely.

It's worth noting that a senior minister from the government also reported receiving a similar notification.

In response, Apple clarified that they did not attribute the threat notifications to any specific state-sponsored attacker. They suggested that some notifications might be false alarms or undetected attacks.

This development follows the previous uproar in 2021 when reports emerged suggesting the alleged use of Israeli-made Pegasus spyware to monitor the activities of journalists, activists and politicians, including members of the Opposition.

DARK WEB SELLER EXPOSES TRUTH BEHIND DATA BREACH

A recent data leak involved the private information of more than 800 million Indian citizens. Resecurity, Inc., an American cybersecurity agency, was the first to discover this breach. The leaked data, which included Aadhaar and Passport information, was put up for sale on the dark web by an individual known as 'pwn0001.'

This 'pwn0001' acquired the extensive data set from a defunct dark web platform by paying $50,000 (INR 41.64 lakh), last year. However, they are now attempting to sell this information for $80,000 (INR 6,667,620.00 convert this amount to lakh as in the first instance) in an effort to make a profit.

During negotiations, 'pwn0001' showcased sample files containing Aadhaar details of 100,000 individuals to potential buyers. Investigations by Resecurity's team confirmed the authenticity of some Aadhaar IDs from this sample data.

However, 'pwn0001' later admitted that the actual data didn't match the initially advertised description. Only 10% of the information consists of Aadhaar details, with a few records containing passport information, contradicting their earlier claims.

This revelation emerged after India passed the Digital Personal Data Protection (DPDP) Act on 9 August 2023. Although this law stipulates hefty fines of up to INR 250 crore on platforms that compromise people's data, its enforcement is pending.

Earlier, Resecurity, Inc. had cautioned about a potential breach in August 2023, hinting at the possibility of 1.8 TB of data originating from an 'Indian internal law enforcement organization.'

INDIA FUTURE FOUNDATION AT IPCP

India Future Foundation (IFF) proudly contributed to the Indo-Pacific Cyber Programme (IPCP) in collaboration with The National Cyber and Encryption Agency (BSSN), Indonesia, the British Embassy- Jakarta, BAE Systems and TAG International. The workshops conducted on 21-22 and 28-29 November 2023 in Indonesia provided an opportunity to explore Indonesia's Cyber Ecosystem. Anong other things these workshops provided a platform to engage with key stakeholders. At these workshops, IFF shared insights from an Indian perspective, thereby reinforcing our dedication to promoting global cyber resilience.

The IPCP, funded by the UK Government, is pivotal to strengthening Cyber Security Capacity in Indonesia and other select nations. IFF’s participation in this consortium reflects our commitment to fortifying global cyber resilience.

The programme aligned with our mission and focused on crucial areas like National Threat Detection and Response, Critical National Infrastructure (CNI) Resilience and Cyber Training and Awareness. These areas perfectly resonate with our goal of empowering nations to navigate the intricate cyber landscape.

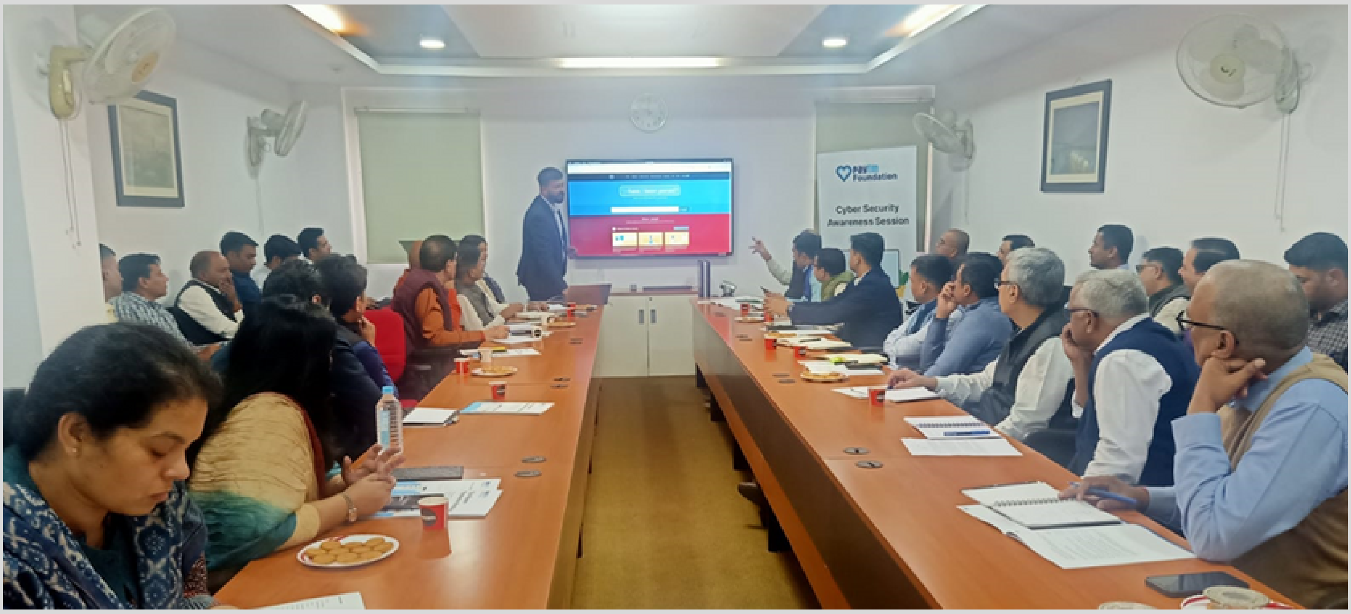
India Future Foundation was represented at these workshops by its Deputy Manager, Mr Nikhil Bansal.

INDIA FUTURE FOUNDATION TRAINS CBI OFFICERS

On Tuesday, 28 November 2023, India Future Foundation (IFF) conducted a one-day training programme for officers of the Central Bureau of Investigation (CBI), at 7 Naval Kishore Road, Hazratganj, Lucknow, in collaboration with Paytm. This training session provided comprehensive insights into Open-Source Intelligence (OSINT) and the Dark Web.

During the training session, real-life case studies, that were relevant to online criminal investigations were showcased. They led discussion at the training sessions veered around different OSINT tools that are vital for identifying and probing illicit, fraudulent and extremist activities on the Internet.

The main objective of this training session was to empower the officers with the necessary expertise and skills to address crimes in the digital landscape. sphere efficiently. Mr Devendra Shukla, Senior Consultant, India Future Foundation was the trainer at this training session.



Team from IFF Team providing training to officials from CBI

IFF TRAINS STATE AND DISTRICT LEVEL JUDGES

On 29 November 2023, India Future Foundation (IFF) conducted a special training session at the Indian Institute of Public Administration (IIPA), New Delhi, for district and state-level judges. The training sessions focussed around three pivotal subjects: Call Data Record (CDR), Internet Protocol Detail Record (IPDR) and Social Media Analysis.

Call Data Record (CDR) involves records maintained by telecommunication service providers. It involves call information and includes details like time of the calls, duration of the call, number to which the calls were made, and much more. IPDR focuses on data regarding Internet usage, including IP addresses and online activities. Service providers and network administrators often use these records to track and analyze Internet usage patterns, monitor network performance and investigate potential security issues or suspicious activities. Social Media Analysis examines and interprets information gathered from various social media platforms for investigative purposes.

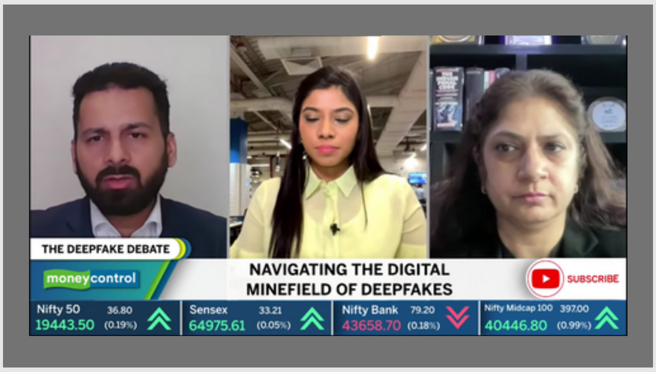
The trainers from IFF made use of practical scenarios to showcase how the above-mentioned technologies aid in investigations. The training session aimed to equip judges with a comprehensive understanding of these tools, enabling them to better comprehend and assess technological evidence presented during legal proceedings.

As the chief guest, at the training session, Dr Surabhi Pandey, Assistant Professor, IIPA added valuable insights to the discussion, enriching the training experience for all participants. The trainers from IFF included Mr Devendra Shukla, Senior Consultant, and Mr Vijay Kumar Lohani, Cyber Security Analyst.

IFF IN THE MEDIA

Kanishk Gaur, CEO, IFF, spoke on Republic TV about use of deepfakes in disinformation campaigns.

Kanishk Gaur, CEO, IFF, shared his insights on Deepfakes on CNBC Awaaz.


THE DEEPFAKE DEBATE
moneycontrol
NAVIGATING THE DIGITAL MINEFIELD OF DEEPFAKES
SUBSCRIBE
Nifty 50 36.80 19443.50 (0.19%)
Sensex 33.21 64975.61 (0.05%)
Nifty Bank 79.20 43658.70 (0.18%)
Nifty Midcap 100 397.00 40446.80 (0.99%)

Kanishk Gaur, CEO, IFF, shared his views on Deepfakes on Moneycontrol.

Kanishk Gaur, CEO, IFF, provided insights o0n the Apple Hacking Alert on CNN-News18.

Kanishk Gaur, CEO, IFF, discusses the potential threat Deepfake Technology poses on Mirror Now.

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