INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

TELEGRAM MARKETPLACES FUEL SURGE IN PHISHING ATTACKS

In a concerning trend, cybersecurity researchers are shedding light on Telegram's growing influence in the world of cybercrime. Guardio Labs has released a report emphasising on Telegram's "democratisation" of the phishing ecosystem, where cybercriminals can orchestrate mass attacks for as little as $230.

Describing the messaging application as a "scammers paradise" and a "breeding ground for modern phishing operations," the researchers, at Guardio Labs, in their report, have highlighted how Telegram has become a bustling hub for cybercriminals, enabling exchange of illicit tools and insights. This has created a well-organized supply chain of devices and victims' data, making it accessible to seasoned criminals as well as to newcomers.

IN THIS NEWSLETTER

The ease of access to free samples, tutorials, kits and even hackers-for-hire on Telegram has transformed the platform into a one-stop-shop for aspiring cyber criminals. Guardio Labs, its report, noted that what was once exclusive to invite-only dark web forums is now available publicly, thereby opening the doors of cybercrime to inexperienced individuals.

The report underlines instances where malicious Telegram bots, such as Telekopye (aka Classiscam), play a pivotal role in crafting fraudulent web pages, emails and SMS messages for large-scale phishing scams. The availability of affordable building blocks for phishing campaigns on Telegram, some even offered for free, makes it feasible to set up scam pages through phishing kits, compromise WordPress websites and utilise backdoor mailers to bypass spam filters.

Guardio Labs, in its report, emphasised the dual responsibility of site owners, urging them to safeguard their platforms against being unknowingly used for hosting phishing operations. Additionally, the researchers revealed that Telegram's digital marketplaces offer expertly designed "letters," branded templates that enhance the authenticity of phishing emails.

To further heighten the success rate of these campaigns, Telegram hosts bulk datasets, referred to as "leads," containing valid email addresses and phone numbers, sometimes enriched with personal information. The specificity of these leads, tailored for different regions, niches and demographics, adds to the credibility of phishing attacks.

The report highlighted the diverse sources of lead lists, ranging from cybercrime forums selling data stolen from breached companies to sketchy websites employing fake surveys to collect personal information. A critical aspect of these phishing campaigns involves monetising stolen credentials by selling them as "logs" to other criminal groups, yielding threat actors a substantial return on investment based on the validity and funds associated with the compromised accounts.

Unfortunately, this report underscores the alarming reality that anyone can initiate a phishing operation on Telegram with a small investment, regardless of prior knowledge or connections in the criminal underworld. Cybersecurity experts are urging increased vigilance and collaborative efforts to counter this growing threat as phishing activities continue to surge on the platform.

ITALIAN BUSINESSES FACE CRYPTOJACKING THREAT

In a concerning development, Italian businesses across various sectors, including health, transportation, construction and logistics, are under attack by a financially motivated threat actor identified as UNC4990. The attack vector involves using malicious USB devices as an initial infection method, with Google-owned Mandiant revealing that the malicious activity has been ongoing since late 2020.

UNC4990's modus operandi involves widespread USB infections, followed by the deployment of the EMPTYSPACE downloader. During these operations, the threat actor relies on third-party websites such as GitHub, Vimeo and Ars Technica to host encoded additional stages, downloaded and decoded via PowerShell early in the execution chain.

While the ultimate goal of UNC4990 remains unclear, there have been instances where an open-source cryptocurrency miner was deployed after months of beaconing activity. The threat actor operates extensively within the Italian infrastructure for command-and-control (C2), prompting concerns about the potential impact on targeted organisations.

The infection process begins when a victim double-clicks on a malicious LNK shortcut file on a removable USB device, triggering the execution of a PowerShell script that is responsible for downloading EMPTYSPACE. This downloader, or BrokerLoader or Vetta Loader, is fetched from a remote server via an intermediate PowerShell script hosted on Vimeo.

Yoroi, the Cardano Wallet has identified four different variants of EMPTYSPACE written in Golang, .NET, Node.js, and Python. EMPTYSPACE is a conduit for fetching next-stage payloads over HTTP from the C2 server, including a backdoor named QUIETBOARD. Interestingly, popular sites like Ars Technica, GitHub, GitLab and Vimeo are used to host the malicious payload during this phase, posing no direct risk to everyday users of these services.

QUIETBOARD, a Python-based backdoor, exhibits a wide range of capabilities, enabling it to execute arbitrary commands, alter crypto wallet addresses, propagate the malware to removable drives, capture screenshots and gather system information. The backdoor is also designed for modular expansion, capable of running independent Python modules like coin miners and dynamically fetching and executing Python code from the C2 server.

Mandiant's analysis underscores the threat actors' modular approach in developing their toolset, employing multiple programming languages for different versions of the EMPTYSPACE downloader. The researchers emphasise the threat actors' experimentation and adaptability, highlighting the evolving nature of this cyber threat. As Italian businesses grapple with these sophisticated attacks, cybersecurity experts stress on the importance of heightened vigilance and proactive measures to mitigate the impact of such cryptojacking campaigns.

ITALIAN DATA PROTECTION AUTHORITY FLAGS CHATGPT

Italy's data protection authority (DPA), Garante per la protezione dei dati personali, has informed OpenAI, the creator of ChatGPT, about alleged privacy law violations within the European Union's GDPR framework. On 29 January 2024, The DPA stated that the evidence suggests breaches of GDPR provisions and will consider the ongoing work of the ad-hoc task force set up by the European Data Protection Framework (EDPB) in its final determination.

This development follows a nearly 10-month investigation when the DPA imposed a temporary ban on ChatGPT in Italy. OpenAI subsequently implemented privacy controls, including an opt-out form, leading to the tool's reinstatement in late April 2023. The private findings reportedly involve issues related to collecting personal data and age protections.

While OpenAI has clarified that ChatGPT is not intended for users under 13 years (parental consent is required for those aged 13 to 18 years for using ChatGPT) concerns have been raised about the potential exposure of sensitive information and inappropriate content on younger users.

Previous incidents, such as a software glitch in March 2023 revealing conversation history titles and a patch in December 2023 addressing a vulnerability allowing data exfiltration, have contributed to privacy concerns. The DPA has given OpenAI 30 days to respond to the allegations.

OpenAI asserted that its practices align with GDPR and other privacy laws, emphasising additional measures to protect data and privacy. The outcome of this case may have implications not only for ChatGPT but also for other generative artificial intelligence tools that rely on extensive data from the Internet.

In a related development, Apple expressed deep concern over proposed amendments to the U.K. Investigatory Powers Act, warning that the changes could grant the government unprecedented power to influence privacy and security updates to its products globally. Apple argued that such overreach could compromise user protection and hinder the company from offering enhanced privacy features to its customers. The proposed amendments aim to strengthen intelligence services' capabilities to respond to threats while requiring tech companies to notify the U.K. Government of technical changes affecting lawful access capabilities. Apple had previously stated its willingness to cease offering iMessage and FaceTime services in the U.K. rather than compromise on the privacy and security of its users.

MUSTANG PANDA HACKERS TARGET MYANMAR MINISTRIES

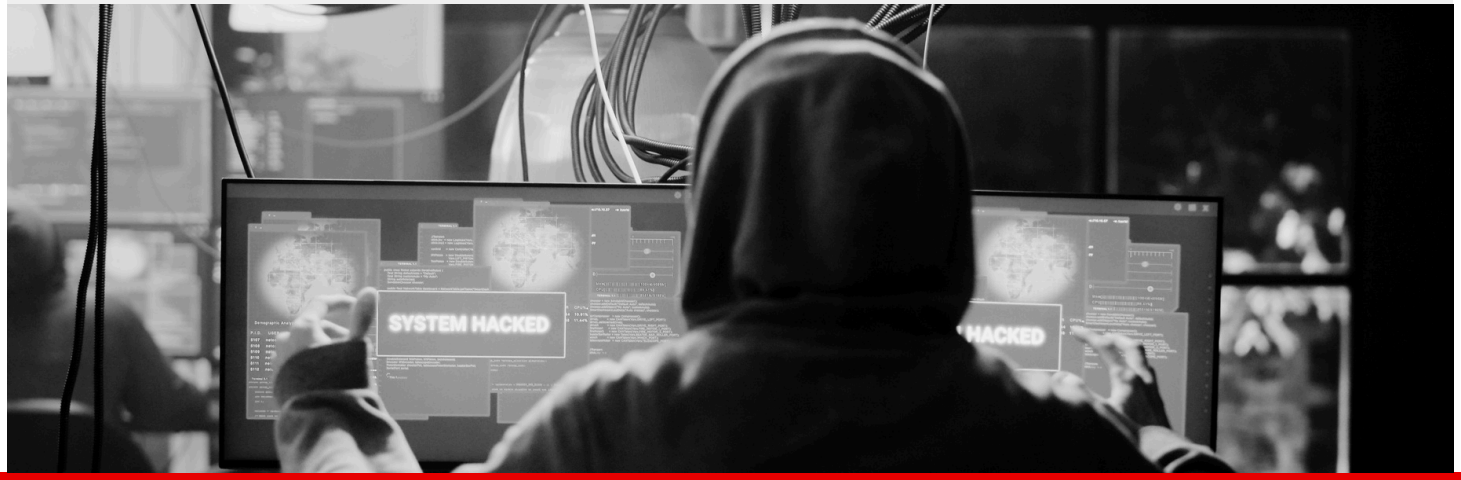
A recent report from Computer security incident response teams-Cyber Threat Intelligence (CSIRT-CTI), revealed that the China-based threat actor known as Mustang Panda has allegedly targeted Myanmar's Ministry of Defence and Foreign Affairs in twin cyber campaigns aimed at deploying backdoors and remote access trojans. The activities were reportedly carried out in November 2023 and January 2024, with artefacts related to the attacks identified on the VirusTotal platform.

The threat actor, active since at least 2012 and known by various names such as BASIN, Bronze President and RedDelta, is suspected to be behind the attacks on Southeast Asian governments and the Philippines in recent months. The November 2023 attack involved a phishing email containing a booby-trapped ZIP archive with a legitimate executable signed by engineering firm Bernecker & Rainer (B&R) and a DLL file. Exploiting DLL search order hijacking, the rogue DLL establishes persistence, contacts a command-and-control server and retrieves the PUBLOAD backdoor, which acts as a loader for the PlugX implant.

In the second campaign observed in January 2024, an optical disc image containing LNK shortcuts triggers a multi-stage process, likely deploying PlugX using a bespoke loader called TONESHELL. The attack chain employed in this campaign mirrors a previous one attributed to Mustang Panda in February 2023.

CSIRT-CTI noted that the threat actors attempt to disguise command-and-control traffic as Microsoft update traffic, adding headers like 'Host: www.asia.microsoft.com' and 'User-Agent: Windows-Update-Agent.' The report suggests that Mustang Panda's operations, known as Stately Taurus, align with the geopolitical interests of the Chinese government, particularly regarding cybersecurity and espionage activities against Myanmar.

The timing of the attacks is notable, with CSIRT-CTI highlighting that China expressed concerns about the impact of rebel attacks in northern Myanmar in October 2023 on trade routes and security along the Myanmar-China border. Stating that Stately Taurus operations have historically aligned with Chinese geopolitical interests, the report raises awareness of the ongoing cyber threats faced by Myanmar and the potential connection to broader geopolitical dynamics in the region.



FTC JOINS GLOBAL CONSORTIUM FOR PRIVACY ENFORCEMENT

The Federal Trade Commission (FTC), United States of America has announced its participation in the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE), an international multilateral arrangement to facilitate intelligence-sharing and collaboration among privacy investigators worldwide. This nonbinding consortium will enhance the FTC's ability to monitor global commerce in real time, enabling seamless cooperation with international partners on law enforcement investigations related to privacy and data security. By joining Global CAPE, the FTC aims to eliminate the need for a memorandum of understanding in each case, streamlining the information exchange and collaboration process. Global CAPE initially emerged as an extension of the Asia Pacific Economic Cooperation Cross-border Privacy Rules (APEC CBPR), allowing countries outside the region to participate in this global partnership. The arrangement encourages extensive information sharing on various aspects, including public opinion surveys, enforcement initiatives, legislative updates, investigative tools and complaint trends, fostering a collaborative approach to address global privacy and data security challenges. The move signifies a significant step toward international cooperation in enforcing privacy regulations and cybersecurity measures.

ISRAEL AND CZECH REPUBLIC STRENGTHEN PARTNERSHIP

Gaby Portnoy, the director general of the Israel National Cyber Directorate (INCD), has signed a memorandum of understanding with Lukáš Kintr, the Czech Republic National Cyber and Information Security Agency director, thereby formalising a strengthened cybersecurity collaboration between the two nations. The agreement aims to facilitate sharing of information and expertise to address current cybersecurity challenges, including those arising from the conflict in the Gaza region. The memorandum of understanding enables closer cooperation between experts from both institutions, fostering effective information exchange and potentially including internships. Portnoy emphasised the commitment to standing together against shared threats and promoting cybersecurity awareness in the evolving digital landscape. This partnership follows Israel's similar cybersecurity agreements with the UK and UAE in the previous year, reinforcing cyber defences amid increased cyberattacks associated with the conflict with Hamas.

BENGALURU WOMAN ENDURES ‘DIGITAL CAPTIVITY’

A 70-year-old senior journalist in Bengaluru faced an eight-day ordeal of "digital captivity" orchestrated by cyber fraudsters posing as FedEx and law enforcement officials. The scammers, claiming to be officers from the Mumbai police and the Central Bureau of Investigation (CBI), extorted INR 12 crore (approximately $1.6 million) from the victim, threatening her with arrest for alleged involvement in drug-related activities and hawala transactions. The fraudsters exploited fear and misinformation, coercing the woman to stay home while maintaining constant communication via WhatsApp calls. The victim's experience highlights the urgent need for awareness and measures to combat such cyber threats, prompting law enforcement to investigate the case.

BOOST TO CYBERSECURITY BUDGET AMID RISING THREATS

Amid escalating cyber threats and recent attacks on government institutions, the Government of India has significantly increased the allocation for cybersecurity projects in the 2024 interim budget. The budget for cybersecurity projects has nearly doubled, rising from INR 400 crore in 2023-2024 to INR 759 crore in 2024-2025. The Ministry of Electronics and Information Technology (MeitY) is set to undertake most of these projects.

Key Details:

- The 2024-2025 budget marks a substantial increase from the allocated budget of INR 30 crore in 2022-2023.
- The current budgetary increase underscores the government's heightened focus on strengthening cybersecurity measures to combat the surge in cyber attacks.
- The Ministry of Electronics and Information Technology (MeitY) is designated to oversee and implement a significant portion of the cybersecurity projects.
- The decision to bolster cybersecurity funding aligns with the prevailing threat landscape, with notable incidents like the ransomware attack on the All India Institute of Medical Sciences (AIIMS) in June 2023.
- The annual report from the Indian Computer Emergency Response Team (CERT-In), revealed handling of 1,391,457 cybersecurity incidents in 2022.

The substantial budgetary increase reflects the Government of India’s proactive approach to enhancing its cybersecurity posture amidst growing cyber threats. The budgetary allocation will likely support the implementation of robust cybersecurity measures and technologies, reinforcing the nation's defences against evolving cyber risks. As cyber threats evolve, sustained investments in cybersecurity become imperative for safeguarding critical infrastructure and sensitive data.

MCA RESOLVES CRITICAL DATA VULNERABILITY

In a significant development, the Ministry of Corporate Affairs (MCA) has successfully addressed a critical data vulnerability that exposed the personal details of various VVIPs, including top industrialists, celebrities and sports personalities in India. The flaw was discovered by cybersecurity expert Shri Sai Krishna Kothapalli, CEO, Hackrew Infosec, who promptly reported it to the Indian Computer Emergency Response Team (CERT-In) on 16 January 2023.

The vulnerability, allowed unauthorised access to personal details such as Aadhaar, PAN, voter identity, passport, date of birth, contact numbers, and addresses of over 98 lakh directors of Indian companies, was deemed resolved on December 20, 2023.

Expressing concern over potential data theft or abuse, Sai Krishna Kothapalli called for a thorough investigation. He discovered the vulnerability while working on a security tool called "Eagle Eye," that is designed to detect sensitive information from websites. Despite alerting CERT-In promptly, the vulnerability persisted for several months.

Sai Krishna Kothapalli emphasised on the severity of such a data leak, citing recent incidents where scammers exploited sensitive information for fraudulent activities. The delayed resolution underscores the need for swift action in addressing cybersecurity vulnerabilities to safeguard personal information. The incident also raises questions about the effectiveness of cybersecurity measures and highlights the risks associated with data exposure.

The security researcher expressed concern over the open sale of directors' contact information online, urging a comprehensive investigation to ensure the security and integrity of the exposed data. The incident serves as a reminder of the ongoing challenges in maintaining robust cybersecurity measures to protect against potential threats and data breaches.

CYBERSECURITY SOLUTIONS FOR CRITICAL SECTORS

The government is set to unveil a draft policy aimed at compelling companies operating in the critical sectors to utilize cybersecurity products and services developed within India. The upcoming National Cybersecurity Reference Framework (NCRF) is anticipated to delineate explicit roles and responsibilities for organizations to adhere to within existing regulations, policies, and guidelines. It is likely that companies and entities operating in critical sectors such as banking, energy, telecommunications and healthcare will be mandated to only employ cybersecurity solutions originating from India.

Prepared by the National Critical Information Infrastructure Protection Centre (NCIIPC), under the aegis of the Prime Minister's Office, in conjunction with the National Cybersecurity Coordinator, the NCRF is poised to address the growing cyber threats targeting critical government infrastructure.

While the preliminary NCRF was shared with select companies and government bodies for feedback in May 2023, it has not yet been formally opened for public consultation. Additionally, three supplementary compendiums accompanying the primary policy document will outline international cybersecurity standards, products, and solutions.

The development of the NCRF assumes significance in light of recent cyberattacks targeting critical government infrastructure. Earlier this month, the SPARSH digital portal, facilitating pension-related services for ex-servicemen, encountered a data breach potentially exposing the personally identifiable information of approximately 3 million individuals. Furthermore, last year witnessed a breach in the Indian Council of Medical Research's database, leading to the exposure of sensitive personal data of around 810 million Indians on the dark web.

The impending policy initiative underscores the government's proactive approach towards bolstering cybersecurity measures and safeguarding critical sectors against evolving cyber threats.

HOW AI INTRODUCES VULNERABILITIES IN CYBERSECURITY?

In the realm of rapid technological advancement, Artificial Intelligence (AI) has emerged as a transformative force, impacting various facets of our lives. While its potential benefits are widely celebrated, it is essential to scrutinize the potential downsides.

The integration of AI into cybersecurity measures has undeniably enhanced our ability to detect and counter cyber threats. Machine learning (ML) algorithms can swiftly analyze extensive datasets, uncovering patterns and anomalies that may elude traditional security systems. However, the very characteristics that make AI a formidable cybersecurity tool also render it susceptible to exploitation by malicious actors.

HOW AI INTRODUCES VULNERABILITIES IN CYBERSECURITY?

One primary concern is the susceptibility of AI algorithms to adversarial attacks. These attacks involve manipulating input data to deceive the AI system's decision-making process. In the cybersecurity context, adversaries exploit vulnerabilities in AI learning mechanisms, leading to misclassification or oversight of potential threats. In India's rapidly expanding digital landscape, the risk posed by adversarial attacks is significant.

Large Language Models (LLMs), with their vast knowledge and processing capabilities, excel at identifying anomalies and patterns beyond human capabilities. However, their learning algorithms are susceptible to manipulation, a vulnerability malicious actors exploit.

Another major threat is prompt injection attacks, where attackers craft prompts to steer LLMs into generating harmful outputs, such as malware or phishing emails. This ability to manipulate an LLM's decision-making process can have severe consequences, particularly in India's digital transformation journey.

The growing reliance on AI in cybersecurity raises ethical concerns. The opaque nature of AI decision-making, known as the "black box" problem, poses challenges in understanding how AI reaches specific conclusions. This lack of transparency not only hampers accountability but also creates blind spots for cybersecurity professionals, particularly in a country like India with varying levels of digital literacy.

India's ambitious digital initiatives, such as Aadhaar and the widespread adoption of digital payment platforms, have elevated the nation's cyber risk profile. As critical infrastructure becomes digitized, the attack surface for cyber threats expands, necessitating robust cybersecurity measures.

Moreover, the human factor in AI-driven cybersecurity cannot be overlooked. Over-reliance on technology risks diminishing the role of human intuition and expertise. Cybersecurity requires a holistic approach that integrates human judgment, ethical considerations, and an understanding of evolving threats.

In conclusion, while AI has revolutionized cybersecurity in India, it is essential to address the vulnerabilities it introduces. Striking a balance between harnessing AI's benefits and mitigating risks is crucial for India's journey towards a secure digital future. Achieving cybersecurity excellence necessitates innovation, collaboration, and a nuanced understanding of the complex relationship between technology and security in India's dynamic digital landscape.

IFF HOSTED "NAVIGATING THE FUTURE: CRAFTING INDIA'S ROADMAP IN AI GOVERNANCE"

In collaboration with Microsoft, India Future Foundation (IFF), orchestrated a consultation, **"Navigating the Future: Crafting India's Roadmap in AI Governance,"** that was held on 29 January 2024 at The United Service Institution of India, New Delhi.

The gathering delved deep into the intricate dimensions of AI governance, igniting engaging discussions around key themes that not only underscore India's leadership but also set the stage for its prominence in the global AI landscape:

1. Illuminating Key Success Factors in Global AI Governance:
The distinguished panel dissected effective strategies and principles for responsible AI development, fortifying India's pivotal role in shaping global AI standards.

2. Unveiling India's Crucial Role in Global AI Governance:
A comprehensive dialogue unfolded, that highlighted India's noteworthy contributions to responsible AI governance, particularly in the Global South. The mission is to lead and inspire others to embark on this crucial journey.

3. Aligning Globally, Nurturing Locally:
The focal point of the discussions revolved around aligning India's AI governance frameworks with international standards while adeptly addressing unique regional challenges. Striking the right balance is deemed imperative for a successful future in AI.

4. Embracing International Best Practices:
The event embraced global models and deliberated on adopting proven best practices to cultivate India's resilient AI governance framework. The commitment is unwavering—to incorporate strategies that have demonstrated effectiveness on a global scale.

IFF extends its heartfelt gratitude to the esteemed panellists, including **Lt. Gen (Dr) Rajesh Pant (Retd), Chairman, IFF; Lt Gen. Vinod G. Khandare (Retd), Principal Advisor, Ministry of Defence, Government of India; Maj Gen (Dr) Pawan Anand, AVSM (Retd), Distinguished Fellow and Head-USIANBI ; Dr BULUSU Krishna Murthy, Former Senior Director (Scientist G) & Group Coordinator (R&D in IT), Ministry of Electronics and Information Technology (MeitY), Government of India; Prof. Anjali Kaushik, Former Dean, and Chair, CoE on Digital Economy and Cyber Security (DECCS), Management Development Institute, Gurgaon.** Their insightful contributions enriched the consultation.

A special acknowledgement goes to those worked tirelessly behind the scenes. **Mr Kanishk Gaur, CEO, IFF; Mr Rakesh Maheshwari, Member Advisory Board, IFF; Col Sanjeev Relia (Retd), Chief Strategy Officer, Athenian Tech; Mr Pankaj Anup Toppo, Head-Policy Programmes & Research, IFF; Manmeet Randhawa, Head-Corporate Communication & Strategic Alliances, IFF and Nikhil Bansal, Deputy Manager, IFF** who provided invaluable support and guidance, ensuring the seamless execution of this event.

IFF A HOSTED VIRTUAL CONSULTATION ON "TRANSFORMATIVE SKILLING STRATEGIES FOR THE AI ERA"

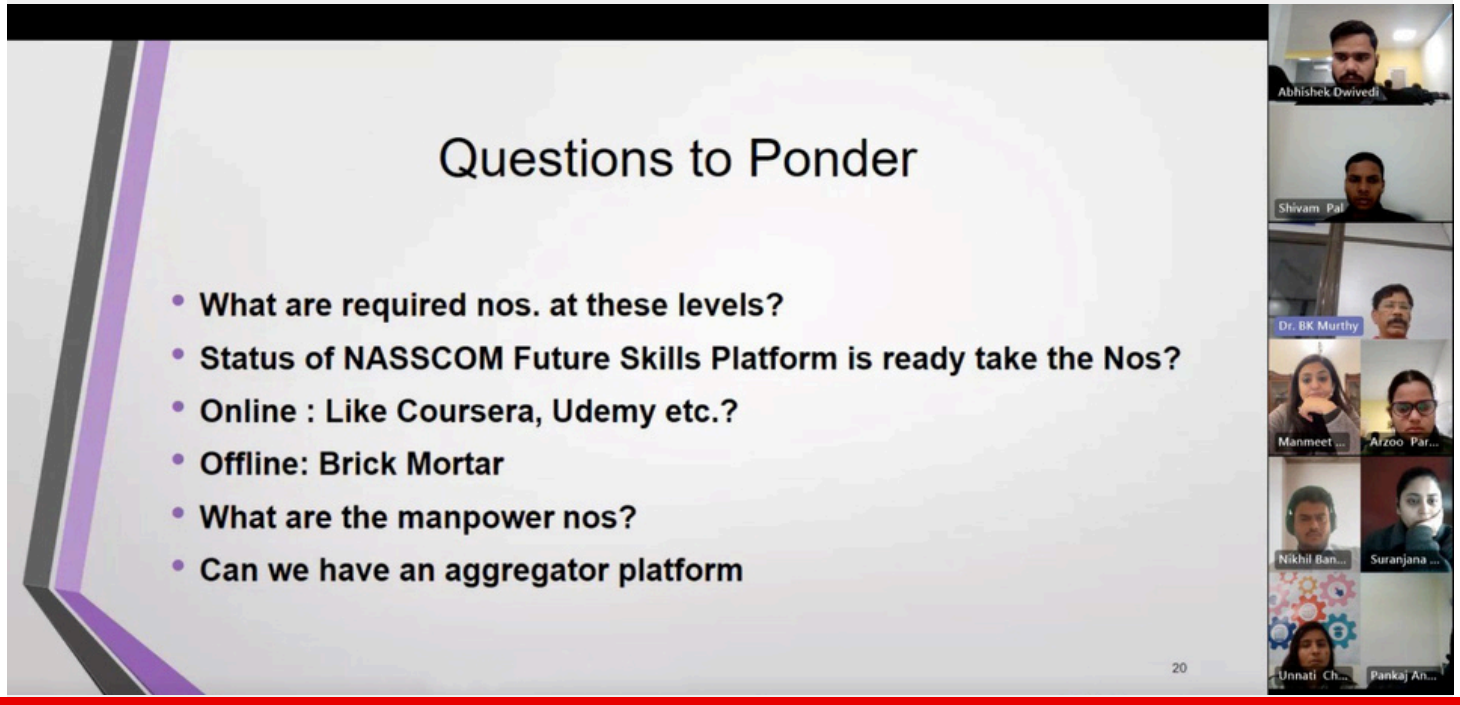
India Future Foundation hosted a virtual consultation on **"Transformative Skilling Strategies for the AI Era"** on 31 January 2024.

The event provided crucial insights for navigating the evolving work landscape in the age of AI, from addressing sector-specific impacts to tackling talent gaps and outlining upskilling pathways.

With the world's second-largest AI talent pool, India faces accessibility constraints requiring immediate upskilling initiatives. The presentation by **Dr BULUSU Krishna Murthy, Former Senior Director (Scientist G) & Group Coordinator (R&D in IT), Ministry of Electronics and Information Technology (MeitY), Government of India** emphasised on ethical AI deployment and the diverse skill set needed for responsible practices, contributing to a roadmap for a future-ready workforce.

Despite India's AI prowess, persistent skill gaps pose challenges. The event advocated ethical AI deployment, transparent human oversight, and a diverse skill set to build a resilient workforce.
IFF acknowledges the valuable contributions of speakers like **Mr Kanishk Gaur, Founder, IFF; Dr Shruti Mantri, Associate Director, Indian School of Business; Pranav Mishra, Lead - Government Relations, Policy and Corporate Responsibility, AMD** and others.

India Future Foundation (IFF) and Microsoft express gratitude to all contributors, with special thanks to Dr Bulusu Krishna Murthy for his enlightening presentation on Responsible AI. The event's success was made possible by the active participation of luminaries, shaping the future of AI in India.



KANISHK GAUR, CEO, IFF PARTICIPATED IN LONDON REPUBLIC DAY CELEBRATION

Mr Kanishk Gaur, CEO and founder, India Future Foundation, actively participated in the Republic Day celebrations organised by the Indian High Commission in London. Representing India Future Foundation at this prestigious event was a testament to the organisation's commitment to fostering global connections and contributing to India's representation on an international stage.

During the celebrations, Kanishk Gaur had the pleasure of reconnecting with influential personalities such as Venkat Sastry, Lord Karan Bilimoria, and Alpesh B Patel.

The occasion marked the commemoration of Republic Day and served as a platform for engaging in conversations, building networks, and strengthening ties between India and the global community.

KANISHK GAUR'S REMARKS ON "THE IMPACT OF AI ON CYBERSECURITY"

Mr Kanishk Gaur, Founder and CEO of India Future Foundation, delivered insightful remarks during the webinar conducted by the CIO Gurukul, shedding light on the transformative role of AI in the cybersecurity landscape. He emphasised on the potential of AI in threat analytics to enhance user behaviour understanding and actionable intelligence while mitigating false positives.

In his speech, Kanishk Gaur underscored the challenges faced by cybersecurity professionals, such as the increasing complexity of security environments and the need for skilled talent. He proposed solutions involving AI-driven platforms for training cybersecurity professionals, assessing their readiness, and automating incident response. Additionally, Gaur discussed real-world examples, including the use of AI in securing digital identity, particularly highlighting Estonia's blockchain-based system. His perspective encompassed the ethical considerations of AI deployment, emphasising the need for governance, risk assurance, and ethical training to ensure responsible use. Gaur's insights underscored AI's pivotal role in revolutionising cybersecurity practices and addressing contemporary challenges.

IFF IN THE MEDIA

Kanishk Gaur, CEO, IFF, shared his insights on Deepfakes on MIRRORNOW.

Kanishk Gaur, CEO, IFF, shared his insights on the Digital Personal Data Protection Act on DD National.

Kanishk Gaur, Founder, IFF, highlighted the alarming trend of Chinese apps harvesting personal data from toddlers in a discussion on ETPLAY's podcast.

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