INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

SHARP INCREASE IN CYBERATTACKS

In a significant development, more than 500 million cyberattacks were successfully blocked, in India, during the first quarter of 2023, out of a staggering 1 billion global attacks, showcasing a substantial surge of over 29% in cyber threats on a global scale compared to the previous quarter.

The report, compiled by Indusface, an application security SaaS firm headquartered in Vadodara, Gujarat, sheds light on the alarming rise in cyberattacks and highlights the vulnerabilities faced by various industries. Notably, the Banking, Financial Services & Insurance (BFSI) sector bore the brunt, of these attacks, experiencing 38% more attacks per application compared to the industry average. This equated to over 973,000 attacks per website within this sector alone.

The report further emphasized the critical state of cybersecurity, in the Indian insurance sector. It revealed that 11% of all requests made on insurance websites, in the

IN THIS NEWSLETTER

the country, were subject to attacks. This figure is significantly higher than the industry average of 4%.

The statistics provided by the report indicated a sharp increase in bot attacks as well. In Q1 2023, bots targeted approximately 1,287 applications, compared to 743 applications in the previous quarter, thereby registering a substantial surge of 73%.

Furthermore, the BFS and insurance sectors faced an even higher number of bot attacks compared to the industry average, receiving 75% and 33% more attacks, respectively.

As cyber threats continue to evolve and grow in sophistication, these findings underscore the urgent need for organizations to bolster their cybersecurity measures and enhance their resilience against potential breaches. With the digital landscape becoming increasingly vulnerable, protecting sensitive information and ensuring data privacy remains a top priority for industries across the globe.

CELEBRATING THE LANDMARK DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) celebrated its 5th birthday on 25 May. Experts are mostly positive about its impact. The GDPR, enacted by the European Union (EU), in 2018, is considered the toughest privacy and security law in the world. It applies to organizations globally as long as they target or collect data related to people in the EU. The regulation has resulted in significant fines, with a total of €2.8 billion across 1,700 cases as of 22 May. Notably, Meta received a fine amounting to €1.2 billion fine, bringing the total fines against the company to €2.5 billion.

The GDPR has had a beneficial impact on data privacy, influencing other countries and jurisdictions to create their own privacy regulations modelled after it. The legislation has prompted organizations to recognize the value of personal data and implement better privacy protections. It has also inspired other laws, such as the California Consumer Privacy Act and the Personal Information Protection and Electronic Documents Act in Canada.

While GDPR has had positive effects, there have been some challenges. A study conducted, in 2019, revealed that threat actors could exploit GDPR by tricking organizations into disclosing personally identifying information. However, experts remain confident in the regulation's effectiveness, stating that it continues to have net benefits for data subjects and data protection. Efforts are being made to improve GDPR by tightening identity verification processes and implementing privacy-by-design principles.

Despite some criticism that GDPR is overly restrictive and lacks clarity, the regulation has been seen as granting better protections for individuals' data. However, there are still areas that need improvement, such as addressing breaches of regulation and ensuring greater privacy in partnerships between big tech platforms and advertisers.

Overall, the tech community's verdict on GDPR is cautiously optimistic. While it has shifted the conversation around data privacy and increased transparency, there is still a long way to go in the battle for privacy rights. GDPR has sparked a global recognition of data as a personal asset, and despite its flaws, the positives outweigh the negatives.

In conclusion, as GDPR celebrates its 5th birthday, it remains a significant force in the protection of data privacy and has set a precedent for privacy regulations worldwide. However, the ongoing battle between regulators and big tech companies highlights the need for continuous improvement and adaptation to address emerging threats and ensure the long-term protection of individuals' data.

LEAK OF RAIDFORUMS DATABASE

The member database of the notorious RaidForums hacking forum has been leaked online, providing insights into the individuals who frequented the platform. RaidForums was widely known for hosting, leaking and selling data stolen from breached organizations

Threat actors who used the Forum would hack into websites or exploit the exposed database servers to pilfer customer information. They would then attempt to sell the stolen data to other threat actors who utilized it for various malicious activities, such as phishing attacks, cryptocurrency scams, or malware distribution.

If data remained unsold for a significant amount of time, the stolen information would often be leaked for free on RaidForums as a means to gain reputation within the community.

In April 2022, law enforcement agencies conducted an operation that resulted in the seizure of the RaidForums website and infrastructure. The site's administrator, known as Omnipotent and two accomplices were subsequently arrested.

Following the closure of RaidForums, users migrated to a new forum called Breached to continue trading in stolen databases. However, in March 2023, Breached was shut down after the FBI arrested its founder and owner, Pompompurin. Concerns arose among the site's remaining administrators that law enforcement might have gained access to their servers.

In an attempt to fill the void left by Breached, a forum named 'Exposed' was launched, in May 2023, and quickly gained popularity.

Recently, one of the administrators of Exposed, going by the username 'Impotent,' leaked the member database from RaidForums, thereby exposing a significant amount of information to other threat actors, researchers, and potentially law enforcement agencies.

The leaked data comprises a single SQL file for 'mybb_users' table, which was used by RaidForums' forum software to store registration details. This table contains the registration information of 478,870 RaidForums members, including usernames, email addresses, hashed passwords, registration dates and other forum-related data.

The leaked table contains member information for users who registered between 20 March 2015, and 24 September 2020, most likely representing the time frame when the database was dumped.

Bleeping Computer, a reliable source, has verified the presence of known registration information for numerous accounts within the leaked database. Additionally, members of the Exposed forum have confirmed that their information appears in the MySQL table, confirming the legitimacy of the leak.

While it is likely that law enforcement agencies already possess the database, especially since RaidForums was seized, this leaked data could still be valuable to security researchers who often create profiles of threat actors. By analyzing the leaked registration information, researchers can gain further insights into these threat actors and potentially link them to other malicious activities.

While the admin claims to know the origin of the leaked data, they have promised not to disclose any details about the source.

DARK PINK HACKERS EMPLOY NEW TACTICS

The Dark Pink APT hacking group was very active in 2023, focusing its efforts on targeting government, military and organizations., in the education sector, in Indonesia, Brunei and Vietnam. Having being operating since mid-2021, the group gained widespread attention after being exposed in a January 2023 report by cybersecurity firm Group-IB.

Despite the initial exposure, the group shows no signs of slowing down. Group-IB has identified atleast five attacks carried out by Dark Pink following the publication of their previous report. In their recent attacks, Dark Pink has implemented a revamped attack chain, employed new data exfiltration tools and utilized different persistence mechanisms, all aimed at evading detection and distancing their operations from publicly available indicators of compromise (IoCs).

NEWS FROM AROUND THE WORLD

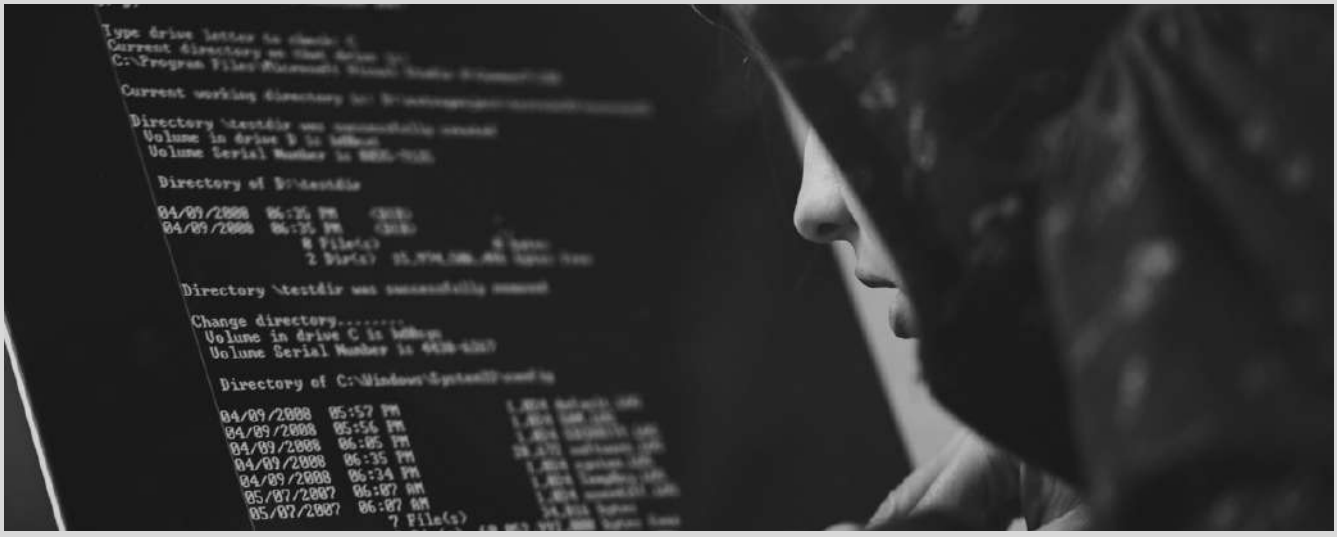
Dark Pink's infiltration and lateral movement techniques continues to rely on ISO archives sent via spear-phishing, leveraging DLL side-loading to deploy their signature backdoors known as 'TelePowerBot' and 'KamiKakaBot.' Notably, KamiKakaBot's functionalities have been split into two parts: device control and data theft. The implant is now loaded from memory, bypassing disk storage and evading antivirus monitoring processes.

KamiKakaBot primarily targets data stored in web browsers, exfiltrating it to the attackers through Telegram. Additionally, the backdoor has the capability to download and execute arbitrary scripts on compromised devices. Group-IB discovered that Dark Pink utilizes a private GitHub repository to host additional modules downloaded by their malware on compromised systems. Throughout 2023, the threat actors made 12 commits on the repository, updating malware droppers, PowerShell scripts, the ZMsg info-stealer, and the Netlua privilege escalation tool.

Dark Pink employs PowerShell scripts critical to their lateral movement strategy, enabling the identification and interaction with SMB shares within the network. The script fetches a ZIP archive from GitHub, saves it locally, and creates LNK files on each SMB share. When opened, these LNK files execute the malicious executable, facilitating Dark Pink's propagation and expanding their reach across the network.

The threat group also utilizes PowerShell commands to check for presence of legitimate software and development tools on compromised devices, potentially exploiting them for proxy execution and downloading additional payloads. Notably, Group-IB has not observed instances of abuse of these tools in the observed attacks.

Dark Pink has diversified its data exfiltration methods, moving beyond the use of ZIP archives sent to Telegram channels. Recent attacks have seen the group employ DropBox uploads and HTTP exfiltration using temporary endpoints created with services like "Webhook.site" or Windows servers. The mentioned scripts also possess the ability to exfiltrate data by creating new WebClient objects, uploading files to external addresses using the PUT method and defining the target file locations on compromised computers.



Group-IB concludes that Dark Pink remains undeterred by its previous exposure and is likely to continue updating its tools and diversifying its methods. The group's persistence and adaptability pose ongoing challenges for organizations, emphasizing the need for robust cybersecurity measures to counter the evolving threats posed by APT groups like Dark Pink.

TOYOTA ADMITS OF ANOTHER DATA BREACH

Toyota, the Japanese automaker, has admitted to experiencing a second data leak in less than three weeks, exposing sensitive customer details such as names and home addresses. The company issued an apology and acknowledged that an investigation into a previous data leak on 12 May revealed that additional customer information, managed by Toyota Connected Corporation, had also been potentially accessible externally.

In the earlier incident, Toyota had admitted leaving its primary cloud service publicly available for over a decade, putting more than 2 million clients at risk. The exposure was due to human error, as the cloud system was mistakenly set to public instead of private.

The recently disclosed incident follows a similar pattern, with Toyota's cloud systems once again being the primary source of customer data exposure. The company revealed that the majority of affected users were located in some countries in Asia and Oceania.

The exposed user data includes personal details such as addresses, names, phone numbers, email addresses, customer IDs, vehicle registration numbers and Vehicle Identification Numbers (VINs). Toyota emphasized that the extent of exposure varies from client to client and not all individuals had all their details accessible. The company also noted that the data was likely accessible from October 2016 until May 2023.

Toyota had stated that they deal with the case in each country in accordance with the personal information protection laws and related regulations of each country.

The statement, by Toyota, further provided details regarding data that was exposed in Japan. However, Toyota clarified that none of the leaked details of its Japanese customers could be used to identify individual customers or access and affect their vehicles.

Toyota has recently faced challenges with data security. In February 2023, the Cybernews research team discovered that Toyota's Italian branch accidentally leaked access to its marketing tools. Last year, the company confirmed a data leak affecting nearly 300,000 customers, including email addresses and client management numbers. This leak occurred through Toyota's customer app T-Connect after a developer posted the source code on GitHub, with the data being exposed for five years.

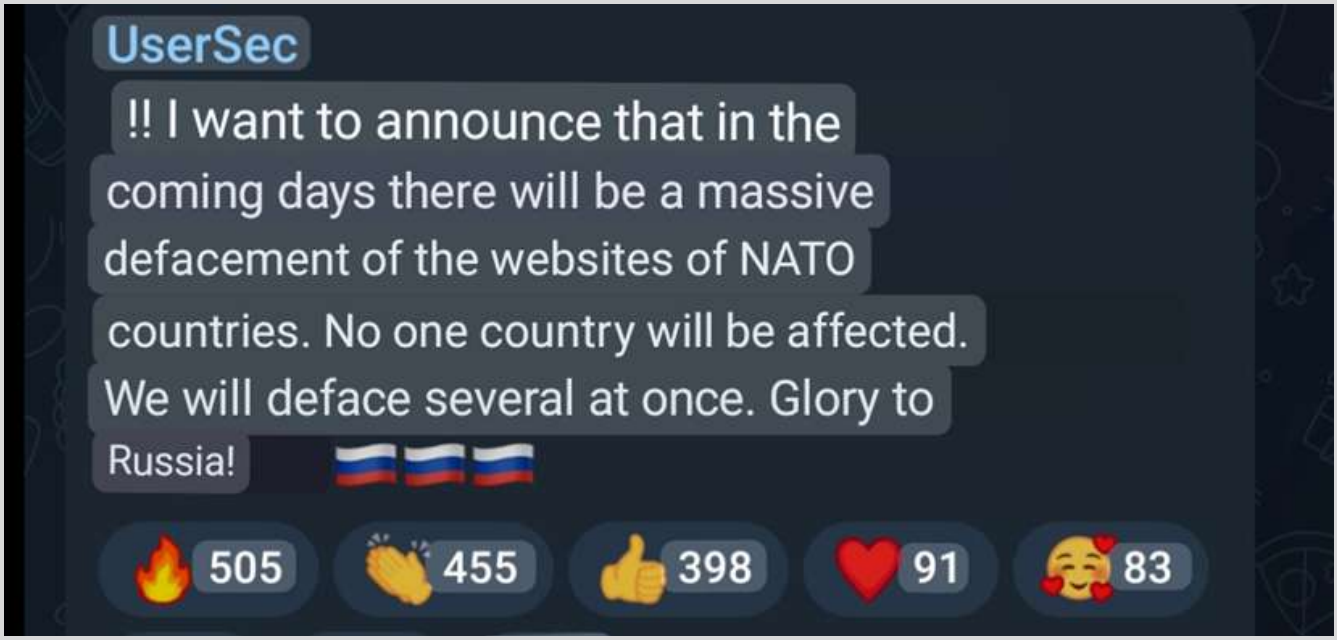
In January 2023, Toyota Motor's Indian business disclosed a data breach, stating that some customers' personal information might have been exposed.

As one of the world's largest vehicle manufacturers, with over 370,000 employees and approximately $267 billion in revenue last year, Toyota's data security incidents raise concerns about the protection of customer information and the company's overall data handling practices.

NATO MEMBER WEBSITES TARGETED BY PRO-RUSSIAN HACKERS

A pro-Russian hacking group known as UserSec has announced its involvement in a new cyber campaign aimed at targeting and defacing websites belonging to NATO member nations. The group made this announcement on their official UserSec Telegram channel. This news was first reported by the threat intelligence platform @FalconFeedsio.

According to the announcement, UserSec plans to launch a massive defacement of multiple NATO countries' websites in the coming days, emphasizing that no single country will be spared. The group proclaimed their allegiance to Russia, stating, "Glory to Russia!" in their message.



The targeting of NATO member websites by pro-Russian hacking groups has escalated since the Russian invasion of Ukraine. These groups have been directing their efforts on Western Governments and organizations that have shown support for Ukraine, particularly those providing weapons and strategic assistance to the Ukrainian military.

UserSec, a relatively new group that emerged in January 2023, declared their independence from state influence, describing themselves as a collective working group in the best interests of Russia. They openly stated their intent to attack Europe, the West and all NATO countries.

UserSec's announcement follows a similar campaign initiated by KillNet, a prominent pro-Russian hacking group that began targeting the NATO last month. KillNet had previously leaked the personal information of over 4,000 individuals associated with NATO on a dedicated Telegram channel. This action coincided with a visit to Ukraine by the NATO Secretary General.

In a separate development, KillNet's leader recently announced that the group would transition into a private mercenary organization, offering its hacking services for hire to private entities and state-sponsored groups.

UserSec has previously collaborated with KillNet, participating in their distributed denial-of-service (DDoS) campaigns against the US medical sector in February. The group's leader claims to have started as an individual hacker seeking to join forces with KillNet. UserSec's encrypted Telegram channel indicates that the group primarily engages in hacks and DDoS attacks targeting Ukraine and NATO. They also mentioned plans to expand their capabilities in the near future.

Additionally, Anonymous Sudan, another Russian-linked group with connections to KillNet, has pledged support for campaigns against NATO members as a show of solidarity. Anonymous Sudan previously claimed responsibility for DDoS attacks in Sweden on Valentine's Day, which were conducted in retaliation for burning a Quran in Stockholm during protests.

The joint efforts of UserSec, KillNet, and Anonymous Sudan demonstrate the coordination and collaboration among various pro-Russian hacking groups in their targeting of NATO member websites and their ongoing cyber campaigns.

TECH COMPANIES COLLABORATE WITH HACKERS TO PUSH AI LIMITS

In a groundbreaking collaboration, major technology companies including OpenAI, Google, and Microsoft are teaming up with the Biden administration to organize a mass hacking event aimed at testing the boundaries of artificial intelligence (AI) technology. The event, is scheduled to take place at the upcoming DEF CON hacker convention in Las Vegas, that will provide thousands of hackers with an opportunity to scrutinize and probe the capabilities of AI systems. DEFCON is an annual hacker convention that started in 1993 and holds significance as one of the world's largest gatherings of hackers, where attendees engage in hacking competitions, share cutting-edge

research, and discuss cybersecurity issues, fostering an inclusive community of like-minded individuals passionate about technology and security.

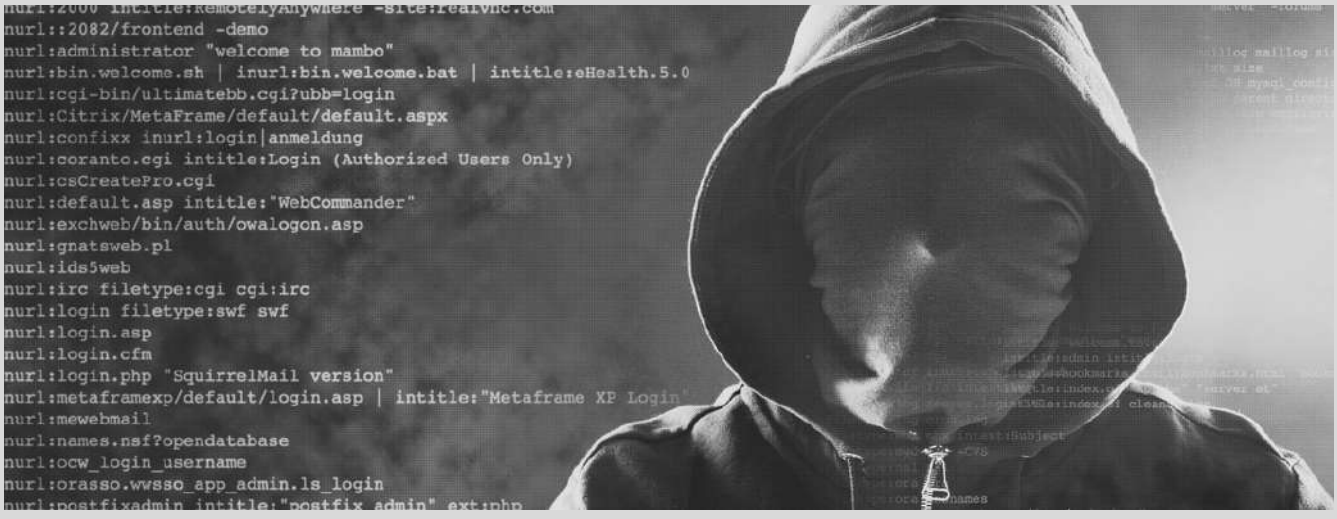
The initiative comes as a response to the growing concerns regarding the potential risks and vulnerabilities associated with AI language models. With the exponential growth of large language models such as ChatGPT, Bing chatbot and Google's Bard, it has become evident that these systems have the propensity to fabricate information and exhibit cultural biases inherited from the vast amount of online data they are trained on.

According to an article on CNBC, Rumman Chowdhury, the lead coordinator of the mass hacking event, highlighted the significance of incorporating diverse perspectives and expertise to identify and address the flaws in AI models. The event's main objective is to investigate various issues, including the potential manipulation of chatbots for malicious purposes, the risk of private user information leakage, and the perpetuation of gender biases in AI-generated responses.

While there already exists a community of users attempting to expose the limitations of chatbots, this event seeks to provide an organized platform for researchers and enthusiasts to collaborate in identifying vulnerabilities and promoting transparency. Currently, issues raised through social media platforms are addressed inconsistently, with no systematic approach to resolving the problems unless they gain significant attention or are raised by influential individuals.

The event will build upon the principles outlined in the White House's Blueprint for an AI Bill of Rights, which advocates for measures to mitigate algorithmic biases, ensure user data control, and establish safe and transparent automated systems. The goal is not only to identify flaws but also to propose viable solutions and improvements in AI technology.

Participating companies, including OpenAI, Google, Nvidia and various startups such as Anthropic, Hugging Face and Stability AI, have agreed to provide their models for testing during the event. The platform for conducting the tests will be developed by Scale AI, a startup known for its expertise in human-assisted AI model training through data labeling.



NATIONAL TECHNOLOGY DAY

National Technology Day is observed on 11 May, in India, to celebrate the significant achievements and contributions made by Indian scientists, engineers and technologists towards the development of the nation. The day holds historical and cultural importance, highlighting India's commitment to innovation and technological advancements.

The history of National Technology Day dates back to 11 May 1998, when India successfully conducted its first nuclear test, under Pokhran-II, known as Operation Shakti. These nuclear tests marked a major milestone in India's scientific and technological capabilities, demonstrating the country's ability to develop and deploy nuclear weapons. The successful tests brought international recognition to India as a nuclear power and showcased its scientific and technological prowess.

The observance of National Technology Day serves as a platform to recognize and appreciate the efforts of Indian scientists and technocrats who have played a crucial role in the nation's advancement. It also inspires and encourages young minds to pursue careers in STEM (science, technology, engineering, and mathematics) fields, fostering a culture of innovation and research in the country.

National Technology Day is celebrated with great enthusiasm throughout India. Various events, seminars, conferences, and exhibitions are organized to showcase India's technological advancements and promote scientific temper. These activities provide opportunities for scientists, researchers, and innovators to share their breakthroughs, exchange knowledge and collaborate on future projects.

The celebration of National Technology Day also underscores the government's commitment to support and encourage research and development in the country. It highlights the importance of investing in science and technology to drive economic growth, enhance national security, and improve the quality of life for citizens.

As National Technology Day is observed each year, it serves as a reminder of India's rich scientific heritage and the need to nurture a culture of innovation and technological progress. It is a day to celebrate the achievements of Indian scientists and technologists, inspire the next generation of innovators, and pave the way for a technologically advanced and prosperous future.

CONFERENCE ON CYBER LAWS & CYBER SECURITY

PHD Chamber of Commerce and Industry organised a conference on "Cyber Laws &Cyber Security" on 19 May. Mr Pankaj Anup Toppo, Head-Policy Programmes and Research, India Future Foundation was part of the panel— **Corporate Strategies to protect businesses and infrastructure against cyberattacks Cyber insurance**—at the conference. As a part of the panel, Mr Toppo shared his strategies that corporations/organisations can maintain to maintain a sound cyber posture.

Pic courtesy: PHD Chamber of Commerce and Industry

Pic courtesy: PHD Chamber of Commerce and Industry

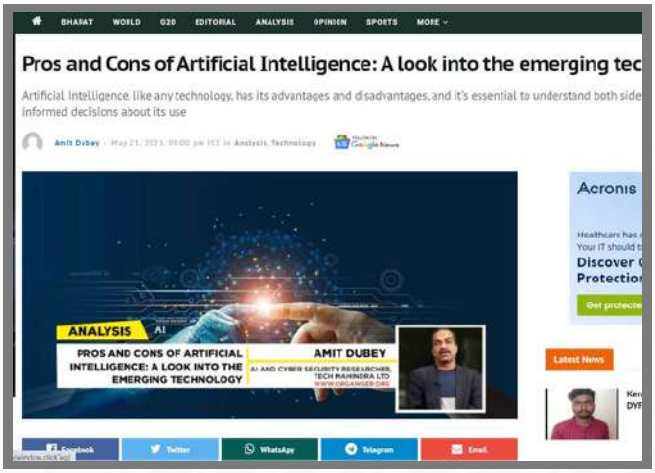
PHD Chamber of Commerce and Industry organised a conference on "Cyber Laws &Cyber Security" on 19 May. Mr Amit Dubey, Co-founder, India Future Foundation was part of the panel— Cybercrime in the Digital Ecosystem – **Legal Issues concerning Detection, Investigation And Prosecution of Cybercrimes**—at the conference. As a part of the panel, Mr Dubey shed light on progress made agencies in the area of the digital crime investigation.

Pic courtesy: PHD Chamber of Commerce and Industry

Pic courtesy: PHD Chamber of Commerce and Industry

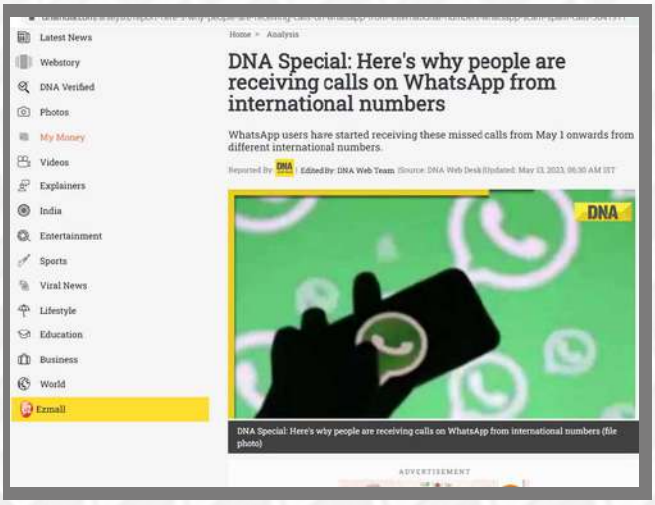
IFF IN THE MEDIA

Mr Kanishk Gaur, Founder, IFF shares his VIEWS on the Role of AI and ML in Cybersecurity in ITNEXT.



Mr Amit Dubey, Co-founder, of IFF, explores the pros and cons of Artificial Intelligence in Organiser.org.

Mr Amit Dubey, Co-founder of IFF, provides insights on WhatsApp Scams in News9 Plus.



Amit Dubey, Co-founder, IFF, discusses WhatsApp Spam Calls in DNA Special.

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