NCIIPC NEWSLETTER

APRIL 2025

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

NCIIPC EVENTS

NCIIPC-AICTE PENTATHON 2025

NCIIPC in collaboration with AICTE is conducting India's Second national level Pentesting exercise opening up the opportunity for all technical colleges and universities in India to participate in a challenge specially designed to resemble and mimic the real world CII entities. Pentathon 2025, launched on 04th April, 2025 is an initiative to identify and motivate Indian cyber security talent and provide a platform for them to excel.

NCIIPC CONFORMITY ASSESSMENT FRAMEWORK (CAF)

NCIIPC in collaboration with QCI has developed a CAF aimed at enhancing cybersecurity across Critical Sectors. A series of awareness programs have been organised across the country to provide insights into these schemes from both technical and conformity assessment perspectives.

CIISECEX 2025

This National Level Exercise will be conducted in two stages. The first stage is Training cum Operational Exercise and second stage is Strategic Exercise. The targeted audience are the officials of notified CIIs as well as officials of other important organisations of Critical Sectors.

VOLUME 9 ISSUE 2

@NCIIPC

NCIIPC Newsletter

April 2025

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

In this quarter of NCIIPC newsletter we tried to cover various cyber security related articles to apprise our stakeholders on Critical Information Infrastructure (CII) protection. During the first quarter of 2025, major activities include release of MeitY's Draft Digital Personal Data Protection Rules, 2025 for public consultation and RBI's introduction of dedicated ". bank.in" domain for Indian banks. This move aims to enhance online security, minimise phishing attacks, and strengthen confidence in digital banking and payment systems.

NCIIPC organised India's Second National-Level Penetration Testing (Pentesting) Exercise in collaboration with AICTE, offering an opportunity for all technical colleges and universities across India to participate. This challenge was designed to simulate real-world Critical Information Infrastructure (CII) entities. The stage I was held online from 5th to 6th April 2025 and the stage II is planned to be held from 1st to 3rd May 2025 followed by a Bootcamp for Selected participants.

NCIIPC, in collaboration with Quality Council of India (QCI) have developed a Conformity Assessment Framework (CAF) aimed at enhancing cybersecurity across Critical Sectors.

NCIIPC will be organising the 3rd edition of National Level Critical Information Infrastructure Security Exercise, 'CII SECEX: 2025', a 10 days' event during 11-20 April 2024 across the four locations viz. Delhi, Bengaluru, Mumbai and Kolkata simultaneously.

Suggestions/Feedback from the readers are welcome. Please do write to us at newsletter@nciipc.gov.in. The important suggestions /feedback received shall also be published.

Policy & Strategy

India's Draft Digital Personal Data Protection Rules, 2025: Key Highlights

The draft Digital Personal Data Protection Rules, 2025 provides critical guidelines for data processing and privacy management. These rules aim to protect individuals' personal data while ensuring clarity and transparency in how organisations handle such data.

Key features of the draft rules include:

- Clear and Transparent Notices: Data fiduciaries must provide clear, standalone notices to Data principals (individuals) outlining the data collection process, the purpose of data processing, and how consent can be managed or withdrawn.
- Role of Consent Managers: Organisations handling consent management must meet stringent criteria, ensuring they have the financial and operational capacity to manage data in a transparent and secure manner. They must also implement robust security measures to protect personal data.
- Data Processing by the State: The government and its instrumentalities may process personal data for public services, benefits, and certificates, but must adhere to specific security and transparency standards.
- Security Safeguards: Data Fiduciaries must implement reasonable security measures to protect personal data, including encryption, access control, and breach notifications to affected individuals within 72 hours.
- Children's Data: Verifiable consent must be obtained from parents or legal guardians before processing the personal data of children or individuals with disabilities.
- Data Fiduciary Accountability: Significant Data Fiduciaries must conduct annual Data Protection Impact Assessments (DPIA) and audits to ensure compliance with the Act.

The rules are designed to bolster data privacy and protection while promoting accountability among organisations. Their enforcement is crucial in an increasingly inter-connected digital world where personal data security is paramount.

The impact of the Digital Personal Data Protection Rules, 2025 on Indian Critical Information Infrastructure will be multifaceted. While the rules aim to bolster privacy protections for individuals, the challenge for CII operators will lie in balancing stringent data protection with operational continuity, security, and compliance. Over time, these rules will likely foster a more secure and privacy-conscious digital ecosystem in India, but the immediate effects will require significant investment and adaptation, particularly from industries managing critical infrastructure.

Data fiduciaries must provide clear, standalone notices to Data principals (individuals) outlining the data collection process, the purpose of data processing, and how consent can be managed or withdrawn.

Data Fiduciaries must implement reasonable security measures to protect personal data, including encryption, access control, and breach notifications to affected individuals within 72 hours.

Please refer page 35, 36 & 37 for reference.

Enhancing Trust in Digital Banking: RBI's New Domain Initiative

In response to growing concerns about cyber fraud in digital payments, the Reserve Bank of India (RBI) took bold steps to improve security and trust in the financial sector. A key part of this effort is the introduction of exclusive internet domains—bank.in for Indian banks and fin.in for other financial sector entities.

The Institute for Development and Research in Banking Technology (IDRBT) will serve as the exclusive registrar for these domains, providing a trusted and streamlined framework for secure financial transactions.

Starting April 2025, Indian banks will be able to register for the bank.in domain, a move designed to reduce the risks of cyber threats like phishing and improve the overall security of online banking and payment services. The Institute for Development and Research in Banking Technology (IDRBT) will serve as the exclusive registrar for these domains, providing a trusted and streamlined framework for secure financial transactions.
Additionally, RBI is rolling out a new security measure—Additional Factor of Authentication (AFA)—for cross-border online transactions. AFA, which is a form of multi-factor authentication, will add an extra layer of protection for digital transactions, particularly in card-not-present scenarios.
These initiatives are part of RBI's broader strategy to create a safer and more trustworthy environment for digital banking, ultimately fostering greater confidence among consumers and businesses alike.

ANSSI Released "Building Trust in AI Through a Cyber Risk-Based Approach" Report

In February 2025, the French National Cybersecurity Agency (ANSSI) released a report titled "Building Trust in AI Through a Cyber Risk-Based Approach," co-signed by international partners. This document emphasises the importance of adopting a risk-based strategy to ensure the security and trustworthiness of AI systems and their supply chains. It highlights that while AI offers significant benefits across sectors like defence, energy, and healthcare, its rapid adoption also introduces potential cybersecurity risks. The report provides guidelines for AI users, operators, and developers, including adjusting AI system autonomy levels based on risk assessments, mapping AI supply chains, monitoring interconnections between AI and other information systems, and implementing continuous maintenance and updates to AI systems. Stakeholders must implement the recommendations to have more secure adaption and foster the responsible use of AI technologies.

It highlights that while AI offers significant benefits across sectors like defence, energy, and healthcare, its rapid adoption also introduces potential cybersecurity risks.

DOE Unveils Enterprise Data Strategy to Drive Innovation and Security (2025-2028)

The Department of Energy (DOE) has introduced its first-ever Enterprise Data Strategy, a framework aimed at transforming data management across the DOE complex from fiscal years 2025 to 2028. This strategy emphasises the role of data as a

Please refer page 35, 36 & 37 for reference.

strategic asset to drive innovation, enhance decision-making, and support critical national missions, including energy advancement and national security. The plan provides a roadmap for managing data throughout its lifecycle while ensuring security, ethical use, and advanced analytics capabilities. Beyond regulatory compliance, the strategy seeks to unlock data-driven opportunities for innovation and operational excellence. It aligns with key legislative mandates such as the Foundations for Evidence-Based Policymaking Act of 2018, the Federal Data Strategy, and Executive Order 14110 on AI development. Additionally, it complements the DOE's upcoming Artificial Intelligence Strategy. Developed through a collaborative effort led by the Enterprise Data Management Program and the DOE's first Chief Data Officer, the strategy reflects input from stakeholders across the agency, ensuring its relevance to all mission areas, including National Laboratories, Field Sites, and Power Marketing Administrations.

The Enterprise Data Strategy helps organisations maximise the value of their data while ensuring that it is protected, compliant, and strategically aligned with broader organisational goals. It drives innovation, improves operational efficiency, and enhances security, making it an essential framework for modern organisations, especially those handling critical infrastructure and large-scale systems.

The Enterprise Data Strategy helps organisations maximise the value of their data while ensuring that it is protected, compliant, and strategically aligned with broader organisational goals.

Federal Agencies Propose Standardised Cybersecurity Workforce Requirements in Contracts

The Department of Defense (DoD), General Services Administration (GSA), and NASA have introduced a proposed amendment to the Federal Acquisition Regulation (FAR) to establish a uniform approach to cybersecurity workforce requirements in federal contracts. This initiative supports Executive Order 13870, which focuses on strengthening federal cybersecurity expertise and readiness. The proposal integrates the National Institute of Standards and Technology's (NIST) NICE Workforce Framework for Cybersecurity, which defines cybersecurity roles, skills, and responsibilities. Key elements include requiring agencies to incorporate the framework into acquisition planning, ensuring contractor compliance with cybersecurity competency standards, and refining procurement processes to align with evolving cybersecurity needs. Federal agencies will need to adjust their acquisition strategies to reflect these standards, while IT and cybersecurity contractors must update their policies to meet federal requirements. While the rule does not impose significant financial burdens, organisations must invest time in understanding and implementing the framework. Public comments are open until March 4, 2025. This initiative complements broader federal efforts to strengthen cybersecurity infrastructure and enhance national security.

The proposal integrates the National Institute of Standards and Technology's (NIST) NICE Workforce Framework for Cybersecurity, which defines cybersecurity roles, skills, and responsibilities.

Please refer page 35, 36 & 37 for reference.

ONCD Launched Cybersecurity Plan to Protect Energy Infrastructure

The office of the National Cyber Director (ONCD) has introduced the Energy Modernisation Cybersecurity Implementation Plan (EMCIP) to strengthen the security of U.S.A's energy infrastructure. As energy systems become more digitised, this plan provides a strategic approach to mitigating cyber risks in power generation, transmission, and distribution. The EMCIP details 32 key initiatives with assigned agencies and completion timelines to enhance energy sector cybersecurity. The Department of Energy is creating a unified cybersecurity framework for digital energy infrastructure, while the Cybersecurity and Infrastructure Security Agency will promote need for secure-by-design in OT in modern energy systems. A major aspect of the plan focuses on five critical energy technologies: battery storage, inverter controls, distributed control systems, building energy management systems, and electric vehicle supply equipment. Efforts include cybersecurity exercises for battery operators, guidelines for securing inverters, testing standards for distributed control software, and vulnerability assessments for building energy platforms. As energy technology advances, integrating cybersecurity from the start will be essential to ensuring grid stability, national security, and economic resilience.

A major aspect of the plan focuses on five critical energy technologies: battery storage, inverter controls, distributed control systems, building energy management systems, and electric vehicle supply equipment.

EU's DORA Cybersecurity Rules Take Effect, Many Financial Firms Lag in Compliance

The European Union's Digital Operational Resilience Act (DORA) has been enforced from January 17, 2025, requiring financial institutions to enhance cybersecurity, manage IT risks, and oversee third-party service providers. However, only 20% of firms are fully prepared, with smaller organisations and non-EU-based institutions facing significant compliance hurdles. DORA aims to strengthen the resilience of banks, investment firms, and crypto service providers by mandating strict cybersecurity measures, incident reporting, and risk management. Companies failing to comply could face penalties of up to 2% of annual revenue, along with operational and reputational risks. Challenges in meeting these requirements stem from fragmented vendor ecosystems, outdated IT systems, and limited resources, particularly for smaller firms. The short timeframe for compliance has added to the difficulties, as some regulations were only finalised in mid-2024. Experts recommend financial institutions assess compliance gaps, focus on critical risk areas, and document their approach to meeting regulatory standards. While enforcement remains unclear, firms are encouraged to create implementation strategies to demonstrate progress toward full compliance.

DORA aims to strengthen the resilience of banks, investment firms, and crypto service providers by mandating strict cybersecurity measures, incident reporting, and risk management.

Please refer page 35, 36 & 37 for reference.

Malaysia Proposed ASEAN Cybercrime Task Force for Stronger Regional Security

Malaysia has put forward a proposal for a regional cybercrime task force within ASEAN to enhance cybersecurity collaboration. As the current ASEAN chair, Malaysia aims to establish a system similar to Interpol, allowing member states to share intelligence and respond to growing cyber threats fuelled by AI, automation, and dark web activities. Malaysia's Deputy Prime Minister Ahmad Zahid Hamidi introduced the initiative at the Asia International Security Summit 2025, emphasising the importance of public-private partnerships and cooperation among governments, law enforcement, and technology firms. The proposal builds on Malaysia's role as the first regional coordinator for the ASEAN Regional CERT, which is supported by Singapore with a $10.1 million budget over ten years to improve incident response and cyber resilience. Additionally, ASEAN has collaborated with China on a law enforcement initiative to combat cybercrime. Malaysia is also advocating for blockchain-based identity verification to reduce fraud and enhance online security. These efforts underscore ASEAN's commitment to strengthening cybersecurity measures and intelligence-sharing across the region. This task force will help to improve intelligence-sharing networks and coordinate regional responses to cybercrime and other illicit activities.

The proposal builds on Malaysia's role as the first regional coordinator for the ASEAN Regional CERT, which is supported by Singapore with a $10.1 million budget over ten years to improve incident response and cyber resilience.

Canada Launched National Cyber Security Strategy to Strengthen Digital Defences

On February 6, Public Safety Minister, David McGuinty introduced Canada's National Cyber Security Strategy (NCSS) to protect individuals, businesses, and critical infrastructure from evolving cyber threats. The strategy focuses on public-private collaboration, stronger regulations, and proactive defence measures to modernise Canada's cybersecurity landscape.

The NCSS is built on three key pillars:

- Strengthening Cyber Defences: Establishing the Canadian Cyber Defence Collective (CCDC) for public-private partnerships, expanding cybersecurity awareness programs, and launching the Cybersecurity Attribution Data Centre (CADC) for AI-driven cyber research.
- Global Leadership in Cybersecurity: Advancing secure-by-design technologies, boosting cybersecurity talent, and enhancing research in post-quantum cryptography and AI security.
- Cyber Threat Detection & Prevention: Expanding cybercrime enforcement, mandating ISP botnet blocking, and

Establishing the Canadian Cyber Defence Collective (CCDC) for public-private partnerships, expanding cybersecurity awareness programs, and launching the Cybersecurity Attribution Data Centre (CADC) for AI-driven cyber research.

Please refer page 35, 36 & 37 for reference.

strengthening nation-state threat mitigation through intelligence agencies.

Experts praise the initiative but highlight challenges in execution, resource allocation, and leadership structure. If implemented effectively, NCSS could position Canada as a cybersecurity leader while bolstering national resilience against digital threats.

OpenSSF Released Security Baseline for Open Source Projects

Developed with input from OpenSSF and other organisations, the OSPS Baseline is a tiered security framework that evolves with a project's growth.

The Open Source Project Security Baseline (OSPS Baseline) initiative aims to improve the security of open-source projects by offering a set of best practices to reduce vulnerabilities and increase trust. Developed with input from OpenSSF and other organisations, the OSPS Baseline is a tiered security framework that evolves with a project's growth. It includes a checklist of tasks, processes, and configurations to guide developers in meeting security expectations. The baseline offers marketing benefits as well, as projects demonstrating strong security practices are more likely to gain users. All projects are encouraged to meet at least level 1, which sets a basic security standard, including requirements like multi-factor authentication (MFA), contribution policies, version control, and project documentation. Projects with a large user base should aim for level 3, which focuses on advanced aspects such as privilege management, release security, and comprehensive testing.

Trends

Quantum Computing's Impact on Cybersecurity and the Road Ahead

To defend against these threats, organisations must adopt quantum-resistant cryptography, such as lattice-based encryption, hash-based signatures, and Quantum Key Distribution (QKD).

Quantum computing offers both significant risks and opportunities for cybersecurity. On the offensive side, quantum advancements could break traditional encryption methods like RSA and ECC, enabling cybercriminals to decrypt stolen data, accelerate password cracking, and enhance AI-driven cyberattacks. Additionally, blockchain security, including cryptocurrencies and smart contracts, could be compromised due to quantum's impact on Elliptic Curve Cryptography (ECC). To defend against these threats, organisations must adopt quantum-resistant cryptography, such as lattice-based encryption, hash-based signatures, and Quantum Key Distribution (QKD). These technologies will help protect sensitive data and combat quantum-driven risks. Quantum-enhanced AI can also improve real-time threat detection, enabling faster identification and neutralisation of cyber threats. Quantum computing also presents implications for autonomous vehicles (AVs). AVs rely on real-time communication and large data processing, making them vulnerable to cyberattacks. Quantum-

*Please refer page 35, 36 & 37 for reference.

powered encryption can secure vehicle-to-vehicle and vehicle-to-infrastructure communications, preventing risks like GPS spoofing and data manipulation. Additionally, quantum-enhanced AI can boost threat detection for AVs, enhancing their overall security.

As quantum technology evolves, businesses must implement post-quantum cryptography, Zero-Trust Architecture, and quantum-resilient key management. Preparing for a quantum-driven future will require collaboration between industry professionals and regulators to secure digital infrastructures against emerging quantum threats.

Quantum-powered encryption can secure vehicle-to-vehicle and vehicle-to-infrastructure communications, preventing risks like GPS spoofing and data manipulation.

Malware Bytes

Malvertising Campaign Targets Google Ads Users

Cybersecurity researchers have uncovered a sophisticated malvertising campaign targeting Google Ads users. The attackers are using fraudulent advertisements to trick businesses and individuals into revealing their login credentials. This scheme involves impersonating Google Ads and redirecting victims to fake login pages designed to harvest sensitive information. The attack specifically targets users searching for "Google Ads" on Google's search engine. Clicking on the malicious ads leads them to fraudulent landing pages hosted on Google Sites. From there, victims are further redirected to phishing sites that capture their credentials and two-factor authentication (2FA) codes using WebSocket connections. This stolen data is then transmitted to a remote server controlled by the attackers. By compromising legitimate Google Ads accounts, the threat actors expand their attack, using the hijacked accounts to run more fraudulent ads and lure additional victims into the scheme. To mitigate risks, users should be cautious when clicking on ads, verify URLs before entering login details, and enable security features such as hardware-based authentication keys.

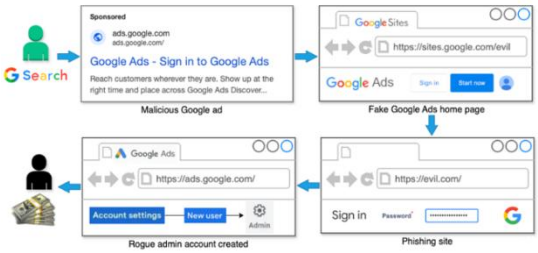


Figure: Working of the Malware

Sneaky 2FA: AitM Phishing Kit

Cybersecurity researchers have identified an Adversary-in-the-Middle (AitM) phishing kit, dubbed Sneaky 2FA, designed to compromise Microsoft 365 accounts. This malicious toolkit is capable of intercepting login credentials and two-factor authentication (2FA) codes, enabling attackers to bypass security measures and gain unauthorised access. Sneaky 2FA employs deceptive authentication pages that automatically fill in victims' email addresses, making them appear more legitimate and increasing the likelihood of successful phishing attempts. Additionally, the kit integrates multiple anti-analysis and anti-bot

Sneaky 2FA employs deceptive authentication pages that automatically fill in victims' email addresses, making them appear more legitimate and increasing the likelihood of successful phishing attempts.

Please refer page 35, 36 & 37 for reference.

techniques to evade detection. It uses traffic filtering and Cloudflare Turnstile challenges to ensure only targeted users reach the credential-harvesting page, effectively blocking automated security scans and researchers attempting to analyse the threat. Further strengthening its defences, the phishing kit executes browser-based checks to detect developer tools and prevent in-depth security analysis. To mitigate risks, users should remain cautious of unexpected login prompts, enable phishing-resistant authentication methods like hardware security keys, and regularly monitor account activity for suspicious access attempts.

Fake CAPTCHA Campaign Spreads Lumma Stealer

Once executed, the HTA file runs a PowerShell command that triggers the next stage of the attack: a PowerShell script. This script unpacks another PowerShell script designed to decode and load the Lumma payload.

A malware campaign was spread by Lumma information stealer through fake CAPTCHA verification pages. Researchers have warned that this attack chain begins when a user visits a compromised website, which then redirects them to a fraudulent CAPTCHA page. The page instructs the victim to copy and paste a command into the Windows Run prompt. This command uses the mshta.exe binary to download and execute an HTA file from a remote server. Once executed, the HTML Application (HTA) file runs a PowerShell command that triggers the next stage of the attack a PowerShell script. This script unpacks another PowerShell script designed to decode and load the Lumma payload. To avoid detection, the malware takes additional steps to bypass the Windows AntiMalware Scan Interface (AMSI), a security feature aimed at detecting malicious activities. The Lumma stealer then operates in the background, quietly stealing sensitive information from the compromised system.

Custom Backdoor Exploited Magic Packet Vulnerability in Juniper Routers

The attack begins when a specially crafted "magic packet" is sent to the targeted device. Upon receiving this packet, the affected router's agent sends a secondary challenge before establishing a reverse shell connection.

Juniper Networks' enterprise-grade routers were targeted by a sophisticated malware campaign known as J-magic. This campaign is particularly notable because it marks one of the rare instances of malware specifically designed for Junos OS, which runs on a variant of FreeBSD and serves the enterprise market. The attack begins when a specially crafted "magic packet" is sent to the targeted device. Upon receiving this packet, the affected router's agent sends a secondary challenge before establishing a reverse shell connection. This shell is directed to the IP address and port specified within the magic packet, allowing attackers to gain full control over the compromised device. Once the reverse shell is active, the attackers can perform various malicious actions, such as stealing sensitive data, compromising device functionality, or deploying additional payloads to further their objectives.

*Please refer page 35, 36 & 37 for reference.

ForceCopy Malware Used to Steal Browser-Stored Credentials

Hacker group known as Kimsuky has been observed conducting spear-phishing attacks to deliver an information stealer malware named forceCopy. These targeted attacks typically begin with phishing emails that contain a Windows shortcut (LNK) file, which is cleverly disguised as a legitimate Microsoft Office or PDF document. Upon opening the attachment, the LNK file triggers the execution of either PowerShell or mshta.exe, both of which are legitimate Microsoft binaries. PowerShell is a task automation framework, while mshta.exe is used to run HTML Application (HTA) files. The execution of these binaries leads to the download and execution of additional malicious payloads from an external source. This multi-stage process ultimately allows Kimsuky to establish a foothold on the victim's system, enabling the theft of sensitive information.

Upon opening the attachment, the LNK file triggers the execution of either PowerShell or mshta.exe, both of which are legitimate Microsoft binaries.

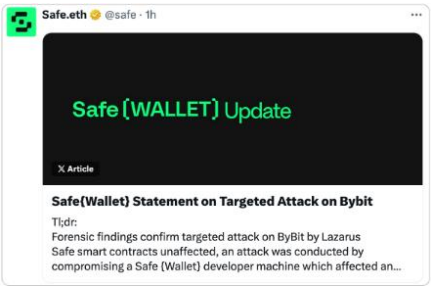
Attackers Used Exposed ASP.NET Keys to Deploy Malware

Microsoft has warned about a threat where attackers exploit static ASP.NET machine keys, which are often found online, to carry out ViewState code injection attacks. These attacks leverage keys such as the validationKey and decryptionKey, which are meant to protect ViewState data from tampering and disclosure. Researchers at Microsoft Threat Intelligence have uncovered that some developers mistakenly use these keys, often exposed on code documentation and repository platforms, in their applications. Cybercriminals exploit this by injecting malicious ViewState data, which is utilised by ASP.NET Web Forms to manage the state of web pages. The attackers craft their ViewStates with a manipulated message authentication code, and when these are sent via POST requests to the target server, the ASP.NET Runtime decrypts and validates them using the correct keys. As a result, the malicious ViewState is processed, allowing attackers to execute arbitrary code on the server, leading to remote code execution (RCE). This enables them to deploy additional malicious payloads, compromising the affected IIS web servers.

Researchers at Microsoft Threat Intelligence have uncovered that some developers mistakenly use these keys, often exposed on code documentation and repository platforms, in their applications.

Bybit Breached: Safe{Wallet} Compromised in Cyberattack

Hackers stole 1.5 billion dollars from Bybit after hacking a developer's device at the multisig wallet platform named Safe{Wallet}. The breach of Bybit's Safe{Wallet} service occurred due to a combination of vulnerabilities in both its infrastructure and security protocols. Early investigations suggested that the attackers leveraged an exploit in the wallet's API endpoints, which allowed unauthorised access to sensitive user data and funds. The exploit began with a targeted SQL injection attack, enabling the attackers to bypass authentication mechanisms. This



Please refer page 35, 36 & 37 for reference.

The breach of Bybit's Safe{Wallet} service occurred due to a combination of vulnerabilities in both its infrastructure and security protocols.

gave them the ability to execute arbitrary queries on the Safe{Wallet} backend. Once inside the system, the attackers gained access to the wallet's private keys, which were poorly secured and stored in plaintext in a local database. With these keys, the attackers could initiate unauthorised transactions, siphoning off funds. Moreover, Bybit's use of outdated encryption algorithms in certain parts of the communication between the wallet service and the blockchain also contributed to the breach. The attackers exploited weak cipher suites, allowing them to decrypt certain communication streams and extract sensitive information.

CISA & FBI Warn of Ghost Ransomware Attacks Across 70 Countries

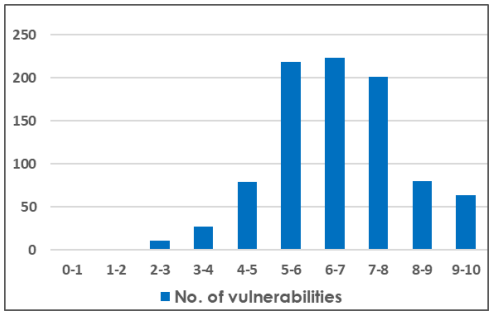
Ghost ransomware actors, a sophisticated group of cybercriminals, have been leveraging public-facing vulnerabilities to gain unauthorised access to networks.

Ghost ransomware actors, a sophisticated group of cybercriminals, have been leveraging public-facing vulnerabilities to gain unauthorised access to networks. Exploiting critical CVEs in widely used systems like Fortinet FortiOS, Microsoft Exchange, and Adobe ColdFusion, they execute advanced attacks with alarming efficiency. Once inside, they deploy web shells and use tools like Cobalt Strike to escalate privileges and execute malicious commands. These actors often bypass defences by disabling security software like Windows Defender and employ techniques such as credential dumping and lateral movement to expand their reach within compromised networks. Their ransomware, including variants like Ghost.exe and Locker.exe, encrypts files and demands ransom, often threatening to sell exfiltrated data if demands aren't met. Despite claims of data theft, their exfiltration efforts are typically limited. The FBI and other agencies have noted Ghost's reliance on tools like Cobalt Strike and encrypted communication methods, including secure email services, to command and control their operations. For organisations, staying vigilant against these advanced persistent threats is crucial to reducing the risk of compromise. NCIIPC has already released alert via advisory: TA-RAN-2025-02-21-008 dated: 21-Feb-2025.

Vulnerability Watch

Quarterly Vulnerability Analysis Report

Alert & Advisory Group, NCIIPC



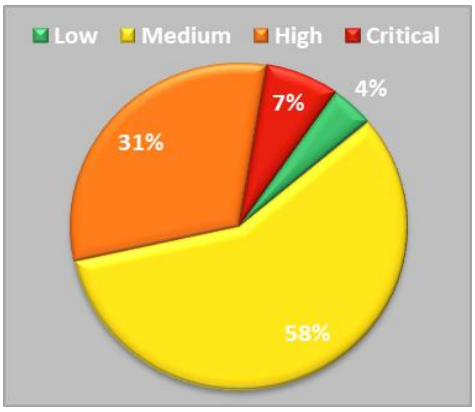
Severity-wise number of vulnerabilities

The cyber security trends have suggested surge in critical vulnerabilities & exploits in the quarter impacting widely used software and cloud services. During the period, a total of 3372 vulnerabilities have been observed. More than 50 percent of total vulnerabilities reported were of Critical & high severity. Linux, Apple, Microsoft, Adobe and Google were the top five vendors having 36% of total reported vulnerabilities. The CVEs have various

Please refer page 35, 36 & 37 for reference.

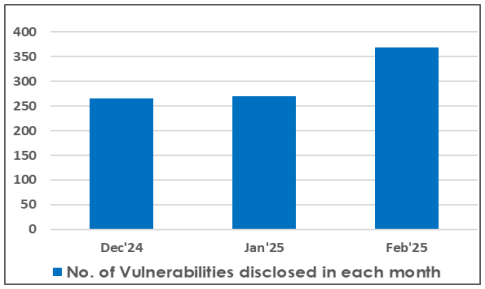
impact for organisations in critical sectors and require vigilance by relevant SOC/IT teams for patch management & cybersecurity measures.

Severity	CVSS v3 Score	Number of Vulnerabilities			Total Vulnerabilities	Severity Total
		Dec'24	Jan'25	Feb'25		
Critical	10-9	19	15	30	64	64
High	9-8	17	10	53	80	281
	8-7	59	64	78	201	
Medium	7-6	36	83	104	223	521
	6-5	102	64	53	219	
	5-4	15	24	40	79	
Low	4-3	16	7	4	27	38
	3-2	2	3	6	11	
	2-1	0	0	0	0	
	1-0	0	0	0	0	
Total		266	270	368		904

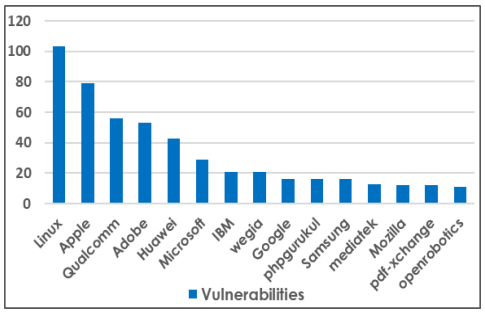


Severity-wise share of vulnerabilities

S. No.	Vendor	No. of Vulnerabilities			Total
		Dec'24	Jan'25	Feb'25	
1.	Linux	35	57	11	103
2.	Apple	35	43	1	79
3.	Qualcomm	13	19	24	56
4.	Adobe	48	0	5	53
5.	Huawei	15	28	0	43
6.	Microsoft	4	3	22	29
7.	IBM	10	2	9	21
8.	wegia	0	0	21	21
9.	Google	2	4	10	16
10.	phpgurukul	4	0	12	16
11.	Samsung	0	0	16	16
12.	mediatek	0	0	13	13
13.	Mozilla	0	0	12	12
14.	pdf-xchange	0	0	12	12
15.	openrobotics	11	0	0	11



No. of vulnerabilities disclosed in each month



Count of vulnerabilities for top 15 vendors

Critical Vulnerabilities in Cisco Identity Services Engine

An Insecure Java Deserialisation vulnerability was discovered in Cisco's Identity Services Engine (ISE), a network security policy management platform. An attacker with valid read-only administrative credentials can exploit this vulnerability by sending a crafted serialised Java object to an affected API, leading to the execution of arbitrary commands with root privileges. This vulnerability has CVE ID CVE-2025-20124 with CVSS score 9.9.

Another Authorisation Bypass vulnerability was discovered in Cisco's ISE. An authenticated, remote attacker with read-only administrative credentials can exploit this vulnerability by sending

Please refer page 35, 36 & 37 for reference.

The critical vulnerabilities have CVE ID: CVE-2025-20124 with CVSS score 9.9 and CVE ID: CVE-2025-20125 with CVSS score 9.1

a crafted HTTP request to the affected API. This vulnerability has CVE ID CVE-2025-20125 with CVSS score 9.1.

The affected versions are Cisco ISE 3.0 to 3.3. The security updates to address these vulnerabilities have been released by Cisco.

NCIIPC has already alert via advisory: VA-2025-02-06-002 dated: 06-Feb-2025.

simplehelp

CVE ID: CVE-2024-57726 with CVSS score 9.9.

Critical Vulnerability in SimpleHelp

A critical vulnerability has been identified in SimpleHelp's remote monitoring and management software versions 5.5.7 and earlier. SimpleHelp is a software for professional support teams to help customers and fix computers from anywhere. This vulnerability allows low-privileges technicians to create API keys with excessive permissions, enabling them to escalate their privileges to the server admin role. The vulnerability has CVE ID CVE-2024-57726 with CVSS score 9.9. To mitigate this threat, users are recommended to update their SimpleHelp software to the latest version.

NCIIPC has already alert via advisory: VA-2025-02-03-001 dated: 03-Feb-2025.

The vulnerability affected FortiOS versions 7.0.0 through 7.0.16, as well as FortiProxy versions 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12. CVE ID: CVE-2024-55591 and CVSS score 9.6

Fortinet Zero-day Vulnerability Exploitation

A critical authentication bypass vulnerability affected Fortinet's FortiOS and FortiProxy products. This flaw, having CVE ID CVE-2024-55591 and CVSS score 9.6, allows remote attackers to gain super-admin privileges by sending specially crafted requests to the Node.js WebSocket module, potentially compromising the security of affected systems. The vulnerability affected FortiOS versions 7.0.0 through 7.0.16, as well as FortiProxy versions 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12. Fortinet later released patches addressing this critical issue.

NCIIPC has already alert via advisory: VA-2025-01-17-008 dated: 17-Jan-2025.

This vulnerability leads to SQL Injection and has CVE ID CVE-2024-13152 and CVSS score 10.

Critical Vulnerability in BSS Mobuy Online Machinery Monitoring Panel

An authorisation bypass vulnerability has been discovered in BSS Mobuy Online Machinery Monitoring Panel, a software solution designed to monitor and manage machinery and equipment in industrial or commercial settings. This vulnerability leads to SQL Injection and has CVE ID CVE-2024-13152 and CVSS score 10. The affected versions are Mobuy Online Machinery Monitoring Panel: before 2.0. Users are recommended to upgrade the application to at least version 2.0.

Please refer page 35, 36 & 37 for reference.

Critical Vulnerabilities in Wavlink AC3000 Wireless Router

Multiple OS command injection vulnerabilities have been discovered in Wavlink AC3000 wireless router, a tri band gigabit router. These vulnerabilities exists within its login.cgi's set_sys_init() function. The affected version is Wavlink AC3000 M33A8.V5030.210505. These vulnerabilities allow unauthenticated remote attackers to execute arbitrary commands on the device. The assigned CVE IDs are CVE-2024-39759, CVE-2024-39761, and CVE-2024-39760 with CVSS score 10.

These vulnerabilities allow unauthenticated remote attackers to execute arbitrary commands on the device. The assigned CVE IDs are CVE-2024-39759, CVE-2024-39761, and CVE-2024-39760 with CVSS score 10.

Critical Vulnerability in Dynamics 365 Integration Plugin for WordPress

Remote Code Execution and Arbitrary File Read vulnerability was discovered in Dynamics 365 Integration plugin for WordPress. This security flaw arises from inadequate input validation and sanitisation within the plugin's render function, leading to a Twig Server-Side Template Injection vulnerability. The assigned CVE ID is CVE-2024-12583 having CVSS score 9.9. The affected versions are Dynamics 365 Integration plugin, all versions up to, and including, 1.3.23. Users are advised to update to version 1.3.24, or a newer patched version.

Remote Code Execution and Arbitrary File Read vulnerability was discovered in Dynamics 365 Integration plugin for WordPress. The assigned CVE ID is CVE-2024-12583 having CVSS score 9.9.

Critical Vulnerability in Arne Informatics Piramit Automation

SQL Injection vulnerability was discovered in Arne Informatics Piramit Automation. This vulnerability arises from improper neutralization of special elements used in SQL commands, enabling attackers to execute blind SQL injection attacks. The assigned CVE ID is CVE-2024-8950 with CVSS score 9.9. The affected versions are Piramit Automation before 27.09.2024.

The assigned CVE ID is CVE-2024-8950 with CVSS score 9.9.

Critical Vulnerabilities in Atlassian

Atlassian has recently addressed multiple Remote Code Execution (RCE) vulnerabilities in its Confluence Data Center and Server products. These vulnerabilities were found in third-party dependencies, Apache Tomcat. The RCE vulnerabilities CVE-2024-50379 and CVE-2024-56337, both were assigned a CVSS score of 9.8, could allow unauthenticated attackers to execute remote code, posing significant security risks. Atlassian has released updates for Confluence Data Center and Server to mitigate these vulnerabilities.

NCIIPC has already alert for CVE ID: CVE-2024-56337 via advisory: VA-2025-01-23-010 dated: 23-Jan-2025.

The RCE vulnerabilities CVE-2024-50379 and CVE-2024-56337, both were assigned a CVSS score of 9.8.

Please refer page 35, 36 & 37 for reference.

Ivanti has released patches addressing these vulnerabilities. CVE-2024-38657 (CVSS score: 9.1), CVE-2025-22467 (CVSS score: 9.9), CVE-2024-10644 (CVSS score: 9.1), and CVE-2024-47908 (CVSS score: 9.1)

Critical Vulnerabilities in Ivanti

Ivanti has addressed critical vulnerabilities in its Connect Secure (ICS) and Policy Secure (IPS) products. The key vulnerabilities and their Impact are mentioned below:

CVE-2024-38657 (CVSS score: 9.1): The external control of a file name in Ivanti Policy Secure before version 22.7R1.3 and Ivanti Connect Secure before version 22.7R2.4 allows a remote authenticated attacker with admin privileges to write arbitrary files.

CVE-2025-22467 (CVSS score: 9.9): A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6 allows a remote authenticated attacker to achieve remote code execution.

CVE-2024-10644 (CVSS score: 9.1): Code injection in Ivanti Connect Secure before version 22.7R2.4 and Ivanti Policy Secure before version 22.7R1.3 allows a remote authenticated attacker with admin privileges to achieve remote code execution.

CVE-2024-47908 (CVSS score: 9.1): OS command injection in the admin web console of Ivanti CSA before version 5.0.5 allows a remote authenticated attacker with admin privileges to achieve remote code execution.

Ivanti has released patches addressing these vulnerabilities.

By exploiting these flaws, an attacker could potentially install malicious firmware, maintain persistence across reboots, and evade traditional security mechanisms.

PANdora's Box Vulnerabilities in Palo Alto Networks Firewalls

Security researchers have discovered a set of critical vulnerabilities, collectively known as "PANdora's Box," affecting specific Palo Alto Networks firewall models, including PA-3260, PA-1410, and PA-415. These vulnerabilities primarily involve Secure Boot bypass techniques that could allow attackers to gain persistent control over the affected devices. Among the key vulnerabilities are BootHole and PixieFail, which target the Secure Boot process and firmware integrity. By exploiting these flaws, an attacker could potentially install malicious firmware, maintain persistence across reboots, and evade traditional security mechanisms.

Learning

Revolutionising Financial Crime Prevention: The Role of ISO 20022 in Enhancing Security, Efficiency, and Transparency

In today's rapidly evolving financial landscape, the battle against financial crimes such as fraud, money laundering, and terrorist financing has become more complex. With global fraud losses reaching a staggering 485.6 billion dollars in 2024 as per reports published in open source, financial institutions are under constant pressure to strengthen their defences against increasingly sophisticated criminal schemes. One of the most promising

Please refer page 35, 36 & 37 for reference.

solutions to this challenge is the adoption of ISO 20022, a new global messaging standard that is set to revolutionise financial crime prevention. By providing more structured and detailed transaction data, ISO 20022 offers enhanced capabilities for detecting and mitigating fraud, streamlining compliance and improving operational efficiency across the financial sector. ISO 20022 offer the financial sector a unified platform for transmitting payment messages and exchanging payment information. This platform utilises a common vocabulary, a standardised modelling approach for executing transactions and incorporates various protocols, including Extensible Markup Language (XML) and Abstract Syntax Notation (ASN.1).

Financial institutions adopting ISO 20022 will be able to automate processes, improve compliance monitoring and streamline operational workflows.

The data-driven insights provided by ISO 20022 are poised to create a more secure, efficient and transparent financial ecosystem. Financial institutions adopting ISO 20022 will be able to automate processes, improve compliance monitoring and streamline operational workflows. ISO 20022's detailed transaction data offers crucial advantages in detecting and preventing financial crimes. Traditional messaging systems often lack the level of detail required to properly assess transaction risk. However, the new standard allows financial institutions to collect and process more comprehensive data, which can be analysed to identify suspicious patterns and behaviours more accurately. For example, ISO 20022 includes information like the origin and destination of funds, the purpose of the transaction and more precise transaction descriptors. This data richness makes it easier to detect potential financial crimes, reduce false positives, mitigate financial crimes like money laundering and fraud more effectively.

The transition to ISO 20022 also facilitates greater interoperability between financial institutions globally, making cross-border transactions more secure and transparent.

ISO 20022 provides the ability to support enhanced sanctions screening and fraud prevention. With more granular data, institutions can more effectively monitor transactions for potential violations of sanctions or regulatory requirements, minimising the risk of non-compliance and financial crime. The transition to ISO 20022 also facilitates greater interoperability between financial institutions globally, making cross-border transactions more secure and transparent. Another key benefit is that ISO 20022 allows for the optimisation of customer onboarding and monitoring. Financial institutions can leverage the enhanced data to assess customer risk profiles with greater accuracy, helping to identify high-risk individuals and entities more efficiently.

The adoption of ISO 20022 will create a more resilient, transparent and secure financial ecosystem that is better equipped to combat evolving financial crimes in the digital age.

Securing Critical Infrastructure: Strengthening Cybersecurity in the Oil and Gas Industry

The oil and gas industry is a cornerstone of the global economy, driving energy production and fuelling essential infrastructure. However, as the sector increasingly integrates digital technologies

Please refer page 35, 36 & 37 for reference.

to enhance operational efficiency, it also faces a growing number of cybersecurity threats. From ransomware attacks to IoT vulnerabilities, the rise in cyberattacks targeting critical infrastructure is a significant concern.

Employees or contractors with access to critical systems and data can intentionally or unintentionally cause harm, including leaking sensitive information or facilitating security breaches.

key threats to the oil and gas industry:
Ransomware Attacks: cybercriminals encrypt critical data or systems, demanding ransom in exchange for restoring access.
Phishing Scams: attackers trick employees into revealing sensitive information, such as login credentials, by impersonating legitimate entities.
IoT Vulnerabilities: The increasing use of Internet of Things (IoT) devices in the industry opens the door for cybercriminals to exploit weaknesses in connected systems, potentially compromising operations or gaining unauthorised control.
Physical Sabotage: Apart from cyber threats, physical sabotage to infrastructure, such as pipelines, rigs, or storage facilities, remains a significant risk.
Insider Threats: Employees or contractors with access to critical systems and data can intentionally or unintentionally cause harm, including leaking sensitive information or facilitating security breaches.
Strategies for strengthening cybersecurity in the oil and gas industry:
Regular Software Updates and Patch Management: continuously update and patch systems, software, and hardware to close security vulnerabilities and prevent exploitation by cybercriminals.
Multi-Factor Authentication (MFA): implement MFA across all systems to add an extra layer of protection, ensuring that unauthorised users cannot gain access even with stolen credentials.

Use predictive maintenance tools powered by IoT devices to monitor systems for potential failures, while securing connected devices to prevent cyberattacks targeting vulnerabilities.

Employee Training and Awareness: Educate employees on cybersecurity best practices, including how to identify phishing attempts, the importance of strong passwords, and safe internet usage.
Predictive Maintenance and IoT Security: Use predictive maintenance tools powered by IoT devices to monitor systems for potential failures, while securing connected devices to prevent cyberattacks targeting vulnerabilities.
Network Segmentation: divide critical networks into isolated segments to limit the spread of attacks. In case of a breach, this helps to contain the damage and prevent unauthorised access to sensitive systems.
Incident Response Plan: Develop and regularly test a comprehensive incident response plan to ensure rapid and effective action in the event of a cyberattack or data breach.
Advanced Threat Detection and AI: deploy artificial intelligence (AI) and machine learning to analyse data and detect anomalies, improving the ability to identify and respond to threats in real time.

*Please refer page 35, 36 & 37 for reference.

Regulatory Compliance: Stay up to date with evolving cybersecurity regulations and industry standards to ensure compliance and avoid potential penalties.
Zero Trust Security Model: Adopt a Zero Trust model, where no user or device is trusted by default, even if they are inside the network. This limits the risk of internal threats and minimises the damage from a breach.
Encryption and Data Protection: Encrypt sensitive data both in transit and at rest to protect it from unauthorised access, ensuring that even if data is stolen, it remains unreadable.
These strategies, when implemented together, form a comprehensive defence against the rising cybersecurity threats targeting the oil and gas sector.

Adopt a Zero Trust model, where no user or device is trusted by default, even if they are inside the network.

Understanding Phishing Attacks: The Rising Threat of Browser-in-the-Browser

Alert & Advisory Group, NCIIPC

In recent years, phishing attacks have emerged as one of the most common and destructive types of cybercrime. These attacks are designed to deceive individuals into divulging sensitive information, such as login credentials, credit card details or other personal data. While phishing attacks come in many forms, one of the most sophisticated and dangerous variations is the Browser-in-the-Browser (BitB) attack.

In recent years, phishing attacks have emerged as one of the most common and destructive types of cybercrime.

Phishing attacks generally rely on social engineering tactics to trick individuals into believing they are interacting with a legitimate entity. Attackers often pose as well-known brands or services, such as banks, government entities or email providers to build trust. The most common phishing methods involve fake emails, messages/emails or websites that ask users to enter their personal information. The information gathered is then used for malicious purposes, such as identity theft or unauthorised access to online accounts.
However, as cybercriminals have grown more sophisticated, phishing attacks have evolved. One of the most recent and advanced techniques in phishing is the BitB attack. Unlike traditional phishing attacks, which often redirect victims to fake websites that impersonate legitimate ones, BitB attacks occur directly within the browser window, making them harder to detect and more convincing.
In a Browser-in-the-Browser attack, the attacker creates a fake login interface that appears to be a legitimate browser window, such as the Google or PayPal login page. This window is not an external pop-up or redirection but is embedded within the malicious website itself using an iframe—an HTML element that allows one webpage to embed another. The attacker takes advantage of the way browsers render pages, creating a seamless look-alike browser window that features the same layout, address

In a Browser-in-the-Browser attack, the attacker creates a fake login interface that appears to be a legitimate browser window, such as the Google or PayPal login page.

*Please refer page 35, 36 & 37 for reference.

bar, and even the HTTPS padlock symbol that users associate with security.

Once the fake login page is displayed inside the browser window, the victim is prompted to enter their login credentials. The victim believes they are logging into a trusted service, but the attacker is actually capturing the sensitive data and can use it to access the victim's accounts. This technique is effective because it appears completely legitimate, using the familiar look and feel of a real browser interface. It bypasses traditional phishing defences, such as URL inspection and user skepticism about pop-ups.

The reason Browser-in-the-Browser attacks are so effective is that they exploit the trust users place in their browser's appearance and the common indicators of security like the HTTPS padlock icon.

The reason Browser-in-the-Browser attacks are so effective is that they exploit the trust users place in their browser's appearance and the common indicators of security like the HTTPS padlock icon. Most users assume that if a website looks like the real thing and has a secure connection, they are safe to enter their credentials. The fact that the attacker has embedded a fake browser window within a legitimate-looking webpage only makes it harder to detect. The victim may not even realise they have been duped until it's too late.

While BitB attacks are a form of phishing, they represent a more advanced and deceptive evolution of the tactic. In traditional phishing, attackers often rely on sending users to a fake website where they enter their information. These attacks are often easier to detect because the website's URL is suspicious or the layout of the page may not match the genuine service's appearance. BitB attacks bypass these issues by simulating an actual browser window, leading users to believe they are interacting with a trusted service.

If the URL doesn't match the domain name of the service being imitated, users should avoid entering any personal information.

- To protect themselves from phishing and BitB attacks, users must be vigilant and follow several security best practices. Users should always check the website's URL carefully. Even though a BitB attack may display what looks like a legitimate website URL, attackers can still spoof these details. If the URL doesn't match the domain name of the service being imitated, users should avoid entering any personal information. Additionally, users should be cautious of websites that ask for login credentials without a clear reason, especially if they are not directly related to the site being accessed.
- Another important security measure is multi-factor authentication (MFA). Even if attackers manage to steal a user's login credentials, MFA can prevent unauthorised access by requiring a second form of verification. This added layer of security significantly reduces the chances of a successful phishing attack.
- Users should also be cautious about entering credentials manually. Instead, they should use password managers, which can help ensure that they are entering their credentials only on legitimate websites. Password managers automatically fill in login forms for trusted sites and can alert users if they attempt to log into a site that doesn't match their stored login information.

Please refer page 35, 36 & 37 for reference.

- For organisations, educating employees about phishing risks is crucial. Many attacks succeed because victims are unaware of the tactics used by cybercriminals. Organisations should train employees to recognise suspicious activity, such as unexpected requests for login information or URLs that seem unusual. Regular security awareness training can reduce the risk of successful phishing attacks within a company.
- Organisations should implement security measures like email filtering to block phishing emails before they reach users. This can help reduce the number of phishing attempts employees are exposed to. Furthermore, adopting strong web filtering solutions that block access to known phishing sites can provide an additional layer of defence.
- Finally, keeping software up to date is essential. Browsers, operating systems and security tools regularly release updates to patch vulnerabilities that attackers could exploit. By ensuring that software is kept current, users and organisations can close off potential entry points for phishing and other types of cyberattacks.

Organisations should implement security measures like email filtering to block phishing emails before they reach users. This can help reduce the number of phishing attempts employees are exposed to.

In conclusion, phishing attacks remain a significant threat to online security and sophisticated variations like Browser-in-the-Browser attacks are making these scams even harder to detect. These advanced phishing techniques exploit users' trust in their browsers and make it difficult to distinguish between a legitimate website and a malicious one. However, by following security best practices—such as verifying URLs, using multi-factor authentication, employing password managers, and staying educated—users and organisations can significantly reduce their risk of falling victim to phishing attacks. Cybersecurity is a shared responsibility, and staying vigilant against phishing scams is a crucial step in protecting sensitive data in today's digital landscape.

Understanding DNSSEC: Enhancing the Security of the Domain Name System

Alert & Advisory Group, NCIIPC

The Domain Name System (DNS) serves as the internet's directory, translating domain names into IP addresses. However, the original design of DNS lacked security features, making it vulnerable to various attacks, such as cache poisoning and man-in-the-middle (MITM) attacks. To address these concerns, the Internet Engineering Task Force (IETF) developed Domain Name System Security Extensions (DNSSEC), a suite of protocols that enhance DNS security by ensuring data authenticity and integrity. DNSSEC is an enhancement to DNS that protects users from receiving forged DNS responses. It achieves this through cryptographic signatures that verify the legitimacy of DNS data. By implementing DNSSEC, organisations and internet users can trust that the responses they

DNSSEC is an enhancement to DNS that protects users from receiving forged DNS responses. It achieves this through cryptographic signatures that verify the legitimacy of DNS data.

Please refer page 35, 36 & 37 for reference.

receive have not been altered or tampered with by unauthorised entities.

Each level in the DNS hierarchy signs its own records and provides authentication through DS records.

How DNSSEC Works: DNSSEC employs public key cryptography to digitally sign DNS records, ensuring their authenticity. The main components of DNSSEC include:

- Key Pair System
  - DNSSEC uses asymmetric encryption, consisting of a private key and a public key.
  - The private key signs DNS records, while the public key, published in DNS, allows verification of signatures.
- New DNS Resource Records
  - DNSSEC introduces additional resource records to support its security functions:
  - RRSIG (Resource Record Signature): Stores digital signatures for DNS records.
  - DNSKEY (DNS Key Record): Holds the public key used for signature verification.
  - DS (Delegation Signer Record): Establishes a link between a child zone's DNSKEY and its parent zone.
  - NSEC (Next Secure Record) and NSEC3: Prevent attackers from forging non-existent domain responses by providing authenticated denial of existence.
- Trust Chain
  - DNSSEC follows a hierarchical structure, beginning from the root zone and extending to lower levels.
  - Each level in the DNS hierarchy signs its own records and provides authentication through DS records.
  - Trust is established by validating signatures from authoritative sources.

Cache poisoning manipulates DNS resolver caches with incorrect responses. DNSSEC prevents this by ensuring all responses are digitally signed and verified.

Advantages of DNSSEC

- Prevention of Cache Poisoning: Cache poisoning manipulates DNS resolver caches with incorrect responses. DNSSEC prevents this by ensuring all responses are digitally signed and verified.
- Data Integrity Assurance: DNSSEC ensures that data retrieved from DNS remains unaltered during transmission.
- Authenticated DNS Responses: By verifying digital signatures, DNSSEC ensures that responses originate from legitimate DNS servers.
- Protection Against MITM Attacks: DNSSEC prevents attackers from intercepting and modifying DNS queries and responses.

Challenges of Implementing DNSSEC

Despite its advantages, DNSSEC implementation presents several challenges:

- Implementation Complexity: Proper configuration and maintenance of DNSSEC require expertise, making adoption difficult for some organisations.
- Increased Response Size and Latency: The addition of cryptographic signatures increases DNS response sizes,

*Please refer page 35, 36 & 37 for reference.

potentially leading to latency issues and packet fragmentation.

- Slow Adoption Rate: Many internet service providers and organisations have yet to implement DNSSEC, limiting its effectiveness as a security solution.
- Key Management Requirements: Regular key rollovers are necessary to maintain security, but poor management can cause disruptions.
- No Encryption for Privacy: While DNSSEC verifies integrity and authenticity, it does not encrypt queries, leaving user privacy exposed.

While DNSSEC verifies integrity and authenticity, it does not encrypt queries, leaving user privacy exposed.

Steps for Deploying DNSSEC

To implement DNSSEC, organisations should follow these steps:

- Generate Cryptographic Key Pairs
  - Create a Zone Signing Key (ZSK) for signing DNS records and a Key Signing Key (KSK) for signing DNSKEY records.
- Sign the DNS Zone
  - Use the private ZSK to sign DNS records, creating RRSIG records.
  - Publish the corresponding public DNSKEY in the DNS.
- Publish the DS Record
  - Submit the DS record to the parent domain (such as a TLD registrar) to establish the trust chain.
- Enable Validation on Resolvers
  - Configure DNS resolvers to validate DNSSEC-signed responses.
  - Use DNSSEC-aware resolvers like BIND, Unbound, or Google Public DNS.
- Implement Key Rollover Procedures
  - Periodically update ZSK and KSK to enhance security and prevent unauthorized use.
- Test and Monitor
  - Use tools such as dnsviz.net, Verisign DNSSEC Debugger, or Google's Public DNSSEC Test to verify DNSSEC configuration and functionality.

Create a Zone Signing Key (ZSK) for signing DNS records and a Key Signing Key (KSK) for signing DNSKEY records.

The Future of DNSSEC: As cyber threats continue to evolve, the importance of DNSSEC grows. However, its effectiveness depends on wider adoption and integration with additional security protocols. The future of DNSSEC may involve:

- Automated Key Management: Enhancing automation to simplify key rollovers and reduce human errors.
- Integration with Other Security Measures: Combining DNSSEC with Transport Layer Security (TLS) and DNS-over-HTTPS (DoH) for a comprehensive security approach.
- Improved Support for Validating Resolvers: Encouraging ISPs and organisations to deploy DNSSEC-validating resolvers to increase security for end users.

DNSSEC provides a crucial layer of security for the Domain Name System, ensuring data integrity and authenticity while protecting against common DNS-based attacks.

DNSSEC provides a crucial layer of security for the Domain Name System, ensuring data integrity and authenticity while protecting against common DNS-based attacks. Though it presents implementation challenges, organisations that prioritise

Please refer page 35, 36 & 37 for reference.

cybersecurity should consider adopting DNSSEC to safeguard their domain infrastructure. As adoption increases and technology evolves, DNSSEC will remain a foundational security measure for the internet.

News Snippets - National

Tata Technologies Hit by Ransomware Attack

Tata Technologies, an Indian tech firm and subsidiary of Tata Motors, has been impacted by a ransomware attack, temporarily suspending some of its IT services.

Tata Technologies, an Indian tech firm and subsidiary of Tata Motors, has been impacted by a ransomware attack, temporarily suspending some of its IT services. The company, which specialises in automotive design, aerospace engineering and R&D, employs over 11,000 people globally. The attack, which affected a few of the company's IT assets, led to the suspension of certain services as a precautionary measure. However, Tata Technologies assured clients that its delivery services remained fully operational and there was no disruption to customer operations. In an official statement to India's national stock exchange, Tata Technologies confirmed that IT assets have been restored and a thorough investigation is underway with cybersecurity experts. While the company is working to uncover further details, there have been no claims of responsibility from any major ransomware groups, and it's still unclear if any data was stolen during the attack. Ransomware incidents, even when mitigated before full encryption, often involve the theft of sensitive data. For tech firms like Tata Technologies, this could potentially expose valuable intellectual property and impact their technological portfolio.

This incident follows a similar attack in 2022, when the Hive ransomware group reported to have targeted Tata Power.

News Snippets - International

US Department of Defence Launched AI Rapid Capability Cell to Accelerate Advanced Technology Adoption

The Pentagon's Chief Digital and Artificial Intelligence Office (CDAO) has unveiled a new initiative aimed at accelerating the adoption of cutting-edge Artificial Intelligence (AI) technology across the Defence Department. Sh. Doug Beck, Defence Innovation Unit (DIU) Director, states that the Artificial Intelligence Rapid Capabilities Cell (AI RCC) & CDAO-DIU partnership will shape critical AI initiatives to incorporate the standards, policy and requirements from the beginning. The AI RCC will collaborate with the DIU to launch four initial Frontier AI pilots, focusing on warfighting and enterprise management use cases. These pilots are designed to integrate generative AI models into key

Please refer page 35, 36 & 37 for reference.

operations to support warfighters and enhance DOD capabilities. CDAO Chief Dr. Radha Plumb emphasised the importance of adopting AI to maintain a technological edge, highlighting the rapid AI advancements by adversaries. The initiative aims to incorporate AI into the department's missions more swiftly and reliably, with a focus on critical areas such as command and control, decision support and cybersecurity. The AI RCC will also establish digital sandboxes for AI experimentation and offer 40 million dollars in funding for small businesses working on generative AI solutions.

The initiative aims to incorporate AI into the department's missions more swiftly and reliably, with a focus on critical areas such as command and control, decision support and cybersecurity.

Proposed HIPAA Security Rule Aims to Strengthen Cybersecurity for Health Data

The U.S. Department of Health and Human Services (HHS) has introduced a proposed rule to bolster cybersecurity protections for electronic Protected Health Information (ePHI) under the HIPAA Security Rule. Released on December 27, 2024, this Notice of Proposed Rulemaking (NPRM) responds to rising cyber threats targeting the healthcare sector and aims to modernise existing standards to keep pace with technological advancements.

The rule applies to ePHI that is maintained or transmitted electronically, ensuring its confidentiality, integrity, and availability. Regulated entities must conduct thorough risk analyses and implement appropriate security measures based on their size and specific risks. They are also required to document security policies and procedures and update them as necessary. Additionally, enhanced safeguards like encryption of ePHI, Multi-Factor Authentication (MFA) and penetration testing will be mandatory. It requires covered entities, such as healthcare providers, health plans and business associates, to implement administrative, physical and technical safeguards to secure ePHI. A new focus on business associate compliance will ensure that third parties meet the same security standards and notify entities within 24 hours of incidents.

The HIPAA security rule aims to balance the protection of sensitive health information with the adoption of new technologies, enhancing both security and the quality of care.

The HIPAA security rule aims to balance the protection of sensitive health information with the adoption of new technologies, enhancing both security and the quality of care.

FCC Launches 'Cyber Trust Mark' to Boost IoT Security

The U.S. government has introduced the U.S. Cyber Trust Mark, a cybersecurity label designed to enhance the security of consumer Internet-of-Things (IoT) devices. Announced by the Federal Communications Commission (FCC), the program aims to help consumers identify smart devices that meet strong cybersecurity standards. Products with the Cyber Trust Mark will feature a QR code, providing access to critical security details, including software update policies, default password requirements and secure configuration guidelines. The compliance process involves

The compliance process involves FCC-recognised labs testing devices to ensure they meet national cybersecurity standards.

Please refer page 35, 36 & 37 for reference.

FCC-recognised labs testing devices to ensure they meet national cybersecurity standards. Eligible products include smart home security cameras, voice assistants, door openers and security systems. UL LLC (UL Solutions) has been selected as the Lead Administrator for the program, which promises to create incentives for manufacturers to adopt better cybersecurity practices, much like the ENERGY STAR program. Manufacturers seeking certification must undergo testing and submit applications through an approved Cybersecurity Label Administrator. This initiative provides consumers with a reliable way to evaluate IoT device security, ensuring safer choices for their connected homes.

DeepSeek AI Data Leak Exposes Over a Million Chat Logs and Sensitive Information

The leak exposed API keys, chat histories and internal system metadata, posing a serious cybersecurity risk.

DeepSeek has suffered a major security lapse, exposing over one million chat logs, backend details and software keys due to an unprotected ClickHouse database. Security researchers at wiz discovered the issue during a routine assessment, revealing that the database was publicly accessible and allowed full control without authentication. The leak exposed API keys, chat histories and internal system metadata, posing a serious cybersecurity risk. Attackers could have used the exposed credentials to manipulate DeepSeek's AI services or gain deeper access to its infrastructure. While DeepSeek responded swiftly by securing the database, it remains unclear whether the data was accessed by unauthorised parties. This breach raises further privacy concerns, especially given DeepSeek's ownership and previous security incidents. Experts warn that AI companies often prioritise rapid development over security, increasing the risk of data exposure. The incident highlights the need for proactive security measures to protect sensitive AI-driven services from cyber threats.

Security App

Bitwarden makes it harder to hack password vaults without MFA

Bitwarden is enhancing account security by adding an email verification step for users who don't have two-factor authentication (2FA) enabled.

Bitwarden is enhancing account security by adding an email verification step for users who don't have two-factor authentication (2FA) enabled. Starting in February, when logging in from an unrecognised device, users will be prompted to enter a verification code sent to their email. This process acts as a form of 2FA, providing an additional layer of protection. However, users who already use 2FA or alternative login methods like API keys or SSO are exempt. The security measure is triggered by actions like logging in from a new device, reinstalling the app, or clearing browser cookies. Bitwarden advises users who store email credentials within the vault to ensure independent access to their

*Please refer page 35, 36 & 37 for reference.

email to avoid being locked out. They also stress the importance of using a strong master password in addition to the new security step.

Cisco Unveils New AI Application Security Solution

Cisco has released AI Defense, a solution designed to help organisations protect development and use of AI applications. This application focuses on enhancing security in two key areas: the use of third-party AI applications and the development of AI applications. For third-party apps, it helps manage risks like data leakage and malicious downloads by providing visibility into app usage, restricting access to unsanctioned tools, and preventing data loss. For enterprises building their own AI, the solution helps discover both authorised and unauthorised applications, tests AI models for vulnerabilities, and ensures runtime protection against threats such as prompt injection and data leakage. Cisco AI Defence is designed to mitigate risks at both the user and application levels, with features like AI access, AI cloud visibility, AI model & application validation, and AI runtime protection. The solution was available to enterprises in March.

This application focuses on enhancing security in two key areas: the use of third-party AI applications and the development of AI applications.

Microsoft Introduced Teams Phishing Attack Alerts

Microsoft has announced that its brand impersonation protection feature for Teams Chat would be available to all Microsoft 365 customers by mid-February 2025. Once activated, the feature will alert users about phishing attacks, particularly those targeting organisations with external Teams access enabled. This allows external users to message internal Teams users, which threat actors have exploited for phishing and malware attacks. The feature, first introduced in late October 2024 and rolled out in mid-November, will now be automatically enabled for all users with no admin configuration required. Users will see a high-risk warning if an external message appears suspicious, requiring them to preview the message before accepting or blocking it. Admins can check the audit log for any detected impersonation attempts, and until the feature is fully available, it's recommended to disable external access if not needed. Teams has over 320 million monthly active users globally.

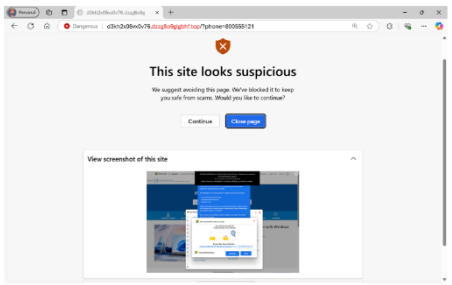


Figure- Edge scareware blocker warning (Microsoft)

Microsoft Edge Scareware Blocker

Microsoft has tested a new "scareware blocker" feature for the Edge browser on Windows PCs to combat tech support scams using machine learning (ML). These scams trick victims into thinking their devices are infected with malware, leading them to contact

Please refer page 35, 36 & 37 for reference.

The new feature enhances protection by detecting scam pages in real time using a local ML model that analyses full-screen pages, comparing them to known scam patterns.

fake tech support. The new feature enhances protection by detecting scam pages in real time using a local ML model that analyses full-screen pages, comparing them to known scam patterns. Once a potential scam is detected, Edge alerts the user and allows them to proceed if they trust the site. Users can report scams to help improve protection across devices. The feature runs locally without sending images to the cloud, and Microsoft encourages reporting false positives to enhance its accuracy. Once it detects a scam page, it alerts users and allows them to continue loading the webpage if they trust the site is safe.

Mobile Security

Samsung Patches Critical Vulnerabilities in to Tackle Zero-Click Exploit

The attack leverages on buffer overflow in the saped_rec function, which writes to dmabuf allocated by the C2 media service.

Samsung has recently patched its smartphones running Android 12, 13, and 14 to address a high-severity vulnerability which is CVE-2024-49415 with CVSS score of 8.1. The flaw, discovered by Google Project Zero's Natalie Silvanovich, affects the Monkey's Audio (APE) decoder in Samsung smartphones, specifically in the libsaped.so library. Monkey's Audio (APE) decoder is used for lossless audio data compression. This out-of-bounds write vulnerability allows remote attackers to execute arbitrary code via a specially crafted APE audio file which can be sent via Google Messages. This attack is successful when Google Messages is set up with Rich Communication Services (RCS), which is the default on Galaxy S23 and S24, as the transcription service decodes incoming audio before the user interacts with the message. The attack leverages on buffer overflow in the saped_rec function, which writes to dmabuf allocated by the C2 media service. By exploiting the large blocksperframe size in certain APE files, attackers can overflow the buffer, and it causes the samsung.software.media.c2 process to crash without user interaction which makes this attacks as a zero-click exploit. Additionally, Samsung's December 2024 update resolves another vulnerability in SmartSwitch (CVE-2024-49413), which could allow local attackers to bypass cryptographic signature verification, potentially installing malicious apps.

New Variant of TgToxic Banking Trojan Introduces Advanced Anti-Analysis Measures

Cybersecurity experts have detected a new variant of the Android malware known as TgToxic (also known as ToxicPanda). It was initially reported by Trend Micro in early 2023 identified it as a banking trojan, which was designed to steal credentials and funds from cryptocurrency wallets, as well as banking and finance related apps. In November 2024, Italian online fraud prevention company Cleafy revealed an updated variant of TgToxic, which

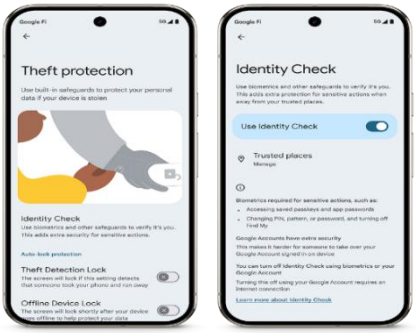
Please refer page 35, 36 & 37 for reference.

introduced extensive data-gathering capabilities and expanded its reach to include Italy, Portugal, Hong Kong, Spain, and Peru. Intel 471's recent analysis has discovered that the malware is spread through dropper APK files, most likely delivered via SMS messages or phishing websites. However, the precise method of distribution remains unclear. There has been a major change in TgToxic's operation which involves replacing hard-coded C2 domains with fake user profiles on forums like the Atlassian community developer forum. These profiles contain an encrypted string directing to the actual C2 server. In later versions of TgToxic, discovered in December 2024, it was found that it is using a domain generation algorithm (DGA) to create new C2 domain names.

There has been a major change in TgToxic's operation which involves replacing hard-coded C2 domains with fake user profiles on forums like the Atlassian community developer forum.

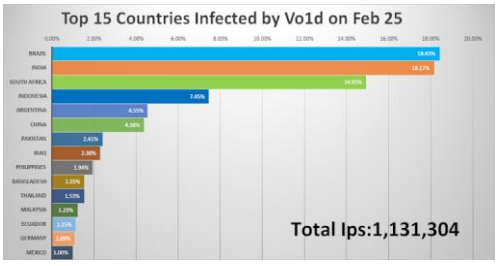
Google Rolling out Identity Check Feature in Android Devices

Google has launched new identity check feature in android devices to enhance security by locking certain device settings when the user is outside a trusted location. This feature provides an additional layer of protection from unauthorised users for making critical changes to the device settings. Identity Check feature uses location-based controls, so when you are not in a pre-defined "trusted" location, certain actions on the device, such as accessing or changing security settings, may be restricted. When Identity check is turned on, the device requires explicit biometric authentication to access sensitive resources. It secures actions such as changing screen locks, viewing passwords, resetting the device, or disabling theft protection. Google rolled out this feature to Google Pixel, Android 15 and Samsung Galaxy phones with One UI7.



Vo1d Botnet's Infected Android TVs, Spanning 226 Countries

The Vo1d botnet has grown significantly, with the latest variant encompassing 800,000 daily active IP addresses, peaking at 1,590,299 on January 19, 2025, affecting 226 countries and regions. Notably, India saw a sharp rise in infections, going from less than 1% (3,901 devices) to 18.17% (217,771 devices) by February 25, 2025. The main purpose of the botnet is believed to be advertisement fraud, but it is also used as a proxy network for various cybercriminal activities. Vo1d's infrastructure is leased out to other malicious groups, further expanding its reach. The Vo1d botnet has enhanced its stealth and anti-detection features, using RSA encryption and XXTEA encryption to secure network communications and complicate analysis. First identified by Doctor Web in September 2024, the malware targets Android TV boxes through a backdoor that downloads malicious executables from a command-and-control (C2) server. While the infection method remains unclear, it's suspected to involve supply chain attacks or unofficial firmware with root access. Google confirmed



The Vo1d botnet has enhanced its stealth and anti-detection features, using RSA encryption and XXTEA encryption to secure network communications and complicate analysis.

*Please refer page 35, 36 & 37 for reference.

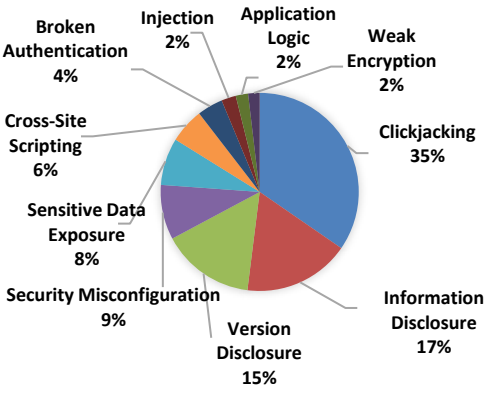
that the affected devices were off-brand and non-Play Protect-certified Android TVs, likely based on Android Open Source Project (AOSP) code, which makes them more vulnerable to such attacks. The botnet's ability to scale and evolve poses a significant cybersecurity threat globally.

NCIIPC Initiatives

NCIIPC Responsible Vulnerability Disclosure Program

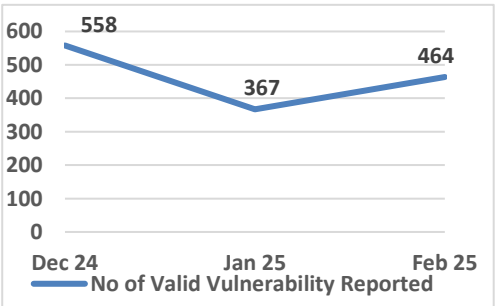
The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 1389 vulnerabilities reported during the first quarter of 2025. The top 10 vulnerabilities are:

- Clickjacking
- Information Disclosure
- Version Disclosure
- Security Misconfiguration
- Sensitive Data Exposure
- Cross-Site Scripting
- Broken Authentication
- Injection
- Application Logic
- Weak Encryption



Around 274 security researchers participated in RVDP programme during the first quarter of 2025. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Aaditya Wadodkar
- Akash kawre
- Ashutosh Kumar
- Dinesh N
- Edwin Shajan
- Gopal Waddar
- Jatin Talreja
- Mohamed Farhan P A
- Prasad R Sonar
- Rajesh Bhandekar
- Ronak Kumar



Last three months' timeline chart for vulnerabilities reported

*Please refer page 35, 36 & 37 for reference.

- Smeet Almeida
- Sravanthi Pachunoori
- Sudha Pal
- Tisha Kanjwani

NCIIPC at Nullcon Goa 2025

The 15th edition of Nullcon, Asia's premier international security conference, took place from February 26 to March 2, 2025, at the BITS Pilani, Goa. The training sessions conducted from 26th to 28th February engaged the participants in hands-on technical training across various cybersecurity topics, enhancing their practical skills. The main conference, held from 1st to 2nd March, featured a series of talks and presentations from global cybersecurity experts, focused on the latest research, vulnerabilities, and hacking techniques. The event also hosted multiple CTF challenges, including HackIM, Winja (a CTF by women for women), Battle Underground, Hardware CTF, and SCADA CTF, providing participants with opportunities to test and enhance their skills in real-world scenarios. NCIIPC officials attended the Nullcon Security Conference & Training. This year's conference emphasised comprehensive view of current challenges and innovations in the cybersecurity domain.

NCIIPC & QCI Developed a Conformity Assessment Framework

NCIIPC, in collaboration with Quality Council of India (QCI) have developed a Conformity Assessment Framework (CAF) aimed at enhancing cybersecurity across Critical Sectors. This framework encompasses several key schemes:

- Certification Scheme for Cyber Security Management System Levels 1, 2, & 3
- Inspection Scheme for Information Technology and Industrial Control Systems
- Personnel Certification Scheme for Cyber Security Professionals
- Accreditation Scheme for IT/ICS Training Bodies and Consultancy Organisations

To promote these initiatives and strengthen the cybersecurity ecosystem, a series of awareness programs were organised across the country:

- Awareness Programme on Accreditation Scheme for IT/ICS Training Bodies & Consultancy Organisations
- Awareness Programme on Scheme for Cyber Security Management System & Inspection of Critical Sector Entities
- Awareness Programme on Personnel Certification Scheme for IT/ICS Cyber Security Professionals

Please refer page 35, 36 & 37 for reference.

NCIIPC at Startup Mahakumbh

Startup Mahakumbh second edition, organised by Federation of Indian Chambers of Commerce & Industry (FICCI), took place from 3–5 April, 2025, at Bharat Mandapam, New Delhi. The theme was 'Startup India @ 2047—Unfolding the Bharat Story'. Startup Mahakumbh featured 3,000 startups, 1,000+ investors and incubators, 10,000+ delegates from 50+ countries, and 50,000+ business visitors, creating an unparalleled platform to shape the future of India's entrepreneurial landscape. The event focused on key sectors like AI, Deeptech & Cybersecurity, HealthTech & BioTech, AgriTech, Energy & Climate Tech and etc. The event was inaugurated by Sh. Jitin Prasada, Hon'ble Union Minister of State for Ministry of Commerce & Industry and Ministry of Electronics & Information Technology. Sh. Piyush Goyal, Commerce and Industry Minister and Sh. Navin Kumar Singh, DG NCIIPC and other delegates were present in the event. The special Programmes at Startup Mahakumbh were:

The delegates at Startup Mahakumbh 2025

- Startup MahaRathi: a high-impact platform designed to identify and accelerate India's most promising early to growth-stage startups.
- Masterclasses: designed for deep learning and skill enhancement.
- B2B Meetings: serve as a powerful networking avenue, connecting startups with investors, corporates, and potential business partners.
- Futurepreneurs: this competition invites 100 top colleges, each represented by 10 student innovators, to showcase AI-driven solutions for local challenges at Startupp Mahakumbh.

Please refer page 35, 36 & 37 for reference.

Events - India

• Startup Mahakumbh 2025, New Delhi	3-5 Apr
• CII-SECEX 2025, New Delhi/Mumbai/Kolkata/ Bengaluru	11-20 Apr
• Global GRC, Data Privacy & Cyber Security ConfEx, New Delhi	22 Apr
• OSINTCon 2025, Virtual	23-25 May
• CyberSec India Expo 2025, Mumbai	11-12 Jun
• Nullcon Hyderabad 2025	12-14 Jun
• CISO INDIA CONNECT 2025, Hyderabad	26 Jun
• Cybersecurity Summit: New Delhi, New Delhi	17 Jul

APRIL 2025

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Events - Global

April 2025

• Black Hat Asia, Singapore	1-4 Apr
• Cyber Security for Critical Assets, Singapore	16-17 Apr
• INTERFACE Anchorage 2025, Anchorage	17 Apr
• 2025 Cyber Threat Intelligence Conference, Berlin	21-23 Apr
• Toronto Cybersecurity Conference, Toronto	24 Apr
• Hack Glasgow, Glasgow	26 Apr
• Generative AI Summit, Santa Clara	29-30 Apr
• Cyber Intelligence Europe 2025, Madrid	29-30 Apr

MAY 2025

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

May 2025

• BSides Calgary 2025, Calgary	1-2 May
• Secure Miami, Miami	7 May
• IEEE Symposium on Security and Privacy	12-15 May
• ItaliaSec Cyber Summit, Rome	13-14 May
• Ignite on Tour Zurich, Zurich	14 May
• SASE Summit Tour, Buenos Aires	15 May
• BSides Tampa 2025, Tampa	17 May
• TyphoonCon Seoul 2025, Seoul	26-30 May

JUNE 2025

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

JULY 2025

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

June 2025

- Convene: Clearwater 2025, Florida 3-4 Mar
- SunSecCon, Pasadena 6-7 Mar
- NICE Conference & Expo, Denver 1-3 Jun
- CONFidence conference, Kraków 2-3 Jun
- Gartner Security & Risk Management Summit, Maryland 9–11 Jun
- Bank IT, New York City 16 Jun
- INCYBER FORUM USA, San Antonio 17-18 Jun
- Montreal Cybersecurity Conference, Montreal 18 Jun
- SecretCon, Minneapolis 19-20 Jun
- 37th Annual FIRST Conference, Copenhagen 22-27 Jun

July 2025

- CYDES 2025, Putrajaya 1-3 Jul
- 8th Party in the Park!, London 3 Jul
- CISO Melbourne, Melbourne 22-23 Jul
- Governance 360 Africa, Kenya 23-25 Jul

General Help helpdesk1@nciipc.gov.in
helpdesk2@nciipc.gov.in

Incident Reporting : ir@nciipc.gov.in

Vulnerability Disclosure : rvdp@nciipc.gov.in

Malware Upload : mal.repository@nciipc.gov.in

Abbreviations

- **AFA:** Additional Factor of Authentication
- **AitM:** Adversary-in-the-Middle
- **AMSI:** AntiMalware Scan Interface
- **ASN:** Abstract Syntax Notation
- **AVs:** Autonomous Vehicles
- **BitB:** Browser-in-the-Browser
- **CADC:** Cybersecurity Attribution Data Centre
- **CCDC:** Canadian Cyber Defence Collective
- **CDAO:** Chief Digital and Artificial Intelligence Office
- **DIU:** Defence Innovation Unit
- **DNS:** Domain Name System
- **DNSSEC**: Domain Name System Security Extensions
- **DOD:** Department of Defense
- **DOE:** Department of Energy
- **DoH:** DNS-over-HTTPS
- **DORA:** Digital Operational Resilience Act
- **DPIA:** Data Protection Impact Assessments
- **ECC:** Elliptic Curve Cryptography
- **EMCIP:** Energy Modernisation Cybersecurity Implementation Plan
- **ePHI:** electronic Protected Health Information
- **FAR:** Federal Acquisition Regulation
- **FICCI:** Federation of Indian Chambers of Commerce & Industry
- **GSA:** General Services Administration
- **HHS:** Health and Human Services
- **IDRBT:** Institute for Development and Research in Banking Technology
- **IETF:** Internet Engineering Task Force
- **ISE:** Identity Services Engine
- **KSK:** Key Signing Key
- **MFA:** Multi-Factor Authentication
- **MITM:** man-in-the-middle
- **NIST:** National Institute of Standards and Technology
- **ONCD:** Office of the National Cyber Director
- **QKD:** Quantum Key Distribution
- **RBI:** Reserve Bank of India
- **TLS:** Transport Layer Security
- **XML:** Extensible Markup Language
- **ZSK:** Zone Signing Key

Sources

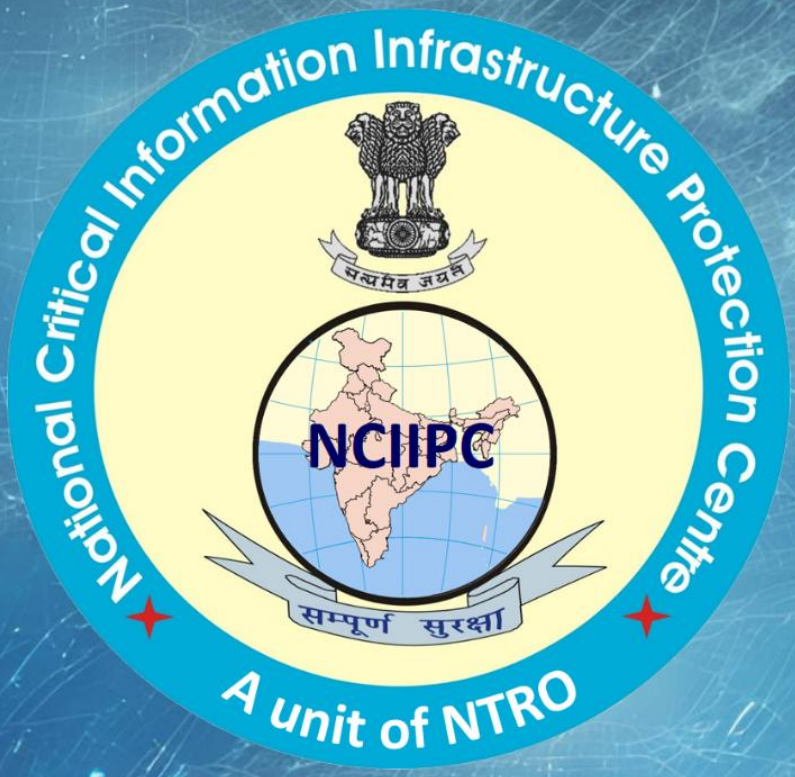
- **DOE Unveils Enterprise Data Strategy to Drive Innovation and Security (2025-2028)**
  https://www.hstoday.us/subject-matter-areas/
  https://www.energy.gov/
- **Federal Agencies Propose Standardised Cybersecurity Workforce Requirements in Contracts**
  https://www.hstoday.us/
  https://www.defense.gov/
- **ONCD Launched Cybersecurity Plan to Protect Energy Infrastructure**
  https://www.hstoday.us/
- **EU's DORA Cybersecurity Rules Take Effect, Many Financial Firms Lag in Compliance**
  https://www.bankinfosecurity.asia/
- **Malaysia Proposed ASEAN Cybercrime Task Force for Stronger Regional Security**
  https://www.bankinfosecurity.asia/
- **Canada Launched National Cyber Security Strategy to Strengthen Digital Defenses**
  https://www.secureworld.io/
- **AI-Focused Modules in Security Awareness and Training Service**
  https://www.fortinet.com/blog/
- **Quantum Computing's Impact on Cybersecurity and the Road Ahead**
  https://www.secureworld.io/
- **Malvertising Campaign Targets Google Ads Users**
  https://thehackernews.com/
- **Sneaky 2FA: AitM Phishing Kit**
  https://thehackernews.com/
- **Fake CAPTCHA Campaign Spreads Lumma Stealer**
  https://thehackernews.com/
- **Custom Backdoor Exploited Magic Packet Vulnerability in Juniper Routers**
  https://thehackernews.com/
- **ForceCopy Malware Used to Steal Browser-Stored Credentials**
  https://thehackernews.com/
- **Attackers Used Exposed ASP.NET Keys to Deploy Malware**
  https://www.bleepingcomputer.com/
- **DragonForce Ransomware Group Targets Saudi Infrastructure in Major Cyberattack**
  https://gbhackers.com/dragonforce-attacks-critical-infrastructure/
- **Bybit Breached: Safe{Wallet} Compromised in Cyberattack**
  https://www.bleepingcomputer.com/
- **Fortinet Zero-day Vulnerability Exploitation**
  https://www.fortiguard.com/psirt/FG-IR-24-535
  https://www.bankinfosecurity.asia/
- **Critical Vulnerability in BSS Mobuy Online Machinery Monitoring Panel**
  https://www.usom.gov.tr/bildirim/tr-25-0033

https://nvd.nist.gov/vuln/detail/CVE-2024-13152

- **Critical Vulnerabilities in Cisco Identity Services Engine**
  https://sec.cloudapps.cisco.com/
- **Critical Vulnerability in SimpleHelp**
  https://nvd.nist.gov/vuln/detail/cve-2024-57726
  https://simple-help.com/
- **Critical Vulnerabilities in Wavlink AC3000 Wireless Router**
  https://talosintelligence.com/
- **Critical Vulnerability in Dynamics 365 Integration Plugin for WordPress**
  https://www.wordfence.com/
- **Critical Vulnerability in Arne Informatics Piramit Automation**
  https://nvd.nist.gov/vuln/detail/CVE-2024-8950
- **Critical Vulnerabilities in Atlassian**
  https://jira.atlassian.com/browse/CONFSERVER-99216
  https://jira.atlassian.com/browse/CONFSERVER-99215
- **Critical Vulnerabilities in Ivanti**
  https://thehackernews.com/2025/02/ivanti-patches-critical-flaws-in.html
- **PANdora's Box Vulnerabilities in Palo Alto Networks Firewalls**
  https://thehackernews.com/
- **Revolutionising Financial Crime Prevention: The Role of ISO 20022 in Enhancing Security, Efficiency, and Transparency**
  https://ciso.economictimes.indiatimes.com/
- **Securing Critical Infrastructure: Strengthening Cybersecurity in the Oil and Gas Industry**
  https://www.secureworld.io/
- **Understanding Phishing Attacks: The Rising Threat of Browser-in-the-Browser**
  https://mrd0x.com/browser-in-the-browser-phishing-attack/
  https://blog.surf.security/browser-in-the-browser-attack?
  https://www.bitdefender.com/
- **India's Draft Digital Personal Data Protection Rules, 2025: Key Highlights**
  https://static.mygov.in/
  https://thehackernews.com/
- **Tata Technologies Hit by Ransomware Attack**
  https://www.bleepingcomputer.com/
  https://www.documentcloud.org/
- **Enhancing Trust in Digital Banking: RBI's New Domain Initiative**
  https://www.rbi.org.in/
  https://thehackernews.com/
- **ANSSI Released "Building Trust in AI Through a Cyber Risk-Based Approach" Report**
  https://www.elysee.fr/en/sommet-pour-l-action-sur-l-ia
- **US Department of Defence Launched AI Rapid Capability Cell to Accelerate Advanced Technology Adoption**
  https://www.defense.gov/

https://www.hstoday.us/

- **Proposed HIPAA Security Rule Aims to Strengthen Cybersecurity for Health Data**
  https://www.hstoday.us/
- **FCC Launches 'Cyber Trust Mark' to Boost IoT Security**
  https://www.fcc.gov/CyberTrustMark
  https://thehackernews.com/
- **DeepSeek AI Data Leak Exposes Over a Million Chat Logs and Sensitive Information**
  https://hackread.com/
  https://chat.deepseek.com/
- **CISA & FBI Warn of Ghost Ransomware Attacks Across 70 Countries**
  https://www.cisa.gov/
  https://www.bleepingcomputer.com/
- **Bitwarden makes it harder to hack password vaults without MFA**
  https://www.bleepingcomputer.com/
- **Cisco Unveils New AI Application Security Solution**
  https://www.securityweek.com/
- **Microsoft Introduced Teams Phishing Attack Alerts**
  https://www.bleepingcomputer.com/
- **Microsoft Edge Scareware Blocker**
  https://www.bleepingcomputer.com/
- **OpenSSF Released Security Baseline for Open Source Projects**
  https://www.securityweek.com/
  https://baseline.openssf.org/
- **Samsung Patches Critical Vulnerabilities in to Tackle Zero-Click Exploit**
  https://thehackernews.com/
- **New Variant of TgToxic Banking Trojan Introduces Advanced Anti-Analysis Measures**
  https://thehackernews.com/
- **Google Rolling out Identity Check Feature in Android Devices**
  https://thehackernews.com/
- **Vo1d Botnet's Infected Android TVs, Spanning 226 Countries**
  https://thehackernews.com/



Feedback/Contribution

Suggestions, feedback and contributions are welcome at newsletter@nciipc.gov.in

Disclaimer

NCIIPC does not endorse any vendor, product or service. The content of the newsletter is for informational purpose only. Readers may validate the information on their own.