NEWSLETTER

April 2024

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

National Critical Information Infrastructure Protection Centre
NCIIPC
सम्पूर्ण सुरक्षा
A unit of NTRO

NCIIPC-AICTE Pentathon 2024

NCIIPC in collaboration with AICTE has conducted India's first national level VAPT 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.

https://nciipc.gov.in/ | @NCIIPC | NCIIPC India | NCIIPC India | helpdesk1@nciipc.gov.in | 1800-11-4430

VOLUME 8 ISSUE 2

@NCIIPC

NCIIPC Newsletter

April 2024

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

NCIIPC Newsletter aims to bring latest developments in the field of cyber security specific to Critical Information Infrastructure (CII). In this regard, a number of developments have taken place during the first quarter of 2024. E.g. RBI has released new IT Governance Guidelines for Financial Entities. U.S. Law enforcements have shut down sites of KV-Botnet, Moobot Botnet, Warzone RAT' and LockBit ransomware etc.

NCIIPC in collaboration with All India Council for Technical Education (AICTE) and MoE's Innovation Cell (MIC) conducted India's first national level Vulnerability Assessment and Penetration Testing (VAPT) exercise for all technical colleges and universities in India. The objective of this exercise was to create a talented pool of ethical hackers/pen testers for finding vulnerabilities in the systems of Critical Information Infrastructure. This witnessed around 200 students-competing in team and as individual in the Grand Finale.

NCIIPC also organised a Pentesting Exercise in order to identify competent ethical hackers/ security researchers/ VAPT professionals who are willing to work for the national cause and find vulnerabilities in Critical Sector Entities (CSEs). Around 70 participants discovered vulnerabilities and loopholes in systems of CSEs which could not be identified by their regular security team or hired vendors during VAPT. They were rewarded.

NCIIPC organised the National Level Critical Information Infrastructure Security Exercise, 'CII SECEX: 2024', a 10 days' event during 5-14 April 2024 across the four locations viz. Delhi, Mumbai, Bengaluru and Kolkata simultaneously. The event saw a footfall of more than 550 participants from CSEs across the country. This National Level Exercise was conducted in three parts: Training cum Operational Exercise, Strategic Exercise and CEO level exercise.

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.

News Snippets - National

RBI's New IT Governance Guidelines for Financial Entities

The Reserve Bank of India (RBI) released a master direction on Information Technology Governance, Risk, Controls and Assurance Practices. This notice was released on 7th November 2023, which was slated to take effect from April 1, 2024. The directive applies to regulated entities, encompassing both banking and non-banking financial companies. Emphasising crucial areas of IT Governance, the directive mandates regulated entities to establish a comprehensive IT Governance Framework. This framework must include robust oversight mechanisms to ensure accountability and effective mitigation of IT and cyber/information security risks. Additionally, the Master Direction outlines specific provisions, such as the adoption of an IT and Information Security Risk Management Framework, formulation of Information Security and Cyber Security Policies, and regular reviews of IT-related risks. This strategic move by the RBI signifies a proactive approach to fortify technological resilience within the financial sector.

Emphasising crucial areas of IT Governance, the directive mandates regulated entities to establish a comprehensive IT Governance Framework.

Department of Telecom Initiates Security Audit

The Department of Telecom has called upon service operators to undergo a security audit in response to claims made by a cybersecurity firm regarding data leak impacting 750 million Indian telecom users. This proactive move by the department aims to address potential vulnerabilities in the telecom sector and ensure the protection of user's data. The request for a security audit is a precautionary step following concerns raised by the cybersecurity firm about a substantial data leak. By encouraging collaboration among operators to conduct thorough security assessments, the Department of Telecom emphasises the significance of maintaining robust cybersecurity practices in the telecommunications industry.

This proactive move by the department aims to address potential vulnerabilities in the telecom sector and ensure the protection of user's data.

News Snippets - International

Orange Spain's RIPE Account Hacked by Malware

As per reports, Orange Spain Mobile network operator suffered a substantial Internet outage on 3rd January 2024, which resulted from a sophisticated cyberattack. The assailant employed administrator credentials acquired from a compromised employee's computer which had fallen victim to the insidious Raccoon Stealer malware in September 2023. Leveraging these credentials the attacker orchestrated a manipulation of Orange

Please refer page 30, 31 & 32 for reference.

The root cause of this cyber incident can be traced back to the malware-infected computer which successfully extracted weak credentials for Orange Spain's RIPE administrator account.

Spain's Border Gateway Protocol (BGP) traffic on the Réseaux IP Européens (RIPE) registry. This strategic interference resulted in severe disruptions impacting nearly 50% of the company's Internet traffic. The root cause of this cyber incident can be traced back to the malware-infected computer which successfully extracted weak credentials for Orange Spain's RIPE administrator account. The password alarmingly simplistic was "ripeadmin". RIPE has encouraged the account holders to update their passwords and enable multi-factor authentication for their accounts.

On 10th January 2024 there was a discernible collapse in internet connectivity originating from Sudachad as observed by network monitoring services.

Anonymous Sudan Launched Cyberattack on Chad Telco

Anonymous Sudan orchestrated a cyber-offensive against Sudachad, the primary supplier of wholesale Internet capacities for Chad. On 10th January 2024 there was a discernible collapse in Internet connectivity originating from Sudachad as observed by network monitoring services. According to Anonymous Sudan, the motive behind the cyber assault was Chad's alleged support for the Rapid Support Forces a paramilitary group with which Chad is purportedly aligned.

The compromised data including information for 1 million Ashkenazi Jews and 4.1 million individuals in the United Kingdom surfaced on both the BreachForums hacking forum and an unofficial 23andMe subreddit.

23andMe Data Breached

Genetic testing provider 23andMe recently confirmed a substantial data breach that occurred over five months from 29 Apr – 27 Sep 2023. The breach resulting from a credential stuffing attack saw hackers gaining unauthorised access to health reports and raw genotype data of affected customers. The attackers utilised credentials pilfered from prior data breaches or compromised online platforms. The compromised data including information for 1 million Ashkenazi Jews and 4.1 million individuals in the United Kingdom surfaced on both the BreachForums hacking forum and an unofficial 23andMe subreddit. In official data breach notifications to affected customers 23andMe disclosed that the threat actors downloaded or accessed uninterrupted raw genotype data and potentially other sensitive information such as health reports derived from genetic data processing. Out of the 14 million existing customers, the breach affected 14,000 user accounts and compromised data from 6.9 million individuals.

Change Healthcare Cyberattack

Change Healthcare, UnitedHealth-owned U.S. based technology company, had shut down its systems for more than a week due to cyberattack. This cyberattack hampered the providers and disrupted pharmacy and other key operations of

Please refer page 30, 31 & 32 for reference.

Change Healthcare. The attack was discovered on 21st February 2024. Change Healthcare for pharmacy services, payments and medical claims systems were affected by the cyberattack. Change Healthcare confirmed that ransomware group AlphV (also known as BlackCat) claimed responsibility for this attack.

U.S. Feds/FBI Shut Down KV-Botnet & Moobot Botnet

The U.S. Government (FBI) took decisive action to dismantle a botnet named KV-botnet orchestrated by threat actor Volt Typhoon. This botnet comprised numerous Small Office/Home Office (SOHO) routers within the United States with a focus on Cisco and NetGear routers that had reached their 'end of life,' lacking manufacturer support for security patches or updates. To disrupt the botnet the U.S. government remotely issued commands to targeted routers, eradicating the KV-botnet malware and preventing re-infection. Furthermore, they severed connections and blocked communications with other controlling devices.

The FBI has also dismantled a botnet comprised of SOHO routers exploited by nation-based threat actor. This extensive network consisting of hundreds of Ubiquiti Edge OS routers infected with Moobot malware served as a conduit for proxying malicious traffic and conducting spear-phishing and credential theft attacks against the United States and its allies.

The FBI has also dismantled a botnet comprised of Small Office/Home Office (SOHO) routers exploited by nation-based threat actor.

Warzone RAT Shut Down by Law Enforcement

The US Justice Department declared the successful dismantling of the Warzone RAT cybercrime operation following a collaborative international law enforcement effort. Authorities seized four internet domains linked to the sale of the Warzone RAT displaying takedown notices as a result of joint actions by agencies from the US, Netherlands, Germany, Malta, Romania, Croatia, Finland, Australia, Canada, and Nigeria with support from Europol. The operation also targeted servers hosting the Warzone RAT infrastructure. The Warzone RAT served as a malicious remote access tool. The Justice Department also announced a dedicated website where victims of the Warzone RAT can file a report with the FBI.

Warzone RAT site taken down by US Justice Department

Please refer page 30, 31 & 32 for reference.

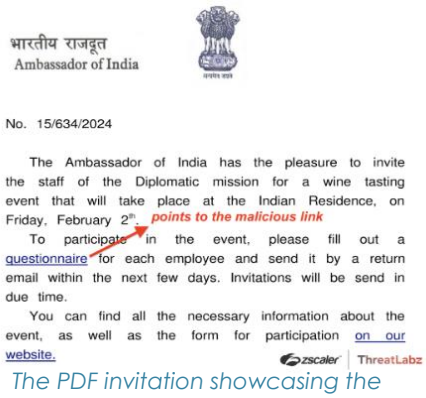
Lockbit site taken down by Operation Cronos

LockBit Ransomware Disrupted by Global Police Operation

In a collaborative effort involving law enforcement agencies from 10 countries, operation Cronos has successfully disrupted the notorious LockBit ransomware operation. The 10 countries are France, Germany, Netherlands, Sweden, Canada, Australia, Japan, United Kingdom, United State and Switzerland. Law enforcement's intervention resulted in the takeover of the LockBit platform, providing comprehensive information on the group and its affiliates. The acquired data includes source code, victim details, extortion amounts, stolen data, and communication records. Operation Cronos has effectively dismantled LockBit's infrastructure dealing a significant blow to the ransomware operation.

Malware Bytes

European Diplomats Targeted by SPIKEDWINE with WINELOADER


भारतीय राजदूत
Ambassador of India

No. 15/634/2024

The Ambassador of India has the pleasure to invite the staff of the Diplomatic mission for a wine tasting event that will take place at the Indian Residence, on Friday, February 2th. *points to the malicious link*

To participate in the event, please fill out a questionnaire for each employee and send it by a return email within the next few days. Invitations will be send in due time.

You can find all the necessary information about the event, as well as the form for participation on our website.

zscaler | ThreatLabz

The PDF invitation showcasing the malicious link

Zscaler's ThreatLabz recently detected a suspicious PDF file uploaded to VirusTotal from Latvia on 30th January 2024. The PDF, disguised as an invitation letter from the Indian Ambassador, purportedly invites diplomats to a wine-tasting event in February 2024. Within the PDF there's a link to a deceptive questionnaire leading users to a malicious ZIP archive hosted on a compromised site triggering the initiation of the infection chain. Upon further investigation, another similar PDF file uploaded from Latvia in July 2023 was discovered. The detailed technical analysis of the attack chain revealed that the PDF was created using LibreOffice version 6.4 on 29th January 2024. The embedded malicious link redirects users to a compromised site. Subsequently, the downloaded HTML Application (HTA) file contains obfuscated JavaScript code, executing the next phase of malicious activities.

New macOS Backdoor: SpectralBlur

SpectralBlur is designed to erase files after opening them and overwriting their content with zeros.

Cybersecurity researchers have discovered a new Apple macOS backdoor called SpectralBlur. SpectralBlur backdoor can download/upload files, run a shell, delete files, update its configuration, hibernate, or sleep, based on commands issued by command-and-control server. After being initialised, the malware executes a function responsible for encrypting/decrypting its configuration and network traffic, then proceeds to perform various actions aimed at hindering its analysis and detection. SpectralBlur is designed to erase files after opening them and overwriting their content with zeros.

Please refer page 30, 31 & 32 for reference.

TimbreStealer Malware Spreading via Tax-themed Phishing Scam

Mexican users were targeted with tax-themed phishing lures by a malware called TimbreStealer. This campaign used financial themed phishing emails directing users to a compromised website where the payload is hosted and tricking them into executing the malicious application. The payload is designed to harvest a wide range of data that includes credential information from different folders, system metadata, accessed URLs, look for files matching specific extensions, and verify the presence of remote desktop software. This phishing campaign used geofencing techniques to target the users in Mexico only, and any attempt to contact the payload sites from other locations were returned with a blank PDF file instead of the malicious file.

This campaign used financial themed phishing emails directing users to a compromised website where the payload is hosted and tricking them into executing the malicious application.

IDAT Loader Attacks Use Steganography to Deploy Remcos RAT

A malicious campaign has been discovered distributing a commercial remote access trojan called Remcos RAT using a malware loader called IDAT Loader. The attack was carried out by a threat actor called UAC-0184. The phishing campaign used war-themed lures as a starting point to start the infection chain, which leads to the deployment of IDAT Loader. The loader then uses an embedded steganographic PNG to locate and extract Remcos RAT.

The phishing campaign used war-themed lures as a starting point to start the infection chain, which leads to the deployment of IDAT Loader.

Malicious Excel document spreads Python Info-Stealer

South Zone, NCIIPC

Reported first in August 2023, the Vietnamese-based threat group spread a sophisticated Python-based information stealer that was distributed via a malicious Excel document. The Python-based info-stealer has all the capabilities of a modern info-stealer like collecting web browser information, the ability to download additional payloads and more. It uses the Malware-as-a-Service (MaaS) model, that has the potential to cause significant damage to organisations and end users. It can be distributed via Phishing, and is capable of collecting sensitive data from a compromised machine while remaining undetected. The malware has been observed being used in ransomware attacks with updated versions. Threat actors are using VPN services to compromise users, specifically targeting those organisations that have not enabled multifactor authentication. The malware has a high degree of configurability and robust anti-tampering controls, making it difficult to detect, analyse and remove.

Threat actors are using VPN services to compromise users, specifically targeting those organisations that have not enabled multifactor authentication.

Targets: The malware targets cryptocurrency wallets, stored card details, autocomplete data and messaging Apps including Telegram.

Please refer page 30, 31 & 32 for reference.

Impact: The malware has various features, including the ability to perform the following actions:

- It can steal Credentials/proprietary information and privilege escalation
- Command and control capabilities
- Extract sensitive information from web-browsers and applications
- Spread viruses and malicious software such as ransomware etc.
- Format all drives
- It can steal network information
- Modify/Update files
- It can perform key logging and screen capturing

The attack uses various stages before deploying its information stealer including simple downloaders.

The attack uses various stages before deploying its information stealer including simple downloaders. The first stage includes an Excel document containing a VBA script.

Once activated, the macros downloads and executes a Python script. It goes to its Command and Control (C2) server and downloads three different files and saves them with different names on the computer that will later scan the victim's machine for sensitive data including passwords, financial information and other personal details. The malware starts its information stealing functionality and creates a folder to store the stolen information. To implement the asynchronous encryption, the attackers used the boost library for both Windows and Linux. It has the ability to encrypt files or data on both Windows and Linux based operating systems. The following practices may help to reduce the risk of information stealer:

The malware starts its information stealing functionality and creates a folder to store the stolen information.

- Do not open suspicious links and attachments in email without verifying their authenticity
- Disable macro execution by default
- Ensure multifactor authentication wherever possible to provide extra layer of security, particularly the accounts that access critical systems
- Hardening of firmware, network, software and all operating systems should be done periodically to reduce security risk by eradicating potential attack vectors and reducing the system's attack surface
- Cyber Security audit of the Infrastructure needs to be carried out regularly
- OS, application and security software like antivirus should be updated regularly
- The unnecessary open ports in the systems/servers need to be closed
- Cybersecurity awareness training, workshops, cyber security mock drills covering the social engineering attacks for the end users to stay across current threats should be conducted on regular basis.

Please refer page 30, 31 & 32 for reference.

Learning

Understanding the Role of CVEs in Cybersecurity

Knowledge Management Team, NCIIPC

In today's digital landscape, organisation face significant risks from cyberattacks. Staying informed about the latest threats and taking appropriate actions to protect systems and data is critical. Common Vulnerabilities and Exposures (CVE) plays a vital role in cybersecurity by acting as a central repository of vulnerability information. There would be confusion and inefficiency in addressing security issues without CVE. Cyberattacks often target these common vulnerabilities to exploit the weaknesses for unauthorised access or data breaches. By providing CVE identifiers and related information, the system aids security teams in quickly identifying and patching vulnerabilities before they can be exploited. CVEs are a common language in the field of cybersecurity, with IDs assigned by security researchers and vendors to vulnerabilities they discover. This standardisation helps IT specialists and businesses understand and resolve security issues efficiently. Nearly all security advisories, whether from vendors or independent researchers, include at least one CVE ID.

By providing CVE identifiers and related information, the system aids security teams in quickly identifying and patching vulnerabilities before they can be exploited.

The Common Vulnerability Scoring System (CVSS) and CVEs: The CVSS is a detailed scoring system that assesses the severity of a vulnerability, taking into account factors such as its potential impact and exploitability. It provides a comprehensive evaluation to help understand the seriousness of a vulnerability. In contrast, CVEs offer unique identification for vulnerabilities, enabling easy reference and tracking.

Categories of Vulnerabilities on CVE: Often vulnerabilities can take many different forms, Sensitive Data Exposure, SQL Injection, Code Execution, Denial of Service, Cross-Site Scripting (XSS), External Entity Injection, and Overflows are some frequent types. These categories need to be understood and dealt with in view of their frequent occurrence in the field of cybersecurity.

CVEs are an essential part of the cybersecurity ecosystem, offering a standardised approach to identifying and addressing vulnerabilities. They enable IT specialists to prioritise and resolve vulnerabilities efficiently, enhancing overall system security. Understanding and responding to CVEs are essential in protecting our digital world from threats. Given the constantly evolving threat landscape, it's crucial to remain vigilant and proactive in addressing vulnerabilities.

Understanding and responding to CVEs are essential in protecting our digital world from threats. Given the constantly evolving threat landscape, it's crucial to remain vigilant and proactive in addressing vulnerabilities.

Challenges of CVE: The CVE system has its share of difficulties in the complex world of cybersecurity.

- Rapidly growing vulnerability landscape: Keeping CVE databases up to date with the exponential growth of vulnerabilities is difficult.

Please refer page 30, 31 & 32 for reference.

- Lack of universal adoption: Although extensively used, CVE is not a required standard.
- CVE identifier shortages: CVE identifiers may run out as vulnerabilities increase.
- Time sensitivity: CVE databases must match the pace of threatactors.
- Data quality Inconsistency: Vulnerability information can be incomplete or unclear. This inconsistency challenges CVE's role in providing accurate guidance regarding vulnerability.
- False positives and negatives: CVE databases can sometimes produce false alerts or overlook threats, creating confusion.

By being aware of these aspects of CVE, cybersecurity professionals can effectively manage vulnerabilities and reduce the risk of security breaches in their organisations.

Secure Coding Practices

Development Team, NCIIPC

Secure coding practices are crucial for developing robust and resilient software that can withstand potential security threats and attacks.

Secure coding practices are crucial for developing robust and resilient software that can withstand potential security threats and attacks. Here are some general secure coding practices applicable to various programming languages:

Input Validation: Validate all user inputs to ensure they meet expected criteria. Input validation helps prevent common vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and buffer overflows. Whitelist based input validation should be used rather than blacklist based mechanism to be more effective.

Output Encoding: Encode output data before rendering it in different contexts (e.g., HTML, JavaScript, SQL) to prevent injection attacks. Use encoding functions provided by the framework or language.

Use secure session management practices, including secure session cookies, session timeout, and session regeneration after login. Store session data securely, and consider implementing features like session logging.

Authentication and Authorisation: Implement strong authentication mechanisms, such as Multi-Factor Authentication (MFA), and enforce proper authorisation checks to ensure users have the necessary permissions for accessing resources.

Password Security: Store passwords securely using strong, adaptive hashing algorithms (e.g., bcrypt, Argon2). Never store passwords in plain text, and use salt to enhance password security.

Session Management: Use secure session management practices, including secure session cookies, session timeout, and session regeneration after login. Store session data securely, and consider implementing features like session logging.

Secure File Uploads: If your application allows file uploads, validate file types, restrict file sizes, and use secure storage locations. Ensure that uploaded files do not contain malicious content.

*Please refer page 30, 31 & 32 for reference.

HTTPS Usage: Always use HTTPS to encrypt data in transit. Secure communication between clients and servers helps prevent man-in-the-middle attacks and protects sensitive information during transmission.

Avoid Hardcoding Secrets: Avoid hardcoding sensitive information like API keys, passwords, or cryptographic keys directly in code. Use secure storage mechanisms such as environment variables or configuration files.

Error Handling: Handle errors gracefully, but avoid exposing sensitive information in error messages. Log errors securely without revealing too much information to end-users.

Regular Updates and Patching: Keep all software components, including libraries, frameworks, and dependencies, up to date to address known vulnerabilities promptly. Regularly check for security updates and patches.

Security Headers: Utilise security headers (e.g., Content Security Policy, Strict Transport Security) to enhance the security of web applications and protect against common web-based attacks.

Code Reviews and Security Audits: Conduct regular code reviews with a focus on security, and perform security audits to identify and address potential vulnerabilities. Peer reviews and third-party security assessments contribute to the overall security of the codebase.

Least Privilege Principle: Follow the principle of least privilege, granting users and processes only the minimum permissions required to perform their tasks. Limit access to sensitive resources.

Data Encryption: Encrypt sensitive data at rest and in transit. Use encryption algorithms of industry-standard to protect data from unauthorised access.

Dependency Management: Regularly update and monitor third-party libraries and dependencies. Be cautious about using deprecated or unsupported libraries that may have security vulnerabilities.

Security Education and Training: Provide ongoing security education and training for development teams. Promote a security-aware culture and keep developers informed about the latest security threats and best practices.

These secure coding practices contribute to building a robust defense against common security threats and help create software that prioritises the confidentiality, integrity, and availability of data. Always adapt these practices to the specific requirements and context of your development environment.

Conduct regular code reviews with a focus on security, and perform security audits to identify and address potential vulnerabilities.

Regularly update and monitor third-party libraries and dependencies. Be cautious about using deprecated or unsupported libraries that may have security vulnerabilities.

Please refer page 30, 31 & 32 for reference.

Shadow AI-Latest Cybersecurity Threat

South Zone, NCIIPC

As AI advances, so does the dark side of AI, called "Shadow AI". This could lead to a cybersecurity crisis nightmare that can endanger the security of an organisation.

Technology changes rapidly and new technical applications appear from time to time. While these applications have become a boon for individuals and businesses, some of them have also created various problems and threats. Cyber-attacks against various critical sectors have increased significantly. These cyber-attacks affected many organisations in various countries in Asia, Europe and America. In particular, ministries were the target of these attacks. Data theft, phishing, social engineering, insider threats, email compromises and code misconfigurations have been prevalent trends in the past decade. To improve their attacks, threat actors use various new emerging techniques to evade security software and infect the network and systems with new malware. AI is becoming a trusted ally supporting both human and business activities. As AI advances, so does the dark side of AI, called "Shadow AI". This could lead to a cybersecurity crisis nightmare that can endanger the security of an organisation. Many users are undoubtedly experimenting with Generative Artificial Intelligence (GenAI) applications such as ChatGPT and Google Bard to see how these tools can help them to do their jobs more efficiently and effectively. Shadow AI can be accidentally or intentionally installed on devices and networks, compromising people's privacy and using sensitive information without their knowledge. Artificial intelligence systems can collect and analyse large amounts of private or sensitive data through data mining and profiling. This is a handy tool that can be used for any attack by a malicious actor, whether it is searching for targets, capturing important data, mapping a network or mining emails to learn to impersonate any user.

Shadow AI can be accidentally or intentionally installed on devices and networks, compromising people's privacy and using sensitive information without their knowledge.

Challenges Thrown Up by Shadow AI:

- Identity Fraud: Because AI privacy applications are complex and adaptive, the hackers can impersonate authorized users or employees. This can be caused by identity theft and illegal access to networks, systems and private information.
- Cybersecurity risk: Deployment of AI for coding is a popular use case, but if used by IT support, the code may contain AI-generated bugs that allow hackers to bypass the security protocols.
- Operational dangers: An AI shadow tool with insufficient training could produce inaccurate data that could impact the decision-making ability of a business.

Manage the risks of shadow AI: As artificial intelligence grows in popularity, the potential for shadow AI to introduce cybersecurity vulnerabilities and cyber security issues increases. Therefore, it has become crucial for organisations to adapt to the changing

Please refer page 30, 31 & 32 for reference.

environment and be alert to prevent such threats. The following steps can help organisations manage shadow AI risks:

- Data classification: Categorise each data asset based on its nature, sensitivity, and organisational value. A company may better understand the value of its data, whether it is at danger, and what controls need to be put in place to lessen those risks by using effective data categorisation. An organisation may choose to allow the use of consumer chatbots, but only for projects involving publicly available information. Instead, sensitive data can be restricted by local AI implementations.
- Create policies for the acceptable use of artificial intelligence: Create guidelines that limit the use of AI to specific tasks in specific roles.
- Educate and train employees: AI policies are useless if employees are not aware of or understand them. With this in mind, prioritise training on the safe use of GenAI, either as part of ongoing cybersecurity training or as a stand-alone initiative. Training should also communicate the risks of using AI, with a particular focus on data protection and compliance requirements.
- Visibility: To ensure that sensitive data kept in shadow databases is not misplaced or misused, it is imperative that enterprises identify and maintain visibility over every data repository in their environments.
- Monitoring and analytics: Organisations must also put in place data analytics and monitoring tools that can identify risks like unusual activity, compromised data and account creation that seems suspicious, or privilege escalation.
- Access Controls: Ensure that only authorised individuals have access to AI technologies. Use role-based access control when you want to limit access to only people who need it for their work.
- Regular Audits: The audits should be done on a regular basis.

AI policies are useless if employees are not aware of or understand them. With this in mind, prioritise training on the safe use of GenAI, either as part of ongoing cybersecurity training or as a stand-alone initiative.

Ensure that only authorised individuals have access to AI technologies. Use role-based access control when you want to limit access to only people who need it for their work.

By adopting a proactive and collaborative approach, companies can effectively reduce the risks associated with shadow AI and focus on leveraging the benefits of AI for continued sustainability growth and progress.

Shadow AI in the future: It is now obvious that the usage of AI will grow much more as workforces and possibilities rise. Thus, managing shadow AI will provide enterprises with yet another challenge. As the usage of AI tools intensifies, organisations lacking an insider risk strategy will face significant challenges in the future as the use of AI technologies increases.

Please refer page 30, 31 & 32 for reference.

NIST Offers Concrete Steps for Secure Software Development

This guidance aligns with NIST's Secure Software Development Framework and the 2021 cybersecurity executive order, providing a roadmap for the latest set of recommendations derived from industry input.

The National Institute of Standards and Technology (NIST) has issued crucial guidance, SP 800-204D, offering tangible steps to enhance the security of software supply chains. Aimed at software providers, the guidelines emphasise the integration of security measures throughout the software development life cycle, specifically within continuous integration and continuous delivery pipelines. Recommendations include the establishment of baseline security requirements for incorporating open-source software and an expanded focus on overseeing provenance data. This guidance aligns with NIST's Secure Software Development Framework and the 2021 cybersecurity executive order, providing a roadmap for the latest set of recommendations derived from industry input. Unlike previous high-level guidelines, the new measures detailed in SP 800-204D offer manufacturers a comprehensive set of actions to fortify supply chain security, including continuous scanning for known vulnerabilities and malware during pipeline execution. As federal software providers prepare to attest to their system's secure development, this guidance provides essential steps to adhere to NIST standards and bolster overall cybersecurity.

CISA Releases Water Vulnerability Scanning Fact Sheet

Regularly backing up OT/IT systems and adhering to best practices such as the NIST 3-2-1 rule for backups safeguards against data loss and facilitates recovery in the event of a compromise.

Water systems face significant cybersecurity risks, prompting the need for proactive measures to mitigate vulnerabilities. The fact sheet outlines key actions that water systems can take to enhance their cybersecurity posture. Reducing exposure to the public-facing internet through cyber hygiene services and vulnerability scanning helps minimise risks associated with internet-connected assets. Conducting regular cybersecurity assessments enables the identification and prioritization of vulnerabilities within Operational Technology (OT) and Information Technology (IT) systems. Changing default passwords and implementing MultiFactor Authentication (MFA) strengthens access controls and reduces the likelihood of unauthorised access. Creating an inventory of OT/IT assets facilitates better understanding and protection of critical infrastructure. Developing and exercising cybersecurity incident response and recovery plans ensures readiness to effectively respond to cyber incidents. Regularly backing up OT/IT systems and adhering to best practices such as the NIST 3-2-1 rule for backups safeguards against data loss and facilitates recovery in the event of a compromise. Additionally, reducing exposure to vulnerabilities through timely patching and keeping systems up to date enhances overall security. Lastly, conducting cybersecurity awareness training educates employees on cybersecurity best practices, empowering them to recognise and mitigate cyber threats effectively. By implementing these actions and leveraging the free resources provided, water systems can bolster their resilience against cyberattacks and safeguard critical water infrastructure.

*Please refer page 30, 31 & 32 for reference.

Safeguarding Against Phishing: Avoid Becoming a Victim

Social Engineering Protection Team, NCIIPC

In the digital age, where technology plays a pivotal role in our daily lives, the threat of phishing has become more prevalent than ever. Phishing attacks targeting unsuspecting individuals, aiming to trick them into divulging sensitive information. It is essential to implement secure practices that will enable you to safely traverse the online environment in order to strengthen your defenses against these adverse attempts.

Stay Informed and Educated: Knowledge is your first line of defense. Stay informed about the latest phishing techniques and scams. Regularly educate yourself and your teams on changing strategies that cybercriminals use.

Verify email addresses and look for subtle discrepancies in domain names or sender information that may indicate a phishing attempt.

Verify Emails and Sender Information: Before clicking on any links or providing personal information, verify the sender's identity twice. Verify email addresses and look for subtle discrepancies in domain names or sender information that may indicate a phishing attempt.

Use Multi-Factor Authentication (MFA): By requiring multiple kinds of proof of identity from users, multi-factor authentication offers an additional degree of security. To gain access, a hacker would still want extra authorisation details even if they managed to obtain someone's password.

Update your antivirus, operating system, and other security products on a regular basis.

Keep Software and Security Systems Updated: Update your antivirus, operating system, and other security products on a regular basis. These updates often include patches for potential vulnerabilities, making it more difficult for hackers to take advantage of holes within a system.

Be Cautious with Hyperlinks and Attachments: Be cautious about clicking on shady links or download attachments from unfamiliar sources. Hover over hyperlinks to preview the URL before clicking, and see the legitimacy of the website. Legitimate organisations are unlikely to request private details through email.

Employ Email Filtering and Security Software: Utilise email filtering tools and security software to effectively identify and block phishing attempts. These technologies can offer an extra degree of security by assisting in preventing fraudulent emails from arriving in your inbox.

Keep a close eye on your bank and credit card statements once in a while. Report any unauthorised transactions immediately.

Regularly Monitor Financial Statements: Keep a close eye on your bank and credit card statements once in a while. Report any unauthorised transactions immediately. Early detection of anomalous activity can prevent further financial damage and help trace the source of the phishing attack.

Secure Your Personal Information: Be cautious about sharing personal information online. Avoid posting sensitive details on social media platforms, as data gathered from online/open sources may potentially produce actionable intelligence for cybercriminals to use. Since, they often use this information to tailor their phishing attacks.

Please refer page 30, 31 & 32 for reference.

Train Employees and Colleagues: If you're part of a team or organisation, conduct regular cybersecurity training sessions to ensure everyone is aware of phishing threats and knows how to how to spot and react to any potential attack.

If you receive a suspicious email or encounter a potentially malicious website, report it to your IT department, email provider, or relevant authorities as soon as possible.

Report Suspected Phishing Attempts: If you receive a suspicious email or encounter a potentially malicious website, report it to your IT department, email provider, or relevant authorities as soon as possible. By reporting these events, we can contribute and strengthen the broader effort to fight against cybercrime as well as getting authorities updated about the novel approaches.

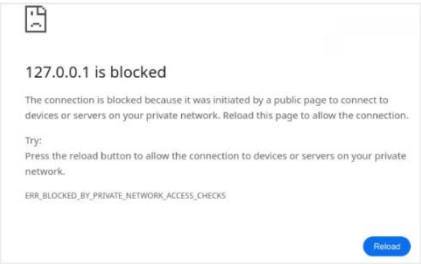
Implement DMARC: Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC) and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.

Beware of Short URLs: Beware that criminals use shortened URLs to direct people to phishing sites and initiate malware downloads.

By adopting these secure practices, you can significantly reduce the risk of falling victim to phishing attacks. Constant vigilance, education, and the implementation of robust security measures are essential in safeguarding your personal and professional information in the ever-evolving digital landscape. Stay informed, stay cautious, and stay secure.

Trends

Google Chrome Feature Blocks Attacks Against Home Networks



Google blocks web page reload request

Google is testing a new feature aimed at safeguarding users' private networks from malicious websites' potential exploits. The initiative seeks to address vulnerabilities in devices and servers within private networks, traditionally considered safe from internet-based threats. It aims to prevent unauthorised access to routers and software interfaces on local devices, particularly concerning as more applications deploy web interfaces lacking adequate protections. Initially explored in 2021, the feature aims to prevent external websites from making harmful requests to resources within private networks, such as localhost or private IP addresses. During the warning stage, even if the checks fail, the feature won't immediately block the requests. Instead, developers will receive a warning in the DevTools console, giving them time to make adjustments before stricter enforcement takes effect. While the primary focus is on mitigating risks like "SOHO Pharming" attacks and CSRF vulnerabilities, the current specification does not extend to securing HTTPS connections for local services, deemed necessary for integrating public and non-public resources securely. This ongoing development underscores Google's commitment to enhancing internet security and protecting users from evolving cyber threats.

The initiative seeks to address vulnerabilities in devices and servers within private networks, traditionally considered safe from internet-based threats.

Please refer page 30, 31 & 32 for reference.

Surge in Ransomware via AI

UK National Cyber Security Centre (NCSC), has issued a warning about the increasing threat of ransomware attacks fueled by advancements in Artificial Intelligence (AI) technology. The NCSC's assessment, drawn from classified intelligence and other sources, predicts a rise in both the frequency and impact of such attacks over the next two years. AI tools are anticipated to enhance various aspects of cyber operations, including reconnaissance, social engineering, malware development, and exploit creation. However, the NCSC suggests that sophisticated AI-driven attacks will likely remain accessible primarily to well-resourced threat actors until at least 2025. The effectiveness of AI in cyber operations hinges on the availability of high-quality data for training purposes. As successful hacks yield more data, threat actors can train increasingly sophisticated AI models, perpetuating a cycle of more effective cyber attacks. The assessment points out that ransomware attacks against British organisations have surged, with 874 incidents recorded in the first three quarters of 2023, compared to 739 for the entirety of 2022. James Babbage of the National Crime Agency emphasises that AI advancements lower the entry barriers for cybercriminals and enhance the speed and scale of their attacks. While AI's role in cyber attacks is seen as evolutionary rather than revolutionary, the NCSC emphasises the importance of adopting secure-by-design practices and following cybersecurity hygiene advice to bolster defences against ransomware and other cyber threats.

AI tools are anticipated to enhance various aspects of cyber operations, including reconnaissance, social engineering, malware development, and exploit creation.

Tech Giants Form Post-Quantum Cryptography Alliance

The Linux Foundation has announced the formation of the Post-Quantum Cryptography Alliance (PQCA), with key members including AWS, Cisco, IBM, and Nvidia. This alliance aims to drive the adoption and development of post-quantum cryptography, addressing the security challenges posed by quantum computing. Quantum computing threatens current security measures by potentially enabling rapid decryption of existing keys. Thus, securing data and communications in the post-quantum era becomes crucial, and the PQCA intends to tackle this issue. The alliance will work on standardised and post-quantum algorithms to support organisations aligning with the Commercial National Security Algorithm Suite 2.0. It plans to engage in technical projects such as developing software for evaluating and deploying post-quantum algorithms. Founding members have been active in post-quantum cryptography standardisation, contributing to the NIST Post-Quantum Cryptography Standardization Project. Projects like the Open Quantum Safe and PQ Code Package will be part of PQCA's initiatives. The launch of PQCA follows IBM's roadmap for post-quantum computing migration and guidance from UK and US government agencies, indicating growing awareness and efforts to prepare for the post-quantum era.

The alliance will work on standardised and post-quantum algorithms to support organisations aligning with the Commercial National Security Algorithm Suite 2.0.

Please refer page 30, 31 & 32 for reference.

Vulnerability Watch

SSH Protocol Found Vulnerable to New Terrapin Attack

Strategic & Public Enterprises Sector, NCIIPC

The Terrapin vulnerability allows attackers to manipulate the sequence numbers and remove/extract messages from servers and clients at the time of SSH handshake protocol by compromising the secure channel integrity.

The widely used protocol for secure communication over the internet is SSH. SSH is used for remote accessing and controlling of servers, transfer of files and encrypt data. However, SSH is not immune to attacks. Security researchers have found a recent vulnerability in OpenSSH version prior 9.6 (CVE-2023-48795), that has exposed a serious flaw in the protocol. The vulnerability is known as Terrapin attack, that can truncate cryptographic information thereby degrading the security of SSH connections. The Terrapin vulnerability allows attackers to manipulate the sequence numbers and remove/extract messages from servers and clients at the time of SSH handshake protocol by compromising the secure channel integrity. Its difficult to detect such attacks since the structure or integrity of cryptographic information of the handshake is not altered. This attack downgrades the authentication methods resulting in weakness of algorithms and disabling protections against keystrokes timing attacks. The terrapin attacks primarily affect:

- SSH servers and clients using vulnerable encryption modes: ChaCha20-Poly1305 and CBC with Encrypt-then-MAC are the main targets.
- Older versions of OpenSSH and Dropbear: versions prior to OpenSSH 9.6 and Dropbear 2022.83 are particularly at risk.

Impact: The potential consequences of the Terrapin attack could be severe, such as:

- Unauthorised Access: Exploiting of password and using them for malicious activities.
- Data breaches: Critical/sensitive information could be leaked or stolen from the vulnerable systems/servers.
- Financial losses: Damage to systems/assets or service interruptions or ransom demand or extortion of money from you.
- Reputation damage: The attack might lead to data leaks that can cause the loss of trust/damage an organisation reputation.

Avoid the usage of vulnerable encryption modes such as ChaCha20-Poly1305 or CBC with Encrypt-then-MAC on both client and server configurations.

Protection Strategies against the Terrapin attack: The following protection strategies may be implemented to avoid the Terrapin attack.

- Immediately update the OpenSSH and other SSH implementations to the latest versions.
- Avoid the usage of vulnerable encryption modes such as ChaCha20-Poly1305 or CBC with Encrypt-then-MAC on both client and server configurations.
- Ensure both client and server support a strict key exchange which is a crucial step that prevents the attack.

*Please refer page 30, 31 & 32 for reference.

- Usage of weak or default passwords should be avoided that can be easily guessed by the attacker. Also, public key (verified and trusted) authentication can be used instead of password authentication.
- Implement a strict security policy on the local networks and monitor the network traffic using tools and IDS particularly around SSH connections.

Usage of a VPN or a firewall to encrypt and protect the SSH traffic from being intercepted and modified by the attacker.

Critical RCE Vulnerabilities in Apache RocketMQ Servers

Security researchers have identified critical vulnerabilities CVE-2023-33246 and CVE-2023-37582, which pose a remote command execution (RCE) risk in Apache RocketMQ servers. A patch was released by Apache for CVE-2023-33246, but it was insufficient for the NameServer component in RocketMQ, continuing to affect versions 5.1 and older. The issue has evolved and is now also tracked as CVE-2023-37582. It is recommended to upgrade the NameServer to version 5.1.2/4.9.7 or above for RocketMQ 5.x/4.x to avoid attacks exploiting the vulnerability. Organisations using Apache RocketMQ should prioritise upgrading their systems and strengthen their security posture to defend against these active threats.

A patch was released by Apache for CVE-2023-33246, but it was insufficient for the NameServer component in RocketMQ, continuing to affect versions 5.1 and older.

Critical Vulnerability in Cisco Products

Critical Remote Code Execution (RCE) vulnerability has been discovered in multiple Cisco Unified Communications and Contact Center Solutions products. This remote code execution vulnerability has CVE ID CVE-2024-20253 having CVSS score 9.9. Due to the improper processing of user-provided data that is being read into memory it leads to RCE vulnerability. A successful exploit could allow an attacker to run arbitrary commands on the underlying operating system with the privileges of the web services user. Software patches from Cisco are available to fix this vulnerability.

Critical Vulnerability in Fortinet Products

Critical out-of-bounds write vulnerability was discovered in FortiOS and FortiProxy. This vulnerability, having CVE ID CVE-2024-21762 and CVSS score 9.8, allows a remote unauthenticated attacker to execute code or commands remotely using maliciously crafted HTTP requests. It is recommended to follow the vendor's instructions to apply mitigations or discontinue use of the product if mitigations are unavailable.

Please refer page 30, 31 & 32 for reference.

Vulnerability in Hugging Face AI Models

It is recommended to follow the vendor's instructions to apply mitigations or discontinue use of the product if mitigations are unavailable.

Researchers have found that it is possible to compromise the Hugging Face Safetensors conversion service to ultimately hijack the models submitted by users and result in supply chain attacks. Hugging Face is a well-known platform that facilitates the hosting, creation, deployment and training of pre-trained machine learning models and datasets. The threat actors have weaponised Safetensors to execute arbitrary code and deploy Cobalt Strike, Mythic, and Metasploit stagers. Researchers of HiddenLayer has found that it's hypothetically possible for an attacker to hijack the hosted conversion service using a malicious PyTorch binary and compromise the system hosting it.

Critical Vulnerability in ConnectWise ScreenConnect

This vulnerability having CVE ID CVE-2024-1709 and CVSS score 10.0 allow an attacker direct access to confidential information or critical systems.

Critical authentication bypass using an alternate path or channel vulnerability was discovered in ConnectWise ScreenConnect, a self-hosted remote desktop software application. This vulnerability having CVE ID CVE-2024-1709 and CVSS score 10.0 allow an attacker direct access to confidential information or critical systems. The affected versions are ScreenConnect 23.9.7 and prior. ConnectWise has provided the patch for all on-premise versions of ScreenConnect 23.9.7 and below and the cloud instances were automatically patched.

Critical Vulnerability in Weston Embedded Server

The overflow occured while parsing the protocol version of an HTTP request when the adversary sends a malicious packet to the targeted machine.

Critical heap-based buffer overflow vulnerability was discovered in the HTTP server functionality of Weston Embedded uC-HTTP git commit 80d4004. Weston Embedded Solutions is a provider of embedded software and engineering services that specialises in the Micrium RTOS family of products. The heap-based buffer overflow vulnerability has been assigned CVE ID CVE-2023-45318 and CVSS score 10.0. The overflow occured while parsing the protocol version of an HTTP request when the adversary sends a malicious packet to the targeted machine.

Critical Vulnerability in Torrentpier

The affected Torrentpier allows an attacker to obtain RCE on the server, which was made possible by deserialising arbitrary data sent by the user.

Critical insecure deserialisation vulnerability was discovered in Torrentpier. The vulnerability was assigned CVE ID CVE-2024-1651 having CVSS score 10.0. TorrentPier is a BitTorrent tracker and indexer engine. The affected version is Torrentpier version 2.4.1. The affected Torrentpier allows an attacker to obtain RCE on the server, which was made possible by deserialising arbitrary data sent by the user.

Please refer page 30, 31 & 32 for reference.

Critical Vulnerability in Loomio

Critical OS command injection vulnerability was discovered in Loomio, a decision-making software and web service. The vulnerability has CVE ID CVE-2024-1297 with CVSS score 10.0. The affected version is Loomio version 2.22.0. To remediate this vulnerability, it is recommended to update Loomio to a patched version that addresses this vulnerability. Failure to address this vulnerability can result in unauthorised access and control over the server, potentially leading to further compromise and data breaches.

Failure to address this vulnerability can result in unauthorised access and control over the server, potentially leading to further compromise and data breaches.

Critical Vulnerability in Jenkins

A critical vulnerability was discovered in the built-in Command Line Interface (CLI) of Jenkins that allows attackers to obtain cryptographic keys, which leads to remote code execution. This vulnerability has CVE ID CVE-2024-23897 and it affects Jenkins 2.441 and earlier and LTS 2.426.2 and earlier, because the command parser (the args4j library) has a feature where an '@' character followed by a file path in an argument is replaced with the file's content. Jenkins 2.442 and LTS 2.426.3 resolve this vulnerability by disabling the command parser feature.

Jenkins

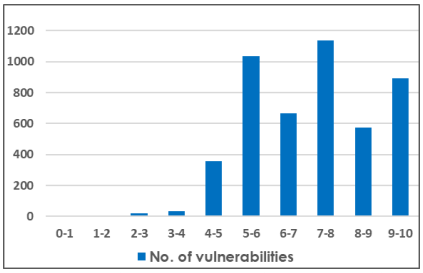
Jenkins 2.442 and LTS 2.426.3 resolve this vulnerability by disabling the command parser feature.

Quarterly Vulnerability Analysis Report

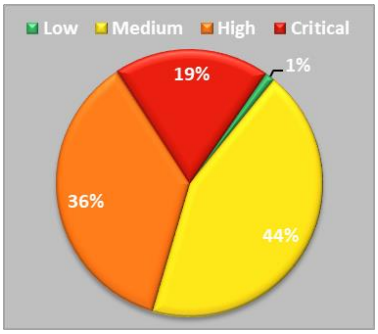
Knowledge Management Team, NCIIPC

During the first quarter of 2024, a total of 4718 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 19 percent of total vulnerabilities reported were of critical severity. Google, Adobe, Microsoft, IBM and unisoc were the top five vendors having 19% of total reported vulnerabilities.

Severity	CVSSv 3 Score	Number of Vulnerabilities			Total Vulnerabilities	Severity Total
		Dec'23	Jan'24	Feb'24		
Low	0-1	0	0	0	0	55
	1-2	0	0	0	0	
	2-3	10	7	2	19	
	3-4	10	21	5	36	
Medium	4-5	156	119	82	357	2059
	5-6	529	317	191	1037	
	6-7	276	291	98	665	
High	7-8	439	487	212	1138	1711
	8-9	285	191	97	573	
Critical	9-10	382	348	163	893	893
Total		2087	1781	850		4718

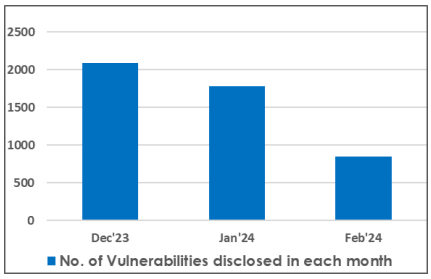


Severity-wise number of vulnerabilities

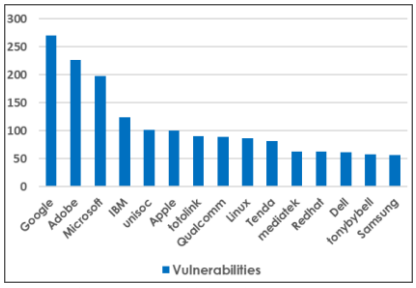


Severity-wise share of vulnerabilities

Please refer page 30, 31 & 32 for reference.



No. of vulnerabilities disclosed in each month



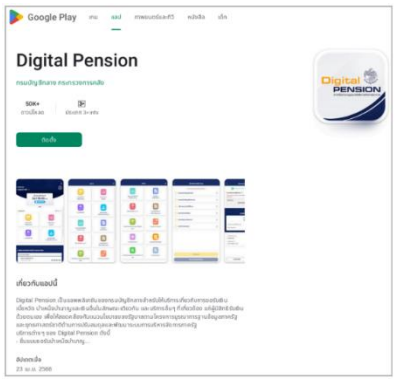
Count of vulnerabilities for top 15 vendors

S. No.	Vendor	No. of Vulnerabilities			Total
		Dec'23	Jan'24	Feb'24	
1.	Google	196	58	16	270
2.	Adobe	220	6	0	226
3.	Microsoft	118	71	9	198
4.	IBM	50	23	51	124
5.	unisoc	80	21	0	101
6.	Apple	56	42	2	100
7.	totolink	32	58	0	90
8.	Qualcomm	38	25	26	89
9.	Linux	29	41	17	87
10.	Tenda	47	33	1	81
11.	mediatek	30	20	13	63
12.	Redhat	29	23	11	63
13.	Dell	32	3	27	62
14.	tonybybell	0	58	0	58
15.	Samsung	30	8	19	57

Mobile Security

Goldpickaxe Steal Faces to Defeat Biometrics in iOS & Android

Security researchers at Group-IB have discovered a new trojan for android and iOS trojan named 'GoldPickaxe', developed by Chinese hacking group GoldFactory,' which is also responsible for malware like 'GoldDiggerPlus', 'GoldKefu' and 'GoldDigger'. This trojan trick users into scanning their faces and IDs and ultimately log in to their bank accounts. It was observed that distribution of GoldPickaxe had started in the month of October 2023 and primarily targeted Thailand and Vietnam. These threat actors approached the victims though phishing messages, impersonating government authorities or services and make them install fake apps like 'Digital Pension'. Once installed the trojan takes the control over the user's phone by passing the biometric security checks and ultimately gets the access over the victim's bank accounts.



Malicious app hosted on a fake Google Play website

MoqHao Malware Variant Unveiled with Auto-Execution Feature

Security experts have detected a new type of Android malware called MoqHao, which operates independently on compromised devices, removing the necessity for user involvement. According to a recent report by McAfee Labs, unlike typical MoqHao variants that require manual launch, this new iteration initiates malicious activity automatically upon installation. Primarily, the Android users in France, Germany, South Korea and Japan are targets of this campaign. MoqHao, also known as Wroba and XLoader, is linked to a financially motivated cybercrime group known as Roaming Mantis or Shaoye. Initial attack vectors involve SMS messages disguised as package delivery notifications, containing deceptive

Please refer page 30, 31 & 32 for reference.

links. Clicking these links on Android devices installs the malware, while iPhone users are redirected to counterfeit Apple iCloud login pages for credential theft. The latest variant employs smishing techniques for distribution, with a notable change being the automatic execution of the malicious payload upon installation. Additionally, the malware now requests risky permissions without launching the app, a tactic reminiscent of HiddenAds malware. To enhance effectiveness, attackers conceal SMS links using URL shorteners sourced from fraudulent Pinterest profiles. MoqHao is equipped with functionalities for data exfiltration, silent calls, and Wi-Fi manipulation, highlighting its sophisticated threat level.

The latest variant employs smishing techniques for distribution, with a notable change being the automatic execution of the malicious payload upon installation.

GrapheneOS: Prevents Firmware Exploit via Android Auto-Reboots

In the realm of mobile security, GrapheneOS continues to be at the forefront with its innovative approach to safeguarding Android devices. The latest advancement in its arsenal is the frequent auto-reboots, designed to thwart firmware-level exploits. When a mobile device is 'at rest,' it indicates that it's either powered off or hasn't been unlocked since booting up, ensuring high privacy protection. However, apps can't fully function in this state due to inaccessible encryption keys. Upon the first unlock post-reboot, cryptographic keys move to quick access memory, transitioning the device to a 'not at rest' state. GrapheneOS emphasises that locking the screen post-usage doesn't return the device to an 'at rest' state, as some security exemptions persist. Rebooting the device clears temporary states, processes, and activities, necessitating authentication to unlock and reactivate security mechanisms. While specific firmware exploits remain undisclosed, GrapheneOS suggests a generic mitigation: an auto-reboot feature. This feature, integrated into their OS, aims to minimize attackers' window of opportunity by resetting device protections more frequently than typical user-initiated reboots. Currently set at 72 hours, GrapheneOS plans to shorten the auto-reboot interval to 18 hours.

GrapheneOS emphasises that locking the screen post-usage doesn't return the device to an 'at rest' state, as some security exemptions persist.

Please refer page 30, 31 & 32 for reference.

NCIIPC Initiatives

Sh. Ankit Sarkar, Director NCIIPC at Pentathon 2024 (Kolkata)

Sh. Akhilesh Variar, Director NCIIPC at Pentathon 2024 (Mysuru)

Sh. Leeladhar Meena, Director West NCIIPC at Pentathon 2024 (Ahemdabad)

Sh. Akhilesh Variar, Director NCIIPC at Pentathon 2024 (Chennai)

NCIIPC AICTE Pentathon 2024

NCIIPC in collaboration with All India Council for Technical Education (AICTE) and MoE's Innovation Cell (MIC) conducted India's first national level VAPT 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 Critical Information Infrastructure (CII) entities. The objective of this exercise was to create a talented pool of ethical hackers/pen testers for finding vulnerabilities in the systems of CII.

The first awareness workshop on the Cyber Security, Ethical Hacking and Information Dissemination on the Pentathon was held in Kolkata at RCC Institute of Information Technology on 6th March 2024. Sh. Ankit Sarkar, Director NCIIPC delivered sessions on cyber security, ethical hacking along with tools used in ethical hacking and various types of VAPT exercises. More than 300 participants including the students and faculty from various Higher Education Institutions and Master trainers from Centre for Development of Advanced Computing (C-DAC) attended the workshop.

The second workshop on Cyber Security, Ethical Hacking and Information Dissemination for Pentathon 2024 was organised om 7th March 2024 at The National Institute of Engineering, Mysuru. Sh. Akhilesh Variar, Director NCIIPC assisted by Sh. Sarim Moin and Sh. Ankush Sharma, Innovation Officers addressed and engaged more than 300 students and faculty participants from Karnataka, Kerala and Tamil Nadu.

Third awareness workshop on the Cyber Security, Ethical Hacking and Information Dissemination on the Pentathon was organised on 9th March 2024 at Entrepreneurship Development Institute of India, Ahmedabad. More than 280 participants including the students and faculty from various HEIs attended the workshop. Sh. Leeladhar Meena, Director West NCIIPC, delivered lecture on VAPT exercises, cyber security, ethical hacking along with tools used in ethical hacking and various types of VAPT excercise and how to approach in certain situations.

The fourth awareness workshop on Cyber Security, Ethical Hacking, and Information Dissemination took place on 11th March 2024 at St. Joseph's Institute of Technology, OMR, Chennai. Over 350 enthusiastic participants, including students and faculty from various institutions across different states, attended the event. Sh. Akhilesh Variar, Director NCIIPC, interacted with participants from various sectors, addressed their queries regarding VAPT, cybersecurity, and ethical hacking, and emphasised the importance of participation in PENTATHON 2024. Mrs. Kalpana B N delivered a lecture on VAPT exercises, cybersecurity, and ethical

Please refer page 30, 31 & 32 for reference.

hacking, discussing tools and their applications in various types of VAPT exercises.

The fifth awareness workshop on the Cyber Security, Ethical Hacking and Information Dissemination was held on 13th March 2024 at CMR college of Engineering & Technology, Kandlakoya, Hyderabad. More than 450 participants from various HEIs attended the workshop. Dr. Punyban Patel, Professor from CSE (Cyber Security dept) by giving his insights and shared his experience on Cybercrime and Awareness session on Cyber Security. Sh. Surendra Kumar, Director NCIIPC, delivered lecture on VAPT exercises, cyber security and ethical hacking.

Sh. Surendra Kumar, Director NCIIPC at Pentathon 2024 (Hyderabad)

NCIIPC Organised Pentesting Exercise

NCIIPC organised a Pentesting Exercise from 11-28 March 2024, where it invited expert pen testers, security researchers and ethical hackers to participate in securing nation's Critical Information Infrastructure (CII) and win handsome prizes. Around 70 experts participated in this exercise of testing the security of CII systems in a controlled environment, as individuals or as a team. The top performers were rewarded up to Rs. 10 lakhs and Commendation Certificates were given based on the severity/ impact of the vulnerabilities found out by them.

NCIIPC Organised Pentesting Exercise

NCIIPC Organised 'CII SECEX: 2024'

NCIIPC organised the Critical Information Infrastructure Security Exercise, 'CII SECEX: 2024', a 10 days' event during 5-14 April 2024. The event saw a footfall of more than 550 participants from Critical Sector Entities (CSEs) across the country. The targeted audience were the officials of notified CIIs as well as officials of other important organisations of critical sectors which are yet to be notified as CII and Chief Information Security Officers (CISOs) of the Critical Sector Ministries.

This National Level Exercise was conducted in two tracks. The first track was Training cum Operational Exercise and second track was Strategic Exercise. The training cum Operation Exercise included key operational personnel (Junior & Middle level) from the Critical Sector Entities to participate. Further, the Senior level officers from the CII Entities were invited to participate in a two-day strategic policy level exercise, so that the Senior Management were aware of the Cyber security issues that could be encountered by their organisations and also get trained for right decision making. A CEO Level half day exercise was also conducted.

Stage1 (Training): 6-Day Training was organised for personnel from CSE entities across the nation at 4 NCIIPC locations viz: New Delhi, Mumbai, Kolkata and Bengaluru.


CII SECEX: 2024

Please refer page 30, 31 & 32 for reference.

Stage 2 (Operation Exercise): The participants who underwent training were given a hands-on experience through operation exercise conducted on 8th to 10th day by forming blue teams across all locations viz Delhi, Mumbai, Bengaluru and Kolkata. The personnel from CSEs participate as Blue Team and the platform providers and NCIIPC personnel acted as Red Team and White Team.

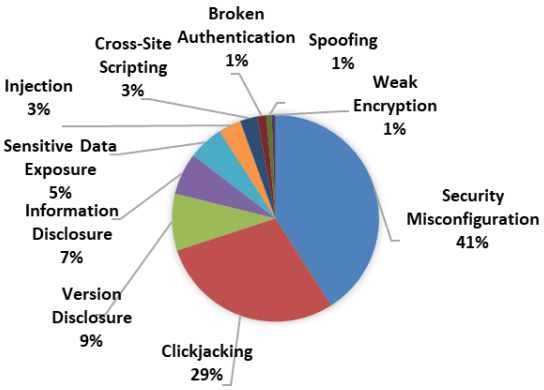
The participants were given hands-on experience that are customised to represent the real world IT and OT environments and recent challenges.

The Strategic Exercise was conducted on the Day 09 and 10 of the exercise. The senior decision makers from CSEs were provided with various real world like scenarios that the top-level management/decision makers from CSEs would encounter and have to take decision to protect their organisation's Critical Information Infrastructures.

Nearly 30 CEOs from CSEs participated in discussions and brainstorming session on various teething issues faced by the senior most management of the CSEs.

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 1102 vulnerabilities reported during the first quarter of 2024. The top 10 vulnerabilities are:

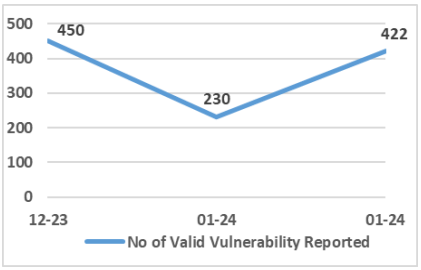


- Security Misconfiguration
- Clickjacking
- Version Disclosure
- Information Disclosure
- Sensitive Data Exposure
- Injection
- Cross-Site Scripting
- Broken Authentication
- Spoofing
- Weak Encryption

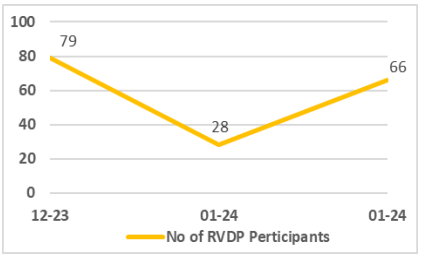
Please refer page 30, 31 & 32 for reference.

Around 173 security researchers participated in RVDP programme during the first quarter of 2024. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- 0x2458
- Abhishrey Gupta
- Ajay G
- Azif Mhammed K
- Chinmay Rana
- Joel I. Patrick
- Kiran Scaria
- Nimal Joseph Devassy
- No Name
- No Name
- Pratik Shirsat
- Sandeep Vishwakarma
- Siddharth Tayade
- Soorya Narayanan AU
- Vaishakhi



Last three months' timeline chart for vulnerabilities reported



Last three months' timeline chart for RVDP participants

*Please refer page 30, 31 & 32 for reference.

Upcoming Events - Global

APRIL 2024

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				

MAY 2024

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	

April 2024

- Public Sector Cybersecurity Summit, Johannesburg — 3 Apr
- Cyber Security for Critical Assets APAC 2024, Singapore — 3-4 April
- SecureWorld Houston, Houston — 4 Apr
- CyberTech Global Tel Aviv 2024, Tel Aviv — 8-10 Apr
- Southeast Cybersecurity Summit 2024, Birmingham — 10-11 Apr
- Dallas Cybersecurity Summit, Dallas — 12 Apr
- Qubit Conference, Prague — 22-24 Apr
- National Cyber Security Show 2024, Birmingham — 30 Apr-2 May

May 2024

- Minneapolis Cybersecurity Conference, Minneapolis — 2 May
- Data Innovation Summit, Dubai — 8-9 May
- CISO Brazil, Sao Paulo — 14-15 May
- AI Cybersecurity Leadership Forum, Chicago — 16 May
- Cyber Risk Summit, San Diego — 20-22 May
- Gartner Data & Analytics Summit, Tokyo — 21-23 May
- Nordic IT Cybersecurity Conference 2024, — 23 May
- SecureWorld Miami, Miami — 30 May

June 2024

- Cyber Security for Government Summit, Canberra — 5-7 Jun
- FIRST Conference 2024, Fukuoka — 9-14 Jun
- Cyber Security for Critical Assets Canada 2024, Canada — 12 Jun
- ICS Security Summit & Training 2024, Orlando — 16 Jun
- OT Cybersecurity Summit, London — 18-19 Jun
- INTERFACE Phoenix 2024, Scottsdale — 21 Jun
- 23rd European Conference on Cyber Warfare and Security, Jyväskylä — 27-28 Jun
- Security BSides Athens 2024, Athens — 29 Jun

July 2024

- PhilSec Cyber Security Summit 2024, Philippines 2-3 Jul
- FinCrime & Cybersecurity Summit, Sydney 4 Jul
- DFRWS USA 2024, Louisiana 9-12 Jul
- INTERFACE Salt Lake City 2024, Salt Lake City 11 Jul
- Healthcare Cybersecurity Summit: New York, New York 18 Jul
- Cyber Strategy Retreat 2024, Atlanta 24-25 Jul
- Cyber Security Expo, Manchester 24 Jul

Upcoming Events - India

- Gartner Data & Analytics Summit, Mumbai 24-25 Apr
- Global Legal ConfEx New Delhi 2024, New Delhi 25 Apr
- Cyber Revolution Summit: India 2024, New Delhi 25-26 Apr
- Cybersecurity Summit: Bengaluru, Bengaluru 2 May
- Global Legal ConfEx New Delhi 2024, Mumbai 12 Jun
- BSides Bangalore Cybersecurity Conference, Bengaluru 28 Jun
- Meridian Conference 2024, New Delhi 3-6 Jul

JUNE 2024

S	M	T	W	T	F	S
30						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

JULY 2024

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			

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

- AICTE: All India Council for Technical Education
- BGP: Border Gateway Protocol
- C2: Command and Control
- CVE: Common Vulnerabilities and Exposures
- CVSS: Common Vulnerability Scoring System
- GenAI: Generative Artificial Intelligence
- IT: Information Technology
- MaaS: Malware-as-a-Service
- MFA: Multifactor Authentication
- MIC: MoE's Innovation Cell
- NCSC: National Cyber Security Centre
- NIST: National Institute of Standards and Technology
- OT: Operational Technology
- PQCA: Post-Quantum Cryptography Alliance
- RBI: Reserve Bank of India
- RIPE: Réseaux IP Européens
- SOHO: Small Office and Home Office
- XSS: Cross-Site Scripting
- VAPT: Vulnerability Assessment and Penetration Testing
- CII: Critical Information Infrastructure
- CSE: Critical Sector Entities
- NCIIPC: National Critical Information Infrastructure
- CERT-In: Indian Computer Emergency Response Team

Sources

- **RBI's New IT Governance Guidelines for Financial Entities**
  https://rbidocs.rbi.org.in/
  https://www.rbi.org.in/
  https://www.dataguidance.com/
- **Department of Telecom Initiates Security Audit**
  https://dot.gov.in/
  https://i4c.mha.gov.in/
  https://telecom.economictimes.indiatimes.com/
- **Orange Spain's RIPE Account Hacked by Malware**
  https://thehackernews.com/
  https://www.ripe.net/
- **Anonymous Sudan Launched Cyberattack on Chad Telco**
  https://www.darkreading.com/
- **23andMe Data Breached**
  https://www.bleepingcomputer.com/
  https://www.23andme.com/en-int/
- **U.S. Feds/FBI Shut Down KV-Botnet & Mootbot Botnet**
  https://www.fbi.gov/history/seal-motto
  https://thehackernews.com/
  https://www.bleepingcomputer.com/
- **Warzone RAT Shut Down by Law Enforcement**
  https://www.securityweek.com/
- **LockBit Ransomware Disrupted by Global Police Operation**
  https://www.bleepingcomputer.com/
- **Change Healthcare Cyberattack**
  https://www.aha.org/
  https://www.cybersecuritydive.com/
- **European Diplomats Targeted by SPIKEDWINE with WINELOADER**
  https://www.zscaler.com/
  https://thehackernews.com/
- **New macOS Backdoor: SpectralBlur**
  https://thehackernews.com/
  https://www.securityweek.com/
- **TimbreStealer Malware Spreading via Tax-themed Phishing Scam**
  https://thehackernews.com/
  https://blog.talosintelligence.com/
- **IDAT Loader Attacks Use Steganography to Deploy Remcos RAT**
  https://thehackernews.com/
- **Malicious Excel document spreads Python Info-Stealer**
  https://www.fortinet.com/
  https://cyware.com/
  https://cybermaterial.com/
  https://izoologic.com/
- **Understanding the Role of CVEs in Cybersecurity**
  https://www.spiceworks.com/
  https://www.linkedin.com/

- **Safeguarding Against Phishing: Avoid Becoming a Victim**
  https://www.digitalguardian.com/
  https://www.valimail.com/guide-to-phishing/
  https://www.ncsc.gov.uk/guidance/phishing
- **Secure Coding Practices**
  https://owasp.org/
  https://kirkpatrickprice.com/blog/secure-coding-best-practices/
  https://owasp.org/
  https://www.codingdojo.com/blog/secure-coding-practices
  https://codesigningstore.com/
- **Shadow AI-Latest Cybersecurity Threat**
  https://www.helpnetsecurity.com/
  https://tech.co/news/what-is-shadow-ai
  https://www.techtarget.com/
- **NIST Offers Concrete Steps for Secure Software Development**
  https://www.bankinfosecurity.asia/
- **CISA Releases Water Vulnerability Scanning Fact Sheet**
  https://www.cisa.gov/
- **Google Chrome Feature Blocks Attacks Against Home Networks**
  https://www.bleepingcomputer.com/
- **British Intelligence Warns Surge in Ransomware via AI**
  https://therecord.media/
- **Tech Giants Form Post-Quantum Cryptography Alliance**
  https://www.securityweek.com/
- **Critical RCE Vulnerabilities in Apache RocketMQ Servers**
  https://op-c.net/
- **Critical Vulnerability in Cisco Products**
  https://sec.cloudapps.cisco.com/
  https://nvd.nist.gov/
- **Critical Vulnerability in Fortinet Products**
  https://www.bleepingcomputer.com/
  https://nvd.nist.gov/vuln/detail/CVE-2024-21762
  https://www.cvedetails.com/cve/CVE-2024-21762/
- **Vulnerability in Hugging Face AI Models**
  https://thehackernews.com/
  https://huggingface.co/
- **Critical Vulnerability in ConnectWise ScreenConnect**
  https://www.connectwise.com/
  https://nvd.nist.gov/vuln/detail/CVE-2024-1709
- **Critical Vulnerability in Weston Embedded Server**
  https://nvd.nist.gov/vuln/detail/CVE-2023-45318
  https://blog.talosintelligence.com/
  https://weston-embedded.com/
- **Critical Vulnerability in Torrentpier**
  https://nvd.nist.gov/vuln/detail/CVE-2024-1651
  https://fluidattacks.com/advisories/xavi/

- **Critical Vulnerability in Loomio**
  https://nvd.nist.gov/vuln/detail/CVE-2024-1297
  https://www.recordedfuture.com/
- **Critical Vulnerability in Jenkins**
  https://www.jenkins.io/security/advisory/2024-01-24/
  https://www.securityweek.com/
- **SSH Protocol Found Vulnerable to New Terrapin Attack**
  https://freemindtronic.com/
  https://thehackernews.com/
  https://www.spiceworks.com/
- **MoqHao Malware Variant Unveiled with Auto-Execution Feature**
  https://thehackernews.com/
- **GrapheneOS: Prevents Firmware Exploit via Android Auto-Reboots**
  https://www.bleepingcomputer.com/

Notes

National Critical Information Infrastructure Protection Centre

NCIIPC

सम्पूर्ण सुरक्षा

A unit of NTRO

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.