NEWSLETTER

July 2023

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

Email Security Best Practices

- Ensure Kavach Multi-Factor Authentication is configured for NIC email
- Download Kavach app from valid app store/website only
- Don't share email password/Kavach OTP with unauthorized person
- Don't use unauthorized/external email services for official communication
- Don't open any link/attachment sent by unknown sender
- Regularly review the past login activities on NIC's email service by clicking on the "login history" tab. If any discrepancy is observed, same should be reported immediately
- Use PGP/digital certificate to encrypt emails that contain important information
- Observe caution with downloaded documents containing macros. Select "disable macros" option and enable protected mode in office applications like MS Office, etc.

VOLUME 7 ISSUE 3

@NCIIPC

NCIIPC Newsletter

July 2023

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

Recently we have seen an upward trend in various cyber security incidents related to Indian entities. Various agencies of Government of India are proactively monitoring this situation and are taking necessary steps to mitigate these emerging threats. National Cyber Security Coordinator (NCSC) has recently announced the first version of National Cyber Security Reference Framework (NCRF) which will serve as a guideline document for Critical Sector Entities (CSE) to implement various cyber security related initiatives. This shall be a living document and will be updated on time-to-time basis as per the developments. Computer Emergency Response Team of India (CERT-In) has released an Information Security Practices guide for Government Entities. This document shall serve as a guiding document for information security implementation in Government organisations. This shall also be a reference document for conducting cyber security audit of these entities. Various Ministries, Departments and attached offices are under the scope of this document.

NCIIPC has also conducted various cyber security awareness programs in association with Critical Sector Entities (CSEs). A session was conducted for BSNL officials during a cyber security webinar conducted by BSNL for its staff members. Similarly, a session was organised for staff members of NTIPRIT. The other CSEs interested in conducting cyber security awareness sessions for their employees may reach out to NCIIPC.

The articles/feedback is solicited from the readers. Please do write to us on newsletter[at]nciipc[dot]gov[dot]in. The selected articles/feedback shall also be published in newsletter. Thank you for all your love and kind support.

News Snippets - National

NCSC Announces National Cybersecurity Reference Framework

Source: www.nationalheraldindia.com/, www.expresscomputer.in/

The National Cyber Security Coordinator Lt. Gen. Rajesh Pant announced the first version of the National Cybersecurity Reference Framework (NCRF) document that has been finalised and is ready for public release. NCRF is a structure guidance on cyber security to the critical sectors of the nation that includes power and energy, finance, telecom, transportation, strategic and government entities and health. The framework will serve as a guiding document for the critical sector entities to develop their governance and management systems as well as their architecture framework for both Information Technology and Operational technology systems. The NCRF can be used by organisations to strengthen their cybersecurity posture, lower their risk of data breach or any cybersecurity incident, ensure compliance with regulations, increase confidence with customers and enhance operational effectiveness. The NCRF will be a living document that will be regularly updated to account for emerging risks and technologies.

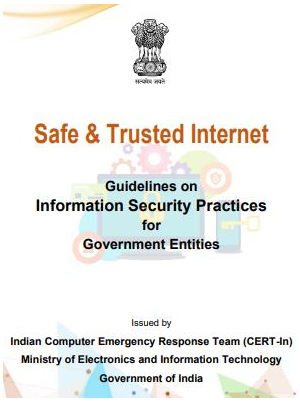
Lt. Gen. Rajesh Pant at the launch of NCRF

The NCRF will be a living document that will be regularly updated to account for emerging risks and technologies.

CERT-In issued Guidelines on Information Security Practices

Source: https://pib.gov.in/, https://www.cert-in.org.in/

The Government of India is fully aware of the growing cyber threats and attacks present in today's digital world and has formulated policies aimed at ensuring safe & trusted and secure cyber space for its users. To further address the goal of safe cyberspace, the Indian Computer Emergency Response Team (CERT-In) has released guidelines on information security practices. These guidelines apply to all Ministries, Departments, Secretariats, and Offices specified in the first schedule to the Government of India (Allocation of Business) Rules, 1961, along with their attached and subordinate offices. The guidelines also include all government institutions, public sector enterprises, and other government agencies under their administrative scope. These guidelines serve as a roadmap for the Government entities and industry to reduce cyber risk, safeguard citizen data and continue to enhance the nation's cyber security ecosystem. It will also serve as a fundamental document for audit teams to assess an organisation's security posture against the specified cybersecurity requirements. The guidelines include various security domains such as application security, network security, identity and access management, data security, third-party outsourcing, security monitoring,



These guidelines serve as a roadmap for the Government entities and industry to reduce cyber risk, safeguard citizen data and continue to enhance the nation's cyber security ecosystem.

incident management, hardening procedures, and security auditing. It also includes guidelines prepared by the National Informatics Centre for Chief Information Security Officers (CISOs) and employees of Central Government Ministries/Departments to enhance cyber security and cyber hygiene.

Panel discussion for 'The API Economy: Building Seamless Security'

The speaker emphasised the need to build offensive strategies to combat organised gangs, pre-emptive arrests, speedy and efficient prosecution, identification and removal of vulnerabilities and security weaknesses, and hacking the hackers.

ETCISO Secufest 2023: Seamless Security for API Economy

Source: https://ciso.economictimes.indiatimes.com/

The Secufest 2023 was filled with informative discussions and workshops on pressing cybersecurity issues facing enterprises today. Attendees had the opportunity to learn from industry experts and CISOs on a wide range of topics, from emerging threats to practical strategies for enhancing cybersecurity. The day started with a keynote emphasising the need to build a cyber-resilient infrastructure for Digital India, highlighting the vulnerability of digital infrastructures and the importance of timely intel to predict and mitigate cyber threats. The speaker also discussed the threat of cyber warfare to national security and the steps needed to tackle cybercrimes, including building capacity, better coordination among agencies, strengthening laws, filling policy gaps, and improving cyber forensic capabilities. The speaker emphasised the need to build offensive strategies to combat organised gangs, pre-emptive arrests, speedy and efficient prosecution, identification and removal of vulnerabilities and security weaknesses, and hacking the hackers. Overall, ETCISO provided attendees with valuable insights and techniques for defending against cyber-attacks.

Image source: https://sunpharma.com/

Sun Pharmaceutical has suffered an information security incident that has impacted its IT assets, with a ransomware group claiming responsibility for the attack.

Information Security Incident in Sun Pharma

Source: https://www.thehindubusinessline.com, https://www.bseindia.com

Sun Pharmaceutical has suffered an information security incident that has impacted its IT assets, with a ransomware group claiming responsibility for the attack. While the company has stated that its core systems and operations have not been affected, it has isolated the impacted assets and is investigating the matter. This latest incident follows similar cyber security breaches reported by Dr. Reddy's Laboratories and Lupin in late 2020, highlighting the high data breach costs incurred by the healthcare sector. Sun has taken immediate steps to contain and remediate the impact of the attack, engaging global cyber security experts and employing additional measures to ensure the integrity of its systems and data. The company has proactively isolated its network and initiated the recovery process, but the incident has impacted its business operations and is expected to reduce revenues in some of its businesses. The company will incur expenses in connection with the

incident and remediation, and other potential adverse impacts of the incident remain uncertain.

Nagpur Unit Making Military Weapons Hit by Hackers

Source: https://theprint.in/

Solar Industries India Limited, a Nagpur-based company that manufactures weapons for the Indian military, has suffered a cyber-attack that has resulted in the sale of its sensitive data online. CloudSEK, a cybersecurity firm based in Bengaluru, confirmed the breach, stating that the leaked data posed a threat to the confidentiality of weaponry used by the Indian military. The attack was carried out on Republic Day by a hacker group known as 'ALPHV' or BlackCat, which claimed to have breached the company infrastructure and stolen 2TB of data, including classified data related to weapons production. The data reportedly includes personal information of employees and customers, details of armament supply chains, blueprints and engineering documentation of the weapons, and government documents revealing details of cooperation. The hacker group has invited bids for the information within 24 hours of the publication of its blog. The incident highlights the growing threat of cyber-attacks and the need for proper vulnerability assessments, security audits, and information security management systems.

Image source: https://solargroup.com/#home

The data reportedly includes personal information of employees and customers, details of armament supply chains, blueprints and engineering documentation of the weapons, and government documents revealing details of cooperation.

Cybercriminals Targeted Bank Customers, CID Sound Alert

Source: https://timesofindia.indiatimes.com/

The Criminal Investigation Department (CID) Jharkhand has issued a warning about a large number of SMS messages containing phishing-related URL links being sent to bank account holders of HDFC, ICICI, SBI, and PNB. Jharkhand CID Director General (DG) Sh. Anurag Gupta has advised against opening such links. The messages appear to be bulk messages sent to bank customers across the country, with the content of the messages urging customers to update their PAN number via a given link. If the customer clicks on the link, an app called Dash Board will be installed on their mobile phones, which will steal their personal data. The CID Jharkhand has advised bank customers not to share their personal information with strangers, avoid clicking on links sent from unknown numbers through SMS, and access the customer care number from the official website only. "The customers who fall prey to cybercriminals should dial 1930", the DG said.

Image source: https://twitter.com/JharkhandCID/

If the customer clicks on the link, an app called Dash Board will be installed on their mobile phones, which will steal their personal data.

DogeRAT Trojan Targets Indian Android Users

Source: https://thehackernews.com/

A new open-source Remote Access Trojan (RAT) called DogeRAT is targeting Android users primarily located in India as part of a sophisticated malware campaign. Cybersecurity firm CloudSEK reports that the malware is distributed via social media and messaging platforms under the guise of legitimate applications like Opera Mini, OpenAI ChatGPT, and premium versions of YouTube, Netflix, and Instagram. Once installed on a victim's device, the malware gains unauthorised access to sensitive data, including contacts, messages, and banking credentials. It can also take control of the infected device, enabling malicious actions such as sending spam messages, making unauthorised payments, modifying files, and remotely capturing photos through the device's cameras. DogeRAT is promoted by its India-based developer through a Telegram channel that has more than 2,100 subscribers since it was created on June 9, 2022. The free version of DogeRAT has also been made available on GitHub. The findings highlight the growing threat of cyber-attacks on Android users in India.

Once installed on a victim's device, the malware gains unauthorised access to sensitive data, including contacts, messages, and banking credentials.

News Snippets - International

FBI Take Down 13 More DDoS-for-Hire Services Domains

Source: https://thehackernews.com, https://www.bleepingcomputer.com

The U.S. Justice Department announced the court-authorised seizure of 13 Internet domains that offered DDoS-for-hire services to other criminal actors. This takedown was a part of an ongoing international initiative called 'Operation PowerOFF' that is aimed to takedown all criminal DDoS-for-hire infrastructures worldwide. It was also observed that 10 of the 13 domains were reincarnations of DDoS-for-hire services that the FBI seized in December 2022, which targeted 48 top booter services. The homepages of seized websites were replaced with seizure notices from the FBI. This seizure was the third wave of action taken by the U.S. law enforcement against well-known booter services that let users pay to launch powerful Distributed Denial-of-Service, (DDoS), attacks that flood targeted computers with information and prevent them from connecting to internet.

cyberstress.org seizure banner (DOJ)

The U.S. Justice Department announced the court-authorised seizure of 13 internet domains that offered DDoS-for-hire services to other criminal actors.

Law Enforcement Takes Down NetWire Cross-Platform RAT

Source: https://thehackernews.com/

The International law enforcement agencies have seized a malicious website and taken down the online infrastructure associated with NetWire, a cross-platform Remote Access Trojan (RAT). It is a licensed commodity RAT offered in underground forums to non-technical actors to carry out their own criminal activities. The malware is typically distributed via malspam campaigns and gives remote adversaries a complete control over any Windows, macOS, or Linux systems. NetWire has the capability to steal password and keylogging. It has been used by multiple threat actors including OPERA1ER and TA2541 to break into targets of interest and harvest sensitive information. The malware also emerged as one of the most prevalent RATs during Q4 2022, according to Avast. A popular tool which used to hijack computers in order to perpetuate cyber fraud, network intrusions and data breaches by threat groups has also been removed by this global campaign.

The malware is typically distributed via malspam campaigns and gives remote adversaries a complete control over any Windows, macOS, or Linux systems. NetWire has the capability to steal password and keylogging.

Daggerfly Campaign Hits African Telecom Services Providers

Source: https://thehackernews.com/

A new spear-phishing campaign tracked as Daggerfly has been targeting Telecommunication services providers in Africa. The threat actors are using spear-phishing as an initial infection vector to drop MgBot loader as well as other tools like Cobalt Strike, a legitimate adversary simulation software and KsRemote,

The malicious actor subsequently moves to set up persistence on the victim machine by creating a local account and deploys the MgBot modular framework.

an Android-based Remote Access Trojan (RAT). Threat campaign also using a PlugX loader and exploiting the legitimate AnyDesk remote desktop software. The group is using Living-off-the-Land (LoL) tools like PowerShell and BITSAdmin to deliver next-stage payloads, including a legitimate AnyDesk executable and a credential harvesting utility. The malicious actor subsequently moves to set up persistence on the victim machine by creating a local account and deploys the MgBot modular framework. MgBot aka BLame or MgmBot comes with a wide range of plugins to harvest log keystrokes, browser data, record audio, capture screenshots and enumerate the active directory service. These capabilities may allow the attackers to collect a significant amount of information from victim machines.

State-Aligned Actors Targeted SMBs Globally

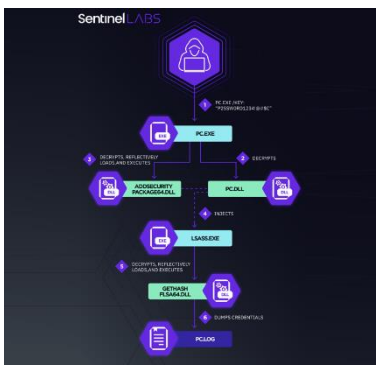
Source: https://www.bankinfosecurity.asia/

It has observed an increase in instances of impersonation or compromise of an SMB domain or email address.

Advanced Persistent Threat (APT) actors have targeted Small to Medium-sized Businesses (SMBs), governments, militaries and major corporate entities by using compromised SMB infrastructure through phishing campaigns. Threat actors have also launched state-aligned financially motivated attacks against SMB financial services firms and supply chain attacks affecting SMBs. It has observed an increase in instances of impersonation or compromise of an SMB domain or email address. These compromises may have been achieved through credential harvesting or through unpatched vulnerability exploitation in case of a web server. After successful compromise, the email address is used to send malicious email to targets. If a web server hosting a domain is compromised, the threat actor abused that legitimate infrastructure to host or deliver malicious malware to a third-party target.

Operation Soft Cell: Middle East Telecom Providers Breached

Source: https://thehackernews.com/



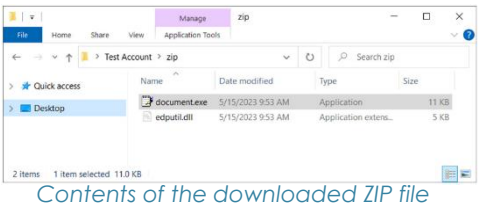
Operation Soft Cell attack flow

A long-running campaign dubbed as Operation Soft Cell has targeted telecommunication service providers in the Middle East. The initial attack phase involves infiltration of unpatched Internet-facing Microsoft Exchange servers to deploy web shells and later used for command execution. Once a foothold is established, the threat actors conduct a variety of reconnaissance, credential theft, lateral movement, and data exfiltration activities. The Soft Cell threat actor, also tracked as Gallium, is known to use tools like Mimikatz to obtain credentials that allows for lateral movement across the targeted networks. Threat actors are using special-purpose modules that implement a range of advanced techniques to achieve maximum stealth. This threat actor shares tactical similarities with APT10, APT27 and APT41.

Malware Bytes

QBot Malware Exploited Windows WordPad to Infect Devices

Source: https://www.bleepingcomputer.com/



Contents of the downloaded ZIP file

QBot threat actors have started a campaign to abuse a DLL hijacking flaw in Windows 10 WordPad program to infect computers, using the legitimate program to evade detection by security software. This campaign uses phishing emails that contains a link to download a randomly named ZIP archive from a remote host. This ZIP file contains a DLL file, edputil.dll and a document.exe (renamed copy of the legitimate Write.exe). When document.exe is launched, it automatically attempts to load a legitimate DLL file called edputil.dll. It does not check for edputil.dll in a specific folder and loads any DLL of the same name found in the same folder as the document.exe executable. This allows the threat actors to perform DLL hijacking by creating a malicious version of the edputil.dll DLL and stores it in the same folder as document.exe so it is loaded instead. Once the DLL is loaded, the malware uses C:\Windows\system32\curl.exe to download a DLL camouflaged as a PNG file from a remote host and executed using rundll32.exe. The QBot then runs in the background, stealing emails for use in further phishing attacks and downloading other payloads.

QBot threat actors have started a campaign to abuse a DLL hijacking flaw in Windows 10 WordPad program to infect computers, using the legitimate program to evade detection by security software.

SmokeLoader and RoarBAT Malware Attacks Against Ukraine

Source: https://thehackernews.com/

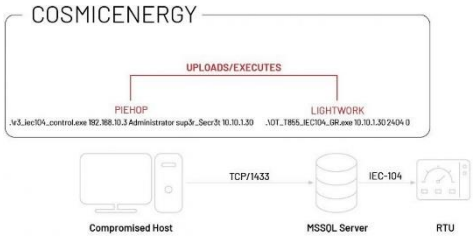
According to the Computer Emergency Response Team of Ukraine (CERT-UA), a phishing campaign with invoice-themed lures was used to distribute the SmokeLoader malware in the form of a polyglot file. The emails were sent using compromised accounts and had a ZIP archive polyglot file containing a JavaScript file and a decoy document. The executable that paves way for the SmokeLoader malware execution is then started by the JavaScript code. Ukraine's cybersecurity authority also revealed an attack that targeted an unnamed state organisation which used RoarBAT, a new batch script-based wiper malware, that performs a recursive search for files with a specific list of extensions before permanently deleting them using the legitimate WinRAR utility.

The emails were sent using compromised accounts and has a ZIP archive polyglot file containing a JavaScript file and a decoy document.

New CosmicEnergy Malware Sabotage Power Grids

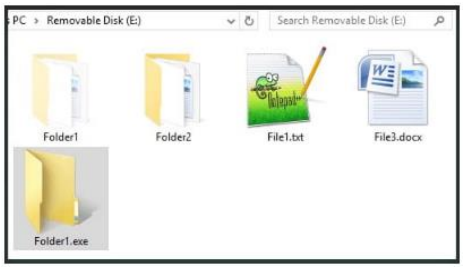
Source: https://thehackernews.com/, https://www.bleepingcomputer.com/

Mandiant has identified a new type of malware called COSMICENERGY that is designed to infiltrate and disrupt industrial environments' critical systems. The malware targets IEC-104-



CosmicEnergy execution chain

compliant Remote Terminal Units (RTUs) that is commonly used in electric transmission and distribution operations across the Middle East, Europe, and Asia. Using the Piehop disruption tool, CosmicEnergy acquires access to the target's OT systems through infected MSSQL servers. Once inside the victim's network, the attackers can use the Lightwork malicious tool to remotely operate RTUs by sending IEC-104 "ON" or "OFF" commands.



The worm executable on a USB drive

GoldenJackal employs a set of custom .NET malware tools that provide various functions, including credential dumping, data stealing, malware loading, lateral movement, file exfiltration, and more.

GoldenJackal Targets Middle East and South Asia Governments

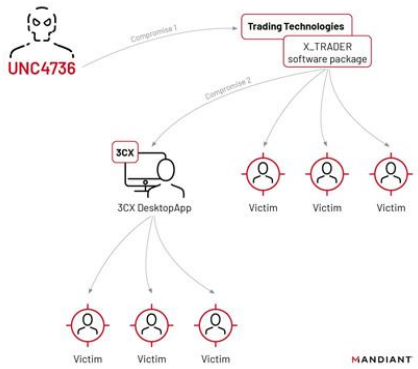
Source: https://www.bleepingcomputer.com/

Kaspersky has discovered a new threat group called GoldenJackal that has been targeting government and diplomatic entities in the Middle East and South Asia for espionage. GoldenJackal employs a set of custom .NET malware tools that provide various functions, including credential dumping, data stealing, malware loading, lateral movement, file exfiltration, and more. The primary payload used first to infect a system is 'JackalControl,' which gives the attackers remote control over the infected computer. The second tool 'JackalSteal' an implant used for data exfiltration from all logical drives on the compromised computer. The third tool 'JackalWorm' infects USB drives to spread on potentially other valuable computers. The fourth tool 'JacklPerInfo' is a basic system information collector with the additional capabilities of identifying and exfiltrating browsing history and credentials stored in web browsers. The fifth tool 'JackalScreenWatcher' is used for snapping screenshots on the infected device. GoldenJackal uses an extensive set of custom tools against a limited number of victims to carry out long-term espionage operations.

3CX Breached by Threat Actors

Source: https://thehackernews.com/

Hackers have targeted 3CX (a business communication solutions & software) with Matryoshka doll-style cascading attack. A malware-laced software package distributed via a tampered X_TRADER installer (trading software by Trading Technologies) resulted in the distribution of a malware-infected software package. This malicious installer contained a setup binary that dropped two trojanised DLLs and a harmless executable, the latter of which is used to side-load one of the DLLs that's disguised as a legitimate dependency. The attack chain then made use of open-source tools like SIGFLIP and DAVESHELL to ultimately extract and execute VEILEDSIGNAL. According to Mandiant's investigation, the adversary was able to access the employee's computer through the backdoor (dubbed VEILEDSIGNAL), steal their credentials, and use that information to move laterally



Cascading supply chain attack on 3CX

across the network of 3CX and compromise the Windows and macOS build environments to insert malicious code.

Improved ViperSoftX InfoStealer Avoids Detection

Source: https://thehackernews.com/2023/04/vipersoftx-infostealer-adopts.html

Researchers of Trend Micro revealed that ViperSoftX malware has adopted many sophisticated encryption and basic anti-analysis techniques like byte remapping and web browser communication blocking. Before downloading the first-stage PowerShell loader, the malware performs a series of anti-monitoring, anti-virtual machine, and anti-malware checks. The loader then decrypts and executes a second-stage PowerShell script retrieved from a remote server, which then takes care of launching the main routine responsible for installing the rogue browser extensions to exfiltrate passwords and crypto wallet data. It has been observed that the primary Command-and-Control (C&C) servers used for the second stage download are changed every month to avoid its detection.

It has been observed that the primary Command-and-Control (C&C) servers used for the second stage download are changed every month to avoid its detection.

NAPLISTENER Malware Bypass Detection

Source: https://thehackernews.com/

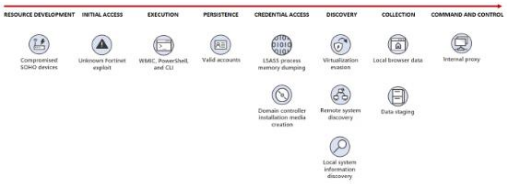
The threat group called REF2924 has deployed a new malware in its attacks aimed at entities in South and Southeast Asia. The threat group exploited the Internet-exposed Microsoft Exchange servers to deploy backdoors. The malware, dubbed NAPLISTENER is designed to evade network-based forms of detection. NAPLISTENER (wmdtc.exe) masquerades itself as a legitimate service Microsoft Distributed Transaction Coordinator (msdtc.exe) in order to fly under the radar and establish persistent access. NAPLISTENER malware create an HTTP request listener, which can process incoming requests from the Internet, reads any submitted data, decodes it from Base64 format, and executes it in memory.

NAPLISTENER (wmdtc.exe) masquerades itself as a legitimate service Microsoft Distributed Transaction Coordinator (msdtc.exe) in order to fly under the radar and establish persistent access.

Volt Typhoon Targets US Critical Infrastructure

Source: https://www.microsoft.com/, https://www.bleepingcomputer.com/

Volt Typhoon threat-actor group has targeted critical infrastructure organisations across the United States. The targets and breached entities span a wide range of critical sectors, including government, maritime, communications, information technology, manufacturing, construction, utilities, transportation, and education. The initial attack vector is the compromise of Internet-exposed Fortinet FortiGuard devices by exploiting an unknown zero-day vulnerability. After breaching the target's networks, the threat-actor group launched a 'living-off-the-land' attacks with



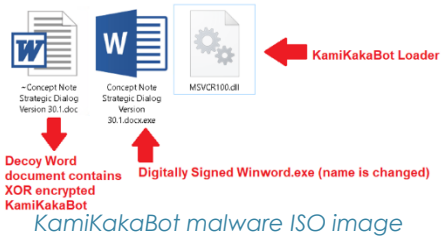
Volt Typhoon attack flow

The initial attack vector is the compromise of Internet-exposed Fortinet FortiGuard devices by exploiting an unknown zero-day vulnerability.

hands-on-keyboard activity and living-off-the-land binaries (LOLBins) like Netsh, PowerShell, Certutil. The threat actors can dump credentials through the Local Security Authority Subsystem Service (LSASS) by utilising the privileged access obtained after compromising the Fortinet devices. The stolen credentials allow the hackers to deploy Awen-based web shells for data exfiltration and persistence on the victim's system.

KamiKakaBot Malware Used to Target Southeast Asian Entities

Source: https://thehackernews.com/



KamiKakaBot malware ISO image contents

The loader loads the KamiKakaBot malware by leveraging the DLL side-loading method to evade security protections and load it into the memory of the Winword.exe binary.

The Dark Pink Advanced Persistent Threat (APT) actor has targeted government and military entities in Southeast Asian countries with a malware called KamiKakaBot. The attacks were in the form of social engineering lures that contain ISO image file attachments in emails to deliver the malware. The ISO image includes an executable (Winword.exe), a loader (MSVCR100.dll), and a decoy Microsoft Word document. The KamiKakaBot payload is embedded in the decoy Microsoft Word document. The loader loads the KamiKakaBot malware by leveraging the DLL side-loading method to evade security protections and load it into the memory of the Winword.exe binary. The objective of KamiKakaBot is to steal data stored in web browsers and execute remote code using Command Prompt (cmd.exe) while avoiding detection. The gathered data is then exfiltrated to a Telegram bot as a ZIP archive.

Charming Kitten's New Malware: BellaCiao

Source: https://www.bitdefender.com/, https://thehackernews.com/

BellaCiao is a custom-developed dropper that has the capability of delivering malware payloads onto a victim machine based on instructions from C2 server.

Threat group Charming Kitten has targeted multiple victims in the U.S., the Middle East, and Europe with a malware called BellaCiao. BellaCiao is a custom-developed dropper that has the capability of delivering malware payloads onto a victim machine based on instructions from C2 server. The payload delivered by BellaCiao is not downloaded instead it is hardcoded into the executable as malformed base64 strings and dumped when requested. To receive instructions from C2 server BellaCiao operates with two fixed values- a hardcoded IP string and the IP address returned by the DNS server controlled by the threat actor.

Poseidon Malware Targeted Indian Government Agencies

Source: https://www.uptycs.com/

The Uptycs threat researchers have discovered a new Linux malware called Poseidon that is deployed by the APT-36 group (aka Transparent Tribe). This APT group has targeted Indian government organisations, military personnel, and defence

contractors. Poseidon malware is a general-purpose backdoor that provides threat-actors with a wide range of capabilities to hijack an infected host. Its functionalities include logging keystrokes, taking screen captures, uploading and downloading files, and remotely administering the system in various ways. The Kavach authentication tool, a two-factor authentication (2FA) solution provided by the Indian government for secure access to their email services, was used as a disguise for the Poseidon payload delivery by APT-36 group. The threat-actor created a backdoored version of Kavach to target Linux users working for Indian government agencies. When a user interacts with the malicious version of Kavach, the legitimate login page is displayed to divert them. The user's system is compromised while the payload is being downloaded in the background.

Poseidon malware is a general-purpose backdoor that provides threat-actors with a wide range of capabilities to hijack an infected host.

Tick APT Targeted East Asian Data-Loss Prevention Company

Source: https://thehackernews.com/

Cyberespionage group Tick has compromised East Asian data-loss prevention (DLP) company that serves government and military entities. The attackers utilised the internal update servers of the DLP company to deliver malware inside the network of the software developer. They also trojanised installers of legitimate tools used by the company, which ultimately led to the execution of malware on the computers of the company's customers. To maintain persistent access, the attackers deployed malicious loader DLLs along with legitimate signed applications vulnerable to DLL search-order hijacking. These DLLs are used to decode and inject payloads into designated processes.

The attackers utilised the internal update servers of the DLP company to deliver malware inside the network of the software developer.

Global Ransomware Attacks and Developments

Knowledge Management Team, NCIIPC

In the second quarter of 2023, Ransomware groups have targeted various major enterprises.

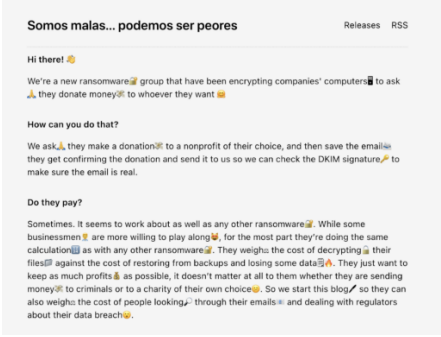
Attackers hacked into poorly secured MS-SQL servers to deliver the Trigona ransomware payloads and encrypt all files. The MS-SQL servers were breached via brute-force or dictionary attacks that take advantage of easy-to-guess passwords. After connecting to a server, the threat actors deployed the malware dubbed CLR Shell. Through a vulnerability in the Windows Secondary Logon Service, this malware gathers system information, modifies the compromised account's configuration, and escalates privileges to LocalSystem. In the next stage, the Trigona ransomware is launched as svchost.exe by installing and running a dropper malware as the svcservice.exe service. The malware disables system recovery and deletes any Windows Volume Shadow copies before it encrypts the system and delivers the ransom notes,

Trigona ransom note

thereby making the recovery impossible without the decryption key. Trigona encrypts all files on victim's device except those in specific folders, including the Windows and Program Files directories.

The Play ransomware group has developed two custom tools in .NET, Grixba and VSS Copying Tool, to improve the effectiveness of its cyberattacks.

The Play ransomware group has developed two custom tools in .NET, Grixba and VSS Copying Tool, to improve the effectiveness of its cyberattacks. The two tools enable attackers to enumerate users and computers in compromised networks, gather information about security, backup, and remote administration software, and easily copy files from Volume Shadow Copy Service (VSS) to bypass locked files. Grixba is a network-scanning and information-stealing tool, it saves all collected data in CSV files, compresses them into a ZIP archive, and then exfiltrates it to the attacker's C2 server, thereby giving them vital information on how to plan the next steps of the attack. The second custom tool, VSS Copying Tool, allows attackers to interact with the Volume Shadow Copy Service (VSS) via API calls using a bundled AlphaVSS .NET library. The VSS Copying Tool enables Play ransomware to steal files from existing shadow volume copies even when those files are in use by applications. The use of custom tools in Play ransomware indicates that the threat actor aims to increase the effectiveness of their attacks and carry out their malicious tasks more efficiently.



MalasLocker ransomware group ransom note

MalasLocker, a new ransomware group, has emerged with a unique modus operandi. This group is exploiting vulnerabilities in Zimbra Collaboration Suite (ZCS), a popular enterprise cloud-hosted collaboration software and email platform, and is demanding an unconventional ransom – donations to charity. Once they successfully infiltrate a system, they encrypt the victim's data and demand a donation instead of a ransom. Despite their unusual philanthropic request, the hacker group actions remain malicious and harmful, as they steal sensitive data and encrypt files, causing significant disruption and potential data leakage.

Buhti's exfiltration tool is a Go-based stealer that receives command-line arguments that specify the filesystem directories it should target.

A new ransomware operation named 'Buhti' also called as 'Blacktail' uses the leaked code of the Babuk and LockBit ransomware families to target Linux and Windows systems, respectively. Blacktail have not developed their own ransomware strain, they have created a custom data exfiltration utility that they use to blackmail victims, this method is known as double-extortion. Buhti's exfiltration tool is a Go-based stealer that receives command-line arguments that specify the filesystem directories it should target. The tool targets the following file types for theft: docx, json, psd, png, pdf, php, ppt, rtf, rar, raw, sql, svg, swf, tar, txt, wmv, wav, wma, xls, xml, yml, zip, aiff, aspx, epub, mpeg, pptx, xlsx, and yaml. After being copied into a ZIP package, the files are eventually transferred to Blacktail's servers.

The ALPHV ransomware group, also known as BlackCat ransomware group, has released an improved version of a

malware known as 'POORTRY'. The POORTRY malware is a Windows kernel driver signed using stolen keys belonging to legitimate accounts in Microsoft's Windows Hardware Developer Program. The new driver used by the BlackCat ransomware operation helps them elevate their privileges on compromised machines and then stop processes related to security agents. The malicious kernel driver exposes an Input and Output Control (IOCTL) interface that allows the user mode client, tjr.exe, to issue commands that the driver would execute with Windows kernel privileges. It only uses one of the exposed Device Input and Output Control (IOCTL) code - Kill Process, which is used to kill security agent processes installed on the system.

The POORTRY malware is a Windows kernel driver signed using stolen keys belonging to legitimate accounts in Microsoft's Windows Hardware Developer Program.

References:

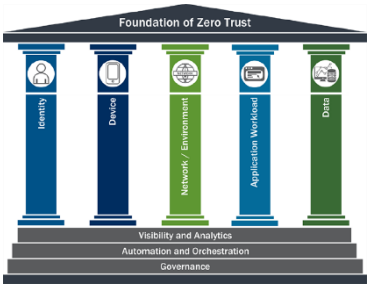
[1] https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/#:~:text=Attackers%20are%20hacking%20into%20poorly,%2Dto%2Dguess%20account%20credentials.
[2] https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/
[3] https://thehackernews.com/2023/05/buhti-ransomware-gang-switches-tactics.html
[4] https://www.bleepingcomputer.com/news/security/malicious-windows-kernel-drivers-used-in-blackcat-ransomware-attacks/
[5] https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/

Trends

CISA's Zero Trust Maturity Model

Source: https://www.cisa.gov/ https://www.intersecinc.com/

The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM) provides an approach to achieve continued modernisation efforts related to zero trust. Recent cyber incidents have highlighted the broad challenges of ensuring effective cybersecurity across the whole private & government organisations. The ZTMM reflects the seven tenets of zero trust as outlined in NIST SP 800-207. It includes five distinct pillars: Identity, Devices, Networks, Applications and Workloads, and Data. Each pillar includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance capabilities. Agencies should use the three stages of the Zero Trust Maturity (ZTM) journey to identify maturity for each zero-trust technology pillar. These stages advance from a Traditional starting point to Initial, Advanced, and Optimal. Agencies should assess their current enterprise systems, resources, infrastructure, personnel, and processes before investing in zero trust capabilities. The ZTMM



Agencies should assess their current enterprise systems, resources, infrastructure, personnel, and processes before investing in zero trust capabilities.

covers many aspects of cybersecurity critical to enterprises, but does not address other aspects such as incident response, logging, monitoring, alerting, forensic analysis, risk acceptance, and recovery.

OWASP TOP 10 API Security Risks: 2023

Source: https://owasp.org/, https://www.rapid7.com/

The Open Worldwide Application Security Project (OWASP) has released the top 10 API security risks list of the highest priority API based threats in 2023. The top 10 security risks are:

The Open Worldwide Application Security Project (OWASP) has released the top 10 API security risks list of the highest priority API based threats in 2023.

Broken object level authorisation: Object level authorisation is a control method that restricts access to objects to minimise system exposures.

Broken authentication: Broken authentication can lead to many issues such as credential stuffing, brute force attacks, weak unsigned keys, and expired tokens.

Broken object property level authorisation: This category focuses on the lack of or improper authorisation validation at the object property level that can lead to information exposure or manipulation by unauthorised parties.

Unrestricted resource consumption: Denial of service attacks result from overconsumption of these resources leading to downtime and racked up service charges.

Broken function level authorisation: This vulnerability allows attackers to access unauthorised functionality.

Unrestricted Access to Sensitive Business Flows: APIs vulnerable to this risk expose a business flow without compensating the potential harm that could result from excessive or automated use of the functionality.

Server-side request forgery: Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URL.

Data consumed from other APIs must be handled with caution to prevent unexpected behaviour. It is possible that third-party APIs could be compromised and leveraged to attack other API services.

Security misconfiguration: This flaw can be the result of incomplete or inconsistent patching, enabling unnecessary features, or improper configuration of permissions.

Improper inventory management: Improper inventory management can result in running unpatched systems and exposure data to attackers.

Unsafe consumption of APIs: Data consumed from other APIs must be handled with caution to prevent unexpected behaviour. It is possible that third-party APIs could be compromised and leveraged to attack other API services.

Learning

Identity and Access Management Best Practices for Administrators

Source: https://www.nsa.gov/

The Cybersecurity & Infrastructure Security Agency (CISA) and National Security Agency (NSA) have released the best practices guide for Identity and Access Management (IAM) to help organisations strengthen their security posture. IAM is a framework of business processes, policies, and technologies that facilitate the management of digital identities and ensure that users only gain access to data when they have the appropriate credentials. The guide provides best practices and mitigations to counter threats to IAM related to identity governance, environmental hardening, identity federation/single sign-on, multi-factor authentication, IAM auditing and monitoring. The release is accompanied by an educational aid presentation and associated talking points to support organisational technical leaders in explaining the benefits of a robust IAM program and the risks of not implementing one. The guidance was developed and published by an NSA and CISA led working panel with Enduring Security Framework (ESF), a public-private cross-sector partnership that aims to address risks that threaten critical infrastructure and national security systems.

The guidance was developed and published by an NSA and CISA led working panel with Enduring Security Framework (ESF), a public-private cross-sector partnership that aims to address risks that threaten critical infrastructure and national security systems.

Security-by-Design and Default Principles

Source: https://www.cisa.gov/

CISA, the FBI, the NSA, and the cybersecurity authorities of Australia, Canada, the United Kingdom, Germany, Netherlands, and New Zealand have jointly developed a guidance document titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and –Default". The document urges manufacturers to take urgent steps to ship products that are secure-by-design and -default, and outlines core principles to guide software manufacturers in building security into their design processes prior to developing, configuring, and shipping their products. The guidance is aimed at advancing an international conversation about key priorities, investments, and decisions necessary to achieve a future where technology is safe, secure, and resilient by design and default.

The guidance is aimed at advancing an international conversation about key priorities, investments, and decisions necessary to achieve a future where technology is safe, secure, and resilient by design and default.

Google Cloud Introduces Security AI Workbench

Source: https://thehackernews.com/

Google's cloud division has launched Security Artificial Intelligence (AI) Workbench, a cybersecurity suite that leverages generative AI models to gain better visibility into the threat landscape. The suite includes VirusTotal Code Insight and Mandiant Breach Analytics for

The suite includes VirusTotal Code Insight and Mandiant Breach Analytics for Chronicle to analyse potentially malicious scripts and alert customers of active breaches in their environments.

Chronicle to analyse potentially malicious scripts and alert customers of active breaches in their environments. Security Command Center AI utilises a specialised large language model called Sec-PaLM to provide operators with near-instant analysis of findings and possible attack paths, as well as impacted assets and recommended mitigations. Google is also making use of machine learning models to detect and respond to API abuse and business logic attacks. The suite is built on Google Cloud's Vertex AI infrastructure, offering customers enterprise-grade capabilities such as data isolation, data protection, sovereignty, and compliance support.

Vulnerability Watch

Critical Vulnerabilities in safe-eval

Source: https://nvd.nist.gov/

Critical vulnerabilities with CVE IDs CVE-2023-26122 and CVE-2023-26121 having CVSS v3 score of 10.0 has been found affecting all versions of safe-eval package which is used for execution of JavaScript code and is a better version of eval().

Critical vulnerabilities with CVE IDs CVE-2023-26122 and CVE-2023-26121 having CVSS v3 score of 10.0 has been found affecting all versions of safe-eval package which is used for execution of JavaScript code and is a better version of eval(). Five functions named __defineGetter__, stack(), toLocaleString(), propertyIsEnumerable.call() and valueOf() are affected by Sandbox bypass (CVE-2023-26122) due to improper input sanitization. By exploiting this vulnerability, an attacker can perform Rremote Ccode eExecution (RCE). CVE-2023-26121 vulnerability is due to Prototype Pollution done via the safeEval function and happens because of improper sanitisation of its parameter content.

Critical Vulnerability in Nexx Smart Home Devices

Source: https://nvd.nist.gov/, https://www.cisa.gov/, https://protergo.id/

Critical vulnerability with CVE ID 2023-1748 having CVSS v3 score of 10.0 has been found in Nexx Smart Home devices.

Critical vulnerability with CVE ID 2023-1748 having CVSS v3 score of 10.0 has been found in Nexx Smart Home devices. The following devices of Nexx have been affected by this vulnerability: Nexx Garage Door Controller (NXG-100B, NXG-200) of version nxg200v-p3-4-1 and prior; Nexx Smart Plug (NXPG-100W) of version nxpg100cv4-0-0 and prior and Nexx Smart Alarm (NXAL-100) of version nxal100v-p1-9-1and prior. The mentioned devices use hard-coded credentials in their firmware and these credentials can be easily obtained by an attacker with Nexx's API with unauthenticated access to the Nexx Home mobile application. By exploiting this vulnerability, one can remotely control garage doors or smart plugs of Nexx devices.

Critical Vulnerability found in AGT Tech Ceppatron

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-2851

Critical vulnerability with CVE ID 2023-2581 having CVSS v3 score of 9.8 has been found in AGT Tech Ceppatron. SQL injection performed by an attacker could lead to command line execution due to improper neutralization of special elements used in an SQL command.

Critical vulnerability with CVE ID 2023-2581 having CVSS v3 score of 9.8 has been found in AGT Tech Ceppatron.

Critical Vulnerability in vm2 Sandbox

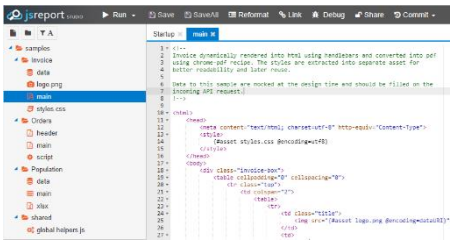
Source: https://nvd.nist.gov/vuln/detail/CVE-2023-32314

Critical vulnerability with CVE ID 2023-32314 having CVSS v3 score of 10.0 has been found in vm2 sandbox where developers can run untrusted code with whitelisted Node's built-in modules securely. The affected versions are vm2 sandbox prior to v3.9.17. By exploiting the sandbox escape vulnerability in vm2, an attacker can perform remote code execution on the machine running the sandbox by bypassing its protections. Users are strongly advised to upgrade to v3.9.18 of v2.

Critical vulnerability with CVE ID 2023-32314 having CVSS v3 score of 10.0 has been found in vm2 sandbox where developers can run untrusted code with whitelisted Node's built-in modules securely.

Critical Vulnerability found in jsreport/jsreport

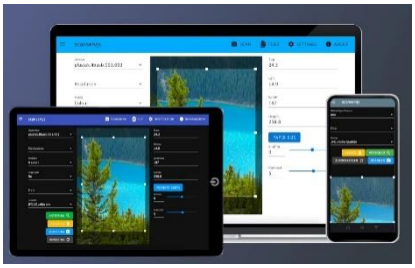
Source: https://nvd.nist.gov/vuln/detail/CVE-2023-2583, https://huntr.dev/



Critical vulnerability with CVE ID 2023-2583 having CVSS v3 score of 10.0 has been found in GitHub repository jsreport/jsreport prior to v3.11.3. jsreport is used by developers to design and render various reports using JavaScript templating and it also supports various report output formats like html, pdf, excel and docx etc. The vm2 module of Nodejs in the jsreport-core component of jsreport was found to have a sandbox escape vulnerability. By exploiting this vulnerability, an attacker can obtain authority of jsreport playground server or attack the jsreport client of a user.

Critical Vulnerability in sbs20/scanservjs

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-2564, https://huntr.dev/



Critical vulnerability with CVE ID 2023-2564 having CVSS v3 score of 10.0 has been discovered in GitHub repository sbs20/scanservjs prior to v2.27.0. The application has been found vulnerable to OS command injection. The application acts as a Web UI frontend to scanners where you can share one or more scanners on a network. It uses SANE library to interact with scanners where it uses two APIs for scanning an image and generating image preview. These APIs are found to be vulnerable to OS command injection via type confusion whenever they are involved in POST body parameters. By exploiting this vulnerability, an attacker can dump and also exfiltrate data using code execution by compromising the system/ server running scanservjs.

Critical Vulnerability Discovered in Home Assistant Software

Source: https://securityonline.info/

A critical security vulnerability, CVE-2023-27482, affecting Home Assistant OS and Home Assistant Supervised installations. With a maximum CVSS score of 10, this vulnerability allows attackers to bypass authentication and gain direct access to the Supervisor API. Exploiting the flaw could grant unauthorised control over Home Assistant updates, add-ons, and backups. The issue has been resolved in Supervisor version 2023.03.1, which has been automatically rolled out via the Supervisor's auto-update feature. Additionally, Home Assistant Core 2023.3.0 includes mitigation for this vulnerability. It is strongly advised to update both the Supervisor and Home Assistant Core to the latest versions for enhanced security. For users unable to update immediately, it is recommended to avoid exposing Home Assistant instances to the internet as a precautionary measure. By promptly updating the software, users can safeguard their Home Assistant installations and protect against this critical security issue.

With a maximum CVSS score of 10, this vulnerability allows attackers to bypass authentication and gain direct access to the Supervisor API.

Critical Vulnerability in eDEX-UI Terminal Emulator

Source: https://www.incibe.es/

eDEX-UI, a science fiction-inspired terminal emulator, has been found to have a critical security vulnerability, CVE-2023-30856, known as Cross-Site WebSocket Hijacking (CSWSH) in versions 2.2.8 and earlier. This vulnerability allows a malicious website to connect to eDEX-UI's internal terminal control WebSocket and execute arbitrary commands on the shell. When eDEX-UI is running and the user is browsing the web, a malicious website can exploit the vulnerability by establishing a WebSocket connection with eDEX-UI's internal terminal control. By doing so, the attacker gains the ability to send arbitrary commands to the shell, potentially compromising the system. Given the lack of an official patch, users are advised to take certain precautions. One workaround is to shut down eDEX-UI when browsing the web to prevent any potential attacks. Additionally, it is recommended to run the eDEX terminal with the lowest possible privileges to limit the impact of a successful exploit. By being aware of the issue and implementing the suggested workarounds, users can minimize the potential impact of this vulnerability.

When eDEX-UI is running and the user is browsing the web, a malicious website can exploit the vulnerability by establishing a WebSocket connection with eDEX-UI's internal terminal control.

Critical Vulnerability in Qihoo 360 Products

Source: https://vulners.com/, https://vulners.com, https://nvd.nist.gov

A Buffer Overflow vulnerability has been identified in Qihoo 360 Chrome v13.0.2170.0, a web browser built on the Chrome engine. This critical security flaw poses a risk of privilege escalation, potentially allowing attackers to gain elevated system privileges. This occurs when the V8 engine improperly handles specific

JavaScript objects, leading to memory corruption. Exploiting this vulnerability grants an attacker the ability to execute malicious code. Users are strongly advised to update to the latest version of Qihoo 360 Chrome or switch to alternative browsers with robust security features. Browser developers should address this vulnerability by patching the V8 engine and implementing proper handling of JavaScript objects. By staying vigilant and taking necessary precautions, users can enhance their online security and mitigate potential threats.

Users are strongly advised to update to the latest version of Qihoo 360 Chrome or switch to alternative browsers with robust security features.

The CVE-2021-33975 vulnerability in Qihoo 360 Total Security v10.8.0.1060 and v10.8.0.1213 has elevated concerns as it consents attackers to exploit a buffer overflow flaw and escalate privileges. The severity of this issue is categorized as critical, with a CVSS base score of 10. The affected component of the software remains undisclosed. The flaw stems from the manipulation of an unidentified input, which triggers a buffer overflow vulnerability. It arises when the program copies an input buffer to an output buffer without validating that the input buffer's size is smaller than the output buffer's size, resulting in a buffer overflow. This vulnerability has far-reaching consequences, impacting the confidentiality, integrity, and availability of the affected system. Users of the affected Qihoo software versions should take immediate action to mitigate this security risk.

The flaw stems from the manipulation of an unidentified input, which triggers a buffer overflow vulnerability.

A critical security flaw, identified as CVE-2021-33972, has been discovered in Qihoo 360 Safe Browser version 13.0.2170.0. This vulnerability, a Buffer Overflow exploit, poses a significant threat to users of the browser, potentially enabling an attacker to gain escalated privileges. A Buffer Overflow occurs when a program writes more data into a buffer than it can hold, resulting in the excess data overflowing into adjacent memory. This overflow can be manipulated by an attacker to execute malicious code, compromising the integrity and security of the system. Users of Qihoo 360 Safe Browser are strongly advised to update to the latest version, which addresses this vulnerability. Additionally, it is recommended to exercise caution while browsing and refrain from visiting suspicious or untrusted websites to minimise the risk of falling victim to such exploits.

A Buffer Overflow occurs when a program writes more data into a buffer than it can hold, resulting in the excess data overflowing into adjacent memory.

Critical Security Vulnerability discovered in vm2 Sandbox

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-30547

A critical security vulnerability, identified as CVE-2023-30547, With a maximum CVSS score of 10, was reported in the vm2 sandbox. The vulnerability affects versions of vm2 up to 3.9.16, allowing attackers to execute unsanitised host exceptions within the handleException() function. Exploiting this flaw enables attackers to escape the sandbox environment and run arbitrary code within the host context, posing significant risks. The developers promptly

Exploiting this flaw enables attackers to escape the sandbox environment and run arbitrary code within the host context, posing significant risks.

addressed this issue and released version 3.9.17 of vm2, which includes the necessary patch to mitigate the vulnerability. Users of affected versions are strongly advised to upgrade to the latest version to protect their systems from potential attacks.

Critical Vulnerability in vm2 Allows Remote Code Execution

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-29199

By exploiting this flaw, attackers can bypass exception sanitisation logic, leak unsanitised host exceptions, and run arbitrary code in the host environment, escaping the intended sandbox boundaries.

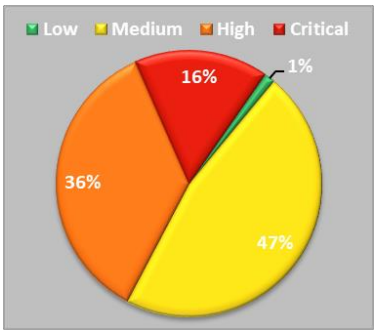
A critical vulnerability has been discovered in vm2, a JavaScript code sandboxing library. The vulnerability, known as CVE-2023-29199, affects versions up to 3.9.15. By exploiting this flaw, attackers can bypass exception sanitisation logic, leak unsanitised host exceptions, and run arbitrary code in the host environment, escaping the intended sandbox boundaries. This can lead to remote code execution and pose a significant threat to affected systems. The severity of the vulnerability is acknowledged by the National Vulnerability Database (NVD) With a maximum CVSS score of 10. Users are strongly advised to update to vm2 version 3.9.16, which includes the necessary patch to address the vulnerability. Immediate action is recommended to mitigate the risk and protect systems from potential exploitation.

Quarterly Vulnerability Analysis Report

Knowledge Management Team, NCIIPC

During Second quarter of 2023, a total of 5737 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 16 percent of total vulnerabilities reported were of Critical severity. Microsoft, Google, Apple, Adobe and Linux were the top five vendors having 23% of total reported vulnerabilities.

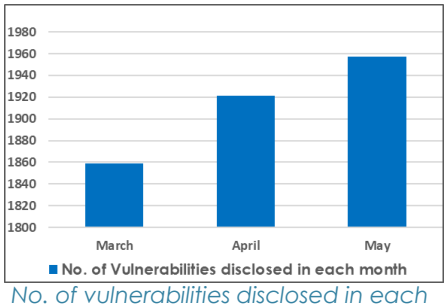
Severity-wise number of vulnerabilities



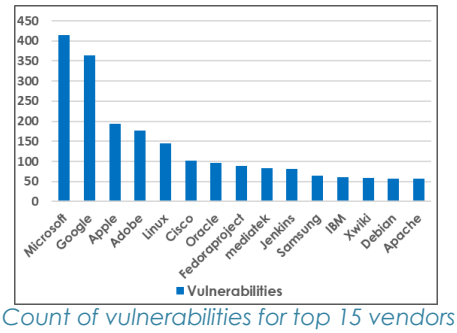
Severity-wise share of vulnerabilities

Severity	CVSSv3 Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Mar'23	Apr'23	May'23		
Low	0-1	0	0	0	0	74
	1-2	0	1	0	1	
	2-3	4	5	5	14	
	3-4	20	18	21	59	
Medium	4-5	184	254	218	656	2679
	5-6	350	321	408	1079	
	6-7	303	367	274	944	
High	7-8	463	440	463	1366	2046
	8-9	210	212	258	680	
Critical	9-10	325	303	310	938	938
Total		1859	1921	1957		5737

S. No.	Vendor	No. of Vulnerabilities			Total
		Mar'23	Apr'23	May'23	
1.	Microsoft	155	195	64	414
2.	Google	215	76	73	364
3.	Apple	62	62	69	193
4.	Adobe	106	57	14	177
5.	Linux	52	66	27	145
6.	Cisco	34	40	28	102
7.	Oracle	2	92	2	96
8.	Fedoraproject	21	30	37	88
9.	mediatek	29	29	25	83
10.	Jenkins	9	37	36	82
11.	Samsung	24	8	32	64
12.	IBM	18	20	23	61
13.	Xwiki	15	38	5	58
14.	Debian	17	15	25	57
15.	Apache	14	19	24	57



No. of vulnerabilities disclosed in each month



Count of vulnerabilities for top 15 vendors

Security App

Decryptor Recovers Data from Partially Encrypted Files

Source: https://thehackernews.com/, https://techviral.net/

CyberArk has developed a new ransomware decryptor called 'White Phoenix' that allows victims to partially recover files encrypted by ransomware strains that use intermittent encryption. Intermittent encryption is a strategy employed by ransomware groups that alternates between encrypting and not encrypting chunks of data. This method allows encryption to be much faster. Ransomware operations that use intermittent encryptions include BlackCat, Play, EsxiArgs, Qilin/agenda and BianLian. Text recovery includes restoration method that includes text chunks in the streams and concatenating them or reverse hex encoding and Character Map (CMAP) scrambling. Recovering image streams is as simple as removing the applied filters. The tool is available for free download from CyberArk's public GitHub repository and can recover data from PDF, Word, Excel, and PowerPoint document formats. However, the tool's effectiveness is directly linked to the extent of the damage to the file.

Google's Framework for Secure Software Supply Chains

Source: https://thehackernews.com/, https://www.immuniweb.com/

Google has released the 0.1 Beta version of GUAC (Graph for Understanding Artifact Composition), an open-source framework that aggregates software security metadata from different sources into a graph database to help organisations determine how one

The GUAC tool provides organised and actionable insights into software supply chain security position. It maps out the relationship between software to understand software security position.

piece of software affects another and create a better picture of the risk profile and visualise the relationships between artifacts, packages, and repositories. The GUAC tool provides organised and actionable insights into software supply chain security position. It maps out the relationship between software to understand software security position. It brings together Software Bill of Materials (SBOM) documents, Supply-chain Levels for Software Artifacts (SLSA) attestations, Open-Source Vulnerabilities (OSV) feeds, deps.dev insights and company's internal private metadata to help create better picture of the risk profile. The goal is to handle high-profile supply chain attacks, generate a patch plan and respond to security compromises. This enables the Chief Information Security Officer to easily create a policy to forbid use of any software.

Mobile Security

New Android Malware Mimicks Govt., Crypto and Banks Apps

Source: https://www.bleepingcomputer.com/, https://blog.cyble.com/

By utilising cleverly crafted interfaces and imitating official app icons, the malware effectively conceals its malicious nature.

'Chameleon' malware has gained significant attention due to its ability to mimic legitimate bank, government, and cryptocurrency applications, posing a serious risk to unsuspecting users. Chameleon malware operates by disguising itself as popular and trusted apps, luring users into providing sensitive information such as usernames, passwords, and even financial details. Security researchers have identified several key features that make Chameleon a particularly potent threat. Firstly, it employs advanced social engineering techniques to trick users into believing they are interacting with legitimate apps. By utilising cleverly crafted interfaces and imitating official app icons, the malware effectively conceals its malicious nature. Moreover, Chameleon possesses the ability to dynamically alter its behaviour based on its environment. It can modify its appearance and functionality based on the user's location, language settings, and even the time of day, further enhancing its camouflage and making it extremely difficult to identify. Once installed on a victim's device, the Chameleon malware can perform various malicious activities. It can intercept and steal login credentials, capture sensitive financial information, and even hijack SMS messages for two-factor authentication. This enables the attackers to gain unauthorised access to the victim's accounts and perform fraudulent activities.

It can intercept and steal login credentials, capture sensitive financial information, and even hijack SMS messages for two-factor authentication.

Fleckpe Android Malware Infected Over 600,000 Devices

Source: https://www.bleepingcomputer.com/, https://thehackernews.com/

Recent reports have surfaced regarding a highly prolific Android malware called "Fleckpe," which has managed to infect over

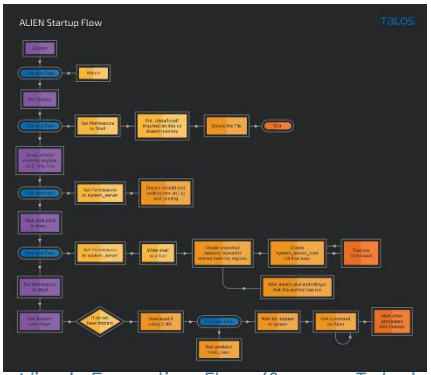
600,000 devices through malicious apps available on the Google Play Store. This alarming discovery serves as a stark reminder that even seemingly trusted sources can be infiltrated by cybercriminals. Fleckpe is a sophisticated form of malware that operates stealthily on infected devices, compromising user privacy and security. It is primarily distributed through seemingly legitimate apps, making it challenging for users to discern its malicious nature. These infected apps are often disguised as useful utilities, popular games, or productivity tools, enticing unsuspecting users to download and install them. Once installed, Fleckpe begins executing its malicious activities in the background, hidden from the user's view. The malware operates as a "dropper," meaning its primary objective is to deliver additional payloads onto the infected device. These payloads can vary, including adware, spyware, or even ransomware, depending on the intentions of the attackers. Security researchers have identified that Fleckpe can establish a remote connection with a command-and-control (C&C) server controlled by the attackers. This enables the malware to receive commands and updates, making it adaptable and capable of evolving its malicious behaviour.

Fleckpe is a sophisticated form of malware that operates stealthily on infected devices, compromising user privacy and security. It is primarily distributed through seemingly legitimate apps, making it challenging for users to discern its malicious nature.

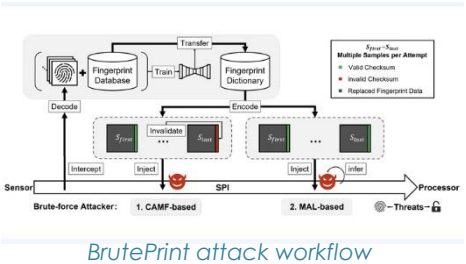
A Deep Dive into Intellexa's Android Spyware 'Predator'

Source: https://www.bleepingcomputer.com/

A technical analysis has been presented by Cisco Talos and Citizen Lab on a commercial Android spyware called 'Predator' and its loader 'Alien'. Predator belongs to Israeli company Intellexa (previously Cytrox). The capabilities include recording of phone calls, stealing messages and hide itself in the system etc. 'Predator' and 'Alien' abuses Android's zero-day vulnerabilities to perform shell code execution on the targeted device. 'Alien' loads/updates the 'Predator' from an external address and executes commands received from 'Predator' by hiding it inside legitimate system processes while bypassing SELinux security. 'Predator' arrives on device as an ELF file and perform various espionage operations by setting up a Python runtime. Both this module together performs the operations like arbitrary shell code execution, certificate poisoning, audio recording, directory enumeration etc. 'Alien' checks the underlying device manufacturer and recursively look into the directories that holds users' sensitive data from email, messages, social media, browser, contact list, images and video. TLS decryption is done by using certificate poisoning.



Alien's Execution Flow (Source: Talos)



BrutePrint attack workflow

The Bruteprint Attack involves an attacker attempting to unlock a smartphone using various fingerprint samples until the correct match is found.

New 'BrutePrint' Attack Exploits Smartphone Fingerprint Security

Source: https://thehackernews.com/

In the ever-evolving world of technology, security vulnerabilities continue to pose significant challenges. Recently, a new threat has emerged in the realm of smartphone security. Dubbed the "Bruteprint Attack", this technique enables attackers to potentially unlock smartphones using a brute force approach against fingerprint-based security systems. However, researchers have discovered a flaw in certain implementations that can leave devices vulnerable. BrutePrint bypasses the limits on number of attempts by using zero-day vulnerabilities and by abusing two security flaws present in Serial Peripheral Interface (SPI) namely – Cancel After Match Fail (CAMF) and Match After Lock (MAL). The Bruteprint Attack involves an attacker attempting to unlock a smartphone using various fingerprint samples until the correct match is found. It is important to note that not all smartphones are susceptible to this attack. Device manufacturers continually enhance security measures and often employ additional safeguards, such as setting limits on failed authentication attempts or incorporating anti-spoofing technologies like liveness detection. To safeguard against this threat, users should regularly update their smartphones with the latest security patches and firmware releases.

NCIIPC Initiatives

NCIIPC at Webinar Held by BSNL

A cyber security webinar was organised by BSNL on 25th April 2023 for capacity building and awareness of BSNL employees. Gp Capt. (Dr.) R.K. Singh, Director Telecom, NCIIPC has taken a session on "Observations and Expectations from BSNL". Around 250 participates joined the session from various zones of BSNL. Following topics were discussed by Director (Telecom) in the webinar:

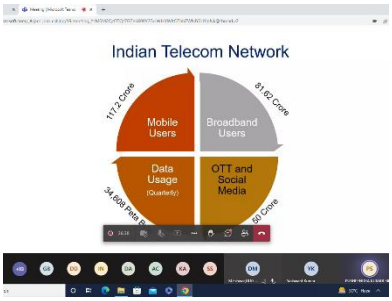
- Introduction, Roles and Responsibilities of NCIIPC
- Rules for the Information Security Practices and Procedures for Protected System, 2018
- Discusses related to Action Taken Report (ATR) of suspected malicious activity reports shared by NCIIPC and pending vulnerabilities.
- Recommendations to BSNL to improve Cyber Security posture.

Screenshot of the presentation

NCIIPC at Webinar Held by NTIPRIT

A webinar on "Telecom Security Ecosystem" was organised by NTIPRIT (National Telecommunications Institute for Policy Research, Innovation & Training) on 10th May 2023. This webinar focuses on role of various organisations like NSCS, CERT-In, NCIIPC, DOT, TEC in Telecom Security. More than 100 participants joined the webinar from various Telecom entities of the Nation. Gp Capt. (Dr.) R.K. Singh, Director Telecom, NCIIPC took a session on "Role of NCIIPC". Following topics were discussed by Director (Telecom) in the webinar:

- Introduction, Roles and Responsibilities of NCIIPC.
- Rules for the Information Security Practices and Procedures for Protected System, 2018.
- NCIIPC function and duties, CII Identification & notification process.
- CII Entities Baseline Compliances.

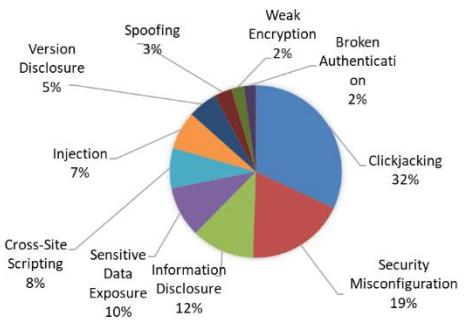


Screenshot of the presentation

NCIIPC Responsible Vulnerability Disclosure Program

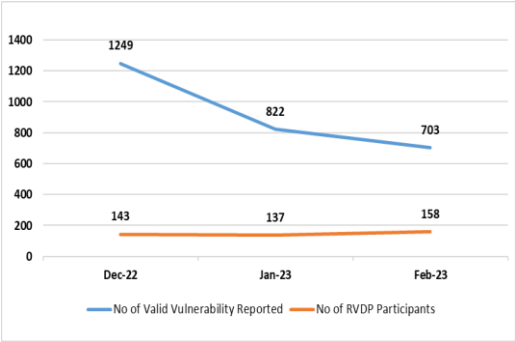
Source: https://nciipc.gov.in/RVDP.html

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 2102 vulnerabilities reported during the second quarter of 2023. The top 10 vulnerabilities are:



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

Around 374 researchers participated in RVDP programme during the second quarter of 2023. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):



Last three months' timeline chart for vulnerabilities and RVDP participants

- Abhijith Jd
- Abishek R
- Bijitha PB
- Jiss Jose
- Kaushal Singh
- No Name (Name of researcher is not available)
- Pallatil Tarun
- Sachin Gupta
- Sachin KS
- Shijin PS
- Shubhranshu Gorai
- Suvendu Dash
- Tarun Yenni
- Vinayphani Kumar
- Yati Kudtarkar

Upcoming Events - Global

July 2023

- World Class Remote Office Security 2023, Leipzig — 4-5 Jul
- Flagship Global 7th CISO 360 Congress, Barcelona — 5-7 Jul
- Internet 2.0 Conference, Las Vegas — 10-12 Jul
- Corinium: CISO Melbourne 2023, Melbourne — 17-19 Jul
- The 2023 Cyber Strategy Retreat Conference, Atlanta — 19-20 Jul
- AIBC Asia 2023, Manila — 19-22 Jul
- DC Metro Cyber Security Summit, Virginia — 20 Jul
- INTERFACE Montana 2023, Montana — 25 Jul

August 2023

- InfoSec Taiwan 2023, Taipei — 1-3 Aug
- Black Hat USA 2023, Las Vegas & Virtual — 5-10 Aug
- The Diana Initiative 2023, Las Vegas — 7 Aug
- DEF CON 31 (2023), Las Vegas — 10-13 Aug
- Detroit Cyber Security Summit, Detroit — 17 Aug
- HITBSecConf2023 - Phuket, Phuket — 21-25 Aug
- SANS Security Awareness: Managing Human Risk Summit 2023, Las Vegas & Virtual — 21-25 Aug
- Apidays Connect Hong Kong 2023, Hong Kong — 30-31 Aug

September 2023

- Data Saturday Oslo 2023, Oslo — 2 Sep
- BSides Kraków 2023, Kraków — 2 Sep
- Korea Blockchain Week 2023, Seoul — 4-10 Sep
- 14th Annual Billington CyberSecurity Summit, Washington DC — 5-8 Sep
- Cybersphere Philippines, Manila — 6-7 Sep
- CryptoVSummit 2023, Dubai — 18-19 Sep
- CyberHealth & Pharma Summit 2023, Barcelona — 21 Sep
- Cyber Security in the Financial Sector 2023, Copenhagen — 20-21 Sep

Corinium connected thinking

black hat

JULY 2023

S	M	T	W	T	F	S
30	31					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

AUGUST 2023

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		

apidays connect HONG KONG 2023

CYBERSPHERE PHILIPPINES 6-7 Sep 2023 Manila, Philippines

SEPTEMBER 2023

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

OCTOBER 2023

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				

October 2023

- Horizon Cyber Security Summit, Kahuku — 1-6 Oct
- Critical Infrastructure Protection & Resilience Europe, Prague — 3-5 Oct
- Cyber Security Summit, Charlotte — 4 Oct
- Health-ISAC European Summit 2023, Dubrovnik — 17-19 Oct
- Critical Infrastructure Cyber Security Summit, Virtual — 20 Oct
- The Rochester Security Summit, Rochester — 25-26 Oct
- SecureWorld Dallas, Dallas — 26 Oct
- Cyber Security Expo London 2023, London — 26 Oct

Upcoming Events - India

- Global CX Summit India 2023, Mumbai — 6 Jul
- BSides Jaipur, Jaipur — 22 Jul
- Exito Cyber Security Summit India, Mumbai — 2 Aug
- ESCON 2023 Cyber Security Leadership X-Change, Kolkata — 4-6 Aug
- NULLCON GOA 2023, Goa — 20-24 Sep
- Seasides Information Security Conference 2023, Goa — 21-22 Sep
- TECHSPO Delhi NCR 2023, New Delhi — 4-5 Oct

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

Incident Reporting : ir@nciipc.gov.in

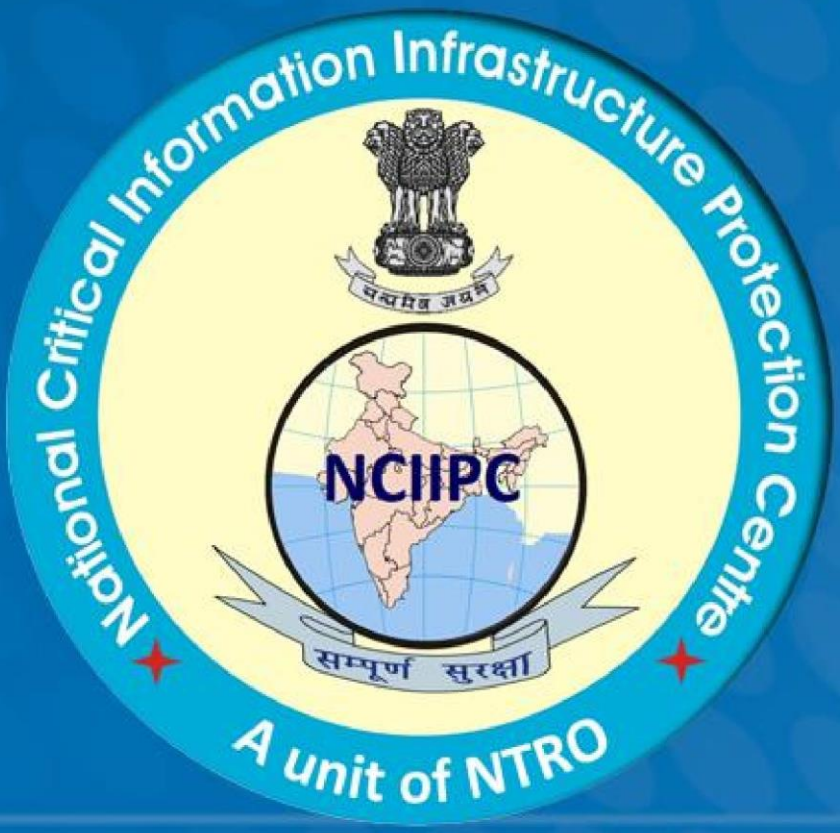
Vulnerability Disclosure : rvdp@nciipc.gov.in

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

Abbreviations

- 2FA: Two-Factor Authentication
- APT: Advanced Persistent Threat
- ATR: Action Taken Report
- C&C: Command-and-Control
- CAMF: Cancel After Match Fail
- CCoE: Cybersecurity Centre of Excellence
- CID: Criminal Investigation Department
- CISA: Cybersecurity and Infrastructure Security Agency
- CISO: Chief Information Security Officer
- CMAP: Character Map
- CSWSH: Cross-Site WebSocket Hijacking
- DDoS: Distributed Denial-of-Service
- DG: Director General
- DLP: Data-Loss Prevention
- DSCI: Data Security Council of India
- FTCCI: Federation of Telangana Chambers of Commerce and Industry
- GoTS: Government of Telangana
- GUAC: Graph for Understanding Artifact Composition
- IAM: Identity and Access Management
- IIB: Insurance Information Bureau of India
- IOCTL: Input and Output Control
- LEAs: Law Enforcement Agencies
- LoL: Living-off-the-Land
- LoLBins: Living-off-the-Land Binaries
- LSASS: Local Security Authority Subsystem Service
- MAL: Match After Lock
- MSME: Small and Medium Cybersecurity Enterprise
- NCRF: National Cybersecurity Reference Framework
- NI-MSME: National Institute of Micro, Small and Medium Enterprises
- NSA: National Security Agency
- NVD: National Vulnerability Database
- OSV: Open-Source Vulnerabilities
- OWASP: Open Worldwide Application Security Project
- RAT: Remote Access Trojan
- RTU: Remote Terminal Unit
- SBOM: Software Bill of Materials
- SLSA: Supply-chain Levels for Software Artifacts
- SMB: Small to Medium-sized Business
- SPI: Serial Peripheral Interface
- SSRF: Server-Side Request Forgery
- ZCS: Zimbra Collaboration Suite
- ZTM: Zero Trust Maturity
- ZTMM: Zero Trust Maturity Model

Notes



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.