NEWSLETTER

April 2023

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

भारत 2023 INDIA
वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

WELCOME TO G20 PRESIDENCY OF INDIA

During India's presidency of G20, MeitY is running a campaign 'Stay Safe Online' aimed at creating awareness among citizens.

The campaign focuses on sensitizing users of all ages about online risk & safety measures and promoting cyber hygiene thereby reinforcing the cyber safety of citizens.

'Stay Safe Online' Awareness Programs

- Pledge
- Quiz
- Quiz Competition
- Competitions
- Add Workshops
- Social Media Addiction
- Digital Addiction
- Winners

Participate at https://staysafeonline.in/

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

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

VOLUME 7 ISSUE 2

@NCIIPC

NCIIPC Newsletter

April 2023

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

It is a matter of pride that India has got the presidency of G20 with effect from 01 Dec 2022 to 30 Nov 2023. During India's presidency of G20, the Ministry of Electronics and Information Technology (MeitY) is running a campaign titled 'Stay Safe Online' aimed at creating awareness among citizens to stay safe in online world where widespread use of social media platforms and rapid adoption of digital payments has become inescapable.

NCIIPC organised a National Level Critical Information Infrastructure Security Exercise (CII-SECEX : 2023) during 22-23 April 2023. The event consists of 'Table Top Exercises' where top/middle management personnel from various Critical Sector Organisations participated and contributed to the brainstorming sessions focused towards emerging security aspects and technological advancements happening in the cyber security fields. Another part of the CII-SECEX : 2023 exercise is Operational Challenge; where employees from Critical Sector Organisation were divided into 40 team span across Delhi & NCIIPC three zonal centres (i.e. Mumbai, Bengaluru & Kolkata) and tried to defend against advance attacks by NCIIPC on Critical Information Infrastructures (CIIs). This Defender exercise was conducted during 22-23 April 2023.

NCIIPC also conducted 'Chintan Shivir' on the topic "Emerging Technologies and Approaches for Critical Information Infrastructure Protection" on 22nd April 2023. Representatives of various Critical Sector Entities (CSEs), Ministries, Regulators and Academia attended this session.

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

The Central Govt. to Build a Task Force to Fight Cyber Espionage

Source: https://theprint.in/

Central government is working on to build a task force, called the National Counter Ransomware Taskforce (NCRT) to prevent ransomware attacks. A three-fold security measure is suggested at All-India Conference of Directors General/ Inspectors General of Police. The conference also includes building an integrated national task force. The government is extremely concerned about cyber terrorism, cyber espionage and ransomware, especially since the ransomware attack at the All India Institute of Medical Science (AIIMS) Delhi in November. It also plans to hold regular conferences of Chief Information Security Officers (CISO) and routine coordination meetings of the state Home Secretaries.

All-India Conference of Directors General/ Inspectors General of Police

Firms Should Invest 10% More of IT Assets in Cyber Security

Source: https://www.thehindu.com/

"Organisations should invest more than 10 percent of their information technology assets to cybersecurity without making any compromises. Once 5G is available, it is anticipated that the current 5 billion Internet users will increase to 25 billion by the end of year 2023 therefore companies must invest in security", Lt. Gen. (Retd.) Dr. Rajesh Pant, National Cyber Security Coordinator said at the 17th India Digital Summit (IDS) organised by the Internet and Mobile Association of India (IAMAI) in partnership with MessageBird and Google. According to the World Economic Forum, cybercrime is the biggest man-made threat to any country's ability to advance economically. The World Economies last year reported a total loss of 6 trillion dollars. India, Australia, United Kingdom, and United States have established an International Counter Ransomware Task Force to battle ransomware, which imposes fines on those who commit cybercrime.

Lt. Gen. (Retd.) Dr. Rajesh Pant, NCSC

News Snippets - International

DDoS Attack Targeted German Airports

Source: https://therecord.media/

Seven German airports' websites were attacked by a series of Distributed Denial-of-Service (DDoS) attack resulting a major IT glitch at Lufthansa, grounding flights. It was a major IT failure at Lufthansa and left thousands of passengers stranded as a result of shutting down of airport website.

Customer had been warned by the company that their accounts might have been compromised in a security breach and around 925,000 people were targeted.

Norton Password Manager Accounts Targeted

Source: https://www.bankinfosecurity.com/, https://therecord.media/, https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com

Norton Life Lock company which provides antivirus software and identity theft protection informed that their customer accounts were compromised by credential-stuffing attack on 19th January 2023. Customer had been warned by the company that their accounts might have been compromised in a security breach and around 925,000 people were targeted. Attackers might have also access to Norton Password Manager users' private vault data, which contains stored passwords used to access online accounts.

Digital Intelligence Firm Cellebrite's 1.7 TB of Data Stolen

Source: https://securityaffairs.com/

Mobile forensics firm named Cellebrite which provides tools for law enforcement and intelligence agencies worldwide, has got its 1.7 TB of data stolen through online mode. This company provides UFED (Universal Forensic Extraction Device) services required to unlock and access data on mobile devices.

Trends

A record-breaking distributed Denial-of-Service (DDoS) attack peaked at over 71 million requests per second (RPS), disclosed by Web infrastructure company Cloudflare.

Massive HTTP DDoS Attack Hits 71 million Requests/Second

Source: https://thehackernews.com/

A record-breaking distributed Denial-of-Service (DDoS) attack peaked at over 71 million requests per second (RPS), disclosed by Web infrastructure company Cloudflare. It is one of the largest HTTP DDoS attacks reported till date and it is 35% higher than the previous 46 million RPS DDoS attack. A popular gaming provider, cryptocurrency companies, hosting providers, and cloud computing platforms are included in the targeted websites. A tsunami of HTTP requests towards a target website is sent in these kind of HTTP attacks, what the website cannot handle, with the goal of making it inaccessible. For criminal actors, the DDoS attacks are lucrative means for earning illicit revenues by demanding ransom from victims, usually in the form of Bitcoin. Aviation, education, gaming, hospitality, and telecom are some of the majorly attacked industry verticals.

Gcore Thwarts Massive 650 Gbps DDoS Attack on Free Plan Client

Source: https://thehackernews.com/

Gcore faced an incident at the beginning of January involving several L3/L4 DDoS attacks with a peak volume of 650 Gbps. Over 2000 servers were exploited by attackers belonging to one of the top three cloud providers worldwide and targeted a client using a free CDN plan. However, due to a large number of peering partners and Gcore's distribution of infrastructure, the attacks were mitigated, and the client's web application remained available. The incident duration was 15 minutes, and at its peak, it reached over 650 Gbps. A possible reason why the incident took such a long duration is that the attackers weighed the ineffectiveness of the attacks against their high cost. DDoS attacks will continue to grow year over year according to Gcore's experience. The attacks reached 300 Gbps in 2021, and by 2022, they increased to 700 Gbps. Therefore, even small and medium-sized businesses need to use distributed content delivery networks such as the CDN and Cloud to protect against DDoS attacks.

A possible reason why the incident took so long is that the attackers weighed the ineffectiveness of the attacks against their high cost.

Researchers Discover New Information Stealer 'Stealc' in the Wild

Source: https://thehackernews.com/

Stealc is a new information stealer advertised on the dark web which could come up as a notable competitor to other malware of its category. The users who are in a search of pirated software on YouTube are the target. As the distribution vectors are using YouTube videos posted from the compromised accounts and these compromised accounts are linked to a website peddling cracked software (rcc-software.com). Stealc code is written in C language. It was first marketed by a person named Plymouth in January 2023, on BHF Russian-speaking underground forums and XSS. It comes with capabilities to steal data from email clients, web browsers, messaging apps and crypto wallets. Stealc is presented as a fully featured, ready-to-use stealer. Its development relied on RedLine, Racoon, Vidar, and Mars stealers.

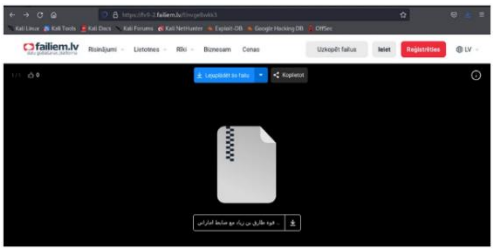
Stealc is a new information stealer advertised on the dark web which could come up as a notable competitor to other malware of its category.

Malware Bytes

Earth Bogle Campaigns Target the Middle East with NjRAT Trojan

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

Geopolitically themed lures are being used in campaign called Earth Bogle to spread the NjRAT remote access trojan to victims in the Middle East and North Africa. The threat actor uses public cloud storage services such as files[.]fm and failiem[.]lv to host malware, and distributes NjRAT through compromised web servers. The next-stage payload is deployed via a Visual Basic



Malicious CAB file hosted on cloud sharing services

To combat this threat, it is advised that users and security teams keep their systems' security solutions updated and their respective cloud infrastructures properly secured.

Script dropper contained in a Microsoft Cabinet (CAB) archive file masqueraded as a sensitive audio file, named using a geopolitical theme as a lure for the victims to open it. The distribution mechanism includes phishing emails, social media, or file sharing. Once the malicious CAB file has been downloaded, an infected or spoofed host is used by the obfuscated VBS script to retrieve the malware. It then retrieves a PowerShell script that injects NjRat into the victim's machine. To combat this threat, it is advised that users and security teams keep their systems' security solutions updated and their respective cloud infrastructures properly secured.

Malware Distributed by Abusing Legitimate GitHub Feature

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

The 'sharing forwarded ports publicly' GitHub Codespaces feature can be abused by malicious actors to create a malware file server using a legitimate GitHub account.

Cybersecurity firm Trend Micro has discovered that it is possible for threat actors to abuse GitHub Codespaces' legitimate feature to deliver malware to victim systems. The 'sharing forwarded ports publicly' GitHub Codespaces feature can be abused by malicious actors to create a malware file server using a legitimate GitHub account. The exploited environments of GitHub Codespaces would not be flagged as suspicious or malicious even as it serves malicious content (such as scripts, malware, and ransomware, among others), and organisations would consider these events as benign or false positives. Considering the potential extensive use of Codespaces for ease in building, developers are strongly advised to properly secure their respective projects by applying threat modelling and testing.

Fortinet Vulnerability Exploited to Drop BOLDMOVE Backdoor

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

Threat actors can remotely manage files, execute commands, create interactive shell, and backdoor control by using the commands supported by BOLDMOVE.

Hackers have exploited a heap-based buffer overflow vulnerability in FortiOS SSL-VPN (CVE-2022-42475, a zero-day) and targeted European government entity and an African MSP with a new custom 'BOLDMOVE' Linux and Windows malware designed mainly to run on FortiOS devices. The Linux variant of BOLDMOVE malware has the capability to read data from a Fortinet-exclusive file format. The Linux variant can also send requests to the internal Fortinet services, thereby allowing threat actors to send network requests to the entire internal network and spread laterally to other devices. BOLDMOVE is a full-featured backdoor written in C that allows hackers to take over the service at a higher-level. Threat actors can remotely manage files, execute commands, create interactive shell, and backdoor control by using the commands supported by BOLDMOVE. The malware also disables and manipulates logging features (called Indicator Blocking) to avoid detection.

Hackers Destroy Windows Domains Using New SwiftSlicer Wiper

Source: bleepingcomputer.com, cyware.com, welivesecurity.com

The researchers of ESET have discovered a new data-wiping malware named SwiftSlicer that aims to overwrite important files used by Windows operating system. SwiftSlicer can be deployed by using Active Directory Group Policy, which allows domain admins to execute scripts and commands throughout all of the devices in Windows network. SwiftSlicer has the capacity to destroy shadow copies and to overwrite crucial files in the Windows system directory, specifically drivers and the Active Directory database. The wiper's targeted destruction of the %CSIDL_SYSTEM_DRIVE%\Windows\NTDS folder suggested that indicates that it is not only meant to destroy files but to also bring down the entire Windows domains. SwiftSlicer wiper overwrites the data by using 4096 bytes blocks that consists of randomly generated bytes. After completion of the data destruction job, SwiftSlicer reboots the systems.

SwiftSlicer has the capacity to destroy shadow copies and to overwrite crucial files in the Windows system directory, specifically drivers and the Active Directory database.

Malicious VPN Installers Disrtibutes EyeSpy Spyware

Source: heimdalsecurity.com, thehackernews.com, www.bitdefender.com

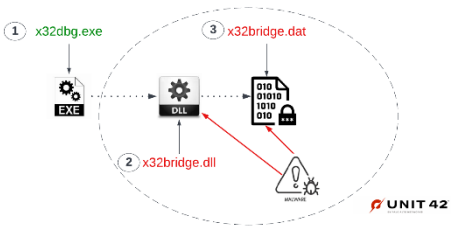
Cybersecurity researchers have discovered a malware campaign that deliver a piece of surveillanceware named EyeSpy. The surveillanceware uses the components of SecondEye, a legitimate monitoring application, to spy on users of 20Speed VPN (an Iranian-based VPN service) via trojanised installers. The attack chain begins with the download of a malicious executable from 20Speed VPN's website. Once installed it stealthily triggers other malicious activities in the background for persistence and next-stage payload downloads in a bid to exfiltrate personal data in compromised computers. EyeSpy has the capability to completely compromise online privacy via keylogging and stealing of sensitive information, such as images, passwords, documents, and crypto wallets. This can lead to identity theft, complete account takeovers and financial loss.

EyeSpy has the capability to completely compromise online privacy via keylogging and stealing of sensitive information, such as images, passwords, documents, and crypto wallets.

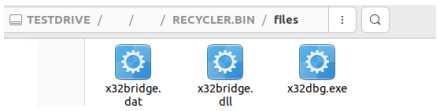
New PlugX Malware Variants Spreads via USB Devices

Source: https://unit42.paloaltonetworks.com/, https://thehackernews.com/

Palo Alto Networks' researchers have discovered new PlugX variants that uses sneaky techniques to infect attached removable USB media devices in order to propagate the malware to other systems. This PlugX variant can spread over USB devices and infect by concealing itself from the Windows operating file system, which makes it impossible for a user to know that their USB device is infected or is being used to steal data from their networks. The PlugX USB variant uses a peculiar Unicode character called non-breaking space (U+00A0) that hide files in a USB device



PlugX DLL sideloading using x64dbg



Ubuntu File Explorer viewing an infected USB device

plugged into a device. The malware is executed from the hidden directory by using a Windows shortcut (.LNK) file that was created in the root folder of the flash drive. A second variant of PlugX has also been discovered that not only infects the USB devices but it also copies all Adobe PDF and Microsoft Word files from the host to a hidden folder created by the malware on the USB device.

ReverseRAT Backdoor Targeting Indian Government Agencies

Source: https://thehackernews.com/

Once ReverseRAT gains persistence, it enumerates the victim's device, collects data, encrypt the data using RC4 and sends it to the Command-and-Control (C2) server.

A phishing campaign aims to deploy a backdoor called ReverseRAT that is targeting Indian government agencies. This backdoor is embedded into a macro enabled Word document which masquerades as a fake advisory from India's Ministry of Communications. Once the file is opened and macros are enabled by the victim, it triggers the execution of malicious code on victim's machine and leads to the deployment of ReverseRAT on the compromised system. Once ReverseRAT gains persistence, it enumerates the victim's device, collects data, encrypt the data using RC4 and sends it to the Command-and-Control (C2) server.

MyloBot Botnet Spreading Rapidly Worldwide

Source: https://thehackernews.com/

The primary function of the botnet is to establish a connection to a hard coded Command & Control domain embedded within the malware and wait for further instructions.

A sophisticated botnet known as MyloBot has compromised thousands of systems and most of them are located in India, the United States of America, Indonesia and Iran. The primary function of the botnet is to establish a connection to a hard coded Command & Control domain embedded within the malware and wait for further instructions. Once MyloBot receives instruction from the Command & Control server, it transforms the infected workstation into a proxy.

Recent Ransomware Attacks Occurred Globally

Knowledge Management Team, NCIIPC

The attack slowed down the process of connecting new customers, customers' enquiry management, and bills delivery.

Ransomware groups were busy in the first quarter of 2023, targeting various major enterprises. Tonga's state-owned telecommunications company Tonga Communications Corporation (TCC) was hit with ransomware attack on 13th February 2023. The ransomware attack encrypted and locked access to part of TCC's system. The attack slowed down the process of connecting new customers, customers' enquiry management, and bills delivery. TCC worked with security companies in order to mitigate the negative impact of this malware attack.

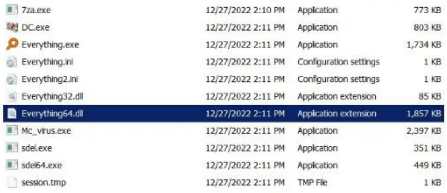
Oakland declared a local state of emergency due to the impact of a ransomware attack that forced the city to take all its IT

systems offline on 8th February 2023. The ransomware attack did not affect the core services like 911 dispatch and fire and emergency resources, while it impacted the non-emergency services. The systems were immediately taken down after the attack to contain the threat. Oakland's IT Department is still working with a leading forensics firm on recovery and remediation of the systems. In its official site Oakland has declared that the personal information of current and former Oakland employees was compromised.

The ASEC researchers discovered the distribution of TZW ransomware affecting South Korean organisations, which encrypts files before adding the 'TZW' file extension to the file's original extension. The ransomware was propagated with the version information marked as 'System Boot Info', as a fake program file associated with boot information.

The ASEC researchers discovered the distribution of TZW ransomware affecting South Korean organisations, which encrypts files before adding the 'TZW' file extension to the file's original extension.

The researchers of Trend Micro have discovered 'Mimic' ransomware that abuses the APIs of a legitimate file search tool called 'Everything' for Windows to search for files targeted for encryption. The payload of Mimic ransomware is contained in a password-protected archive that is disguised as Everything64.dll and dropped by the executable Mimic along with several other binaries and tools to disable Windows Defender. It is a versatile ransomware that uses command line arguments to target specific files and can use multiple processor threads to encrypt data more quickly.



7za.exe	12/27/2022 2:10 PM	Application	773 KB
DC.exe	12/27/2022 2:11 PM	Application	803 KB
Everything.exe	12/27/2022 2:11 PM	Application	1,734 KB
Everything.ini	12/27/2022 2:11 PM	Configuration settings	1 KB
Everything2.ini	12/27/2022 2:11 PM	Configuration settings	1 KB
Everything32.dll	12/27/2022 2:11 PM	Application extension	85 KB
Everything64.dll	12/27/2022 2:11 PM	Application extension	1,857 KB
Mc_virus.exe	12/27/2022 2:11 PM	Application	2,397 KB
sdel.exe	12/27/2022 2:11 PM	Application	351 KB
sdel64.exe	12/27/2022 2:11 PM	Application	449 KB
session.tmp	12/27/2022 2:11 PM	TMP File	1 KB

Mimic ransomware's dropped components

Clop ransomware group took advantage of a zero-day vulnerability in GoAywhere MFT secure file transfer tool. The ransomware group stole data from over 130 organisations after breaching servers vulnerable to exploits targeting this flaw. GoAnywhere MFT's developer Fortra disclosed to its customers that the vulnerability was being exploited as a zero-day in the wild. The company provided emergency security updates for its customers to secure their servers from future incoming attack attempts.

Recently, cybercriminals have used a variant of Xorist commodity ransomware named 'MortalKombat' along with the Laplas clipper in various cyberattacks. Laplas, a cryptocurrency hijacker, monitors the Windows clipboard for crypto addresses and, when found, replaces them with addresses that are under the attacker's control. The ransomware is initiated through a phishing email, in which the attackers impersonate Coin Payments, using malicious ZIP attachment having a BAT loader script that downloads an archive from a remote resource. The loader script executes the downloaded payload as a process in the compromised system and thereby deletes the downloaded files to reduce the chances of detection.

The ransomware is initiated through a phishing email, in which the attackers impersonate Coin Payments, using malicious ZIP attachment having a BAT loader script that downloads an archive from a remote resource.

References:

[1] https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware

[2] https://www.oaklandca.gov/news/2023/city-of-oakland-

targeted-by-ransomware-attack-core-services-not-affected

[3] https://www.bleepingcomputer.com/news/security/city-of-oakland-declares-state-of-emergency-after-ransomware-attack/

[4] https://asec.ahnlab.com/en/46812/

[5] https://www.trendmicro.com/en_us/research/23/a/new-mimic-ransomware-abuses-everything-apis-for-its-encryption-p.html#:~:text=Ransomware-,New%20Mimic%20Ransomware%20Abuses%20Everything%20APIs%20for%20its%20Encryption%20Process,updates%20for%20minimal%20resource%20usage.

[6] https://www.bleepingcomputer.com/news/security/new-mimic-ransomware-abuses-everything-windows-search-tool/

[7] https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

'Dark Power'- New Ransomware Gang

South Zone, NCIIPC

A nascent gang of ransomware named Dark Power is attacking various organisations worldwide for a reasonable small ransom demand. Its payload is written in 'Nim' language. It is a compiled high-level systems programming language, which is now more widespread and popular among threat actors since it has cross-platform capabilities making it suitable for malware conception. It also features high degree of configurability; and robust anti-tamper controls resulting in the detection, analysis and removal harder or highly challenging.

Threat actors have used this ransomware to target wide range of large businesses, educational institutions, enterprises and critical infrastructure organisations including transport, manufacturers, healthcare and medical industries.

Targets: Threat actors have used this ransomware to target wide range of large businesses, educational institutions, enterprises and critical infrastructure organisations including transport, manufacturers, healthcare and medical industries. As this type of Ransomware is extremely active in USA, France, Israel, Turkey, Czech Republic, Algeria, Egypt, and Peru, the targeting space is global.

Modus Operandi: Once the Ransomware is executed, it creates an arbitrary 64-character ASCII string, which is then used to initialise the encryption algorithm. The randomisation confirms that the key is exclusive each time the code is executed. Therefore, it is unique on each hacked machine, hampering the creation of a decryption tool. After collecting victim's sensitive data, the threat actor can stop explicit services which includes back-up & anti-

malware services, processes. The threat actor can also delete shadow copies of the targeted machine making it difficult for the victim to recover those files. In order to mitigate counter analysis, ransomware gang clears the system logs and console.

Attacker then send a ransom note in a PDF file. The message also offers free decryption of one encrypted file for proving the legitimacy of the attacker and also a brief about how they have hacked the machine. That pdf file contains instruction on how they should contact them over the messenger.

The message also offers free decryption of one encrypted file for proving the legitimacy of the attacker and also a brief about how they have hacked the machine.

Best practices: Ransomware attacks can be hard to prevent, as these spread often through social engineering mechanisms. Following are some of the critical cybersecurity best practices that create the first line of defence against attackers:

- Security software definitions should be up to date regularly.
- Always update operating system and installed programs timely.
- Implement a robust backup and recovery system by maintaining numerous copies of sensitive data and servers both on-site and off-site in a completely separate, segmented, and safe location and also ensure that all backup data is encrypted.
- Organisations should have Incident Response Plan in place.
- Implement multifactor authentication wherever possible to provide extra layer of security particularly the accounts that access critical systems.
- Harden the firmware, software and all operating systems periodically to reduce security risk by eliminating potential attack vectors and abridging the system's attack surface.
- All user accounts need to be audited.
- Follow the principle of least privilege while configuring the access controls.
- Always disable unused ports.
- Cybersecurity awareness training should be conducted for the end users to stay updated about the current threats on regular basis.

Harden the firmware, software and all operating systems periodically to reduce security risk by eliminating potential attack vectors and abridging the system's attack surface.

References:

[1] https://www.bleepingcomputer.com/news/security/new-dark-

power-ransomware-claims-10-victims-in-its-first-month/

[2] https://www.darkreading.com/vulnerabilities-threats/dark-power-ransomware-extorts-10-targets-less-than-a-month

[3] https://techdator.net/dark-power-ransomware-mechanism/

New Evasion of Emotet Malware

Knowledge Management Team, NCIIPC

The new form of Emotet has become a highly modular threat as it can allow attackers to distribute largely to users via PDF file attachment, malicious files within the emails with variety of modular Payloads.

Emotet is a highly adaptable malware first emerged in 2014. Attackers have been using this malware to target the banking sector. The malware method of self-Propagation and brute forcing passwords makes the detection, analysis and removal harder or highly challenging. The new form of Emotet has become a highly modular threat as it can allow attackers to distribute largely to users via PDF file attachment, malicious files within the emails with variety of modular Payloads. New version of Emotet uses elliptic curve cryptography encryption structure for command-and-control communication. Malware has the capability to support any payload. It had discrete payloads modules for its loader, Distributed Denial of Service (DDoS) attacks, banking fraud, credentials theft, ability to verify blacklisted IP on a spam list, extracting email address, ransomware and mail spam and more.

Once machine is infected, attacker performs anti-analysis check to confirm that it is not being run on a malware analysis machine, then downloads the key component and executes additional malicious payloads to gain access to other machines on the same network.

Modus Operandi: Malware reaches users via spam emails with malicious file attached to it. Once machine is infected, attacker performs anti-analysis check to confirm that it is not being run on a malware analysis machine, then downloads the key component and executes additional malicious payloads to gain access to other machines on the same network. Once taken control the module is then able to affect the processing of each and every request. Network spreading ability of the malware can infect the machine without user interaction. Emotet uses Command & Control servers run by the attackers to collect updates.

Best practices:

- Download software from certified pages and genuine stores only.
- Downloads from third-party downloaders, P2P networks (e.g., torrent clients) should be avoided.
- Double-check emails before opening their contents.
- Refrain from opening suspicious links and attachments in email without verifying their authenticity.
- Do not trust advertisements.

- Configure regular scans and settings
- Cybersecurity awareness training should be implemented for the end users to stay across current threats on regular basis.
- Limit file-sharing.
- Implement email security and spam protection.
- Always update operating system and installed programs timely.
- Usage of firewall or endpoint security solution should be managed and monitored
- Periodically apply latest security updates.
- Keep antivirus & threat protections always enabled.

Usage of firewall or endpoint security solution should be managed and monitored

References:

[1] https://symantec-enterprise-blogs.security.com/blogs/evolution-emotet-trojan

[2] https://heimdalsecurity.com/blog/emotet-malware-history/

[3] https://en.wikipedia.org/wiki/Emotet

Exploitation of The Popularity of ChatGPT

South Zone, NCIIPC

The massive popularity of ChatGPT (Chat Generative Pre-trained Transformer) is now being exploited by cybercriminals thereby creating fake apps and distributing these apps endlessly through various means by luring uninterrupted and free access of the premium version. Fake ChatGPT is being promoted by third-party malicious apps to perform suspicious activities thereby pushing and spreading malwares by giving false offers to the users and in addition, redirecting users to various phishing pages. Threat actors by means of fake ChatGPT are spreading malwares via fake social media pages and email attachment. In order to make fake ChatGPT more legitimate, attackers are using official logos and by posting content such as text and videos of various tools to trick the victims and carry out malicious activities like steal sensitive and personal information.

ChatGPT on Mozilla Firefox
Image source:
https://en.wikipedia.org/wiki/ChatGPT

Modus Operandi: Once user clicks on the link of the cloned app, he/she ends up downloading a fake malicious ChatGPT client that would infect them or else it will redirect to a phishing page to capture their login information. The malware then downloads the malicious script into the memory of the victim system, which act as

a main or final payload and can execute malicious activities in the system. Once taken control, the module is then able to affect the processing of each and every request, in no time, it can even take control of network without user interaction.

Once taken control, the module is then able to affect the processing of each and every request and in no time, it can take control of network without user interaction.

The following best practices may help to reduce the risk of incidents caused by fake Chat GPT:

- Hardening of firmware, software and all operating systems should be done periodically to reduce security risk by eliminating potential attack vectors and abridging the system's attack surface.
- Audit all user accounts and configure access controls according to the principle of least privilege.
- If a victim suspects that he or she downloaded a fake ChatGPT app that may contain malware, the app should be uninstalled immediately.
- Always disable unused ports.
- Do not trust advertisements.
- Configure regular scans and monitor various security settings of the system.
- Implement email security and spam protection.
- Do not use unofficial tools to update the software.
- Double-check emails and links before opening their contents.
- Download software from certified pages and genuine stores only.

If a victim suspects that he or she downloaded a fake ChatGPT app that may contain malware, the app should be uninstalled immediately.

References:

[1] https://www.bleepingcomputer.com/news/security/hackers-use-fake-chatgpt-apps-to-push-windows-android-malware/

[2] https://www.theatlantic.com/technology/archive/2022/12/chatgpt-openai-artificial-intelligence-writing-ethics/672386/

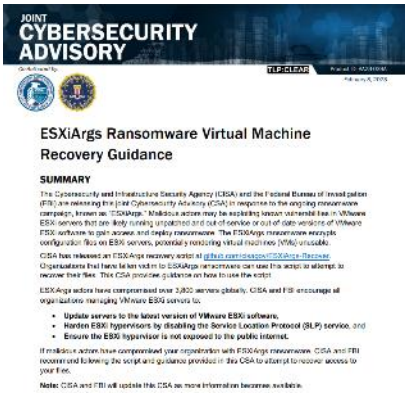
[3] https://www.gadgetsnow.com/featured/chatgpt-sms-gaming-and-other-fake-apps-that-hackers-use-to-steal-your-money/articleshow/98288672.cms

Learning

CISA & FBI Release Recovery Guidance on ESXiArgs Ransomware

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

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have issued a Joint Cybersecurity Advisory (CSA) regarding the ongoing ransomware campaign known as 'ESXiArgs'. Attackers are exploiting known vulnerabilities in VMware ESXi servers, which are running on unpatched and outdated software versions. ESXiArgs ransomware encrypts configuration files rendering Virtual Machines (VMs) unusable and has compromised more than 3,800 servers worldwide. To restore files, CISA has released the ESXiArgs recovery script on GitHub, and provides guidance on how to use it. This script does not attempt to delete encrypted profiles, but rather attempts to create new profiles that allow access to the virtual machine. It is also recommended to disable the Service Location Protocol (SLP) service, update to the latest version of VMware ESXi software, and ensure that the ESXi hypervisor is not exposed to the public Internet.


JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

ESXiArgs Ransomware Virtual Machine Recovery Guidance

SUMMARY

Identity and Access Management

Source: https://media.defense.gov/

Identity and access management (IAM) is a framework of business policies, processes, and technologies that facilitate the management of digital identities to ensure that users only gain access to the data when they have the appropriate credentials. In addition to managing physical users, IAM administrators must also manage service and system accounts within their organisations. The critical infrastructure organisations have responsibility to implement, maintain, and monitor secure IAM solutions and processes to protect not only their own business functions and information but also the organisations and individuals with whom they interact.

The critical infrastructure organisations have responsibility to implement, maintain, and monitor secure IAM solutions and processes to protect not only their own business functions and information but also the organisations and individuals with whom they interact.

IAM Threat Mitigation Techniques: the best practices and mitigations provide tactics that help to counter threats to IAM through prevention, detection, damage limitation, deterrence, and response related to: Identity Federation and Single Sign-On, Identity Governance, Multi-Factor Authentication, Environmental Hardening, and IAM Monitoring and Auditing.

Identity Governance: Identity governance is the method by which an organisation centralises orchestration of its service and user accounts management in accordance with their policies. Identity governance provides organisations with better visibility to identities and access privileges, along with better controls to detect and prevent inappropriate access. It is comprised of a set of processes

and policies that cover the segregation of duties, logging, access review, role management, analytics, and reporting. Identity governance solutions can manage the entire identity and access lifecycle for an organisation's workforce. It provides a comprehensive view of an organisation's identity management practices and identify gaps in the identity management lifecycle. This centralised control and visibility helps to mitigate the risk that identities and privileges will be mismanaged, as well as the risk that attackers can exploit different systems within an organisation without being detected. Effective identity governance can mitigate the impacts of many prevalent IAM threats:

Identity governance solutions can manage the entire identity and access lifecycle for an organisation's workforce.

- Social engineering, phishing, or spear phishing
- Insider threats
- Creating accounts to maintain persistence

Environmental Hardening: Hardening the enterprise environment includes making sure the foundations and implementations of IAM are sufficiently secured, assured, and trusted. The degree of hardening will vary depending on what is being protected. Environmental hardening secures the hardware components and software in the enterprise environment around the IAM solution. Combining environmental hardening (patching, asset management, and network segmentation) best practices with sound IAM foundations and implementations reduces the likelihood of a compromise and limits potential damage. Bad actors target IAM solutions because they can provide access to a significant amount of sensitive data, enables persistence, and be used for future malicious cyber operations. IAM solution components must be hardened to prevent footholds for attackers to pivot to more critical systems. Hardening the enterprise environment, including the IAM systems as critical resources, helps to limit the potential for a compromise and keep the IAM system safe and accessible.

Hardening the enterprise environment, including the IAM systems as critical resources, helps to limit the potential for a compromise and keep the IAM system safe and accessible.

Identity Federation and Single Sign-On (SSO): Identity Federation and SSO simplifies identity management internally within an enterprise and with trusted external partners by reducing the need for users to maintain multiple identities in both internal and external directories, applications, and other platforms, eliminating the need for local identities at each asset. It allows for seamless integration with other security controls such as privileged access management for step-up authentication and increases confidence that only active users are allowed access. Organisations should develop and deploy SSO friendly applications and platforms to eliminate all local accounts and/or identities. This will improve the user experience while also significantly reducing the risk associated with local accounts which are difficult to manage and monitor.

It allows for seamless integration with other security controls such as privileged access management for step-up authentication and increases confidence that only active users are allowed access.

Multi-Factor Authentication (MFA): MFA mitigates common attacks

against passwords such as brute force guessing and credential stuffing as well as common password misuse practices like password sharing by requiring the presentation of another factor in addition to the password. Unless an attacker can defeat the MFA authentication mechanism, knowing the password by itself does not enable impersonation of the user. MFA can provide strong protection against many of the most prevalent attacks against authentication systems.

IAM Monitoring and Auditing: IAM auditing and monitoring includes not only check for compliance, but also monitor for threat indicators and anomalous activities. This encompasses the generation, collection, and analysis of logs, events, and other information to provide the best means of detecting compliance related infractions and suspicious activities. These auditing and monitoring capabilities can be integrated with automated tools that orchestrate response actions to counter these IAM attacks. Effective reporting from auditing and monitoring also provide situational awareness of the security posture of an organisation's IAM.

These auditing and monitoring capabilities can be integrated with automated tools that orchestrate response actions to counter these IAM attacks.

Vulnerability Watch

Critical Vulnerability in Avast Antivirus

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-4291

A potentially exploitable heap corruption vulnerability was discovered in aswjsflt.dll library from Avast Antivirus that could allow an attacker to bypass the sandbox of application it was loaded into. The CVE ID for this vulnerability is CVE-2022-4291 with CVSS v3 score of 10. This issue was resolved in version 18.0.1478 of the Script Shield Component. To mitigate this vulnerability, it is recommended that users should update their security software as well as their tech devices to the latest version available.

Image source: https://www.avast.com/

Critical Vulnerability in XSA-423 Version 2

Source: https://xenbits.xenproject.org/xsa/advisory-423.txt

It has been observed that NIC interface reset/abort/crash can be triggered by guests via netback. The CVE ID for this flaw is CVE-2022-3643 with CVSS v3 score of 10. Successful exploitation of this vulnerability allows unprivileged guests to cause network Denial of Service (DoS) of the host by sending network packets to the Linux based network backend causing the related physical NIC to reset, abort, or crash. All systems using a Linux based network backend with kernel 3.19 and newer are vulnerable. To mitigate the vulnerability, it is recommended to use another PV network backend or a dedicated network driver domain per guest.

To mitigate the vulnerability, it is recommended to use another PV network backend or a dedicated network driver domain per guest.

Critical Vulnerability in Rack

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-30123

This vulnerability allows a possible shell escape in the Lint and CommonLogger components of Rack.

Critical sequence injection vulnerability has been discovered in Rack application which provides a minimal interface between web servers that support Ruby and Ruby frameworks. This vulnerability allows a possible shell escape in the Lint and CommonLogger components of Rack. The affected versions are: Rack prior to 2.0.9.1, Rack prior to 2.1.4.1 and Rack prior to 2.2.3.1. The CVE Id for this vulnerability is CVE-2022-30123 with CVSS v3 score of 10.0.

Critical Vulnerability in Jenkins Email Extension Plugin

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-25765

Critical Arbitrary code execution vulnerability has been discovered in Jenkins Email Extension Plugin. Jenkins Email Extension Plugin allows a user to configure every aspect of email notifications. It was discovered in Jenkins Email Extension Plugin that the templates defined inside a folder were not subject to Script Security protection. This vulnerability can allow an attacker to define email templates in folders to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM. The affected versions are Jenkins Email Extension Plugin 2.93 and below. The CVE Id for this vulnerability is CVE-2023-25765 with CVSS v3 score of 9.9.

Neutrino 430

Nova 430e

Nova 436i

Nova 436Q

Image source: https://na.baicells.com/

Critical Vulnerability in Baicells

Source: https://nvd.nist.gov/, https://baicells.zendesk.com/

A remote shell code exploitation via HTTP command injections affected the Baicells products.

Critical vulnerability with CVE Id CVE-2023-0776 having CVSS v3 score of 10.0 has been discovered in Baicells. Baicells provides LTE Outdoor Base Stations and LTE Indoor Base Stations products. A remote shell code exploitation via HTTP command injections affected the Baicells products. The affected products are Baicells Nova 430i, Nova 436Q, Nova 430e, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7. To mitigate this vulnerability the firmware is to be updated to QRTB 2.12.8 and later.

Critical Vulnerability found in Synology VPN Plus Server

Source: https://www.cve.org/, https://nvd.nist.gov/

Synology®

Synology VPN Plus Server has been found to have Out-of-bounds write vulnerability in Remote Desktop Functionality. The CVE ID for the vulnerability is CVE-2022-43931 with CVSS v3 score of 10.0. The vulnerability allows execution of arbitrary commands via unspecified vectors by remote attackers. Users of VPN Plus Server for SRM 1.3 and VPN Plus Server for SRM 1.2 are advised to upgrade to version 1.4.4-0635 or above and 1.4.3-0534 or above respectively.

Critical Vulnerability found in Mozilla Firefox and Thunderbird

Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4140

A critical vulnerability has been found affecting Mozilla Firefox ESR prior to 91.5, Firefox prior to 96, and Thunderbird prior to 91.5. The CVE ID for the vulnerability is CVE-2021-4140 with CVSS v3 score of 10.0. With the help of this vulnerability, one can bypass an iframe sandbox by constructing specific Extensible Stylesheet Language Transformations (XSLT) markup. Using XSLT, XML documents can be transformed into other formats. Users are requested to update to latest version of Firefox and Thunderbird.

Critical Vulnerability found in Netgear Router

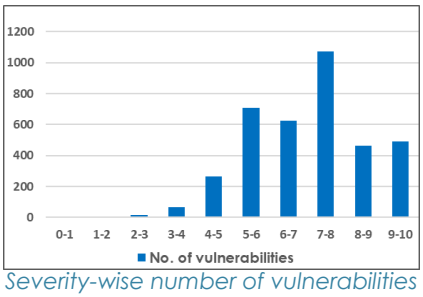
Source: https://www.cve.org/CVERecord?id=CVE-2022-4390

NETGEAR RAX30 AX2400 series of routers with versions prior to 1.0.9.90 has been found to be vulnerable with CVSS v3 score of 10.0 (CVE-2022-4390) due to a network misconfiguration. These routers have IPv6 enabled by default for the WAN interface. It has been found that, firewall restrictions are already in place for IPv4 traffic but they are not applied to IPv6. So, any device listening to services at SSH (port 22) and Telnet (port 23) getting arbitrary access which leads to an attacker can get access to devices internal to network.

Quarterly Vulnerability Analysis Report

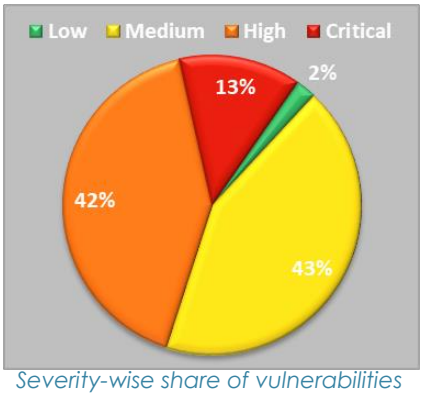
KMS Team, NCIIPC

During first quarter of 2023, a total of 3701 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 13 percent of total vulnerabilities reported were of Critical severity. Google, Microsoft, Apple, Adobe and Tenda were the top five vendors having 28% of total reported vulnerabilities.

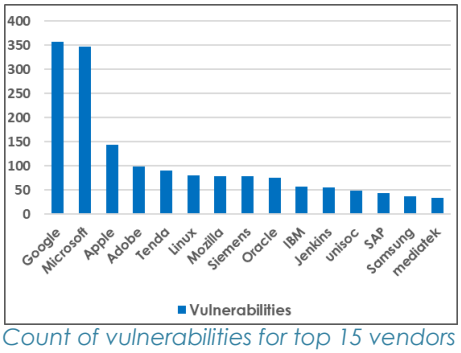


Severity-wise number of vulnerabilities

Severity	CVSSv3 Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Dec'22	Jan'23	Feb'23		
Low	0-1	0	0	0	0	81
	1-2	0	0	0	0	
	2-3	8	4	4	16	
	3-4	35	9	21	65	
Medium	4-5	118	63	84	265	1594
	5-6	323	142	241	706	
	6-7	344	123	156	623	
High	7-8	520	226	326	1072	1535
	8-9	199	95	169	463	
Critical	9-10	223	70	198	491	491
Total		1770	732	1199		3701



Severity-wise share of vulnerabilities



Count of vulnerabilities for top 15 vendors

S. No.	Vendor	No. of Vulnerabilities			Total
		Dec'22	Jan'23	Feb'23	
1.	Google	274	33	50	357
2.	Microsoft	80	142	125	347
3.	Apple	60	33	50	143
4.	Adobe	39	31	28	98
5.	Tenda	77	6	7	90
6.	Linux	42	12	26	80
7.	Mozilla	79	0	0	79
8.	Siemens	38	0	40	78
9.	Oracle	1	73	1	75
10.	IBM	46	4	8	58
11.	Jenkins	6	38	11	55
12.	unisoc	49	0	0	49
13.	SAP	13	9	22	44
14.	Samsung	7	0	31	38
15.	mediatek	18	0	16	34

Security App

Decryptors Released for BianLian, MegaCortex Ransomware

Source: https://www.securityweek.com/, https://decoded.avast.io/

Decryptor for BianLian

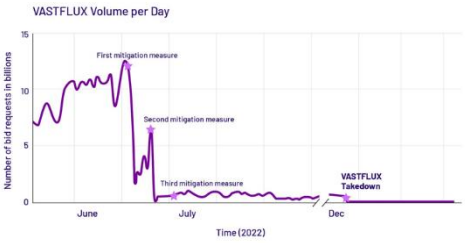
Avast has released decryptor for BianLian. The decryption tool only works with specific variant of the Ransomware and available on Avast's website. BianLian Ransomware written in Golang is used for targeting Critical Organisations. Once executed on victim's machine, ransomware encrypts all available drives. It is known for its fast encryption capabilities. It appends .bianlian extension to the affected files and drops ransom note. Another decryptor for MegaCortex Ransomware is released by Bitdefender in cooperation with NoMoreRansom Project, Europol and Swiss law enforcement. The decryption tool is available on Bitdefender's website with step-by-step guide for using the tool.

Mobile Security

A Massive Ad Fraud used 1,700 Spoofed Apps

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

An expensive ad fraud campaign comprising 1,700 spoofed apps from 120 publishers has impacted over 11 million devices. As per HUMAN Security, a cybersecurity firm, it was a malvertising attack called VASTFLUX that allowed the stacking of many invisible video ad players one behind another by injecting malicious JavaScript code. Its name comes from DNS evasion technique Fast Flux and digital Video Ad Serving Template (VAST). After exploiting the restricted in-app environments, rogue JavaScript code was injected into the hijacked ad slot and the list of target apps was retrieved from a remote server, which also included bundle IDs of legitimate apps so that the fraudulent app passed by spoofing as a legitimate app. The end goal was to show as many as 25 video ads atop of one another and keep loading until the ad slot containing the malicious code was closed. Three months after the disruption of Scylla (which was a fraud operation targeting advertising SDKs with 80 Android and 9 iOS apps), VASTFLUX was taken down. VASTFLUX was latest among the fraud botnets that have been shut down recently, after PARETO, Methbot and 3ve.



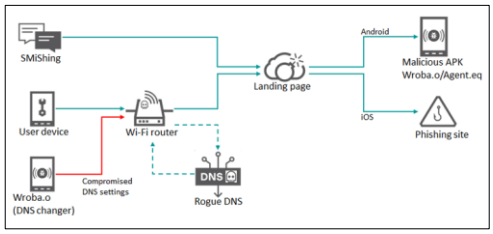
VASTFLUX Volume per Day 2022

> *The end goal was to show as many as 25 video ads atop of one another and keep loading until the ad slot containing the malicious code was closed.*

Roaming Mantis Spreads Mobile Malware That Hijacks WiFi Routers

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

Since 2018, Kaspersky has been tracking Roaming Mantis malware. This malware spreads via mobile phone roaming between Wi-Fi networks. Malware uses malicious Android app to control infected android devices and steal device information. The new variant of Roaming Mantis malware has DNS changer functionality. The new DNS changer functionality of Roaming Mantis (Wroba.o) malware directs the device to modify the DNS settings of vulnerable Wi-Fi routers and spread the infection to other devices connected with that router. A DNS changer is a malicious program that redirects connected devices to a server under the control of a threat actor instead of a legitimate DNS server. On that malicious page, the potential victim is prompted to download malware that can steal and download credentials. When an infected device connects to non-infected (healthy) routers in public places, Wroba.o malware can infect these routers also and affect other connected devices as well. DNS changing functionality enables cybercriminals disabling updates of the router. According to Kaspersky, in India 28 malicious APK downloads from malicious landing pages were created by Roaming mantis infected routers till December 2022.



Latest campaign attack diagram (Kaspersky)

> *The new DNS changer functionality of Roaming mantis (Wroba.o) malware directs the device to modify the DNS settings of vulnerable Wi-Fi routers and spread the infection to other devices connected with that router.*

New Feature to Protect Users from Zero-Click Malware Attacks

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

Samsung has released a new feature known as Message Guard to protect users from zero-click attacks. This new security feature is available on Samsung Galaxy S23 series. The zero-click attacks are highly-targeted and sophisticated attacks that exploit zero-days in software to trigger execution of malicious code without any user interaction. The zero-click exploits take benefit of vulnerabilities of messaging, SMS or email apps that automatically receive and process untrusted data. Threat actor weaponise malicious image in such a way that when it is sent to target's device, it automatically executes the code embedded within it. The Message Guard works against a number of image formats. It quarantines images received from the rest of the operating system. It ensures that file cannot infect the rest of the device.

The Message Guard works against a number of image formats. It quarantines images received from the rest of the operating system.

Google Hardens Firmware to Boost Android Security

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

Google is hardening firmware to boost the Android Security. Firmware is a component of the software stack that interacts directly with the various processors of System on Chip (SoC). Google is extending the security to other processor on the SoC for dedicated tasks like cellular communication, media processing and other security modules. Google is exploring several protection mechanisms such as Compiler-based sanitisers, Exploit mitigations and Memory Safety features. Compiler-based sanitisers can catch memory safety issues allowing security flaws or crashes during the code compilation stage. Memory Safety Features is aimed to prevent memory errors such as buffer overflows, use-after-free attacks and null-pointer dereferences. Other used techniques are Control Flow Integrity (CFI), Kernel Control Flow Integrity (kCFI), ShadowCallStack, and Stack Canaries.

Google is extending the security to other processor on the SoC for dedicated tasks like cellular communication, media processing and other security modules.

NCIIPC Initiatives

NCIIPC at Symposium on Preparing for Cyber Security Measures and Readiness in Financial Services Sector

Department of Financial Services (DFS), Ministry of Finance, organised a half-day symposium on cyber security titled Financial Services Cyber Security (FINSCY) on 18th Jan 2023. Dr. Vivek Joshi, Secretary, DFS, inaugurated the symposium. The symposium was attended by Sh. Navin Kumar Singh, DG, NCIIPC, and many senior officers of the Department of Financial Services, Ministry of Electronics and Information Technology (MeitY), Ministry of Home Affairs, Government agencies viz., CERT-In, Indian Cyber Crime Coordination Centre; Regulators in the financial services sector viz., RBI, IRDAI, and PFRDA; Public Sector Banks and Insurers, leading Private Sector Banks and Insurers, and major financial institutions such as SIDBI, NABARD, EXIM Bank and National Housing Bank. DG NCIIPC shared his views on various cybersecurity measures and plans to address the growing threats in financial services.

Sh. Navin Kumar Singh, DG, NCIIPC at Financial Services Cyber Security symposium

NCIIPC at 'Cyber Security upskilling through Educational Institutions'

NCIIPC participated in the 1st round table conference on 'Cyber Security upskilling through Educational Institutions' held at Veer Madho Singh Bhandari Uttarakhand Technical University (VMSBUTU), Dehradun. Uttarakhand Technical University organised the conference along with Communication Multimedia And Infrastructure (CMAI), Association of India. The conference was held on 18th January 2023 with participation of Lt. Gen. (Dr.) Rajesh Pant (National Cyber Security Coordinator), Kaspersky, Quickheal, Wipro, C-DAC India, IBM, TCS, OPPO India and many more.

The participants of the round table conference

NCIIPC at the 2nd India-Netherlands Cyber Dialogue

The 2nd Cyber Dialogue between India and the Netherlands was held on 3rd February 2023 at New Delhi. The cyber dialogue was co-chaired by Ms. Muanpuii Saiawi, Joint Secretary (Cyber Diplomacy Division), Ministry of External Affairs (MEA) and Ms. Nathalie Jaarsma, Ambassador at-Large for Security Policy and Cyber, Government of the Netherlands. The 2nd India-Netherlands Cyber Dialogue was held in the context of recent developments in global cyberspace and to form a deeper and comprehensive cyber cooperation between the respective cyber agencies/departments of India and the Netherlands. This Cyber Dialogue provided both the countries a common platform to discuss contemporary topics of importance in cyberspace and

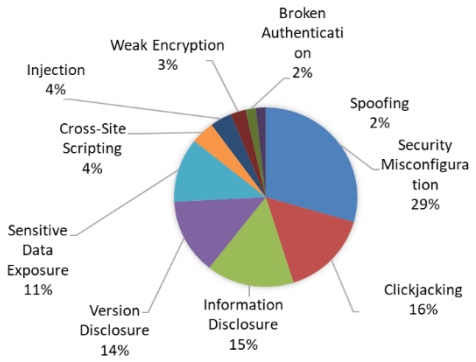

NCIIPC at the 2nd Cyber Dialogue between India and the Netherlands

also a range of high-profile issues of their mutual interest. The Indian delegation consisted of senior officials from National Critical Information Infrastructure Protection Centre (NCIIPC), MEA, Ministry of Home Affairs (MHA), CERT-In, Ministry of Electronics and Information technology (MeitY), and Department of Telecommunications (DoT).

NCIIPC Responsible Vulnerability Disclosure Program

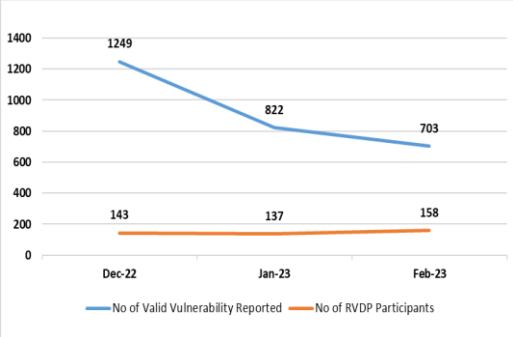
Source: https://nciipc.gov.in/RVDP.html

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 2774 vulnerabilities reported during the first quarter of 2023. The top 10 vulnerabilities are:



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

Around 379 researchers participated in RVDP programme during the first 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 U.G.
- Abhishrey Gupta
- Adith S
- Bijitha P B
- Darshan Prajapati
- Ginczy S
- Jayesh Thakur
- No Name (Name of researcher is not available)

- Prashanth Kumar Konda
- Ramansh Sharma
- Ritik Singh
- Sachin Gupta
- Sanjoy Ghosh
- Vedant Roy
- Vipin M

Upcoming Events - Global

APRIL 2023

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

MAY 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			

April 2023

- KubeCon + CloudNativeCon Europe 2023, Amsterdam — 18-21 Apr
- IANS: Ransomware in the Real World: A Case Study Approach 2023, Boston — 19 Apr
- IANS: CISO Roundtable West 2023, Virtual — 20 Apr
- AISA Australian Cyber Conference, Brisbane — 21 Apr
- Zer0Con, Seoul — 21-22 Apr
- RSA Conference, San Francisco — 24-27 Apr
- National Cybersecurity Show, Birmingham — 25-27 Apr
- RiskWorld Atlanta 2023, Atlanta — 30 Apr-3 May

May 2023

- Dallas Cyber Security Summit, Dallas — 2 May
- SecureWorld Kansas City, Kansas City — 3 May
- Black Hat Asia, Singapore & Virtual — 9-12 May
- DACHsec IT Security Summit, Frankfurt — 16-17 May
- HealthSec Summit USA, Boston — 23-24 May
- AppSec Israel 2023, Tel Aviv-Yafo — 16-17 May
- x33fcon, Goynia — 29-30 May
- Global GRC, Data Privacy & Cyber Security ConfEx, New York — 31 May

June 2023

- NICE Conference & Expo: Resetting Expectations, Seattle — 5-7 Jun
- SecureWorld Chicago, Chicago — 8 Jun
- RECON 2023 CONFERENCE, Montreal — 9-11 Jun
- Cybersecurity for Critical Assets (CS4CA) Canada 2023, Calgary — 13-14 Jun
- SANS Ransomware Summit 2023, Virtual — 23 Jun
- EuskalHack Security Congress VI, San Sebastian — 23-24 Jun
- Data Connectors Detroit Cybersecurity Conference, Detroit — 26 Jun
- Confidential Computing Summit 2023, San Francisco — 29 Jun

July 2023

- World Class Remote Office Security 2023, Leipzig 4-5 Jul
- e-Crime & Cybersecurity Financial Services Summit, London 5 Jul
- Flagship Global 7th CISO 360 Congress, Barcelona 5-7 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

Upcoming Events - India

- CXO Global Security Summit & Awards 2023, Mumbai 25 Apr
- Global Legal ConfEx Bangalore 2023, Bengaluru 11 May
- Global Legal ConfEx Mumbai 2023, Mumbai 14 Jun

JUNE 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	

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

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

- C2: Command-and-Control
- CFI: Control Flow Integrity
- ChatGPT: Chat Generative Pre-trained Transformer
- CISA: Cybersecurity and Infrastructure Security
- CISO: Chief Information Security Officers
- CMAI: Communication Multimedia And Infrastructure
- DDoS: Distributed Denial-of-Service
- DFS: Department of Financial Services
- DoT: Department of Telecommunications
- FBI: Federal Bureau of Investigation
- FINSCY: Financial Services Cyber Security
- IAMAI: Internet and Mobile Association of India
- IDS: India Digital Summit
- kCFI: Kernel Control Flow Integrity
- MEA: Ministry of External Affairs
- MeitY: Ministry of Electronics and Information Technology
- MHA: Ministry of Home Affairs
- NCRT: National Counter Ransomware Taskforce
- NISPG: National Information Security Policy Guidelines
- SLP: Service Location Protocol
- SoC: System on Chip
- TCC: Tonga Communications Corporation
- VMSBUTU: Veer Madho Singh Bhandari Uttarakhand Technical University

Notes

National Critical Information Infrastructure Protection Centre

सत्यमेव जयते

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.