NEWSLETTER

October 2021

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

Sabka Saath
Sabka Vikas
Sabka Vishwas
Sabka Prayas

Azadi Ka Amrit Mahotsav

Celebrating and commemorating 75 years of progressive India and the glorious history of it's people, culture and achievements.

India's Digital Revolution & Cyber Security Initiatives

- **1976** — National Informatics Centre established
- **2000** — Information Technology Act, 2000 enacted
- **2004** — CERT-In formed
- **2008** — IT (Amendment) Act, 2008 released
- **2013** — National Cyber Security Policy (2013) formed
- **2014** — National Critical Information Infrastructure Protection Centre formed
- **2015** — Digital India initiative launched
- **2016** — Ministry of Electronics and Information Technology carved from Ministry of Communications and Information Technology
- **2018** — Rules for the Information Security Practices and Procedures for Protected System released
- **2020** — Indian Cyber Crime Coordination Centre formed
- **2021** — India ranked 10th in the Global Cybersecurity Index 2020

VOLUME 5 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2021

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

Our great nation is celebrating National Cyber Security Awareness Month during October 2021. During this month, NCIIPC is hosting a number of events and engagements with the cyber security community at large.

Last quarter, the world noticed continued disruption in critical services caused by Ransomware. Ransomware As a Service (RaaS) has become a de facto practice by threat actors. There is a need for public private partnership to fight such malicious attempts and secure nation's Critical Information Infrastructures. The cyber security community is coming up with encryption breaking algorithms and tools to counter such Ransomware attacks.

October is also the birth anniversary of the Father of the Nation, Mohandas Karamchand Gandhi. We celebrate Swachh Bharat Mission during this month. Let us also pledge to learn, understand and adopt the best cyber hygiene practices to keep ourselves, our families, businesses, enterprises and the nation protected and resilient in the cyberspace.

Comments, suggestions and feedback are solicited from the readers. Selected letters shall also be published. You may write to us at newsletter@nciipc.gov.in Wishing a very happy Deepawali.

News Snippets - National

Phishing Websites Targeting Indian Banking Customers

Source: https://cert-in.org.in/

A new type of phishing attack is targeting Indian banking customers using NGROK platform. The platform is being used to host phishing websites which impersonates Internet banking portals of Indian banks; which in turn are being used by malicious actors to collect sensitive information of the customers like Internet Banking credentials, mobile number, OTP etc. to perform fraudulent transactions. Phishing attacks have been triggered through SMSes containing links ending with ngrok.io/xxxbank. Once a victim clicks on the link and logs in to the phishing website using Internet banking credentials, attacker generates OTP for 2FA which is delivered to the victim's phone number.

A new type of phishing attack is targeting Indian banking customers using NGROK platform.

Nearly 140 Phishing Incidents observed during H1 2021

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

Around 140 phishing incidents were observed by CERT-In in 2021 (up to June) and 280 such incidents were observed in 2020. While, 454 and 472 phishing incidents were observed during the year 2018 and 2019, respectively. Government has taken various measures for reporting and investigation of online frauds. CERT-In has been working in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites.

Image source: https://www.cert-in.org.in/

Four Load Dispatch Units Came under Cyberattack

Source: https://www.livemint.com/

Four of India's five regional centres that help oversee the country's critical electricity load management functions faced cyberattack. Cyber incidents were reported at Southern Regional Load Dispatch Centre (SRLDC), Western Regional Load Dispatch Centre (WRLDC), Northern Regional Load Dispatch Centre (NRLDC) and North Eastern Regional Load Dispatch Centre (NERLDC) of Power System Operation Corporation (POSOCO), NTPC Kudgi and Telangana State Transco. However, necessary isolation and other protective measures were taken and no data breach was detected.

Tamil Nadu Government Systems Faced Ransomware Attack

Source: https://www.newindianexpress.com/

The Tamil Nadu government's Public Department faced a ransomware attack, wherein a malware was used to encrypt computer files and a payment of $1,950 in cryptocurrency was demanded for handing over the decryption code. However,

Image source: https://www.tn.gov.in/

none of the confidential files were lost as they were handled manually. Securin, a Chennai-based cyber security company investigated the attack and found one vulnerability (environment.tn.gov.in) which was exploited by WannaCry ransomware. Further investigations revealed that over 400 public facing assets linked to the domain were vulnerable. Continuous vulnerability scanning and an automated attack surface management programme is the need of the hour for all government entities.

News Snippets - International

Rise in Cyber Espionage Activity by Hackers

Source: https://thehackernews.com/

Cybersecurity firm Recorded Future has identified ties between threat group "RedFoxtrot" and People's Liberation Army (PLA) Unit 69010. RedFoxtrot has been targeting defence, government, and telecommunications sectors across Central Asia, India, and Pakistan. Attacks staged by the threat actors involve a mix of open and closed source tools such as PlugX, Royal Road RTF weaponizer, QUICKHEAL, PCShare, IceFog, and Poison Ivy RAT. Use of AXIOMATICASYMPTOTE infrastructure has also been observed which includes a modular Windows backdoor called ShadowPad that has been previously attributed to APT41 and subsequently shared between other Chinese state-backed actors. Also, domains "inbsnl.ddns[.]info" and "adtl.mywire[.]org" have been registered by RedFoxtrot which suggest that they might have set their sights on Indian telecom service provider Bharat Sanchar Nigam Limited (BSNL) and Alpha Design Technologies Limited (ADTL) that specialises in research and development of missile, radar, and satellite systems.

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

RedFoxtrot has been targeting defence, government, and telecommunications sectors across Central Asia, India, and Pakistan.

S. Korean Atomic Energy Research Institute Suffered Cyberattack

Source: https://www.securityweek.com/

The South Korean Atomic Energy Research Institute (KAERI) suffered a cyberattack in May 2021. It confirmed that an unknown third-party gained unauthorised access to its systems by exploiting vulnerability in the VPN system being used within its environment. The investigation revealed the usage of several IP addresses, including one that was previously associated with Kimsuky. In response to the cyberattack, the VPN was updated and the attackers' IP address was blocked.

Image Source: https://www.kaeri.re.kr/eng/

CISA Teams up with Public & Private Sectors to Fight Ransomware

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

CISA announced the launch of Joint Cyber Defence Collaborative (JCDC) which is a partnership across public and private sectors aimed at defending US critical infrastructure from ransomware and other cyber threats. The initiative will allow CISA in developing cyber defence plans in collaboration with federal agencies, SLTT (state, local, tribal and territorial) partners, and private sectors. Government partners include the Department of Defence, the Department of Justice, the Federal Bureau of Investigation, the National Security Agency, the U.S. Cyber Command, and the Office of the Director of National Intelligence. The industry partners that have joined the JCDC include Amazon Web Services, AT&T, Crowdstrike, FireEye Mandiant, Google Cloud, Lumen, Microsoft, Palo Alto Networks, and Verizon.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

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

Critical Infrastructure Organisations in South East Asia Targeted

Source: symantec-enterprise-blogs.security.com, thehackernews.com

An espionage campaign was carried out from November 2020 to March 2021 targeting four critical infrastructure organisations in South East Asia. The organisations that were targeted are a communications company, a defence organisation, a power company, and a water company with evidence that the attackers were interested in information related to SCADA systems. It appeared that the same attacker was behind all the attacks, as same IP address was seen in attacks on two of the organisations, also certain artifacts were present on machines in the different organisations, including a downloader and a keylogger. A Boston based cybersecurity firm Cybereason linked the campaign to three different Chinese threat actors, namely Naikon APT (aka APT30 or Lotus Panda), Gallium (aka Soft Cell), and TG-3390 (aka APT27 or Emissary Panda) collectively named as DeadRinger.

The organisations that were targeted are a communications company, a defence organisation, a power company, and a water company with evidence that the attackers were interested in information related to SCADA systems.

Interpol Calls for New Ransomware Mitigation Strategy

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

In wake of the rising ransomware threats to supply chain and critical infrastructure, Interpol announced that it will boost the role of country-specific National Central Bureaus to fight ransomware. The proposed plan includes expanding of Interpol's secure communications network in order to assist national police and border control agencies to fight cybercrime and other security threats. The agency also called for strengthening of regional partnerships to fight against various cyberthreats globally.

INTERPOL

Image Source: https://www.interpol.int/

Chinese Citizens to Report Zero Day Vulnerabilities to its Govt

Source: https://www.seyfarth.com/, https://www.securityweek.com/

The Law covers the full cycle of data activities and addresses both electronic and non-electronic data.

In June 2021, China passed its Data Security Law w.e.f from September 1, 2021. The Law covers the full cycle of data activities and addresses both electronic and non-electronic data. As per the new Law any Chinese citizen who finds a zero-day vulnerability must report it to the Chinese government and must not sell or give the knowledge to anyone outside of China (apart from the vulnerable product's manufacturer).

Trends

First Quantum Network with Open Access Launched

Source: https://www.ehackingnews.com/

The quantum network developed by Russian scientist is an interuniversity network based on an open architecture which uses technology of quantum key distribution.

The first quantum network with open access has been launched by Russian scientists in which all interested organisations can participate. Quantum network allows quantum devices to exchange information using laws of quantum mechanics. In quantum devices like quantum computer or quantum processor data are encoded in form of qubits. These qubits follow superposition principle which is the core of quantum mechanics. Due to the superposition qubits can simultaneously exist in both 0 and 1 states. Quantum network provides safer communication compared with existing classical network. Security of most classical communication is based on algorithm for creating keys, which is difficult but possible to break by hackers whereas, this emerging field of quantum network have concept of Quantum Key Distribution (QKD). During transmission, if there is any kind of eavesdropping, QKD can easily detect it. Law of quantum mechanics do not allow to copy the states of light particles exchanged by participants in quantum network. The quantum network developed by Russian scientist is an interuniversity network based on an open architecture which uses technology of quantum key distribution. Existing fibre optic lines are used for key and data transmission in the network. This network can be used by interested organisations for development of modern software applications in the field of information security based on the use of quantum keys.

Image Source: https://thehackernews.com/

Glowworm Attack Spies Using Device's LED Power Indicator

Source: https://threatpost.com/

Researchers have found a new kind of TEMPEST attack Glowworm which exploits audio output device's LED power light. This attack is developed from a bug that emits light so it is known as Glowworm. It measures audio output device's LED power light and convert it into audio which allow cyber attackers to listen conversations.

The researchers have demonstrated how Glowworm attack work by pointing a telescope with an electro-optical sensor from 35 meters away at speakers. The fluctuations in LED signal strength can be read with a photodiode coupled to an optical telescope. There is an optical correlation between the sound and intensity of power indicator LED because LED of various devices is connected directly to the power line and intensity of a device's power indicator is correlated with power consumption. The researchers also revealed that many devices such as Google Home Mini, Google Nest Audio, Logitech - Z120 Speakers, S120 speakers, JBL - JBL Go 2 etc. are vulnerable to the Glowworm attack. This attack could be easily stopped by placing a black tape over a device's power indicator LED. The manufacturers should also consider this attack during the designing of products to make them Glowworm-safe.

This attack could be easily stopped by placing a black tape over a device's power indicator LED.

Malware Bytes

Victory Backdoor Targeting Southeast Asian Governments

Source: https://cyware.com/

APT group SharpPanda has launched a threat campaign using Victory backdoor to target primarily government organisations. Threat actors are using spear-phishing emails heavily loaded with malicious Word documents to gain initial access. The attachments are weaponised copies of legitimate-looking official documents. A template is downloaded by these malicious documents from multiple URLs, which are .RTF files created with RoyalRoad weaponiser. The RoyalRoad-generated RTF document has a shell code and an encrypted payload. The campaign is also exploiting older Office security vulnerabilities. This multi-stage infection chain ultimately installs the backdoor module. It can manipulate files such as create, read, delete, and rename, take screenshots, collect information on the top-level opened windows, and shut down the computer. It can also get TCP/UDP tables, registry keys information, CD-ROM drives data, and victim's computer information. Threat actors are observed using anti-analysis and anti-debugging techniques in order to hide the Victory backdoor. Organisations should use a reliable anti-malware solution on all connected devices to protect their infrastructure from such type of threats.

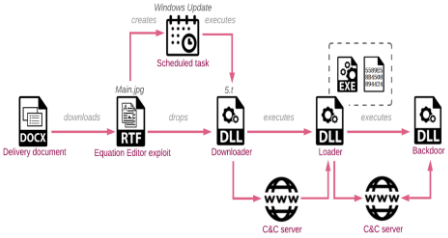


Image source: https://blog.checkpoint.com/

A template is downloaded by these malicious documents from multiple URLs, which are .RTF files created with RoyalRoad weaponiser.

Cyber Espionage Group Targeting Critical Sector Organisations

Source: https://www.ehackingnews.com/

A new Cyber espionage campaign dubbed as "BackdoorDiplomacy" is targeting various critical sector organisations. The threat campaign targeting both Windows and Linux operating systems, servers with Internet-exposed ports and exploiting unsecured vulnerabilities to implement the China Chopper web shell for initial access.

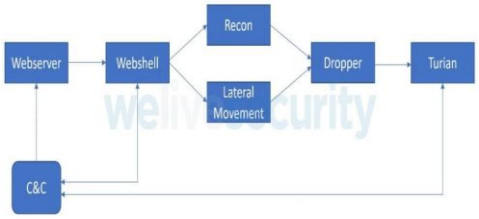


Image source: https://www.securitynewspaper.com/

Flaws in F5 BIG-IP devices (CVE-2020-5902), Microsoft Exchange servers, and Plesk web hosting control panels are observed being exploited by this threat group. After gaining initial access to the targeted system, it conducts reconnaissance and install the Turian backdoor. The group is capable of carrying out various cyber-hacking operations, move laterally across the network, gather system information, take screenshots, ex-filtrate sensitive data stored on removable media. The operators employed similar Tactics, Techniques, and Procedures (TTPs) in each case, but modified the tools used even within close geographic regions, making it difficult to track the group.

GhostEmperor: A New Threat Actor Targets Southeast Asia

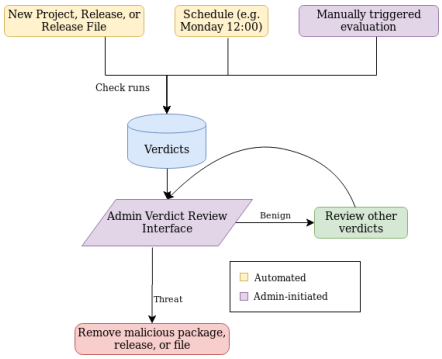
Source: https://securityaffairs.co/

A formerly unknown Windows kernel-mode rootkit is being used by threat actors in this campaign.

A new threat group tracked as "GhostEmperor" is exploiting Microsoft Exchange vulnerabilities to target high-profile victims. A formerly unknown Windows kernel-mode rootkit is being used by threat actors in this campaign. Rootkits provide remote control access over the targeted servers. Rootkits are well known for hiding threat activity from investigators and security solutions. GhostEmperor uses a loading scheme which involves a component of an open-source project named "Cheat Engine". This loading scheme allows it to bypass the Windows Driver Signature Enforcement mechanism.

Malicious Typosquatted Python Libraries Found on PyPI Repository

Source: https://thehackernews.com/



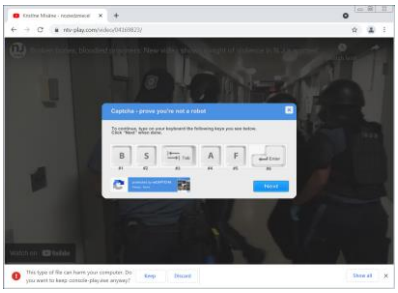
Automatic malware checks
Image source: https://jaxenter.com/

The Python packages that were found to be obfuscated using Base64 encoding are - pytagora, pytagora2, noblesse, genesisbot, are, suffer, noblesse2, noblessev2.

It has been reported that typosquatted packages in PyPI are downloading and executing a malicious payload shell script. The payload retrieves third-party cryptominer such as PhoenixMiner, ubqminer, or T-Rex for mining Ethereum and Ubiq on victim systems. Threat actors are using public software repositories as a platform to spread malware whether through dependency confusion, typosquatting, or simple social engineering attacks due to the lack of moderation and automated security controls. As many as eight Python packages that were containing malicious code have been removed from the PyPI portal. The Python packages that were found to be obfuscated using Base64 encoding are - pytagora, pytagora2, noblesse, genesisbot, are, suffer, noblesse2, noblessev2. These packages could be abused to become an entry point for more sophisticated threats. The attacker could execute remote code on the target machine, steal credit card information and passwords auto-saved in Chrome and Edge browsers, gather system information, and even steal Discord authentication tokens to impersonate the victim. Preventive measures such as verification of library signatures, and employing automated application security tools that scan for suspicious code should be an integral part of any CI/CD pipeline on the developers' side.

Malware Uses Clever 'Captcha' to Bypass Browser Warning

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

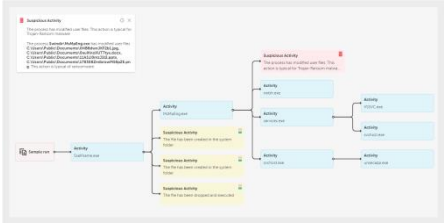


A fake captcha prompt has been used by threat actors to trick users into bypassing browsers warnings to download the Gozi/Ursnif baking trojan. In a specific case, when user click on the play button of an embedded YouTube video, a file, console-play.exe is downloaded. Google Chrome automatically warns it as an executable and prompts whether to 'Keep' or 'Discard' the file. The threat actors are displaying a fake reCaptcha image to bypass this warning. The fake reCaptcha image eventually tricks to download and save the file to the computer potentially making users to think that the successful 'captcha' allowed it. If user runs the executable, it will install numerous decoy files and launch an executable, BouncyDotNet.exe. The BouncyDotNet.exe will read various strings from the Windows Registry used to launch PowerShell commands while running. A .NET application will be compiled by these PowerShell commands using the built-in CSC.exe compiler that launches a DLL for the Ursnif banking trojan. Once running, Gozi can steal account credentials, execute commands issued remotely by threat actors and download further malware to the computer. If infected by this malware, users should immediately change the passwords for online accounts.

The fake reCaptcha image eventually tricks to download and save the file to the computer potentially making users to think that the successful 'captcha' allowed it.

REvil Ransomware Launched a Global Supply Chain Attack

Threat Assessment Group, NCIIPC



Execution map for the "agent.exe" dropper – Kaspersky Cloud Sandbox

REvil also known as Sodinokibi provides Ransomware-as-a-Service (RaaS). In recent times with the decline of many alternative RaaS offerings, REvil has become the primary choice among threat actors. REvil uses a mix of Curve25519 (asymmetric) and Salsa20 (symmetric) cryptography algorithms for encrypting the content of files on the victim's machine. Decryption of files encrypted by REvil ransomware is not possible without the attacker's key due to highly secure cryptographic scheme in the malware. After an attack, REvil threats the victim to publish encrypted data on their page 'Happy Blog'.

Activities of REvil: In the past it has been seen that customers of Managed Service Providers (MSPs) have been targeted by REvil ransomware, including a ransomware outbreak in 2019 that affected the systems of Texas municipalities in which attackers demanded US $2.5 million. Again, On 2nd July a new global supply chain ransomware attack was launched by REvil, that targeted computer systems of several companies across the world, including 800 physical grocery stores of Sweden's Coop, that were shut down after the attack. In this global supply chain attack hackers from the REvil cybercrime gang had compromised systems of IT firm Kaseya using a zero-day exploit on the Kaseya's VSA remote management server platform.

In the past it has been seen that customers of Managed Service Providers (MSPs) have been targeted by REvil ransomware, including a ransomware outbreak in 2019 that affected the systems of Texas municipalities in which attackers demanded US $2.5 million.

On July 11, Kaseya released a VSA version 9.5.7a On-Premises patch with restoration of VSA SaaS infrastructure to fix three zero-day vulnerabilities used in the ransomware attack.

They used the server to deliver malicious update package to VSA agent applications running on managed Windows devices to target users of Kaseya's VSA remote monitoring and management platform. As a result, the ransomware reached to its resellers and end customers such as Coop who was using its software. The REvil hackers demanded $70 million (roughly Rs. 520 crores) to restore encrypted data of Kaseya. On July 11, Kaseya released a VSA version 9.5.7a On-Premises patch with restoration of VSA SaaS infrastructure to fix three zero-day vulnerabilities used in the ransomware attack.

References:

[1] https://securelist.com/revil-ransomware-attack-on-msp-companies/103075/

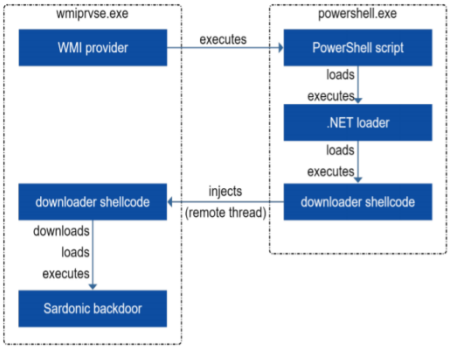
[2] https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

[3] https://gadgets.ndtv.com/internet/news/revil-kaseya-ransomware-attack-coop-resellers-affected-firms-malware-could-take-weeks-to-recover-2480184

[4] https://www.fortinet.com/blog/threat-research/new-supply-chain-ransomware-attack-targets-kaseya-platform

FIN8 Adds New "Sardonic" Backdoor to its Arsenal

BFSI Sector, NCIIPC



Execution Flow

This cybercriminal group is known for using social engineering and spear-phishing techniques to infiltrate into target organisations.

FIN8 is financially motivated cybercriminal group which usually targets the healthcare, hospitality, retail, and entertainment industries with the goal of stealing payment credentials. It has been around since 2016. This cybercriminal group malicious arsenal includes a large variety of techniques and tools, ranging from Point-of-Sale malware to Windows zero-day exploits. New backdoor Sardonic, is under development by the FIN8 cybercrime group and identified in an unsuccessful attack on a U.S. financial institution. This malware is very powerful and adaptable, allows attackers to deploy new threats on the fly, without the need to update any of its components. Sardonic features include upgraded capabilities like screen capturing, proxy tunneling, file less execution, and credential theft.

Attack Flow: This cybercriminal group is known for using social engineering and spear-phishing techniques to infiltrate into target organisations. After penetrating into the network, the attackers begin with network reconnaissance, collecting information about the domain and continue with lateral movement and privilege escalation. In addition, offensive features of FIN8's includes signature backdoor and BADHATCH loader. By using PowerShell scripts, BADHATCH loader is deployed which is downloaded from

some malicious IP address using the sslip.io service. The same is also used during reconnaissance, lateral movement and privilege escalation.

Protective measures:

- E-mail security solution may be configured to automatically discard suspicious attachments.
- Isolate the Point-of-Sale network from the ones used by employees.
- Integrate the threat intelligence into existing SIEM or security controls for relevant indicators of compromise.
- Endpoint Detection and Response (EDR) / Extended Detection and Response (XDR) and other such security defences may be implemented.

By using PowerShell scripts, BADHATCH loader is deployed which is downloaded from some malicious IP address using the sslip.io service.

References:

[1] https://www.bitdefender.com/files/News/CaseStudies/study/401/Bitdefender-PR-Whitepaper-FIN8-creat5619-en-EN.pdf

[2] https://www.cybersecurity-help.cz/blog/2286.html

[3] https://threatpost.com/fin8-bank-sardonic-backdoor/168982/

[4] https://thehackernews.com/2021/08/researchers-uncover-fin8s-new-backdoor.html

[5] https://www.acronis.com/en-eu/cyber-protection-center/posts/sardonic-backdoor-targets-stored-payment-credentials/

Learning

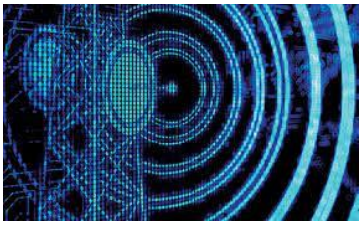


Image source: https://encrypted-tbn0.gstatic.com/

To reduce risks of radio-based assaults on smartphones, it is suggested to turning off radios (especially Wi-Fi and Bluetooth) while not in use or when in public.

Safeguard Your Smartphones from Radio-based Attacks

Source: https://www.ehackingnews.com/

Smartphones involve a range of radios – generally cellular, Wi-Fi, Bluetooth, and Near Field Communication (NFC) – that permit wireless communication in a range of situations. These radios are made to remain turned on while the user transports around the world. Security errors in these interfaces are a matter of concern, whether built into the protocol or discovered in a particular implementation. An IMSI catcher is a piece of equipment, also known as a cell-site simulator, that acts like a genuine cell tower, letting a targeted smartphone to connect to it rather than the actual mobile network using white noise to jam the competing 5G/4G/3G frequencies. There are other attacks like Karma attack, BlueBorne and NFC attacks which are used for exploiting Wi-Fi network, Bluetooth, NFC technology for payment respectively. To reduce risks of radio-based assaults on smartphones, it is suggested to turning off radios (especially Wi-Fi and Bluetooth) while not in use or when in public. Also turn off auto-join for hotspots on Wi-Fi and install security updates for Bluetooth as soon as they become available to confirm that any known Bluetooth flaws are addressed.

Best Practices for Ransomware Protection

KMS Team, NCIIPC

Patch backup software on a regular basis to prevent attackers from exploiting any known flaws they might have.

Ransomware has become a serious threat to businesses and individuals during the past two years. The current ransomware variants mostly encrypt files on the infected network/system (i.e., crypto ransomware). Once the user's access to the system is blocked, the threat actors demand a ransom in order to unlock the files, often in bitcoins or any other cryptocurrency. The ransomware variants opportunistically target victims, infecting an array of devices from computer systems to smartphones.

Best Practices for Ransomware Prevention

- Regular Backups are Important:
  - Make regular offline backups of the most important files. Frequently test backups for data integrity to ensure it is operational.
  - Patch backup software on a regular basis to prevent attackers from exploiting any known flaws they might have.
  - Ensure that the offline backups are kept in a different location from the network or in a cloud service designed for this purpose, as ransomware can target the backups to increase the likelihood of payment.
  - Ensure that the cloud service saves the previous versions of the backup from being immediately deleted and can be

restored to them.

- Keep the Security Software Updated:
  - As new ransomware variants keep on appearing often it is a good practice to keep the security software up to date to protect the systems or devices against ransomware.
  - Regularly patch and update the Software and Operating Systems to the latest available versions in order to patch the known vulnerabilities.
- Vulnerability Scanning: Scans externally facing systems (internet-facing devices) for vulnerabilities on a regular basis, and build protocols for quickly patching systems when critical vulnerabilities are detected through scanning or public disclosure in order to limit the attack surface.

Regularly patch and update the Software and Operating Systems to the latest available versions in order to patch the known vulnerabilities.

General Practices and Guidance against Ransomware:

- Use Multi-Factor Authentication (MFA) at all remote access points into the network, all possible services and accounts that access critical systems.
  - When using passwords, use strong passwords and do not reuse the password of different accounts.
  - MFA helps to authenticate users so that if the threat actor steals the credentials, they won't be able to easily reuse it.
- Malicious actors frequently look for privileged accounts to leverage to help saturate networks with ransomware.
  - Remove unessential accounts and groups and restrict admin access.
  - Restrict user permissions to run and install applications.
  - The user accounts should be frequently audited, especially the remote monitoring and management accounts that can be publicly accessed.
- Apply physical or logical means of separation of networks and data. Categorise and separate the data based on its organisational value and implement virtual environments.
- Restrict usage of PowerShell, and Group Policy to specific users on a case-by-case basis.
- Disable macros scripts, as macros can be used to deliver ransomware it is best to disable macro scripts for Microsoft Office files transmitted via email.
- Restrict the Internet Access:
  - Use a proxy server also consider using ad-blocking software.
  - Apply restrictions to access common ransomware entry points like personal e-mail accounts or social-networking sites.
- Secure the End-Users:
  - Provide the end-users (or employees) with training on social engineering and phishing. Advise them not to open suspicious emails, not to click on links or open attachments enclosed with such emails, and to be cautious before

Use Multi-Factor Authentication (MFA) at all remote access points into the network, all possible services and accounts that access critical systems.

Apply restrictions to access common ransomware entry points like personal e-mail accounts or social-networking sites.

visiting unknown websites.
- Instruct the users to close their browser when not using it.
- Perform email filtering preferably in combination with spam filtering which can block malicious emails and remove executable attachments.
- Ensure the staff knows how to identify and report suspicious activities.

➢ Frequently, look for brute-force attempts and clearing of event logs like security event log and PowerShell operational logs.
➢ Turn on the tamper protection features to prevent the malicious actors from stopping security services.

Frequently, look for brute-force attempts and clearing of event logs like security event log and PowerShell operational logs.

Restoration and Recovery after Ransomware Attack:

- Reset the credentials for administrator and other system accounts but be careful not to lock yourself out of systems that are needed for recovery.
- After the malicious actors have encrypted the system or data determine if a decryptor is available for the ransomware. As now-a-days security researchers have already broken the encryption algorithms for many ransomware variants.
- Keep track of the systems and devices that are not impacted by ransomware so that they can be assigned low priority for restoration and recovery. This method enables the organisation to get back to business in an efficient way.
- Safely erase the infected devices and reinstall the OS.
- Before the backup is restored it is important to verify that it is free from any malware.
- Run antivirus scans and monitor the network traffic to identify if any infection remains.

Keep track of the systems and devices that are not impacted by ransomware so that they can be assigned low priority for restoration and recovery.

References:

[1] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

[2] https://threatpost.com/takeaways-colonial-pipeline-ransomware/166980/

[3] https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/

[4] https://thehackernews.com/2021/06/5-critical-steps-to-recovering-from.html

[5] https://calnet.ie/resource/infographic-ransomware-is-on-the-rise/

Kubernetes Hardening Guidance

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

National Security Agency (NSA) and Cybersecurity Infrastructure Security Agency (CISA) have released a Cybersecurity Technical Report related to Kubernetes Hardening Guidance. This report provides configuration guidance of Kubernetes environments for minimising the risk. Kubernetes is an open-source container orchestration platform that automates manual processes involved in deploying, managing and scaling containerised applications. Three most common reasons for which Kubernetes is targeted are data theft, computational power theft and denial of service. Below are the recommendations provided by this report:

- Kubernetes Pod security
- Run applications as non-root users in containers
- Run containers with immutable file systems
- Scan container images for vulnerabilities or misconfigurations

This report provides configuration guidance of Kubernetes environments for minimising the risk.

Pod Security Policy to enforce a minimum level of security includes:

- Prevent privileged containers
- Deny container features such as hostPID, hostIPC, hostNetwork, allowedHostPath
- Reject containers that execute as the root user
- Hardening applications against exploitation using security services such as SELinux, AppArmor, and seccomp

Network separation and hardening:

- Lock down access to control plane nodes using firewall
- Provide Role-Based Access Control (RBAC)
- Limit access to the Kubernetes etcd server
- Configure control plane components to use authenticated, encrypted communications using Transport Layer Security (TLS) certificates
- Set up network policies to isolate resources
- Place all credentials and sensitive information in Kubernetes Secrets

Hardening applications against exploitation using security services such as SELinux, AppArmor, and seccomp

Authentication and authorisation:

- Disable anonymous login
- Use strong user authentication

Log auditing:

- Enable audit logging

Persist logs to ensure availability in the case of node, Pod, or container level failure

- Persist logs to ensure availability in the case of node, Pod, or container level failure
- Configure a metrics logger

Upgrading and application security practices:

- Apply security patches and updates
- Perform periodic vulnerability scans.

Vulnerability Watch

Image source: https://discuss.flarum.org/

It was discovered that Flarum's translation system allowed string inputs to be converted into HTML DOM nodes when rendered.

Critical Vulnerability in Flarum

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-32671

Flarum is a forum software for building communities. It was discovered that Flarum's translation system allowed string inputs to be converted into HTML DOM nodes when rendered. This vulnerability could allow any user to type malicious HTML markup within certain user input fields and have this execute on client browsers. This attack could also be modified to perform AJAX requests on behalf of a user, possibly modifying their settings or profile, deleting discussions, or even modifying settings on the Admin panel if the attack was targetted towards a privileged user. This vulnerability has been tracked as CVE-2021-32671 having CVSS score 10.

Image source: https://www.eq-3.com/

Critical Vulnerability in eQ-3

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-33032

Critical Remote Code Execution (RCE) vulnerability was discovered in the WebUI component of the eQ-3 HomeMatic CCU2 firmware and CCU3. The vulnerability is tracked as CVE-2021-33032 having CVSS score 10. This vulnerability allows a remote unauthenticated attacker to execute system commands as root via a simple HTTP request. The affected versions are eQ-3 HomeMatic CCU2 firmware version 2.57.5 and below, and CCU3 firmware version 3.57.5 and below.

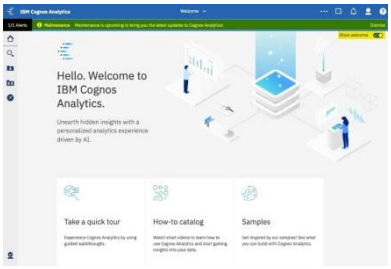


Image source: https://qmetrix.com.au/

Critical Vulnerability in IBM Cognos Analytics

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-4561

A critical vulnerability discovered in IBM Cognos Analytics DQM API allows submitting of all control requests in unauthenticated sessions. This vulnerability tracked as CVE-2020-4561, having CVSS score 10, allows a remote attacker, who can access a valid CA endpoint, to read and write files to the Cognos Analytics system. The affected versions are IBM Cognos Analytics 11.0 and 11.1.

Critical Vulnerability in libsflacextractor library

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-25387

An Improper Input Validation vulnerability has been discovered in sflacfd_get_frm() in libsflacextractor library prior to that allows attackers to execute arbitrary code on mediaextractor process of Android. This vulnerability is tracked as CVE-2021-25387 with CVSS score 10.

This vulnerability is tracked as CVE-2021-25387 with CVSS score 10.

Critical Vulnerability in Microsoft OneFuzz

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-37705

It has been discovered that an Incomplete Authorisation check in OneFuzz allows an authenticated user from any Azure Active Directory tenant to make authorised API calls to a vulnerable OneFuzz instance. This vulnerability is tracked as CVE-2021-37705 and has a CVSS score of 10. This vulnerability could lead to read/write access to private data like crash information, software vulnerability, and security testing tools. Through authorised API calls, this vulnerability could enable tampering with the existing data and unauthorised code execution on Azure compute resources. As a workaround users can restrict access to the tenant of a deployed OneFuzz instance by redeploying in the default configuration, which omits the `--multi_tenant_domain` option.

Image source: https://opengraph.githubassets.com/

This vulnerability could lead to read/write access to private data like crash information, software vulnerability, and security testing tools.

Critical Vulnerability in SolarWinds Serv-U

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

Microsoft has discovered a critical Remote Code Execution vulnerability in the SolarWinds Serv-U. This vulnerability is tracked as CVE-2021-35211, having CVSS score 10, exists in Serv-U's implementation of the Secure Shell (SSH) protocol. If the SSH of Serv-U is exposed to the internet, successful exploitation would enable the attackers to remotely run arbitrary code with privileges, allowing them to perform actions like install and run malicious payloads, or view and change data. SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP for Windows prior to 15.2.3 HF2 are affected by this vulnerability. A hotfix has been developed by SolarWinds to resolve this vulnerability.

Multiple Critical Vulnerabilities in CODESYS Industrial Automation

Source: https://thehackernews.com/

Multiple critical vulnerabilities have been discovered impacting CODESYS automation software that could be exploited to achieve Remote Code Execution (RCE) on Programmable Logic Controllers (PLCs). CVE-2021-30189 is a Stack-based Buffer Overflow vulnerability, CVE-2021-30190 is an Improper Access Control

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

Multiple vulnerabilities have been discovered impacting CODESYS automation software that could be exploited to achieve remote code execution on programmable logic controllers (PLCs).

vulnerability, CVE-2021-30191 is a Buffer Copy without Checking Size of Input vulnerability, CVE-2021-30192 is an Improperly Implemented Security Check vulnerability, CVE-2021-30193 is an Out-of-bounds Write vulnerability, and CVE-2021-30194 is an Out-of-bounds Read vulnerability. All these vulnerabilities have CVSS score of 10. CVE-2021-30186 is a Heap-based Buffer Overflow vulnerability, CVE-2021-30188 is a Stack-based Buffer Overflow vulnerability, and CVE-2021-30195 is an Improper Input Validation vulnerability. These three vulnerabilities have CVSS score of 8.8. CVE-2021-30187 is a flaw in the CODESYS Control V2 Linux SysFile library having CVSS score 5.3.

Top 25 Most Dangerous Software Weaknesses

Source: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

Data from the National Vulnerability Database (NVD), National Institute of Standards and Technology (NIST) as well as the Common Vulnerability Scoring System (CVSS) scores associated with each Common Vulnerabilities Exposure (CVE) record has been used to compile the most frequent and critical errors that could lead to serious vulnerabilities in software to release the 2021 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses list. These weaknesses are dangerous because they are often easy to find, exploit, and could allow adversaries to completely take over a system, steal data, or prevent an application from working. The CWE top 25 are:

These weaknesses are dangerous because they are often easy to find, exploit, and could allow adversaries to completely take over a system, steal data, or prevent an application from working.

- CWE-787 Out-of-bounds Write
- CWE-79 Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')
- CWE-125 Out-of-bounds Read
- CWE-20 Improper Input Validation
- CWE-78 Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')
- CWE-89 Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')
- CWE-416 Use After Free
- CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-352 Cross-Site Request Forgery (CSRF)
- CWE-434 Unrestricted Upload of File with Dangerous Type
- CWE-306 Missing Authentication for Critical Function

- CWE-190 Integer Overflow or Wraparound
- CWE-502 Deserialisation of Untrusted Data
- CWE-287 Improper Authentication
- CWE-476 NULL Pointer Dereference
- CWE-798 Use of Hard-coded Credentials
- CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer
- CWE-862 Missing Authorisation
- CWE-276 Incorrect Default Permissions
- CWE-200 Exposure of Sensitive Information to an Unauthorised Actor
- CWE-522 Insufficiently Protected Credentials
- CWE-732 Incorrect Permission Assignment for Critical Resource
- CWE-611 Improper Restriction of XML External Entity Reference
- CWE-918 Server-Side Request Forgery (SSRF)
- CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability in Random Number Generator Affects IoT Devices

Source: https://thehackernews.com/

A vulnerability has been discovered in hardware random number generators, which is used in billions of Internet of Things (IoT) devices, that causes them to fail to generate random numbers effectively, thus jeopardising the security of the IoT devices and exposing them to attacks. Researchers of Bishop Fox have discovered that the 'randomly' chosen numbers are not always random when it comes to IoT devices. This problem is unique to the IoT landscape as they lack an operating system that typically comes with a randomness API. This vulnerability can be remediated with software updates. IoT device manufacturers and developers may include a Cryptographically Secure Pseudorandom Number Generator (CSPRNG) API that is seeded from a set of diverse entropy sources and ensure the code does not ignore error conditions, or fail to block calls to the RNG when no more entropy is available.

Researchers of Bishop Fox have discovered that the 'randomly' chosen numbers are not always random when it comes to IoT devices.

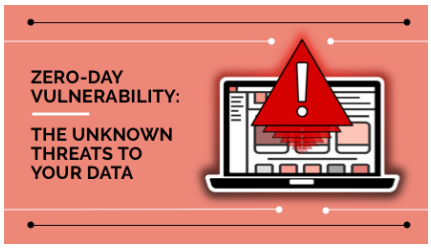


Image source: https://spanning.com/

Zero-day Vulnerability

Strategic & Public Enterprises Sector, NCIIPC

Zero-day is a flaw in software, hardware or firmware that is unknown to the vendor or developer or parties responsible for patching or fixing the flaw. The term zero-day refers to the vulnerability itself, or an attack that has zero days between the time the vulnerability is discovered and the first attack which means they have "zero days" to fix it. The words vulnerability, exploit, and attack are typically used alongside zero-day, and these are helpful to understand the difference:

- A zero-day vulnerability is a software flaw or vulnerability discovered by attackers before the vendor could become aware of it. Since the vendors are unaware of it, no patch exists for zero-day vulnerabilities which means attacks are likely to succeed.
- A zero-day exploit is the method attackers or hackers use to attack systems with a previously unidentified vulnerability.
- A zero-day attack is the use of a zero-day exploit to cause damage to a system or steal data from a system having a zero-day vulnerability.

A zero-day exploit is the method attackers or hackers use to attack systems with a previously unidentified vulnerability.

A zero-day hack can exploit vulnerabilities in a variety of systems like operating systems, web browsers, office applications, open-source components, Hardware and firmware, Internet of Things (IoT).

Identifying zero-day attacks: Zero-day vulnerabilities can take multiple forms such as missing data encryption, broken algorithms, missing authorisations, bugs, problems with password security, and so on. These can be challenging to detect. Detailed information about the zero-day exploits is available only after the exploit is identified because of the nature of these types of vulnerabilities. Organisations which are attacked by a zero-day exploit might have an unexpected traffic or suspicious scanning activity originating from a client or service. Some of the zero-day detection techniques include:

Zero-day vulnerabilities can take multiple forms such as missing data encryption, broken algorithms, missing authorisations, bugs, problems with password security, and so on.

- Reference can be taken from existing databases of malware and how they behave. Even though these databases are updated very quickly and can be useful, zero-day exploits are new and unknown. So, there is a limit to how much we can obtain from an existing database.
- Some alternative techniques look for zero-day malware characteristics based on how they interact with the target systems. These techniques look at the interactions they have with existing software and tries to determine if they result from malicious actions instead of examining the code of incoming files.

- Based on data of past and current interactions with the system, machine learning is increasingly used to detect data from previously recorded exploits to establish a baseline for safe system behaviour. The more such type of data is available, the more reliable the detection becomes.

Protection against Zero-day attacks:

- Use only essential applications since the usage of more software might contain more potential vulnerabilities. You can reduce the risk to your network by using needful application only.
- Use a firewall since it plays an essential role in protecting your system against zero-day threats. Maximum protection may be ensured by configuring it to allow only necessary transactions.
- Educate users within the organisations. Many zero-day attacks capitalize on human error. Educating employees and users about good safety and security habits will help to keep them safe and protect organisations from zero-day exploits and other digital threats.

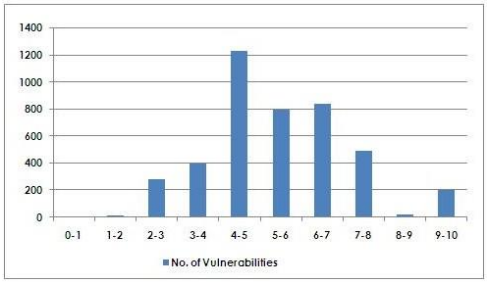
Use a firewall since it plays an essential role in protecting your system against zero-day threats. Maximum protection may be ensured by configuring it to allow only necessary transactions.

References:

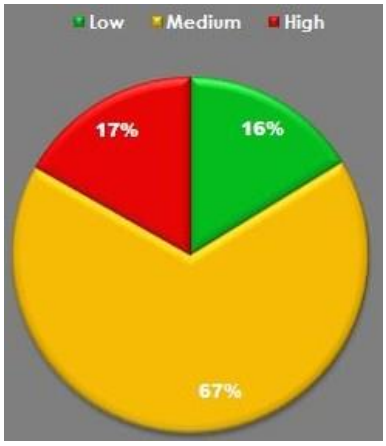
[1] https://www.kaspersky.co.in/resource-center/definitions/zero-day-exploit

[2] https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

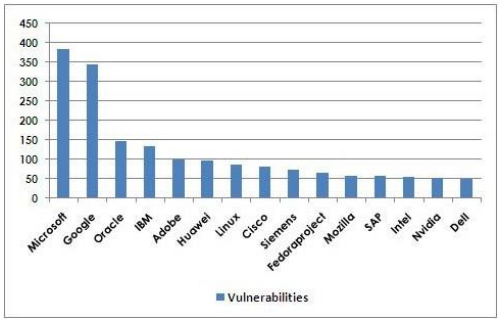
[3] https://www.illumio.com/cybersecurity-101/zero-day-attacks



Severity-wise number of vulnerabilities



Severity-wise share of vulnerabilities



Count of vulnerabilities for top 15 vendors

Quarterly Vulnerability Analysis Report

KMS Team, NCIIPC

A total of 4280 vulnerabilities have been observed during last quarter, out of which majority of vulnerabilities have score ranging from 4-7. 17 percent of total vulnerabilities reported were of high severity. Microsoft, Google, Oracle, IBM and Adobe were the top five vendors having 26% of total reported vulnerabilities.

Severity	CVSS Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Jun	Jul	Aug		
Low	0-1	0	0	0	0	695
	1-2	9	4	2	15	
	2-3	111	69	100	280	
	3-4	99	144	157	400	
Medium	4-5	394	363	473	1230	2867
	5-6	251	259	287	797	
	6-7	265	216	359	840	
High	7-8	159	157	177	493	718
	8-9	6	12	5	23	
	9-10	53	53	96	202	
Total		1347	1277	1656		4280

S. No.	Vendor	No. of Vulnerabilities			Total
		Jun	Jul	Aug	
1.	Microsoft	89	149	147	385
2.	Google	172	37	137	346
3.	Oracle	9	136	3	148
4.	IBM	42	64	29	135
5.	Adobe	19	1	79	99
6.	Huawei	48	6	44	98
7.	Linux	17	35	34	86
8.	Cisco	27	25	29	81
9.	Siemens	8	55	10	73
10.	Fedoraproject	28	10	29	67
11.	Mozilla	37	0	22	59
12.	SAP	40	13	5	58
13.	Intel	37	1	16	54
14.	Nvidia	27	15	11	53
15.	Dell	10	8	31	49

Security App

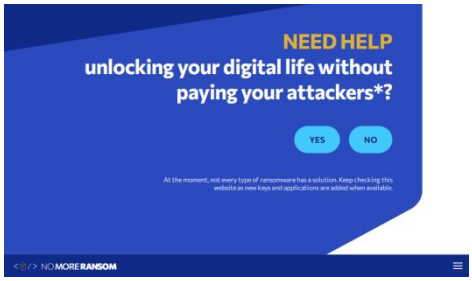
Tools and Websites to Fight Against Ransomware Attacks

Sources: www.cisa.gov, www.zdnet.com, *bleepingcomputer, ehackingnews, therecord.media, portswigger.net*

Ransomware has become a huge problem now-a-days. To help organisations and individuals fight against ransomware some cybersecurity agencies have launched tools and websites for guidance to protect businesses from ransomware attack. Some of these tools and websites are mentioned below:

StopRansomware.gov

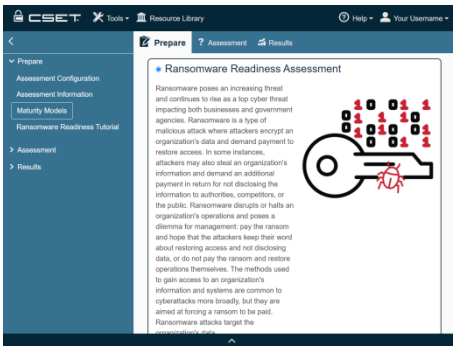
StopRansomware.gov website: It was launched by Department of Homeland Security's (DHS), Cybersecurity and Infrastructure Security Agency (CISA) provides cybersecurity resources, tools and other information for everyone to fight against ransomware attack. This website contains malware removal tools, cybersecurity guidance documents, helpful links on how organisation can protect itself from attack and what steps to take if it's attacked by cybercriminals who have encrypted all of its files and demand money before they'll decrypt them again.



No More Ransom
Image source:
https://www.nomoreransom.org/

No More Ransom website: nomoreransom.org was jointly launched by Europol, the Dutch National Police, Kaspersky Lab, and McAfee. This website provides guidance and information to unlock encrypted files. This website also provides decryption tools for many ransomware families. The motive behind No More Ransom website was to bring together the law enforcement and private industry to combine the efforts in the fight against cybercrimes.

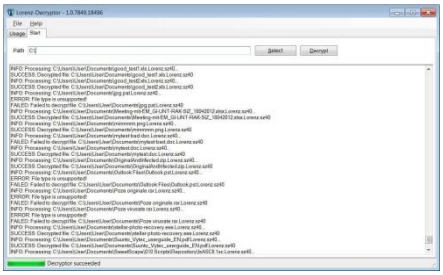
Ransomware Readiness Assessment Tool: Ransomware Readiness Assessment (RRA) tool released by CISA is a desktop software tool that guides network defenders through a step-by-step process to evaluate cybersecurity practices on their networks. It can be used with both Informational Technology (IT) as well as Industrial Control System (ICS) networks. The RRA is a self-assessment based on set of practices to help organisations know about how well they are equipped to defend and recover from a ransomware attack.



Ransomware Readiness Assessment Tool
Image source:
https://raw.githubusercontent.com/

Hopper: It is a tool that provides different methods to spot any hostile activities in a corporate network. It examines an organisation's login records to look for indicators of lateral movement attacks. Hopper has two main components: a causality engine to track the login paths and a score algorithm that determines which login paths contain lateral movement attack features. It can identify which behaviours require additional inspection by filtering and reviewing the login pathways based on these two vectors.

Enfilade is an open-source tool which can detect internet-facing MongoDB instances and determine if they have been infected with ransomware or Meow malware. It reconnaissance and gather information on MongoDB instances, Checks access permissions for



Lorenz ransomware decryptor

assessing remote command execution and perform user enumeration. This tool is available on GitHub.

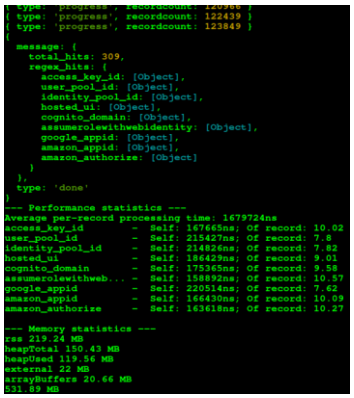
Lorenz Decryptor: It has been released by Cybersecurity firm Tesorion to help victims of Lorenz Ransomware to recover encrypted files without paying the ransom. It can decrypt files of type such as Microsoft documents, PDF files and some images and movie types. This free decryption tool is available on No More Ransom. However, some files cannot be decrypted due to bug in Lorenz Ransomware. During encryption last 48 bytes are not written to the encrypted file due to the bug and are permanently lost.

Prometheus Decryptor: CyCraft, a Taiwanese security firm, has released decryptor for Prometheus ransomware to help victims recover and decrypt some of their files for free. Prometheus decryptor is available on GitHub. It works on the principle of brute-forcing the encryption key used to lock the victim's data. As Prometheus ransomware uses Salsa20 with a tickcount-based random password to encrypt [files], the password use [the] tickcount as the key, which can be guessed brutally. The only disadvantage of this decryptor is that it can handle brute-forcing the decryption key from small files only. But after release of this decryptor the Prometheus gang ceased operations within two and half weeks later.

Prometheus decryptor is available on GitHub. It works on the principle of brute-forcing the encryption key used to lock the victim's data.

Allstar: Enforces Security Best Practices for GitHub Projects

Source: https://www.securityweek.com/



The Allstar app, developed by Google, can be used to automatically and continuously enforce security best practices for GitHub projects. It continuously checks the GitHub API states and then file contents against defined security policies. In case they don't match, it applies user-defined enforcement actions. The security policy enforcements of Allstar includes branch protection, detection of binary artifacts in a repository, checking presence of a security policy file for vulnerability disclosure, and verify that users with administrator privileges belong to the owning organisation. Allstar provides security scorecards which help users to understand which specific areas need to be improved in order to strengthen the security posture of their project.

Security Tool UChecker for Linux Servers

Source: https://www.zdnet.com/

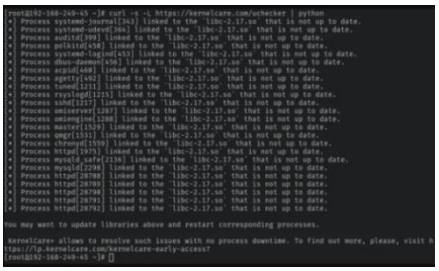


Image source: https://ostechnix.com/

CloudLinux company has released an open-source program UChecker to improve Linux's operational security. UChecker which is an abbreviation of userspace checker scans Linux servers for out-of-date libraries both on disk and in memory. It works with all modern Linux distributions. It provides detailed report of vulnerable library used by applications, relevant process ID and process name. It can be easily integrated with monitoring, logging and

management tools such as Nagios for better security defences. After running UChecker from the shell, it provides two options for updating libraries. Libraries can be updated using packaging system or TuxCare LibraryCare service.

Google releases Security Scorecard

Source: https://www.zdnet.com/

According to research, 95% of commercial programs contain open-source software. Majority of the code contains outdated or insecure code. Google and the Open-Source Security Foundation (OSSF) provides OpenSSF Security Scorecards to tell which libraries and components are safe. Scorecard's project is an automated security tool for open-source program that produces a risk score based on a set of pass/fail checks. This reduces manual work of a developer to evaluate changing packages while maintaining project's supply chain. Scorecard checks are based on checks whether repository is active or not, automatic-dependency-update, binary-artifacts, branch-protection, CI-tests, CII-Best-practices, Code-Review, Contributors, Fuzzing, Frozen-Deps, packaging, Security-policy, Token-Permissions etc.

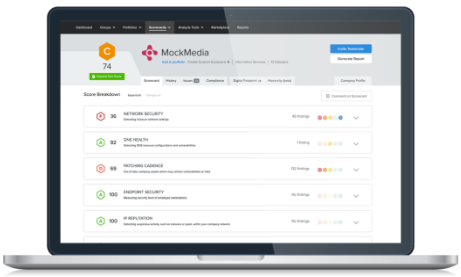


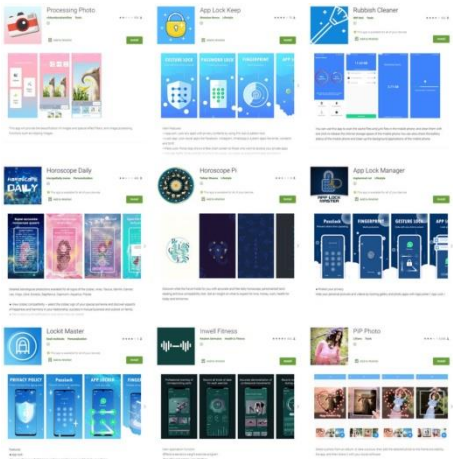
Image source: https://instant.securityscorecard.com/

Mobile Security

Apps Stealing Facebook Logins and Passwords

Source: https://news.drweb.com/

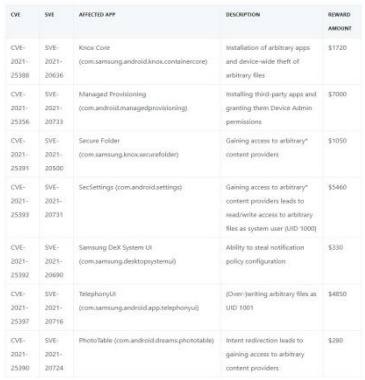
According to Doctor Web, nine malicious apps were found in Google Play Store stealing Facebook user's login and passwords. The Trojans were installed more than 5,856,010 times. Upon installations, users were asked to disable in-app ads and to do so, they were prompted to log into their Facebook accounts. After clicking on the Facebook login form, the app received necessary JavaScript from C&C server, which was then loaded along with legitimate Facebook web page in the same WebView. Now, whenever a user tried to log into his/ her Facebook account, the Facebook credentials along with cookie details got stolen and passed onto the C&C server. The malware also outputs data into the log in Chinese language. The malicious apps are 'Processing Photo' by the developer chikumburahamilton, 'App Lock Keep' from the developer Sheralaw Rence, 'App Lock Manager' by the developer Implummet col, 'Lockit Master' from the developer Enali mchicolo, 'Rubbish Cleaner by the developer SNT.rbcl, 'Horoscope Daily' from the developer HscopeDaily momo, 'Horoscope Pi' by the developer Talleyr Shauna, 'Inwell Fitness' from the developer Reuben Germaine and 'PIP Photo' by the developer Lillians. Dr. Web has dubbed these malwares as Android.PWS.Facebook.13, Android.PWS.Facebook.14, Android.PWS.Facebook.15, Android.PWS.Facebook.17 and Android.PWS.Facebook.18. Users



are requested to install apps only from known and trusted developers at Google Play Store.

Vulnerabilities in Samsung Pre-Installed Apps

Source: https://thehackernews.com/



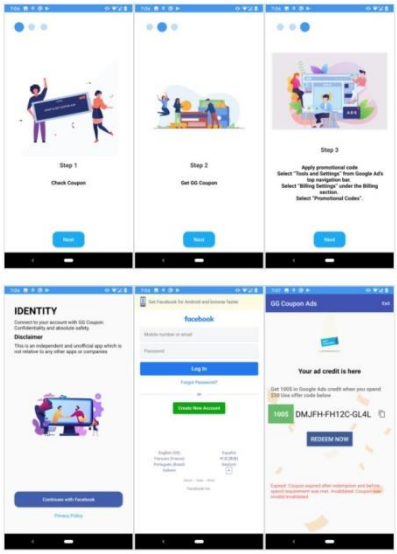
CVE	SVE	AFFECTED APP	DESCRIPTION	REWARD AMOUNT
CVE-2021-25388	SVE-2021-20636	Knox Core (com.samsung.android.knox.containercore)	Installation of arbitrary apps and device-wide theft of arbitrary files	$1720
CVE-2021-25356	SVE-2021-20733	Managed Provisioning (com.android.managedprovisioning)	Installing third-party apps and granting them Device Admin permissions	$7000
CVE-2021-25391	SVE-2021-20500	Secure Folder (com.samsung.knox.securefolder)	Gaining access to arbitrary* content providers	$1050
CVE-2021-25393	SVE-2021-20731	SecSettings (com.android.settings)	Gaining access to arbitrary* content providers leads to read/write access to arbitrary files as system user (UID 1000)	$5460
CVE-2021-25392	SVE-2021-20690	Samsung DeX System UI (com.samsung.desktopsystemui)	Ability to steal notification policy configuration	$330
CVE-2021-25397	SVE-2021-20716	TelephonyUI (com.samsung.android.app.telephonyui)	(Over-)writing arbitrary files as UID 1001	$4850
CVE-2021-25390	SVE-2021-20724	PhotoTable (com.android.dreams.phototable)	Intent redirection leads to gaining access to arbitrary content providers	$280

Image source: https://blog.oversecured.com

Mobile security startup Oversecured has recently discovered multiple critical flaws in pre-installed Samsung apps. The seven vulnerabilities which are CVE-2021-25356, CVE-2021-25388, CVE-2021-25390, CVE-2021-25391, CVE-2021-25392, CVE-2021-25393 and CVE-2021-25397, if exploited could lead to theft of user's personal data without their consent and take control of devices. It can also lead to unauthorised access to victim's contacts, calls, SMS/MMS etc. Arbitrary apps with device administrator rights can also be installed which can alter the device's settings. These vulnerabilities were reported in February 2021 and were patched by monthly security updates of April and May 2021. Users are requested to update their Operating System.

FlyTrap Android Malware

Source: blog.zimperium.com



Zimperium's zLabs mobile threat research teams have discovered a new Android Trojan targeting Facebook accounts. The malware dubbed as FlyTrap is active since March 2021 and has spread to at least 140 countries via Google Play and third-party app stores. The malware lured its targets by posing as apps distributing free Netflix coupon codes, Google AdWords coupon codes etc. After installation and initial engagement with the users, the malware shows Facebook's login page and asks its users to login to collect app rewards. Using pre-configured WebView, it injects malicious JavaScript code into the legit URL and extracts Facebook ID, location, email address, IP address, cookie and token associated with the Facebook account etc. It then sends those login credentials to its C&C server. The harvested credentials are then used to abuse victim's social media accounts by spreading propaganda through personal messaging or running disinformation campaign based on victim's geolocation details.

PJobRat targeting Officers

Image source: blog.cyble.com

Source: cyware.com/news/, gbhackers.com, blog.cyble.com

According to researchers at Cyble and 360 Core Security Lab, a spyware campaign has been uncovered targeting Indian officers since January 2021. Spyware dubbed as PJobRat, posing as dating and instant messaging apps, is being used in this campaign. It has disguised itself as Trendbanter (dating app) and Signal (instant messaging app) app for its users. It also imitates

other apps like HangOn, SignalLite, Rita, Ponam etc. Upon installation, it imitates WhatsApp's icon on the user's home screen but in the settings, it reveals the Trendbanter icon of the spyware app. It asks for dangerous permissions from users and exfiltrates data from victim's device without his/ her knowledge. It steals document files like pdf, doc, docx, xls, xlsx, ppt and pptx files from the victim's device. Apart from that, it uploads address book, SMS, audio files, video files, image files etc. to its C&C server.

It steals document files like pdf, doc, docx, xls, xlsx, ppt and pptx files from the victim's device.

FMWhatsApp hit by Trojan Triada

Source: securelist.com

Popular modified version of WhatsApp called FMWhatsApp (v16.80.0) has recently been hit by Trojan Triada via an advertising Software Development Kit (SDK). It has been detected as Trojan.AndroidOS.Triada.ef. After installation, the app registers the device by sending unique device identifiers like Device IDs, Subscriber IDs, MAC addresses and the app package name to its C&C server. After successful device registration, the C&C server responds with a link of malicious payload which gets deployed on the user end. The malware also gets permission to read user's SMS messages. The malware then displays full-screen advertisements to users, runs invisible ads in the background, signs up for paid/ premium subscriptions without user's consent. Users are advised to download WhatsApp from official sources only.

Image source: gbplus.net

Guidance on Securing Wireless Devices in Public Settings

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

Methods used to compromise devices and data are constantly progressing. As telework becomes more common, users are more often bringing themselves and their data into unsecured settings and risking exposure. By following the guidance issued by NSA, users can detect potential threats and put best practices into action when teleworking in public settings. Best practices for securing wireless devices:

- Keep software and applications updated with latest patches.
- Use anti-virus/anti-malware software.
- Use multi-factor authentication (MFA) whenever possible.
- Reboot regularly after using untrusted Wi-Fi.
- For Laptops, enable firewalls to restrict inbound and outbound connections by application.
- Connect to a personal/corporate wireless hotspot with strong authentication and encryption if possible.
- Disable Wi-Fi when not in use and also disable Wi-Fi network auto-connect.
- Only connect to secure public Wi-Fi.
- Turn off the device file and printer sharing on public networks.

By following the guidance issued by NSA, users can detect potential threats and put best practices into action when teleworking in public settings.

Use an allow list or deny list of applications that can use the device's Bluetooth.

- Disable the Bluetooth feature when it is not being used.
- Use an allow list or deny list of applications that can use the device's Bluetooth.
- Disable NFC feature when not needed (if possible).

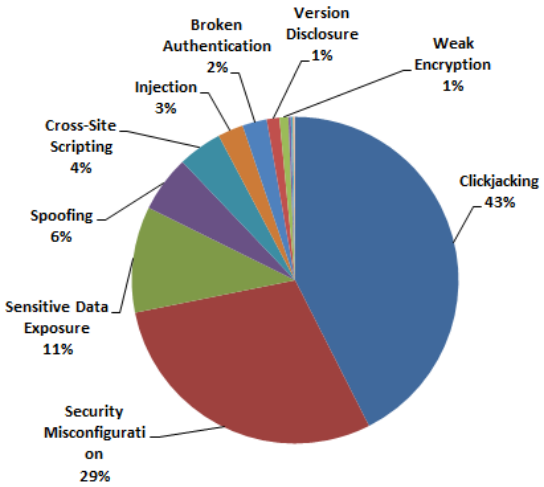
Complete security is never guaranteed, but to protect your devices and data in public settings when teleworking, the above points are highly recommended.

NCIIPC Initiatives

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 3913 vulnerabilities reported during the third quarter of 2021. The top 10 vulnerabilities are:



- Click Jacking
- Security Misconfiguration
- Sensitive Data Exposure
- Spoofing
- Cross-Site Scripting
- Injection
- Broken Authentication
- Version Disclosure
- Weak Encryption
- Denial of Service

Around 404 researchers participated in RVDP programme during the third quarter of 2021. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Aman Kumar
- Ashish Khare
- Ashutosh R Mishra
- Bhavak Dipakkumar Kotak
- Bismaya Kumar Panda
- Chinmay Vishwas Divekar
- Harsh Banshpal
- Jay Kumar Pandey
- Naved Shaikh

- Onkar Nandkumar Kshemkalyani
- Prince Prafull
- Rahul Mishra
- Samprit Das
- Shubhdeep
- S Rahul

Webinar on 'Safety of Power Utilities from Cyber Attack'

NCIIPC East Zone participated in webinar on "Safety of Power Utilities from Cyber Attack" organised by InfoSec Foundation and Supported by Institute of Electrical and Electronics Engineers (IEEE) ComSoc on 27th August 2021. The program was inaugurated by Sh. Hari K. Kusumakar (IPS), Secretary Home and Hill Affairs, CISO, Govt of West Bengal. Sh. Sanjay Kumar Das, Jt Sec, Dept of IT& E, Govt of West Bengal moderated the session. Other esteemed panelists were from different power utilities of India, like Calcutta Electric Supply Corporation (CESC), Tata Power Ltd, State Load Despatch Centre (SLDC) Meghalaya, Maharashtra State Electricity Distribution Company Limited (MSEDCLe), etc. Sh. Tathagata Datta, Consultant, NCIIPC highlighted the need of Role-Based Access Control (RBAC) systems, hardening of security equipment, regular patching as some of the basic cyber hygiene to be maintained. Special emphasis was given on the threats emerging from Supply Chain Contamination and need of timely reporting of cyber incidents to national nodal agencies was also explained.

Upcoming Events - Global

GLOBAL CYBER INNOVATION SUMMIT 2021

OCTOBER 2021

S	M	T	W	T	F	S
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	30

NOVEMBER 2021

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				

TEL AVIV תל אביב DEVOPSDAYS

.droidcon SAN FRANCISCO DEC. 13th - 14th 2021 #DCSF21

October 2021

- 16th International Conference on Cyber-Technologies and Cyber-Systems 2021, Barcelona 3-7 Oct
- The 4th International Workshop on Attacks and Defences for Internet-of-Things , Darmstadt 4-8 Oct
- European Symposium on Research in Computer Security 2021, Virtual 4-8 Oct
- Global CISO Forum 2021, Atlanta & Virtual 7-8 Oct
- INTERFACE Spokane 2021, Virtual 14 Oct
- DevSecCon London 2021, London & Virtual 20-21 Oct
- Industrial Control Systems Cyber Security Conference, Atlanta & Virtual 26-28 Oct
- Global Cyber Innovation Summit 2021, Baltimore 27-28 Oct

November 2021

- Ekoparty Security Conference 2021, Virtual 2-6 Nov
- SecureWorld Dallas, Dallas 3-4 Nov
- Black Hat Europe 2021, London & Virtual 8-11 Nov
- 8th annual Control Systems Cybersecurity Europe Conference, London 9-10 Nov
- 16th Annual API Cybersecurity Conference For The Oil & Natural Gas Industry, Texas & Virtual 9-10 Nov
- CyberConference – AISA Melbourne, Virtual 15-17 Nov
- DeepSec In-Depth Security Conference 2021, Vienna 16-19 Nov
- DevOpsDays Tel Aviv 2021, Tel Aviv 24-25 Nov

December 2021

- SecureWorld West Coast 2021, Virtual 2 Dec
- 2nd International Conference on New Computer Science and Engineering 2021, Virtual 3-4 Dec
- Acronis CyberFit Summit World Tour 2021, Dubai 8-9 Dec
- Des Moines Cybersecurity Conference, Virtual 9 Dec
- Droidcon San Francisco 2021, San Francisco 13-14 Dec
- The Great Lakes Virtual Cybersecurity Summit, Virtual 14 Dec
- Atlanta CyberSecurity Conference, Virtual 15 Dec
- Asian Hardware Oriented Security and Trust Symposium 2021, Shanghai 16-18 Dec

January 2022

- World Conference on Cyber Security and Ethical Hacking, Singapore 2-3 Jan
- Real World Crypto Symposium, Amsterdam 10-12 Jan
- International Conference on Mobile Application Security, Bali 14-15 Jan

Upcoming Events - India

- 2nd International Conference on Future Communication & Computing Technology, Virtual 27-28 Oct
- International Conference on Cyberlaw, Cybercrime & Cybersecurity 2021, Virtual 24-26 Nov
- International Conference on Network Security and Blockchain Technology, Kolkata 2-4 Dec
- 22nd International Conference on Cryptology in India Jaipur 12-15 Dec
- International Conference on Computational Intelligence, Cyber Security and Computational Models, Virtual 16-18 Dec

DECEMBER 2021

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	

JANUARY 2022

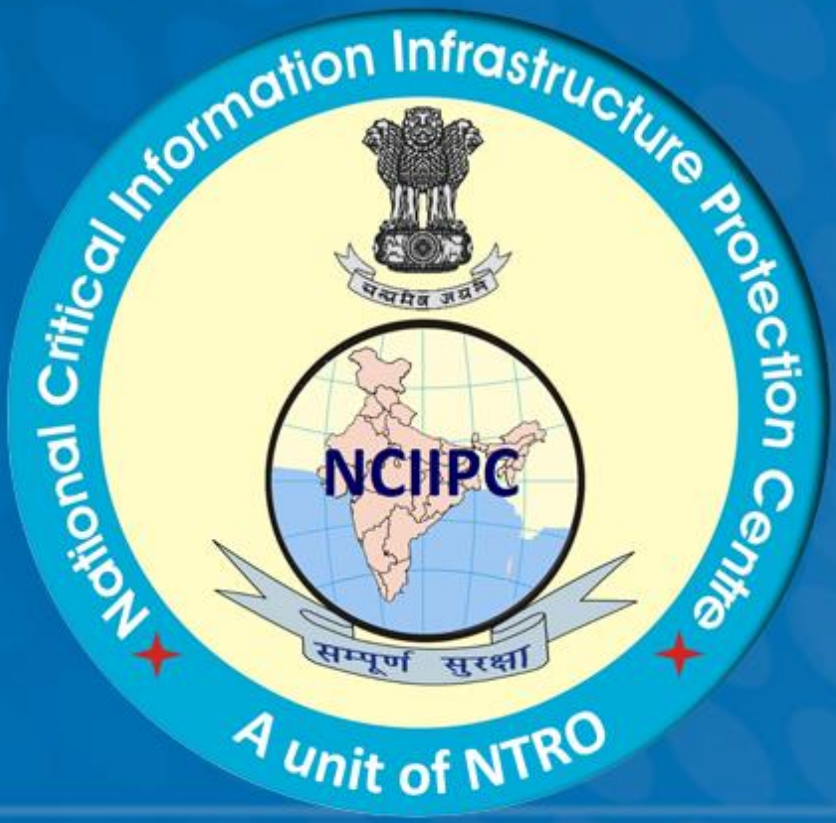
S	M	T	W	T	F	S
30	31					1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
24	25	26	27	28	29	30

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

- ADTL: Alpha Design Technologies Limited
- BSNL: Bharat Sanchar Nigam Limited
- CESC: Calcutta Electric Supply Corporation
- CISA: Cybersecurity and Infrastructure Security Agency
- CRS: Civil Registration System
- CSPRNG: Cryptographically Secure Pseudorandom Number Generator
- CVE: Common Vulnerabilities Exposure
- CVSS: Common Vulnerability Scoring System
- CWE: Common Weakness Enumeration
- DHS: Department of Homeland Security
- FBI: Federal Bureau of Investigation
- ICS: Industrial Control System
- IEEE: Institute of Electrical and Electronics Engineers
- IoT: Internet of Things
- IT: Informational Technology
- JCDC: Joint Cyber Defence Collaborative
- KAERI: The South Korean Atomic Energy Research Institute
- LEA: Law Enforcement Agency
- MFA: Multi-Factor Authentication
- MSEDCLe: Maharashtra State Electricity Distribution Company Limited
- NERLDC: North Eastern Regional Load Dispatch Centre
- NFC: Near Field Communication
- NIST: National Institute of Standards and Technology
- NRLDC: Northern Regional Load Dispatch Centre
- NSA: National Security Agency
- NVD: National Vulnerability Database
- OSSF: Open Source Security Foundation
- PLA: People's Liberation Army
- POSOCO: Power System Operation Corporation
- QDK: Quantum Key Distribution
- RaaS: Ransomware as-a-Service
- RBAC: Role-Based Access Control
- RCE: Remote Code Execution
- RVDP: Responsible Vulnerability Disclosure Program
- SLDC: State Load Despatch Centre
- SLTT: State, Local, Tribal and Territorial
- SMB: Server Message Block
- SRLDC: Southern Regional Load Dispatch Centre
- TLS: Transport Layer Security
- TTPs: Tactics, Techniques, and Procedures
- VLE: Village Level Entrepreneur
- WRLDC: Western Regional Load Dispatch Centre

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.