**Cyber Security Advisories**

**Date: 18 February 2025**

1. **TA-PHI-2025-02-18-015**

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:**

in.gov.indiana.com

www.estbengalpolicegov.infogini.com

bnd.ndmc.gov.in.web.viewcrti.info

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

nrsec-gov-in.online

dfsin.top

email.g0v.in

tspscgov.info

getkavach.com

dc.crsorgi.gov.in.dcbirth.in

gov.in.dcbirth.in

indotingov.info

yrspc-gov.info

dcbirth.in

dc-crsorgi-gov.shop

dc.crsorgi.gov.in.svlprint.site

www.gov.in.cscvle.store.droft.shop

gov.in.igaxis.site

www.ladlilaxmi.mp.gov.in.consulting

mp.gov.in.consulting

\*.gov.in.consulting

\*.in.svlprint.site

\*.in.cscvle.store.droft.shop

in.reset-password.com

email-gov-in.reset-password.com

www.reset-password.com

rrbgov.info

bio.iircin.com

iircin.com

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

1. **TA-MAW-2025-02-18-015**

It has been observed that DC RAT (Dark Crystal RAT), a powerful Remote Access Trojan (RAT), is actively used by threat actors to conduct cyber-espionage, system control and for data exfiltration. The DC RAT is capable of executing remote commands, stealing credentials, logging keystrokes, capturing screenshots and establishing persistent access.

The DC RAT is often deployed via spear-phishing emails, malicious attachments and fake software installers. DC RAT has been observed in targeted cyberattacks against government, defense, financial, and critical infrastructure organizations, posing a significant security risk.

**Key Features of DC RAT**

* Remote System Control – Adversary can manipulate infected systems remotely.
* Keystroke Logging & Credential Theft – Monitors user activity and steals sensitive information.
* Data Exfiltration – Extracts confidential documents and personal data.
* Persistence Mechanisms – Ensures long-term access by modifying system files and registry entries.
* Command & Control (C2) Communication – Uses encrypted traffic to evade detection while C2 communicating with servers.

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

**IP:**

182.188.47.2

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

1. **TA-MAW-2025-02-18-016**

It has been observed that presence of various malware campaign has been found in indian cyberspace. This malware campaign target various sectors, including government (defence, external affairs etc.), finance, technology, and critical infrastructure. Its objectives range from espionage and data theft to sabotage and disruption.

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

* Phishing and Social Engineering: Attackers frequently use phishing emails or social engineering tactics to trick users into downloading malware or revealing sensitive information.
* Exploiting Vulnerabilities: Malware may exploit known software vulnerabilities to gain access to systems. This includes zero-day exploits that target unpatched software.
* Remote Access Trojans (RATs): Many malware variants include RATs, which allow attackers to control infected systems remotely, facilitating data exfiltration and further attacks.
* Command and Control (C2) Communication: Infected devices often communicate with C2 servers to receive instructions or send stolen data. This communication can be obfuscated to evade detection.
* Use of Malware Kits: Attackers may employ sophisticated malware kits, which simplify the creation of malware and the exploitation of vulnerabilities, making attacks more efficient.
* Fileless Malware: Some malware variants operate without writing files to disk, making detection more challenging. They reside in memory and execute scripts to carry out malicious activities.

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

**Domains:**

rov.noon.dns04.com

picture.efanshion.com

fashion.fashpopstyle.com

comaset.ns01.info

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

1. **TA-MAW-2025-02-18-017**

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

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

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

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

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

**Domain:**

cloud.glowman554.gq

**IP:**

20.151.161.144

**Hashes:**

02baaf03a93b0ab4234a64c5db4b32cbe5d646f575fdbb7126ba93841d8f7058

082951a1e8a16359bcfd2e2c5f2ba25b570cb3979a259f73dea1d992ec6f4c74

0d019c6f5f3068ab39bf2b1ebb1f8701b872d0b41218635f247abf6474c52bf7

0fd3af45929fb34ab43d21c25ef2afe152eecbb031c92ecbcfd3ce07e833b68c

4c745184646da9c4766e493ef1cc8f8296cda52127be37f8024eb2c200a81731

4ffe9a7211f050abea769c240a40003624f5ef0dc0b8d1006ee5e6742fa93678

563e5577d6e119054b7781374d3de4b0ee1d29777e8b49e7cfb56afab8111720

767c37b6de102114360aeae2c3394df36cdb7820d875d0b5f0f7335ca65268f6

b6efaa05937e4646c3c22e16b61daadb4a087ca6ced1c236390dd3d746e0b206

c88ddb547da45338a74712616f844d7744ab2c719dd3b33f91a4f41931786745

cc5a2c207bfbd16a5cb647a7a8dbf31c9dfef965653512e58f8f5de5a47acf11

d062cd0119ae81dbfa3e06754334879a439c586a95eb7846d2ee1e3be0e66a67

eac92d362bbf8550a1945184dfeb6a703c9862dba988f2e8c7163818aede8b7c

fcd0e23f24528171794770dee1627b4de135689efd02bfcdb92ee4dcbc92f85f

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

1. **TA-APT-2025-02-18-003**

Reference is made to earlier advisories on APT36 Campaign.

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

**Domains:**

https://secdesk.xyz/drivers\_files

http://secdesk.xyz:8062

secdesk.xyz

\*.secdesk.xyz

ip-api.com (genuine domain but used by the threat actors to obtain public IP address of the victim machine)

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

1. **TA-APT-2025-02-18-004**

Reference is made to earlier advisories on APT SideCopy.

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

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

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

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

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

**Domains:**

bsli.pcdaopune.site

winsoft.pcdaopune.site

winsofts.pcdaopune.site

sopos.mypressonline.com

\*.pcdaopune.site

h791yuwbecdn8lfcundipxyzx.canarytokens.com

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

1. **TA-RAN-2025-02-18-007**

Reference is made to earlier advisories on the RA WORLD RANSOMWARE.

It has been observed that RA World ransomware, a malicious software variant involved in cyber extortion campaigns, particularly linked to state-sponsored espionage activities. Adversary is used against a medium-sized software and services company in South Asia. Recently, tools typically associated with  state-sponsored espionage actors were identified in a ransomware attack involving the RA World ransomware.

The following ransomware families have been linked to the use of  state sponsored espionage tools:

* LockFile - A ransomware variant implicated in attacks attributed to the espionage group Bronze Starlight.
* AtomSilo - Another ransomware family linked to the same group.
* NightSky - Included in the set of ransomware used by the Bronze Starlight group.
* LockBit - Frequently associated with various cybercriminal activities, also noted in the context of espionage-linked attacks.

Technical Details:

* Proxy tool NPS- The NPS (Network Proxy Service) is a proxy tool associated with cyberattacks, particularly those linked to espionage operations. It has been recently reported as one of the tools used in ransomware attacks, specifically by actors involved with the RA World ransomware.
* Toolset: The same toolset used in previous espionage attacks was employed in the RA World ransomware incident, indicating a continuity in operational tactics.
* DLL and Payloads: The attacker used a legitimate Toshiba executable to sideload a malicious DLL, which acted as a loader for a heavily obfuscated payload. This payload was linked to a variant of PlugX, a custom backdoor associated with espionage threat actors.

Impacts of RA World  Ransomware:

* Financial losses due to ransom payments.
* Operational disruptions within targeted organizations.
* Data theft or exposure, compromising sensitive information.
* Long-term reputational damage to affected companies.

The distribution methods for this ransomware attack include:

* Exploiting known vulnerabilities, such as those in firewall software (e.g., CVE-2024-0012).
* Utilizing phishing or social engineering tactics to gain initial access .
* Deploying malware via compromised legitimate software or DLL hijacking techniques.
* Attackers utilized legitimate executables (e.g., toshdpdb.exe) to sideload malicious DLLs (e.g., toshdpapi.dll), which act as loaders for encrypted payload.

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

**Hashes:**

7bae7f21bd4adf84eb3cc281fcc3d5fc3d1e47edd0dadd86587ce8ec63df1b8f

c1e6955acdefa9769a7ae0c1abf54a26e2158154dd6ec07cc71eb06c575193d5

18127cfd08cc49be08714d29e09ec130dcc0b19b7fcddc22c71d28fd245eb1b1

e177eb358f93ccc1ac4694feb0139e82c62d767388872d359d7c2ed0a05c2726

6ac81aa8d3f9d86ad5a18ea42fa1829b055dd25f123f9ee90002d64d4ef7a394

2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813

38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25

bb5740d2129663ae1c46b1ea1bdd0b8c423b6eb8f6e6f2b0b158a9e833496a01

**Domains:-**

plugins.jetbrians.net

police.tracksyscloud.com

caco.blueskyanalytics.net

**IPs:**

158.247.213.167

154.223.18.123

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