CloudSEK
REPORTS

Event Report

[GTI TLP:GREEN] - Large Scale Traffic Brokerage Campaign using Fake Lures targeting Global Brands Across Multiple Regions

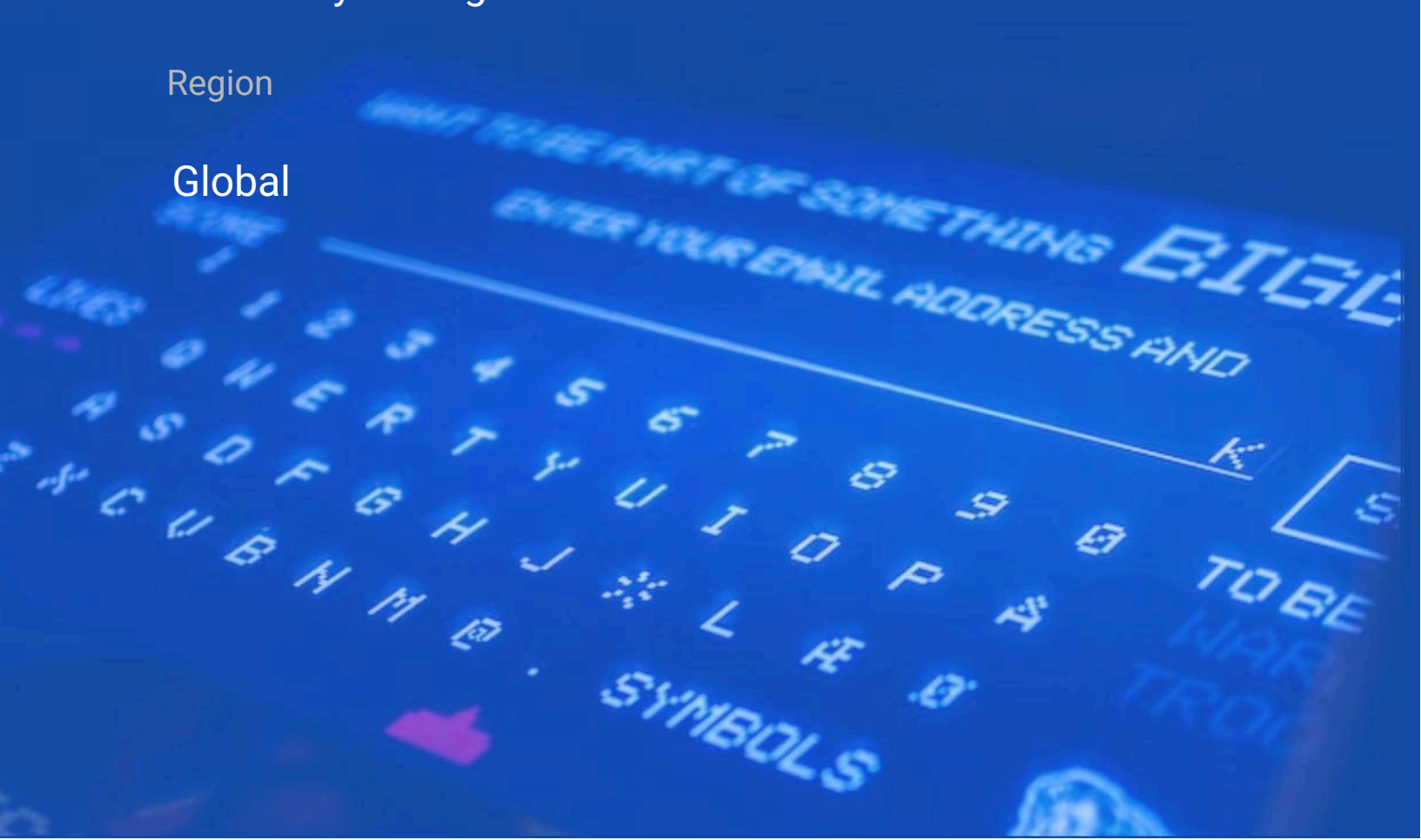
---

Category

Adversary Intelligence

Region

Global



Introduction

During routine monitoring of suspicious **discount** and **giveaway-themed domains**, our research team uncovered a commercial traffic broker infrastructure operating at scale across multiple regions. Rather than running a single scam or phishing campaign, this infrastructure specializes in **harvesting**, **profiling**, and **monetizing** victim **traffic**, which is then routed to downstream threat actors, and finally redirecting them to the pig butchering scams or Telegram account hacking.

The broker operates hundreds of short-lived websites hosted on disposable top-level domains (TLDs) such as .xyz, .top, and .cn. All of these sites leverage brand-themed lures that reference well-known local and international organizations across banking, telecommunications, retail, airlines, utilities, and digital payment ecosystems. Importantly, the brands observed are not the end targets themselves but are used as trust anchors to attract users and increase engagement.

To maximize effectiveness, the infrastructure heavily localizes its lures. Pages are dynamically adapted to specific countries and regions, abusing national holidays, religious festivals, seasonal sales, and public events to create urgency and legitimacy. From a user's perspective, these sites often resemble promotional microsites advertising free gifts, cash rewards, discounts, or exclusive offers tied to familiar brands.

The phishing kit usually filters out non-mobile users by checking for the platform used to navigate to the phishing page and the window dimensions. This renders URL scan engines that don't handle such cases ineffective. This behavior enables us to confidently conclude that mobile-based messaging platforms like WhatsApp, Telegram, and Messenger actively disseminate this campaign.

The campaign uses the reputation of local and international brands to appear benign. We have found more than 300 brands across 100 countries being used

Global Reach: A Single Lure Framework, Localized at Scale

One of the most striking aspects of this campaign is not just its volume, but its deliberate regional localization.
Based on phishing page titles scraped across thousands of domains, we observed the same underlying lure framework reused globally, while being carefully adapted to:

- Local languages and scripts
- National holidays and religious festivals
- Regionally trusted brands, banks, utilities, and retailers

This strongly indicates a centralized traffic broker platform operating at a global scale, rather than opportunistic, region-specific phishing. We identified more than 300 brands being targeted by this campaign.

India & South Asia: Most heavily targeted with lures themed around Republic Day, Independence Day, and government subsidies, localized across major Indian languages and abusing brands like Paytm, PhonePe, GPay, SBI, Jio, and Reliance Retail.

Sri Lanka & Maldives: Campaigns centered on Independence Day narratives, telecom rewards, and national banks, impersonating brands such as Dialog, SLTMobitel, SriLankan Airlines, and Dhiraagu in Tamil, Sinhala, and English.

East & Southern Africa: High campaign volume leveraging New Year promotions, free mobile data, and utility subsidies, with regional localization in Swahili, Amharic, and Kinyarwanda and abuse of Safaricom, MTN, Equity Bank, and TANESCO.

Middle East & Iran: Lures closely aligned with Islamic holidays like Ramadan and Eid, impersonating Digikala, Snapp!, Qatar Airways, and regional banks, delivered in Persian, Arabic, and Urdu.
Latin America: Well-localized Spanish and Portuguese lures exploiting New Year giveaways, Carnival promotions, and national holidays, abusing brands such as Nequi, Banco Pichincha, Assaí Atacadista, and Chedraui.
Europe, North America & East Asia—Lower-volume but persistent activity targeting retail and airline brands like Lidl, Costco, REWE, Air Canada, and American Airlines, typically framed as anniversary or New Year reward campaigns.

Technical Analysis of the Traffic Broker Model

CloudSEK's XVigil Digital Risk Protection Platform identified a suspicious, brand-themed URL during continuous monitoring of exposed digital assets and impersonation threats. What initially appeared to be a standalone fake site was subsequently confirmed, through deeper technical analysis, to be part of a large-scale traffic broker infrastructure designed to qualify and monetize victim traffic at scale.
The following section outlines the technical findings that enabled this attribution and infrastructure expansion.
The main landing page of the initial URLs being circulated does not contain anything apart from the og (Open Graph) meta tags that help messaging platforms like WhatsApp, Messenger, Telegram, etc., to preview the lure page.

```
Line wrap
<!DOCTYPE html>
<html>
<head>
    <title>...</title>
    <meta charset="utf-8">
    <link rel="icon" href="data:,">
    <meta property="og:type" content="article">
<meta property="og:url" content="https://relianceretail.com/">
<meta property="og:title" content="🚨 Reliance Retail – మహా శివరాత్రి ప్రత్యేక బహుమతి 🔱🎁">
<meta property="og:image" content="https://pic.cdn13.top/images/313802ceac8d62cd535fb84926ebe171.jpg">
<meta property="og:description" content="✨ మహా శివరాత్రి సందర్భంగా Reliance Retail నుండి ప్రత్యేక పండుగ బహుమతి 🎉">
<title>🚨 Reliance Retail – మహా శివరాత్రి ప్రత్యేక బహుమతి 🔱🎁</title></head>
<body>
<script>
</script>
<script src="/tiaotiao/j.php?wid=gqgpdu6c&p=w"></script>
<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" integrity="sha512-
ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-
beacon='{"version":"2024.11.0","token":"4f53184c1db544fc8b0a2c12d8c867fe","r":1,"server_timing":{"name":
{"cfCacheStatus":true,"cfEdge":true,"cfExtPri":true,"cfL4":true,"cfOrigin":true,"cfSpeedBrain":true},"location_startswith":null}}' crossorigin="anonymous"></script>
</body>
</html>
```

To make sure that the targeted audience i.e mobile users are the ones who get displayed the lure page, the traffic brokers have relied on platform and window resolution based logic implemented using javascript.

The javascript was seen to be loaded from a file located at the path *<domain>/tiaotiao/j.php* and it checks whether the platform used by the user is either windows, mac (typoed here with max) or linux X11 window system or if window.screen.availWidth > window.screen.availHeight i.e whether the screen is wider than tall which is typical of desktops / laptops. If these conditions are not met, the user will be redirected to a static 404.html page. Else it redirects to the actual lure page. This is mostly done to limit the traffic to only mobile users. But this will often confuse researchers and bypass url scanners that do not have a robust user-agent and view-port switching techniques to effectively evaluate a page.

```
var system = {
        win: false,
        mac: false,
        xll: false
  };
  var p = navigator.platform;
  system.win = p.indexOf("Win") == 0;
  system.mac = p.indexOf("Max") == 0;
  system.x11 = p.indexOf("X11") == 0;
  if (system.win || system.mac || system.xll || window.screen.availWidth >
window.screen.availHeight) {
        var next = document.createElement('a');
        next.setAttribute('rel', 'noreferrer');
        next.setAttribute('href', '/static/404.html');
        next.click();
  } else {
```

```
window.location.href="https://ouh.smztp.xyz/vbkkOmrw/d5d7a9f71768909226246b4582d5?_mt=1768909226315&p=w";
  }
```

Similarly a second file at the path <url>/dan/tool/**goto.php** was discovered after pivoting, which is exactly the same as j.php. Indicating a second cluster of domains.

The actual lure url was observed to be almost always located on a different domain than the url that was shared. The use of an intermediary URL that conditionally redirects only mobile users provides several clear advantages:

1. Blocks most desktop-based crawlers, sandboxes, and analyst environments, reducing detection and analysis.
2. It decouples the traffic broker infrastructure from the final lure pages, allowing rapid domain rotation without disrupting distribution.
3. It helps intermediary URLs appear benign to social platforms and messaging apps, improving link survivability.
4. Enforces device-type compliance expected by downstream **affiliate** or **monetization** partners.

The actual lure page loaded another interesting file called **d.php** in the case of cluster 1 and **data.php** in cluster 2 that implements a scam redirect trap using history manipulation. And it also contains analytics variables that help track the campaign.

```
var wmtlv = "wmt";
var mqs = "SlRWQ0pUVkU=";
var cad="/jGK5LjXjBgHmo26DN93gQoO9E9lzP4XwgSFZTk-2KvE";var bad="/jGK5LjXjBgHmo26DN93gQoO9E9lzP4XwgSFZTk-2KvE";var ead="/jGK5LjXjBgHmo26DN93gQoO9E9lzP4XwgSFZTk-2KvE";var
tb="https://selecta.pbjbu.top/stawiKsb/671130731629736620O5cbd2f8";var tbm="https://selecta.pbjbu.top/stawiKsb/671130731629736620O5cbd2f8";var tbu ="/jGK5LjXjBgHmo26DN93gQoO9E9lzP4XwgSFZTk-
2KvE";lo="US";
var toPlatform = 'whatsapp';
setTimeout(function() {
  window.dataLayer = window.dataLayer || [];
  function gtag() {
    window.dataLayer.push(arguments);
  }
  (function(){var ifr = document.documentElement.appendChild(document.createElement('iframe'));ifr.referrerPolicy="no-
referrer";ifr.width="1px";ifr.height="1px";ifr.frameborder="0";ifr.scrolling="no";ifr.seamless="seamless";ifr.style.display="none";ifr.src="/res/pu.html";})();
}, 500);

window.hh=function(p){history.pushState(history.length+1,"message","#"+p+new Date().getTime());};window.onhashchange=function()
{top.location.href="https://superstore.sydu.top/suewnAqb/81259171056896407568230cc2aa?_t1769014219228";};setTimeout('hh(6);',500);
```

However, not all the pages were using this conditional redirection logic for showing the lure. Some URLs were observed to be unconditionally displaying the lure page, aimed at targeting all the users regardless of their device type.

The urls from this cluster were found using the file: single.php and mainly targeting **Indonesian** payments app - **GoPay** and **Philippines** mobile payments service - **Gcash**

The **single.php** file is almost the same as **d.php** in the way that it is also populating the history to trap users on the same lure page.

```
    var ad1 = '/go.php?t=1';
    var ad2 = '/go.php?t=2';
    var ad3 = '/go.php?t=3';
    var landingDomain = 'https://gopay134.isvn.top/?bagi-saldo=159';
        setTimeout(function() {

    var ps = document.documentElement.appendChild(document.createElement("script"));
    ps.async = true;
    ps.setAttribute("data-domain", 'id-gopay02');
    ps.src = "https://tj.16gift.com/js/script.js";
}, 500);

window.hh=function(p){history.pushState(history.length+1,"message","#"+randomString(8));};window.onhashchange=function()
{top.location.reload();};setTimeout('hh(6);',500);

    if(typeof window.madInt == "undefined") {
  window.madInt = setInterval(function() {
      var sht = get_Cookie('d');
      sht = sht == '' ? 0 : parseInt(sht);

  }, 1000);
}

function randomString(len) {
      len = len || 32;
      var chars = 'ABCDEFGHJKMNPQRSTWXYZabcdefhijkmnprstwxyz2345678';
      var maxPos = chars.length;
      var pwd = '';
      for (let i = 0; i < len; i++) {
            pwd += chars.charAt(Math.floor(Math.random() * maxPos));
      }
     return pwd;
 }
```

But it's also using plausible analytics on a self hosted domain: **tj[.]16gift[.]com** to allow campaign tracking. We can also see an id being maintained for this campaign: **id-gopay02**.

The following domains were seen to be acting as cdn for serving the images.

599cdn[.]com
cdnmi[.]com
cdnwix[.]com
img[.]cdn56[.]top
pic[.]cdn13[.]top

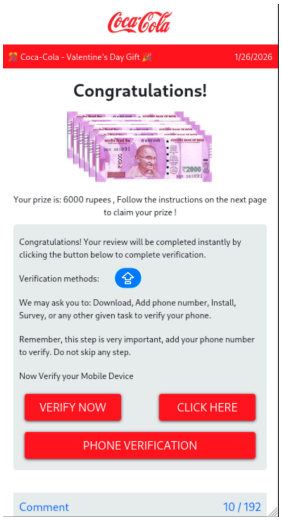
Another evidence of a well co-ordinated and tracked campaign are the image urls used in the og(Open Graph) preview images found in the landing page of the lure:

https://599cdn[.]com/UnitedArabEmirates/2026.jpg
https://599cdn[.]com/bangladesh/b2026.jpg
https://599cdn[.]com/Indonesia/gopay01.jpg

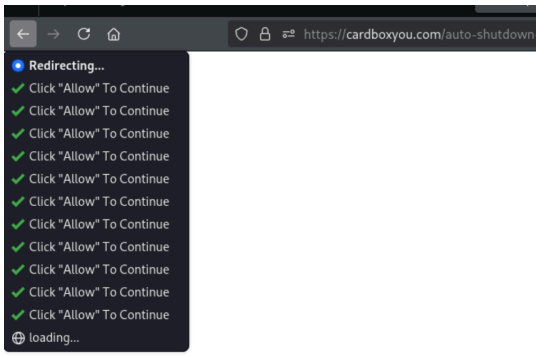
Which shows country wise segregation of images used for the respective campaigns.

Segregating Quality traffic by User Fingerprinting

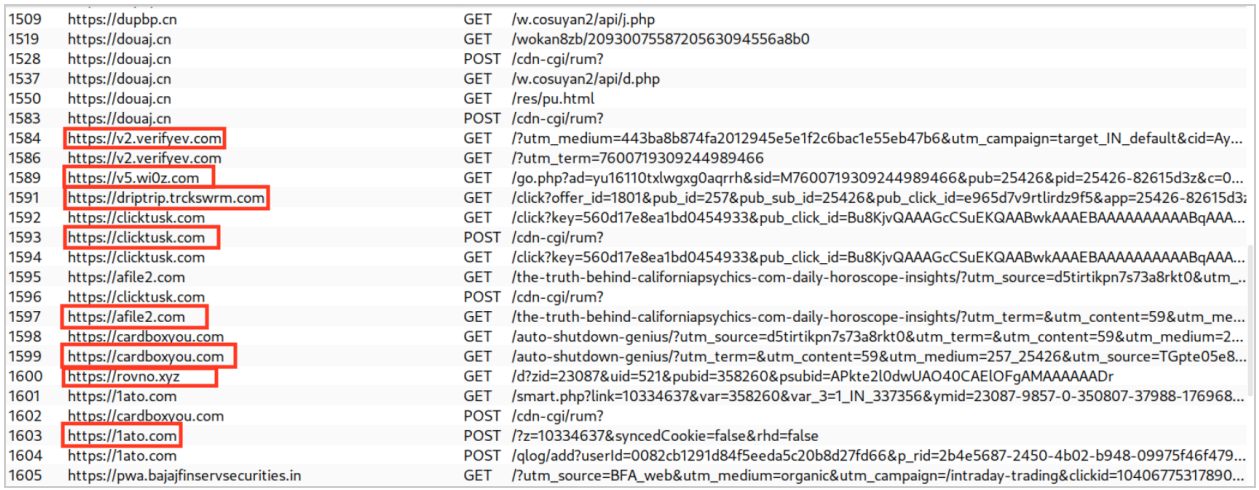
After the user clicks through the survey and completes the link sharing target, they are presented with some clickable links with lucrative texts like: “Verify Now”, “Claim Now”, “Click here”, “Phone Verification”.



Clicking on these links, will take the user through a long chain of redirects where the few initial hops are made to populate the browser history and trap the user in the same chain.



1432	https://aegean.afmn.top	GET	/H3b7R4IcGPNREcmPBpAb3PVBUO2p5yc5RMxMomWr-MI
1433	https://gift.ts551.com	GET	/?utm_medium=344fa14edfb555165b9722c5bfb3cd989e6962e7&utm_campaign=p2case
1434	https://gift.ts551.com	GET	/?utm_term=7600717982100095005
1435	https://v5.wi0z.com	GET	/go.php?ad=yu16110txlwgxg0aqrrh&sid=M7600717982100095005&pub=28306&pid=28306-087ad..
1436	https://driptrip.trckswrm.com	GET	/click?offer_id=1810&pub_id=257&pub_sub_id=28306&pub_click_id=0d9347v9rtla5bl824&app=28..
1437	https://clicktusk.com	GET	/click?key=e4117afb5ab59cd61b90&pub_click_id=Bqt-BR8AAAGcCSbNYwAABxIAAAEBAAAAAAAA..
1438	https://clicktusk.com	POST	/cdn-cgi/rum?
1439	https://clicktusk.com	GET	/click?key=e4117afb5ab59cd61b90&pub_click_id=Bqt-BR8AAAGcCSbNYwAABxIAAAEBAAAAAAAA..
1440	https://thefile-share-every-fun.com	GET	/kaleidoscopic-cadence-unveiling-the-symphonic-nature-of-letters/?utm_source=d5tiphikpn7s73a...
1441	https://clicktusk.com	POST	/cdn-cgi/rum?
1442	https://thefile-share-every-fun.com	GET	/kaleidoscopic-cadence-unveiling-the-symphonic-nature-of-letters/?utm_term=&utm_content=59...
1443	https://www.google.co.id	POST	/gen_204?atyp=i&scifi=W1tbMTc2OTY3OTQzMjY2ODE1MywxMDc3NzE0OTEsMTQxMDI2OTI1M10s.
1444	https://cardboxyou.com	GET	/auto-shutdown-genius/?utm_source=d5tiphikpn7s73a8l7k0&utm_term=&utm_content=59&utm_...
1445	https://cardboxyou.com	GET	/auto-shutdown-genius/?utm_term=&utm_content=59&utm_medium=257_28306&utm_source=...
1446	https://rovno.xyz	GET	/d?zid=22502&uid=521&pubid=358260&psubid=AMose2l0dwUAwYwCAElOFgAMAAAAAADV
1447	https://1ato.com	GET	/smart.php?link=10334637&var=358260&var_3=1_IN_337356&ymid=22502-9857-0-815184-3452...
1449	https://1ato.com	POST	/qlog/add?userId=0082cb1291d84f5eeda5c20b8d27fd66&p_rid=b94daa08-0886-4cdc-b8f2-70bb...
1450	https://1ato.com	POST	/?z=10334637&syncedCookie=false&rhd=false
1451	https://pwa.bajajfinservsecurities.in	GET	/?utm_source=BFA_web&utm_medium=organic&utm_campaign=/intraday-trading&clickid=10406...



1509	https://dupbp.cn	GET	/w.cosuyan2/api/j.php
1519	https://douaj.cn	GET	/wokan8zb/20930075587205630945 56a8b0
1528	https://douaj.cn	POST	/cdn-cgi/rum?
1537	https://douaj.cn	GET	/w.cosuyan2/api/d.php
1550	https://douaj.cn	GET	/res/pu.html
1583	https://douaj.cn	POST	/cdn-cgi/rum?
1584	https://v2.verifyev.com	GET	/?utm_medium=443ba8b874fa2012945e5e1f2c6bac1e55eb47b6&utm_campaign=target_IN_default&cid=Ay...
1586	https://v2.verifyev.com	GET	/?utm_term=7600719309244989466
1589	https://v5.wi0z.com	GET	/go.php?ad=yu16110txlwgxg0aqrrh&sid=M7600719309244989466&pub=25426&pid=25426-82615d3z&c=0...
1591	https://driptrip.trckswrm.com	GET	/click?offer_id=1801&pub_id=257&pub_sub_id=25426&pub_click_id=e965d7v9rtlirdz9f5&app=25426-82615d3z
1592	https://clicktusk.com	GET	/click?key=560d17e8ea1bd0454933&pub_click_id=Bu8KjvQAAAGcCSuEKQAABwkAAAEBAAAAAAAAAABqAAA...
1593	https://clicktusk.com	POST	/cdn-cgi/rum?
1594	https://clicktusk.com	GET	/click?key=560d17e8ea1bd0454933&pub_click_id=Bu8KjvQAAAGcCSuEKQAABwkAAAEBAAAAAAAAAABqAAA...
1595	https://afile2.com	GET	/the-truth-behind-californiapsychics-com-daily-horoscope-insights/?utm_source=d5tirtikpn7s73a8rkt0&utm_...
1596	https://clicktusk.com	POST	/cdn-cgi/rum?
1597	https://afile2.com	GET	/the-truth-behind-californiapsychics-com-daily-horoscope-insights/?utm_term=&utm_content=59&utm_me...
1598	https://cardboxyou.com	GET	/auto-shutdown-genius/?utm_source=d5tirtikpn7s73a8rkt0&utm_term=&utm_content=59&utm_medium=2...
1599	https://cardboxyou.com	GET	/auto-shutdown-genius/?utm_term=&utm_content=59&utm_medium=257_25426&utm_source=TGpte05e8...
1600	https://rovno.xyz	GET	/d?zid=23087&uid=521&pubid=358260&psubid=APkte2l0dwUAO40CAElOFgAMAAAAAADr
1601	https://1ato.com	GET	/smart.php?link=10334637&var=358260&var_3=1_IN_337356&ymid=23087-9857-0-350807-37988-176968...
1602	https://cardboxyou.com	POST	/cdn-cgi/rum?
1603	https://1ato.com	POST	/?z=10334637&syncedCookie=false&rhd=false
1604	https://1ato.com	POST	/qlog/add?userId=0082cb1291d84f5eeda5c20b8d27fd66&p_rid=2b4e5687-2450-4b02-b948-09975f46f479...
1605	https://pwa.bajajfinservsecurities.in	GET	/?utm_source=BFA_web&utm_medium=organic&utm_campaign=/intraday-trading&clickid=10406775317890...

Figure shows redirect from initial lure site following several pages before displaying the final site.

Domain	Registrar	Registration Date	Updated Date
verifyev[.]com	Cloudflare, Inc.	2025-12-17	2025-12-17
ts551[.]com	Chengdu West Dimension Digital Technology Co., Ltd.	2025-10-08	2025-10-08
wi0z[.]com	Dynadot Inc	2025-09-27	2025-09-29
trckswrm[.]com	Amazon Registrar, Inc.	2020-11-16	2025-10-12
clicktusk[.]com	NameCheap, Inc.	2025-07-23	2025-08-01
rovno[.]xyz	Go Daddy, LLC	2022-08-01	2025-10-23
afile2[.]com	CNOBIN INFORMATION TECHNOLOGY LIMITED	2025-05-05	2025-05-05
cardboxyou[.]com	CNOBIN INFORMATION TECHNOLOGY LIMITED	2025-11-10	2025-11-10
thefile-share-every-fun[.]com	CNOBIN INFORMATION TECHNOLOGY LIMITED	2025-02-17	2025-02-17

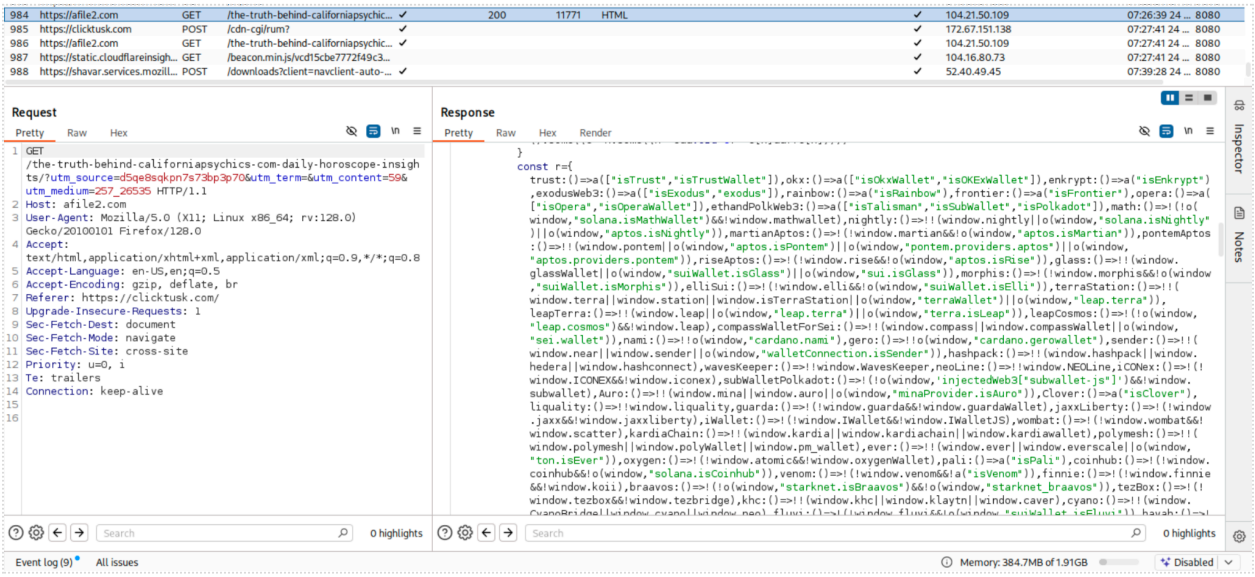
In the redirect chain,

1. The initial hops are made to **verifyev[.]com** and **ts551[.]com** which gather basic profile of the user containing the OS, Browser, location and network which is communicated with a subdomain of wi0z[.]com

2. A **v*[.]wi0z[.]com** subdomain then forwards the traffic along affiliate styled tracking domains such as **driptrip[.]trckswrm[.]com** and **clicktusk[.]com** which gathers further information of the browser and device like is javascript enabled, browser version, window dimensions etc.
3. From here the user is redirected to one of the more sophisticated user profiling webpages hosted on domains like **afile2[.]com** and **thefile-share-every-fun[.]com** which are deliberately designed to look like legitimate blog/file sharing sites. But in reality host javascript functions that perform very sophisticated fingerprinting and user profiling. The page also displays a strategic “Downloading file” prompt while the profiling code is being run in the background.

The user profile is done using the following techniques:

- Bot/Automation Detection
- Crypto Wallet detection: Detects over 50+ crypto wallets
- Canvas Fingerprinting: Generates SHA-256 hash of a complex rendered image on HTML canvas to fingerprint based on GPU/rendering differences
- Detects software renderers used by bots.
- Comprehensive Browser Profiling by detecting parameters like: Timezone offset, GPU renderer, Device pixel ratio, outer window width, inner window width, no touch support, CPU core count, device memory (GB), audio sample rate, Apple font availability, Chrome DevTools detection, canvas fingerprint hash, canvas offset detection, canvas prototype tampering, canvas extension interference, crypto wallets found



An example user profile JSON looks like this:

{"tz":480,"rndr":"llvmpipe, or similar","dpr":1,"ow":1920,"iw":1920,"ntch":true,"hc":4,"dm":0,"ar":48000,"af":true,"cfp":"288f50f2928d3f6cbd7d9a6faa87a1b8ea6342d35b21166d8e9ba53f1d65548a","co":false,"cduo":false,"cox":false,"ext_cw":["metaMask"],"pl":"Linux x86_64 "}

We can see that it detected the presence of a MetaMask wallet in the browser, which allows it to determine which user has crypto assets and can be redirected to:

1. Fake airdrops
2. Wallet connection phishing
3. Approval drainers
4. NFT mint scams
5. DeFi impersonation sites

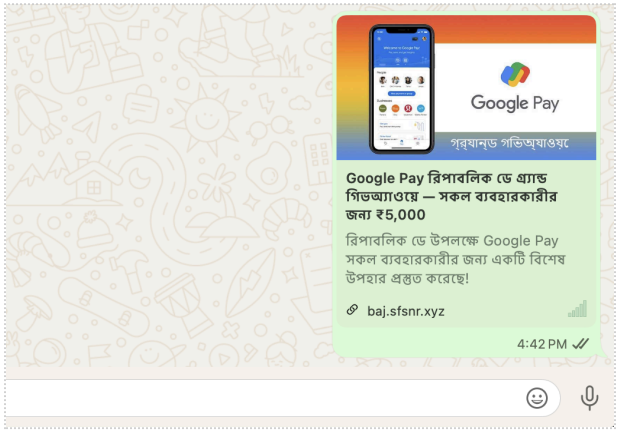
Delivery Mechanism

Analysis revealed hundreds of domains built on a repeatable delivery pattern, suggesting automated domain generation at scale. These short-lived domains, commonly registered under TLDs like .xyz, .cn, and .top, are used to deploy lure pages that serve as the first step in a broader redirection chain, one that ultimately feeds pre-qualified victims into scam and fraud ecosystems.

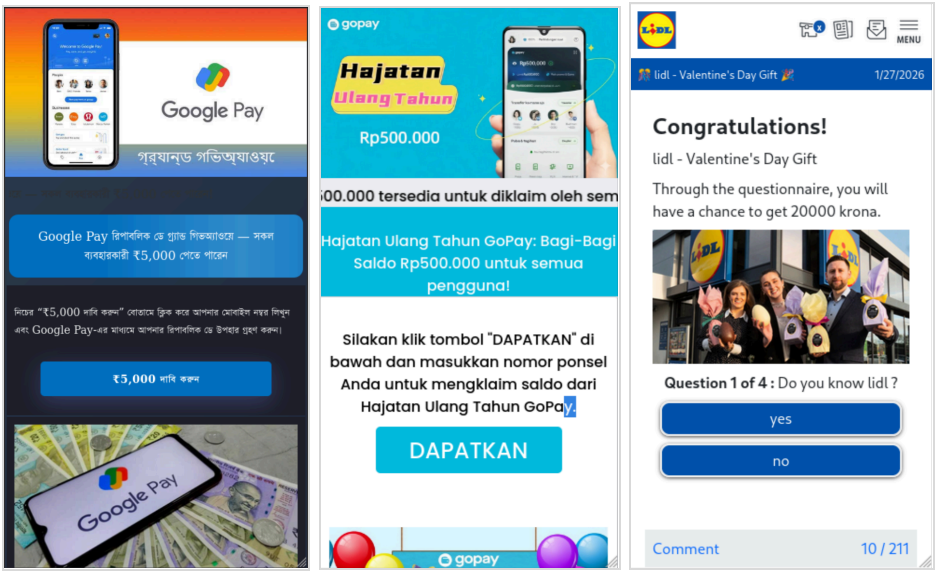
The main medium of delivery was most likely mobile-based messaging applications like WhatsApp, Facebook, Telegram, etc. Attributing to the fact that the files *j.php* and *goto.php* filtered mobile users and also all the lure pages were found to contain Open Graph Meta tags which are mainly used to render preview in these messaging applications.

At a high level, the phishing flow is intentionally simple and familiar.

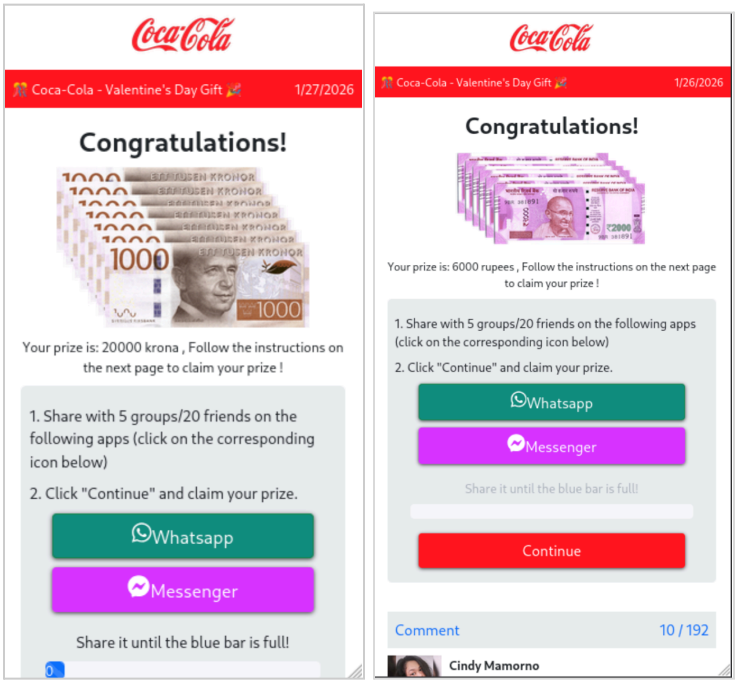
- Users encounter a discount, reward, or giveaway offer, often distributed via messaging platforms such as WhatsApp or Telegram.



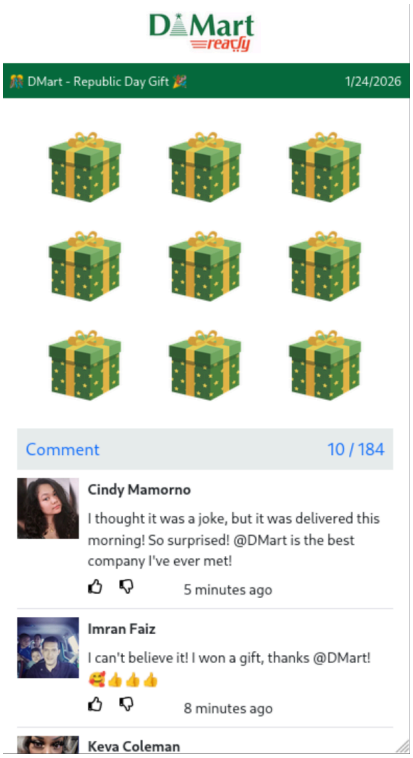
- The page references region-specific brands, for example, Airtel, SBI, and Google Pay in India; GoPay in Indonesia; and GCash in the Philippines to increase credibility.
- Users are then guided through a short questionnaire.



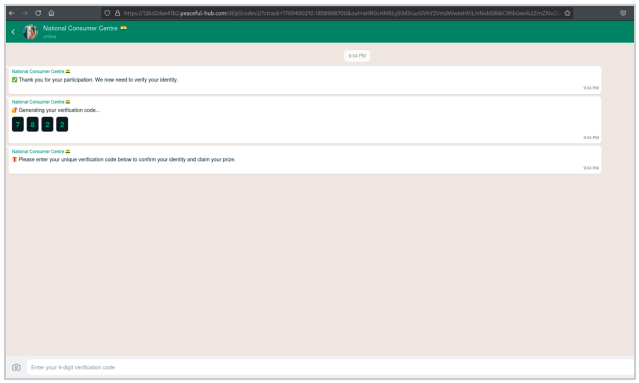
- Following the questionnaire, users are prompted to open “mystery boxes,” which reveal purported cash rewards. The displayed currency typically corresponds to the user’s geographic location.

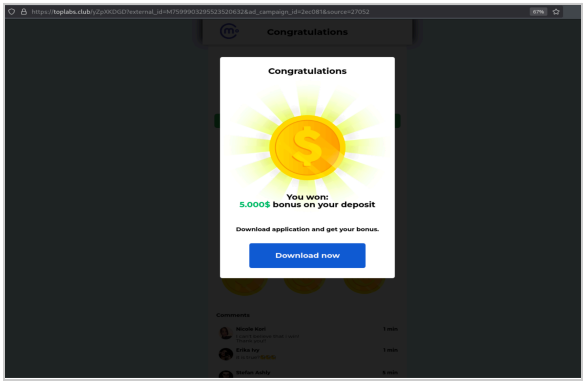


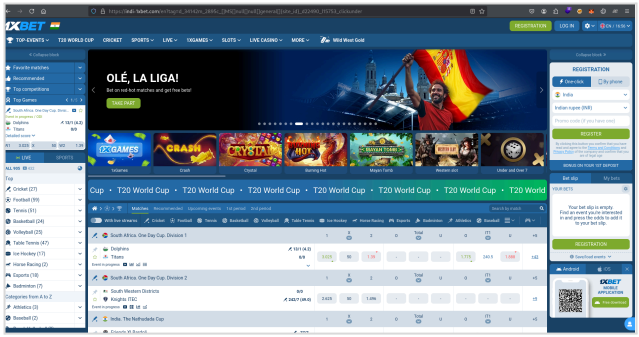
- Social proof, in the form of fabricated reviews and comments, is used to reinforce the illusion of legitimacy. Users are subsequently encouraged to share the link with others via WhatsApp or Messenger.



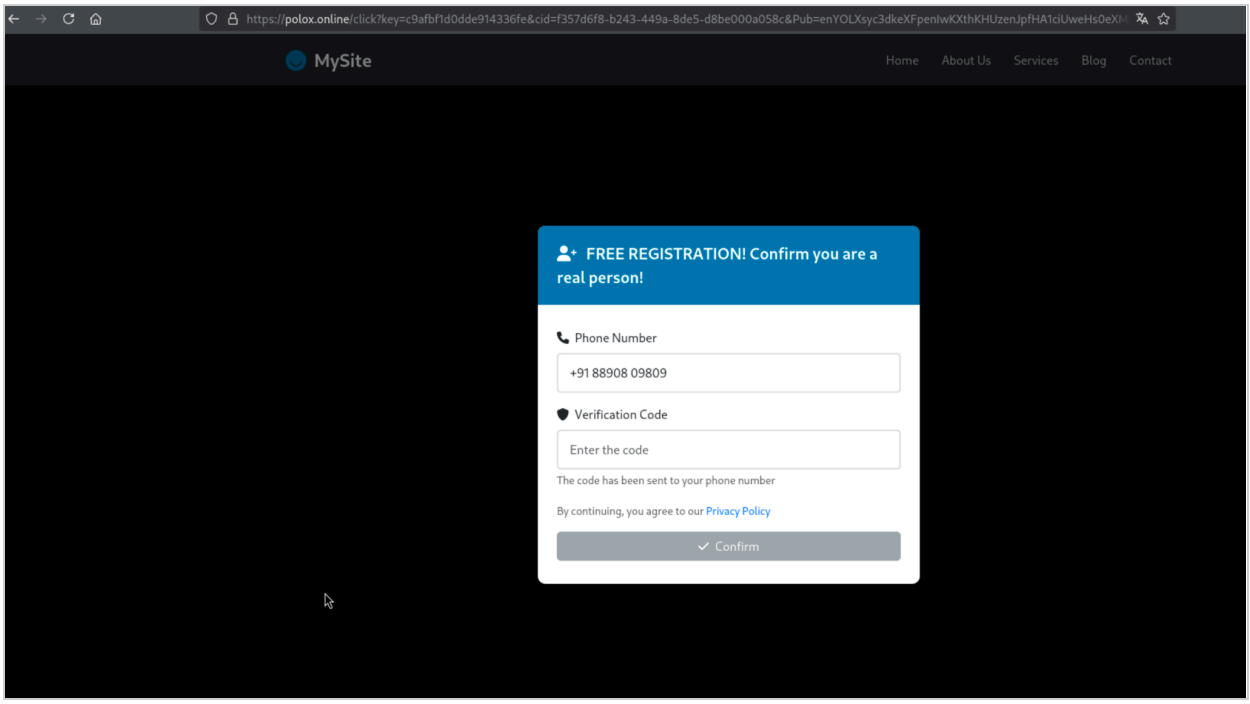
- After completing these steps, users are redirected to an external website, often associated with betting or other fraudulent activity, upon clicking the links presented.
- At no stage does the page overtly resemble traditional phishing interfaces, allowing it to evade immediate suspicion.







For instance, the site shown in the snapshot prompts users to enter their mobile number under the pretext of verifying that they are real individuals. After the number is entered, the website attempts to register new accounts or compromise existing accounts across platforms such as Telegram, Trylo, and Simply Cues. These compromised or newly created accounts are subsequently sold by threat actors on underground forums.



Uncovering the scam at scale - Pivoting methodology

To expand visibility beyond a single lure instance, our investigation pivoted away from individual domains and instead focused on repeatable infrastructure artifacts observed across multiple deployments.

Identifying a shared redirector pattern

Initial analysis revealed a common redirector file, **j.php**, consistently embedded across multiple suspicious domains. This script exhibited conditional behavior: when accessed from a mobile browser, it forwarded visitors to a brand-themed lure page, while desktop or non-mobile requests were served a benign 404.html response. This selective delivery strongly suggested environment-aware filtering, a tactic commonly used to evade automated scanners and casual inspection.

The earliest instance was observed on a domain registered under the .xyz TLD—an extension frequently abused for short-lived and disposable infrastructure. Based on this observation, we expanded our analysis to include additional low-cost TLDs commonly associated with similar activity patterns, including .icu, .top, .vip, .cn, and .cyou.

Using this hypothesis, we queried our internal database for URLs matching this redirector behavior and file structure. This initial pivot surfaced over 1,400 related URLs, indicating the activity was far broader than isolated lure pages.

Secondary pivots via shared assets

Inspecting individual results revealed additional common artifacts, including a shared favicon, which provided a second pivot point. Searching for this favicon hash across our dataset significantly expanded coverage, returning over 1,700 associated URLs.
Further inspection of these results identified another redirector file, goto.php, which was functionally identical to j.php. Pivoting on this filename uncovered additional infrastructure previously missed, confirming that the operators were rotating filenames while retaining identical logic.
Expanding the query to include both redirector variants dramatically increased the dataset. However, this broader search also introduced noise, as it captured unrelated sites using similar filenames.

Noise reduction and refinement

To isolate infrastructure belonging to the same operation, we refined our filtering to include domains that also served identical decoy responses, including 404.html and a structurally similar path (/emit/404/p). These files were consistently returned to non-targeted visitors and acted as a reliable fingerprint for the campaign.

Applying this refinement reduced the dataset to approximately 7,000 URLs, all exhibiting the same redirector logic, response behavior, and deployment patterns. Out of these more than 3500 URLs were found to be live at the time of writing this blog.

CDN-based expansion and lure discovery

Analysis of these URLs revealed another notable characteristic: nearly all instances loaded preview images and lure assets from a small set of self-hosted CDN domains, including:

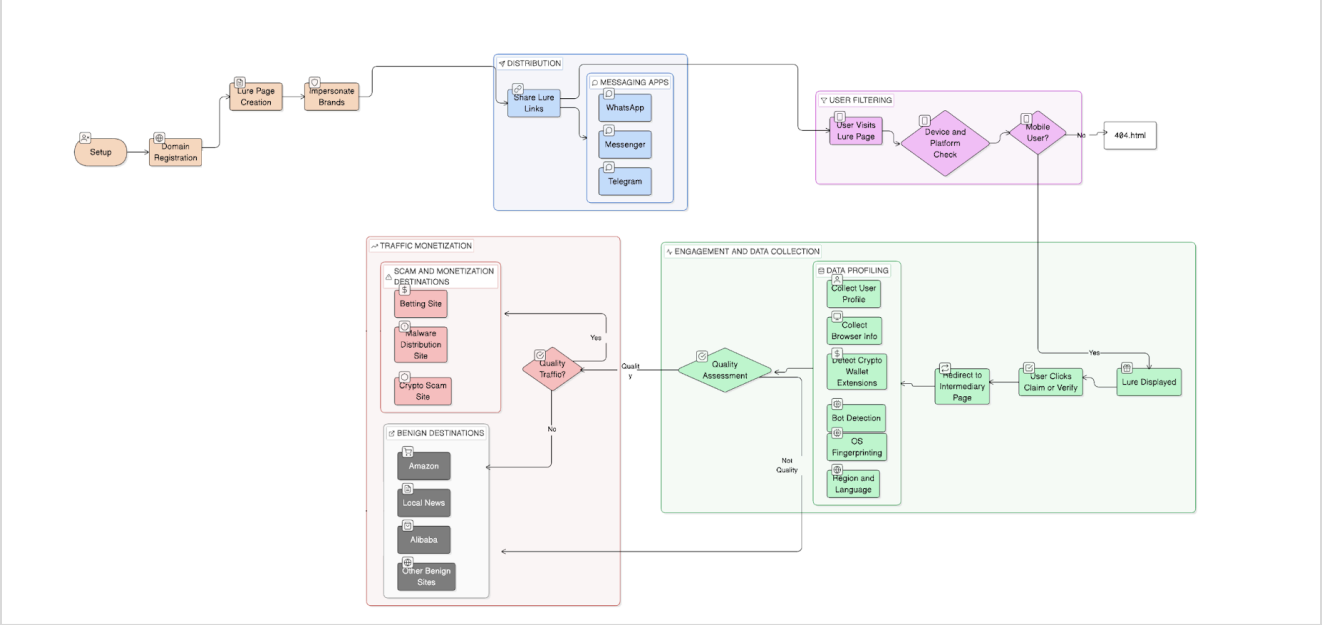
CDN DOMAINS
599cdn[.]com
cdnmi[.]com
cdnwix[.]com
img[.]cdn56[.]top
pic[.]cdn13[.]top

These CDN endpoints provided an additional pivot vector, allowing us to identify further domains that shared visual and structural components but did not initially match earlier redirector-based queries.
Following this pivot surfaced numerous brand-themed lure pages impersonating popular digital payment platforms and financial services.

Final pivot: lure template identification

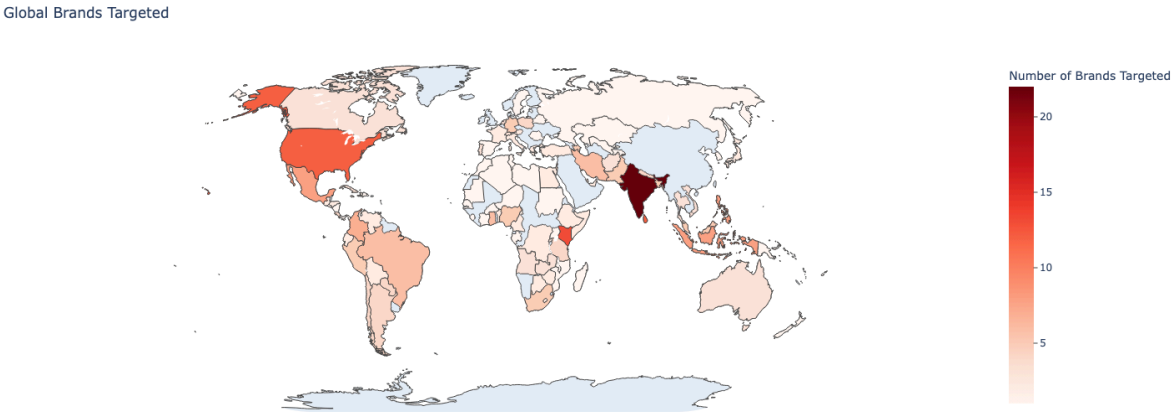
Inspecting these newly identified URLs led to the discovery of another recurring file, single.php, which served as the core lure template. Pivoting on this filename across the same TLD set revealed over 3,000 additional URLs, all validated to be using the same engagement-driven phishing template.
At this point, the infrastructure clearly demonstrated characteristics of a modular traffic brokerage platform, capable of rapidly deploying, rotating, and scaling brand-themed lures while maintaining consistent backend logic.

Campaign Kill Chain



Scale and Infrastructure used in the Campaign

1. More than **300 brands** targeted across over **100 countries**.



2. No of working **URLs** - **3718**

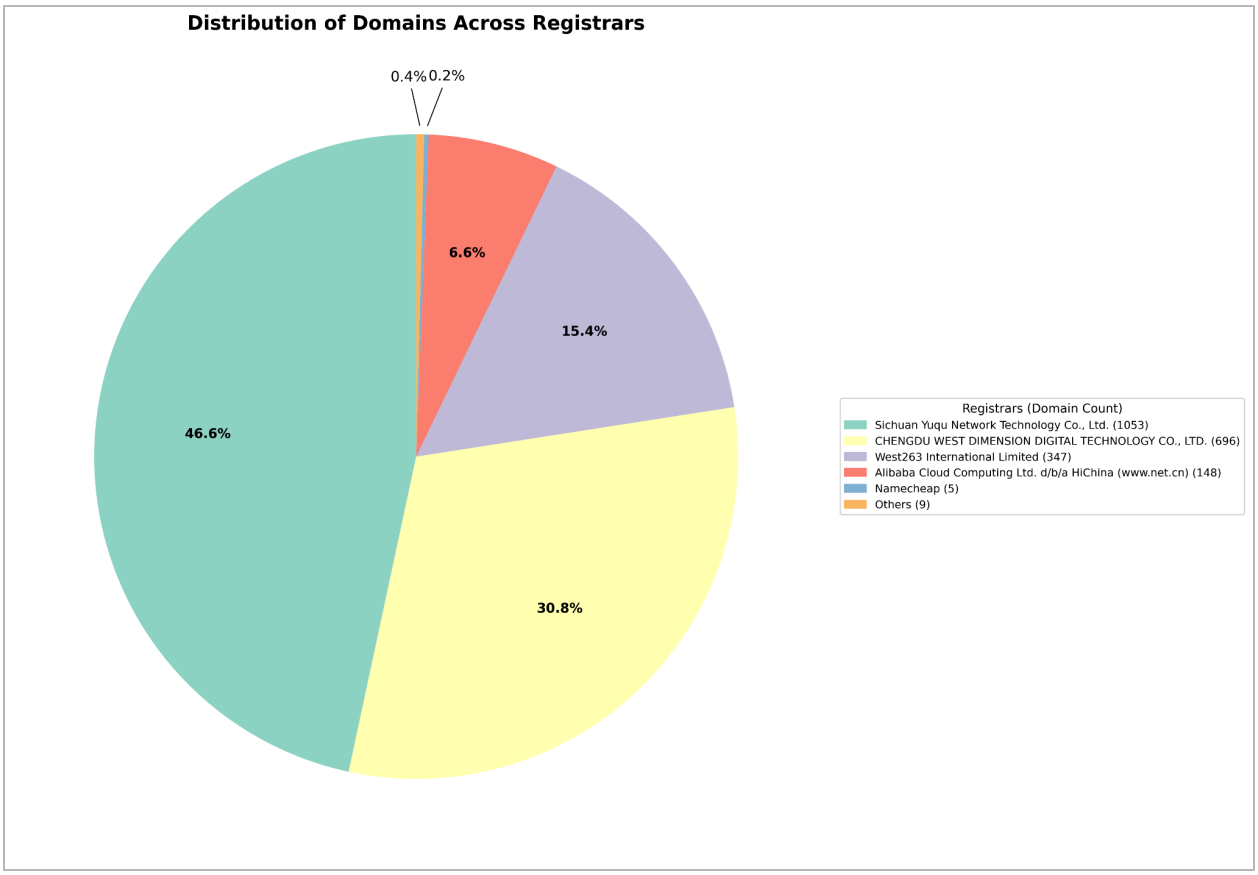
3. Unique **subdomains** identified - **2690**
   It should be noted that these are just primary lure URLs and the actual page was found to be hosted always on a different subdomain than the subdomain of the initial URL. Also the redirect chain contains at least one other domain with the same TLD and domain name format known to be associated with this campaign. So the actual scale of the campaign is even larger.

Domains being used as CDNs

CDN Domain	Registrar	Registrant	Registrated At	Updated At
599cdn[.]com	Cloud Yuqu LLC	Redacted	2025-07-04	2025-07-04
cdnmi[.]com	Porkbun LLC	Redacted	2023-04-11	2025-03-30
cdnwix[.]com	Porkbun LLC	Redacted	2025-12-09	2025-12-09
cdn56[.]top	Alibaba Cloud Computing Co., Ltd.	Redacted	2024-12-03	2024-12-03
cdn13[.]top	成都西维数码科技有限公司 (Chengdu Xiwei Digital Technology Co., Ltd.)	Redacted	2025-11-25	2025-11-25

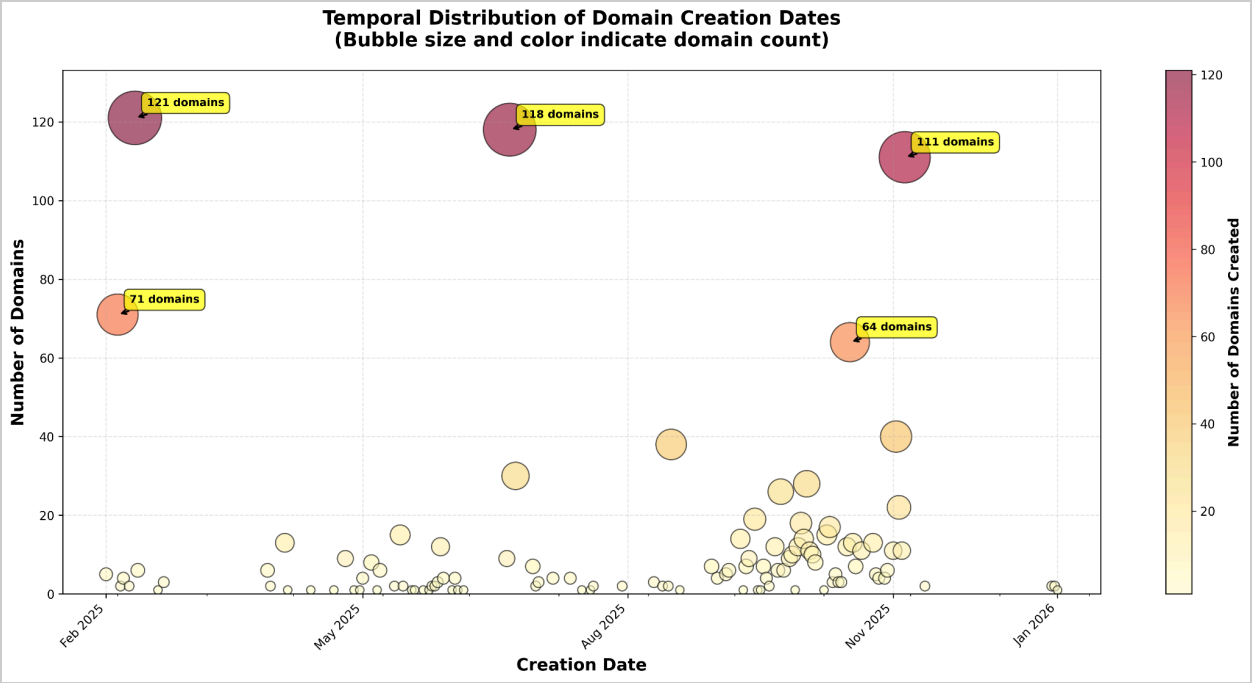
Plausible Analytics Domain

Domain	Registrar	Registrant	Registration Date	Updated Date
tj[.]16gift[.]com	Hefei Juming Network Technology Co., Ltd	Redacted	2023-12-30	2025-11-08

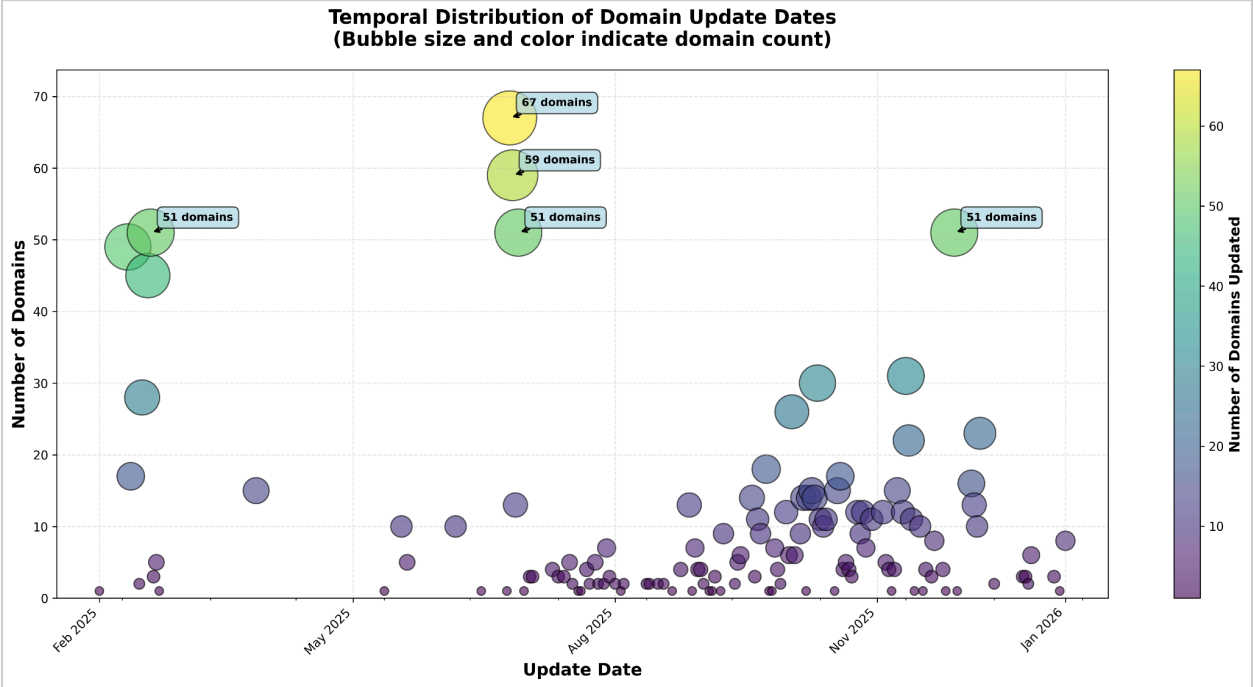


Distribution of phishing domains registered across registrars. Nearly all the domains were registered on China-based registrars.

distribution of phishing domains across TLDs (.top, .cn, .xyz), segmented by registrar.



Graph showing the timeline of creation dates for the phishing domains detected.



Graph shows the timeline of updations of the phishing domains which shows a clear pattern of increasing activity towards early 2026

Impact

Traffic broker–driven phishing ecosystems significantly amplify the scale and effectiveness of online scams. By splitting the process of getting traffic from the actual scam or malware, these brokers let different criminals use the same system with very little risk.

For end users, the result is increased exposure to financial fraud, identity theft, and malicious downloads—often under the guise of trusted brands and culturally relevant events. The progressive filtering and profiling of victims significantly increases the likelihood of conversion for those who reach the final stage, resulting in heightened financial losses.

For organizations, the damage is indirect but severe. Brand impersonation erodes customer trust, increases support and fraud response costs, and exposes businesses to regulatory scrutiny. Many brands remain unaware of the abuse until customer complaints or financial losses surface, as it occurs outside official infrastructure.

Recommendations

Disrupting traffic broker ecosystems requires intervention upstream, not just at the final scam page.

Organizations should prioritize:

- Early detection of fake domains and brand-abusing lures before mass distribution
- Correlation of shared redirectors, scripts, and infrastructure to identify broker-level activity
- Rapid takedown of malicious assets to reduce campaign lifespan
- Customer awareness campaigns during high-risk seasonal or regional events

Traditional phishing defenses alone are insufficient against engagement-driven scams that do not immediately request credentials. Proactive external monitoring is critical.

Why Digital Risk Protection Matters

Modern phishing and scam campaigns operate entirely outside an organization's network, abusing brand trust rather than exploiting technical vulnerabilities. This makes Digital Risk Protection (DRP) essential.

A DRP platform like CloudSEK XVigil enables organizations to:

- Detect brand impersonation, fake promotions, and scam domains in real time
- Track large-scale infrastructure patterns used by traffic brokers
- Identify emerging campaigns before they reach peak distribution
- Accelerate takedowns and reduce customer exposure

By providing visibility into the external threat landscape, Digital Risk Protection allows brands to shift from reactive response to proactive disruption—reducing fraud, protecting customers, and preserving trust.

References

- *Intelligence source and information reliability - Wikipedia

- #Traffic Light Protocol - Wikipedia

CloudSEK

We Predict Cyber Threats

Monitor. Analyse. Predict.

Secure your Tomorrow,Today!

Request for a Free Demo of our platform:

SCAN ME

OR

Mail us at **info@cloudsek.com**
or visit **https://cloudsek.com**

Gain access to a free trial and Detailed POC on CloudSEK Platform

Registered Office:

CloudSEK Research Pte Ltd.
51 Chin Swee Rd. #07-12 Manhattan House,
Singapore 169876

Regional Office: United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901
United States

Regional Office: India

CloudSEK Information Security Pvt Ltd
16/1, WINGS, Cambridge Rd, Halasuru,
Cambridge Layout, Jogupalya,
Bengaluru, Karnataka, India - 560008

Regional Office: United Kingdom

CloudSEK, 4th floor, Rex House,
4, 12 Regent Street, London,
SW1Y 4PE - United Kingdom