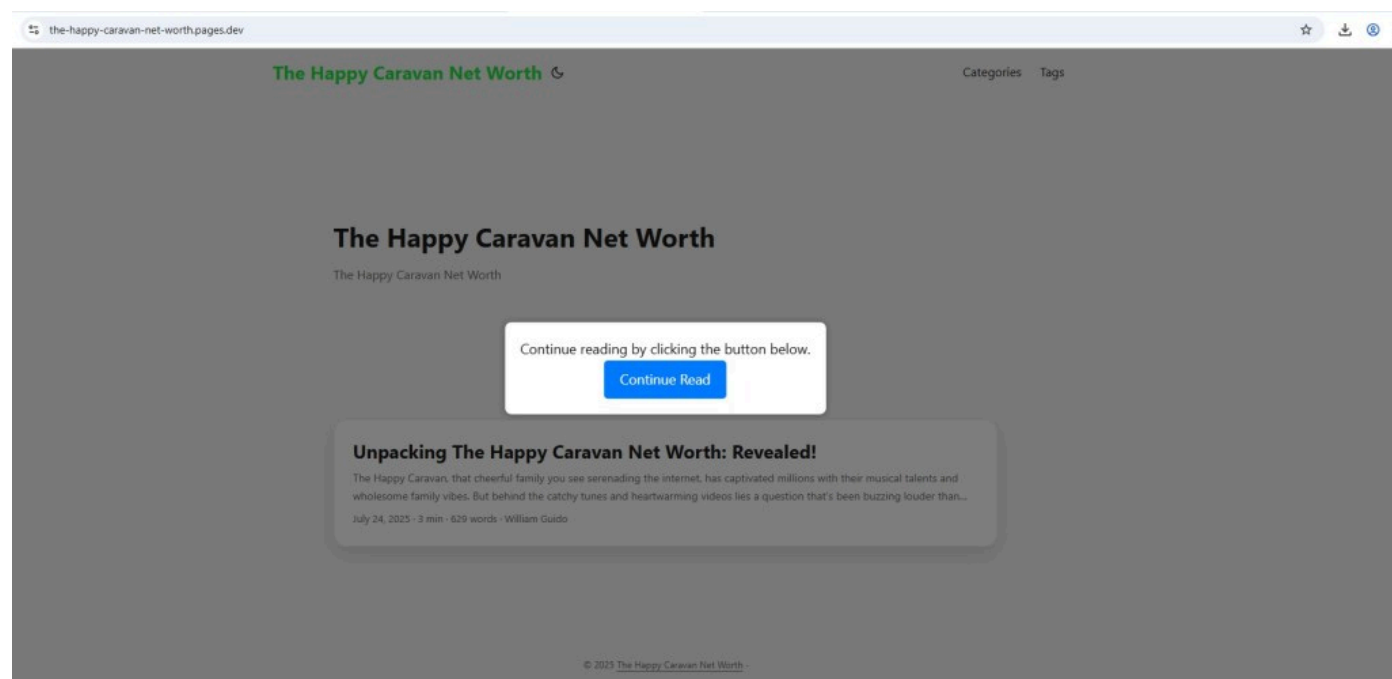


Cloudflare Pages “Continue Read” Redirect Kit Abused for Phishing, Adware, and Malware Delivery – Malware Analysis, Phishing, and Email Scams

malwr-analysis.com/2026/02/15/cloudflare-pages-continue-read-redirect-kit-abused-for-phishing-adware-and-malware-delivery

Anurag Gawande

February 15, 2026



I identified a long-running redirect infrastructure abusing Cloudflare Pages (pages.dev) to host benign-looking SEO articles (for example, celebrity “net worth” blogs or gaming help content) that display a forced **“Continue reading / Continue Read”** pop-up shortly after page load.

Once the user clicks the button, the browser is redirected into downstream infrastructure that may lead to:

- Credential-harvesting phishing pages
- Adware / PUP installers
- Trojan or malware droppers
- Fake browser download lures (observed: Opera-themed “diagnostics” funnel)
- QR-code / fake CAPTCHA social-engineering pages

More than 250 URLs were observed using the same visual template and behavior, and historical evidence from [URLScan](#) shows activity persisting for 5 months, suggesting deliberate reputation building and SEO indexing.

Initial Infection Vector: Benign SEO Content on Cloudflare Pages

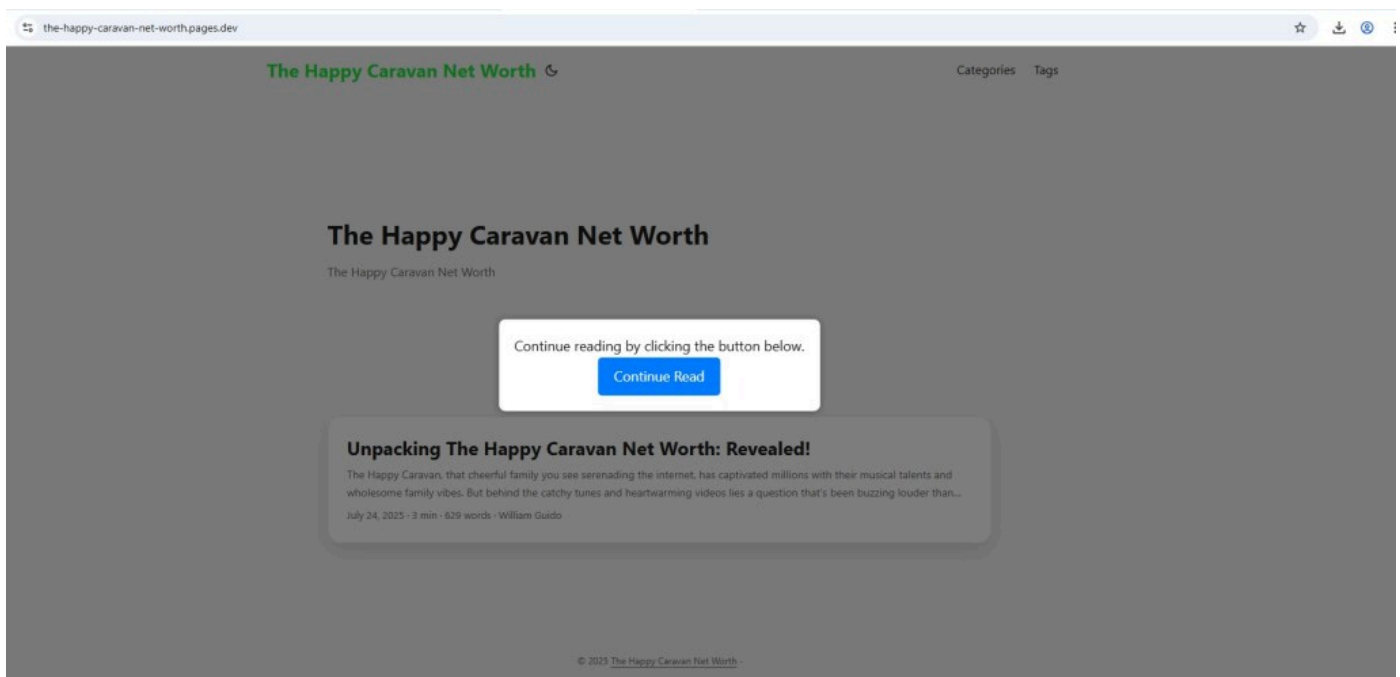
The landing pages appear as normal blog articles but automatically display a modal message:

“Continue reading by clicking the button below.”

This design ensures the redirect is user-initiated, helping bypass automated scanners and reputation systems.

Common characteristics

- Hosted on: *.pages.dev
- SEO-style article content
- Modal overlay appears a few seconds after page load
- Redirect only occurs after button click



Scale, Persistence, and Search Engine Exposure

Across the analyzed samples, more than 250 distinct URLs were identified showing identical UI and UX behavior, indicating the use of the same phishing template or kit deployed across different article topics. The activity has remained visible for approximately five months based on [URLScan](#) observations, suggesting persistence rather than short-lived campaigns. Additionally, some of these pages have been indexed in Google search results, significantly increasing the likelihood of exposure to real users and amplifying the overall risk posed by the operation.



Cloudflare

<https://the-happy-caravan-net-worth.pages.dev>

The Happy Caravan Net Worth

The Happy Caravan, that cheerful family you see serenading the internet, has captivated millions with their musical talents and wholesome family vibes. [Read more](#)



Cloudflare

<https://the-happy-caravan-net-worth.pages.dev> › tags

Tags

The Happy Caravan Net Worth.



Cloudflare

<https://the-happy-caravan-net-worth.pages.dev> › categories

Categories

The Happy Caravan Net Worth.



Cloudflare

<https://harbor-freight-fargo.pages.dev>

Harbor-Freight-Fargo

In Fargo, North Dakota, one name often comes to mind for a wide array of tools and equipment at competitive prices: Harbor Freight. More than just a store, the ... [Read more](#)



Cloudflare

<https://harbor-freight-fargo.pages.dev> › posts › harbor-fr...

Harbor Freight Fargo Reviews & Shopping Tips for Smart Local ...

Fargo-First Tools: Prioritize items like PREDATOR generators, VIKING battery maintainers, and heavy-duty tarps – essential gear for Fargo's extreme weather.

Redirect Logic (Click-Gated Pre-Lander Behavior)

The redirect mechanism is implemented using delayed modal display and a click-triggered JavaScript redirect.

Key Observation

Across many different pages, most samples use the same redirect destination inside `window.open()`

```

<script>
  setTimeout(function() {
    document.getElementById("popup-container").style.display = "block"
  }, 3e3);

  function continueReading() {
    window.open("https://preservationwristwilling.com/utx3iw6i?key=0e17c9d3ecd4124fb8f180f439fd2bfb", "_blank"), document.getElementById(
      "popup-container").style.display = "none"
    }
  }
</script>

```

This is important because it shows that the pages.dev sites are probably not standalone phishing pages created one by one. Instead, they appear to work more like traffic pre-landers that quietly direct visitors to a shared backend system. The **key=** parameter in the URL also looks intentional rather than random, and it is likely being used for tracking or routing within the campaign, possibly as a campaign ID, an affiliate tracking token, or even a value used to classify or group potential victims.

In short:

Multiple benign-looking SEO pages are acting as entry points into a centralized redirect infrastructure.

Central Redirector Role in the Infection Chain

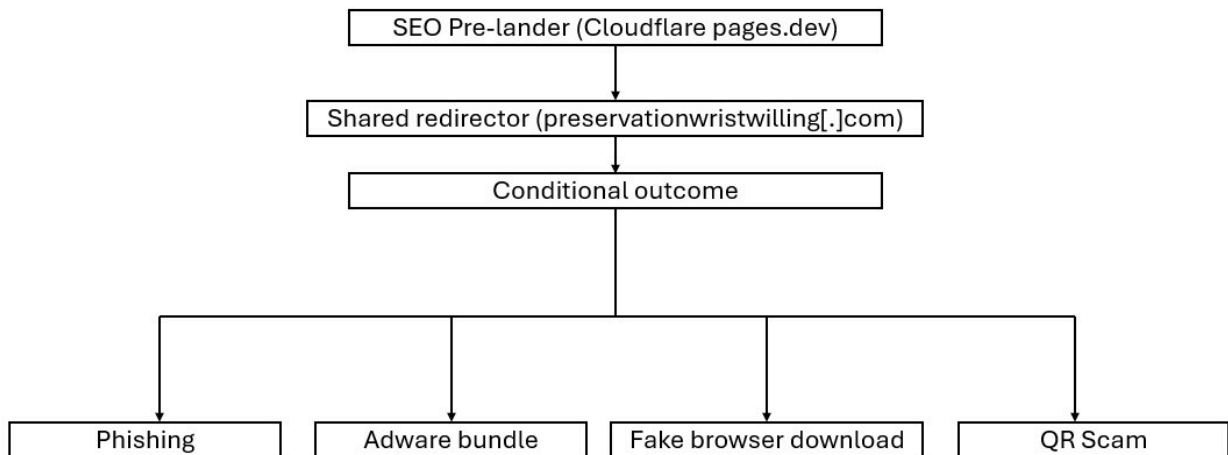
The shared redirect endpoint:

1 [https://preservationwristwilling\[.\]com/utx3iw6i?key=<token>](https://preservationwristwilling[.]com/utx3iw6i?key=<token>)

likely serves as a Traffic Distribution System (TDS) decision node, responsible for:

- Geo/IP filtering
- Proxy/VPN detection
- User-agent validation
- Campaign routing
- Conditional payload delivery

Simplified Kill Chain



Anti-Analysis Behavior: Proxy / VPN Detection

During testing, downstream pages performed VPN/Proxy checks.

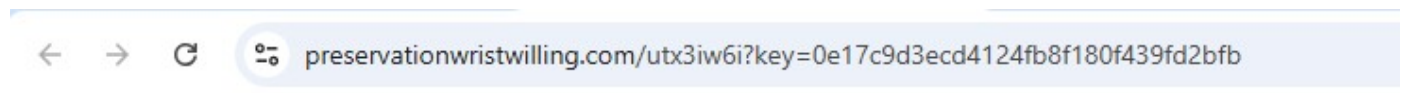
If anonymity was detected, the page displayed:

| “Anonymous Proxy detected.”

and stopped further redirection.

Security Impact

From a security perspective, this behavior is particularly concerning because it makes deeper analysis much harder. By blocking or redirecting automated environments, it can prevent sandboxes and researchers from ever reaching the real payload, which in turn leads to very low antivirus detection rates. As a result, automated scans may incorrectly appear clean, creating a false sense of safety even though malicious activity may still be present behind the scenes.



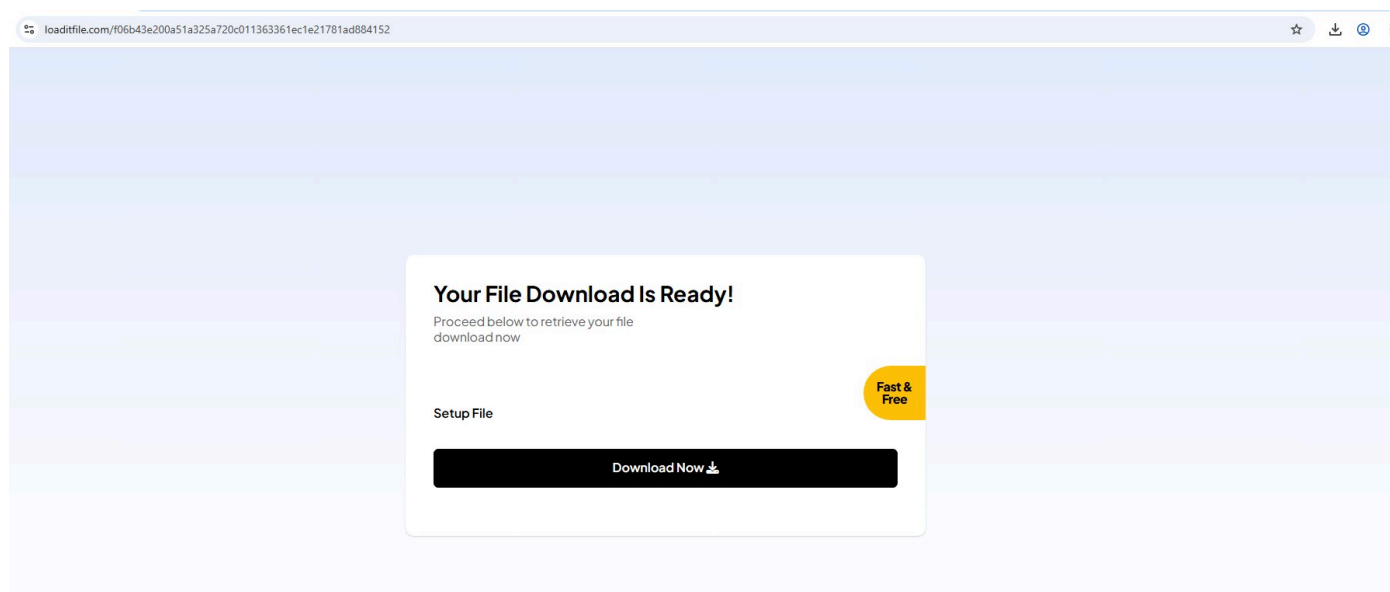
Anonymous Proxy detected.

Observed Downstream Outcomes

1) Fake File Download Funnel – S3 ZIP Payload

One redirect path showed a “**Your File Download Is Ready**” page, leading to:

- Intermediate download host (e.g., loaditfile[.]com)
- Final payload stored on Amazon S3 (SetupFile-xxxx.zip)

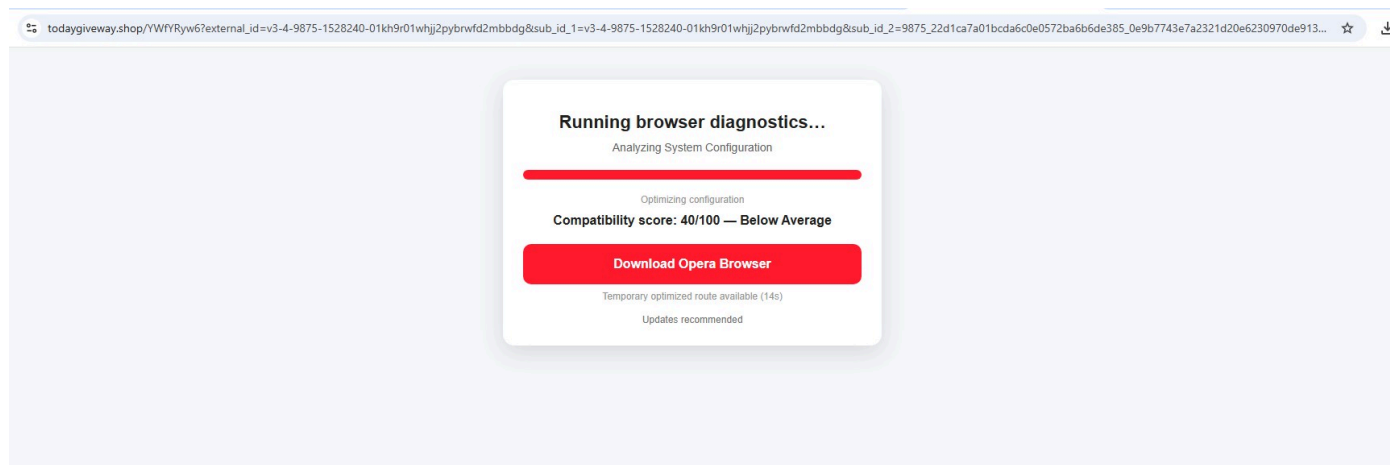


2) Fake Browser Diagnostics – Opera Download Lure

Another branch displayed a fake compatibility/diagnostics score (e.g., 40/100) urging users to:

“Download Opera Browser”

This pattern feels very similar to the affiliate-driven browser installation funnels often seen in malvertising campaigns, where traffic is quietly redirected through multiple steps before reaching the final payload or monetization stage.

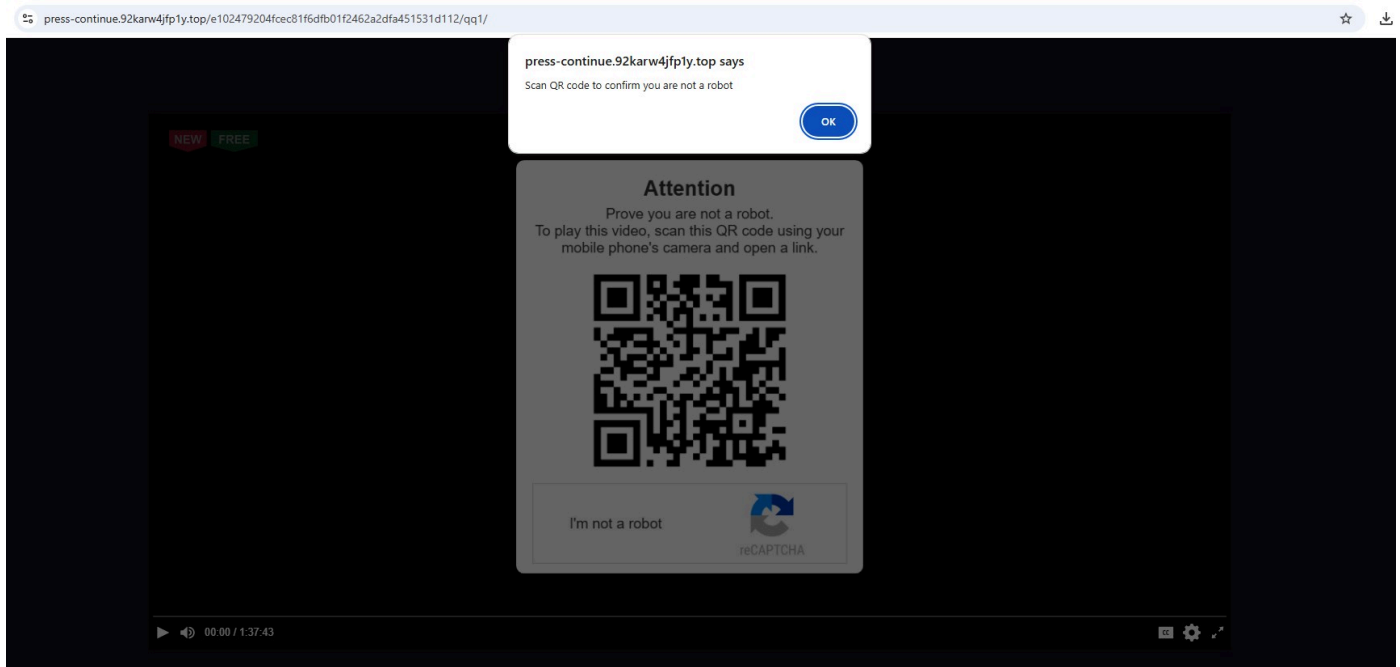


3) QR Code / Fake CAPTCHA Social Engineering

Some redirects presented:

- “Prove you are not a robot”
- QR code requiring mobile scan

Flows like this are commonly designed to move victims step by step toward the attacker’s real objective. In many cases, the final destination can be a phishing page that steals credentials, a subscription fraud scheme that silently charges the user, or even the delivery of mobile malware disguised as a legitimate download.



Payload Example and Low Detection Context

One observed executable sample (adware/PUP classification):

SHA256: be590100ecdcae5ce4b7b42f87082e201fcb2f38c114c8fbc6640ad9b9a0708a

VirusTotal showed detection

6 / 71
Community Score -1

6/71 security vendors flagged this file as malicious

Reanalyze Similar More

be590100ecdcae5ce4b7b42f87082e201fcb2f38c114c8fbc6640ad9b9a0708a
ApplInstallSoft_295461.exe
Size: 43.49 MB | Last Analysis Date: a moment ago | EXE

peexe overlay checks-user-input

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: adware.specialsearchoffer | Threat categories: adware | Family labels: specialsearchoffer

What makes this particularly notable is that the overall setup closely matches how modern malvertising Traffic Distribution Systems (TDS) typically operate. The infrastructure shows several familiar patterns, such as abusing a trusted hosting platform like Cloudflare Pages, allowing pages to be indexed by search engines to attract organic traffic, and using click-gated redirects to evade automated analysis. Behind the scenes, everything appears to funnel through a centralized redirect endpoint where the final payload can be delivered conditionally, depending on the visitor. This kind of design also supports multiple monetization paths rather than a single outcome. Taken together, it suggests we are not looking at just one phishing kit, but a broader shared redirect ecosystem designed to distribute traffic at scale.

Indicators of Compromise (IOCs)

Domain

- preservationwristwilling[.]com
- Path: /utx3iw6i
- Query Parameter: key=<token>
- loaditfile[.]com

Malicious Sample

- be590100ecdcae5ce4b7b42f87082e201fcb2f38c114c8fbc6640ad9b9a0708a
- Windows Executable
- Classification: Adware/PUP
- [VirusTotal Detection](#)

Network Indicator

| preservationwristwilling[.]com/utx3iw6i?key=

[URLScan.io search result](#)

This campaign highlights how attackers carefully blend several techniques to stay under the radar and keep their operation running for long periods. By abusing legitimate hosting services, leveraging SEO poisoning to attract real users, using click-triggered redirects to avoid automated detection, and routing visitors through a centralized traffic system, they create a stealthy and resilient infrastructure capable of quietly delivering malware or other malicious outcomes over time