

Fake “Fast Ray VPN” Site on Cloudflare Pages Leading to PUA Downloads – Malware Analysis, Phishing, and Email Scams

While reviewing historical scans on URLScan, I came across a VPN-themed website hosted on Cloudflare Pages

```
1 hxxps://fast-ray-vpn.pages.dev/
```

At first glance, the site looks like a harmless VPN review blog. It features clean formatting, long-form written content, fake ratings, and well-structured download sections. Nothing immediately stands out as malicious, which is likely why the site has remained accessible for months.

What makes this case notable is that [URLScan](#) shows this **domain has been publicly reachable for at least eight months**, with multiple scans recorded over time. This is not a short lived phishing page or a throwaway redirect, it appears to be stable infrastructure.

 URL	Age	
 fast-ray-vpn.pages.dev/	Public	1 hour
 fast-ray-vpn.pages.dev/	Public	21 hours
 fast-ray-vpn.pages.dev/	Public	3 months
 fast-ray-vpn.pages.dev/	Public	8 months

A Convincing VPN Review That Builds False Trust

The landing page presents itself as a review article titled “**Fast Ray VPN Review: Secure & Fast Mobile VPN?**”. It includes a star rating of 4.8, all designed to look credible.

Fast Ray VPN Review: Secure & Fast Mobile VPN?

May 7, 2025 · 4 min · 691 words · Jessica Cardenas

▼ Table of Contents



Fast Ray VPN vs. RayVPN: A Comparative Review

The world of VPNs is a crowded marketplace, filled with promises of speed and security. This review compares Fast Ray VPN, a free service, with RayVPN, a paid alternative, to help you navigate this landscape. We'll examine their features, focusing

Choosing a Secure Paid Mobile VPN: Key Considerations

Navigating the VPN market can feel overwhelming. This section clarifies how to choose a truly secure, paid VPN with transparent logging policies.

Key Takeaways:

- Independent audits provide critical verification of a VPN provider's security claims.
- Transparency is paramount: A reputable VPN will clearly explain its data handling practices.
- Jurisdiction is important: A VPN provider's location impacts its legal obligations.
- Advanced features, such as RAM-only servers and kill switches, enhance security.

File Name: Fast Ray VPN Review: Secure & Fast Mobile VPN?

★★★★☆ (4.8)

[Download via Link 1](#)

[Download via Link 2](#)

Last updated: Friday, May 09, 2025

Download Links That Don't Deliver a VPN

Near the bottom of the page, two links are presented as:

“Download via Link 1”

“Download via Link 2”

Clicking either of these does not lead to an app store, an official vendor site, or even a branded installer page. Instead, users are redirected to a third-party domain:

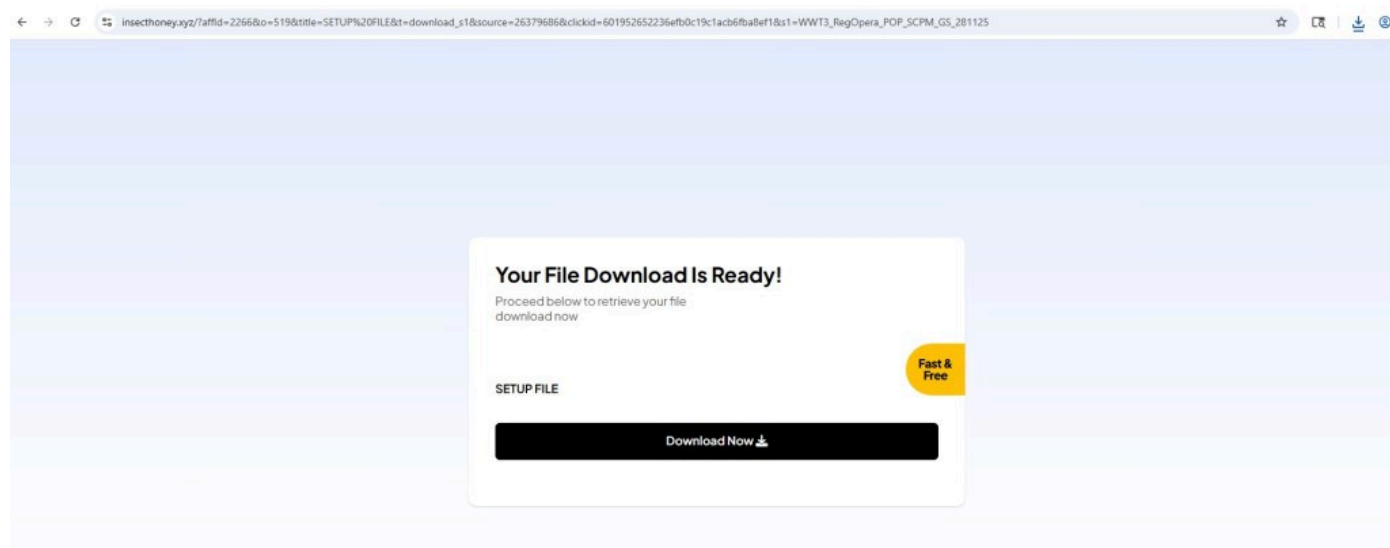
1 [hxxps://normallydemandedalter\[.\]com](https://normallydemandedalter[.]com)

The URLs include long query strings with tracking keys, strongly suggesting affiliate or traffic broker infrastructure rather than software hosting.

In many cases, the redirect lands on a generic page stating

“Your File Download Is Ready!”

There is no mention of a VPN, no vendor name, no file hash, and no explanation of what is about to be downloaded.



As shown in the above screenshot, one such redirect path leads to **insecthoney[.]xyz**, where clicking the download button results in [OperaSetup.exe](#) being delivered. While Opera itself is legitimate software, the context is deceptive. Users are led to believe they are downloading a VPN client, but instead receive an unrelated browser installer distributed.

This OperaSetup.exe is getting delivered through below domains:

- **insecthoney[.]xyz**
- **valueeye[.]xyz**

Pixelsee PUA Delivered Through One Redirect Path

During sandbox testing, both redirect paths associated with the two download links were observed delivering a **PUA payload**, including the Pixelsee sample previously referenced. However, the behavior was not consistent. The same URLs did not always result in a file download and, in

several cases, redirected to unrelated advertising or affiliate destinations instead. This indicates that payload delivery is randomized or condition-based, likely controlled by backend traffic distribution logic rather than being tied to a single fixed URL.

```
1 1. hxxps://normallydemandedalter.com/y4gw4zmhi3?  
2 key=14baee5d6a64addb406346147543b508  
3 2. hxxps://normallydemandedalter.com/bhb7puzj?  
   key=13033e82c537ba388cf82fed63dcfc88
```

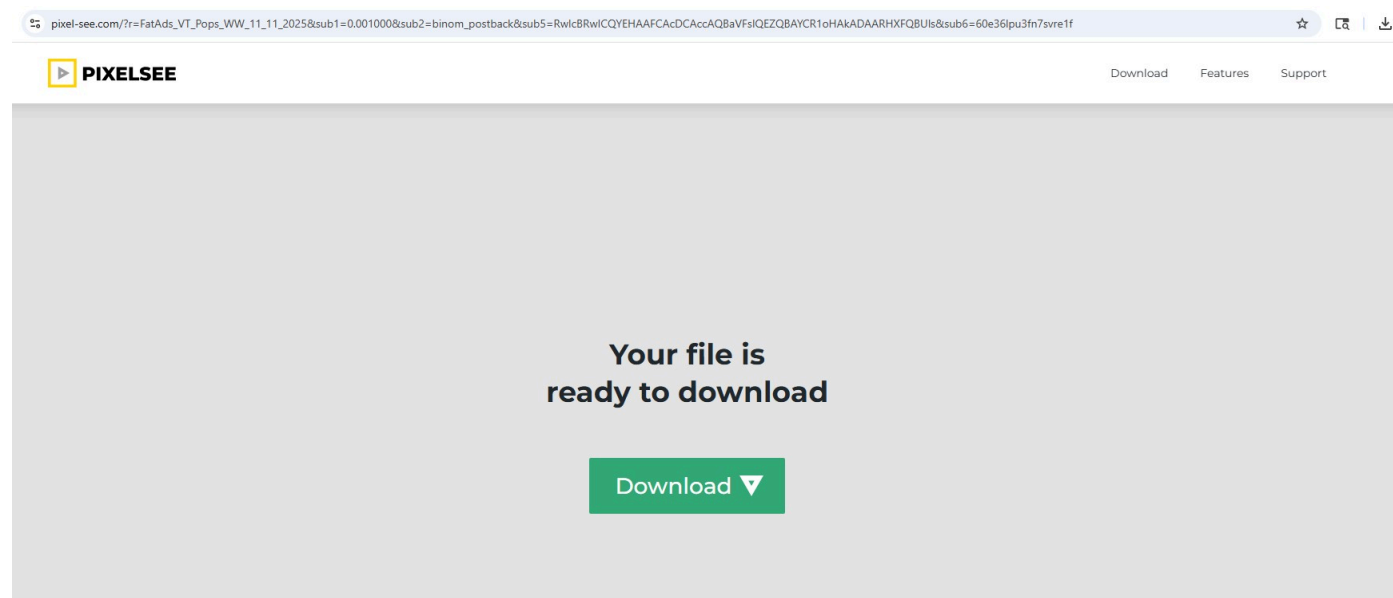
That file is already flagged on [VirusTotal](#) and detected as **Pixelsee PUA**. The **Pixelsee** site itself again presents a clean, minimal download page with a prominent “Download” button and almost no transparency about the software’s purpose.

File Hash: 3856355ad00016cf21e0492fc5db2fd6

File Name: PixelSee_id1604692id.exe

File Size: 4.35MB

File Type: PE32



31

/ 70

Community Score

31/70 security vendors flagged this file as malicious

Reanalyze

Similar

More

17d9094e06d2edcaeb07b72263ee2f12009f98e079daf3e3ca48df5fc5b04586

Size

4.36 MB

pixelsee

Last Analysis Date

7 hours ago

peexe

overlay

signed

EXE

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 3

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

Popular threat label

trojan.luminati/vnvis

Threat categories

trojan

adware

pua

Family labels

luminati

vnvis

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	PUP/Win.Bundler.C5800595	AliCloud	ProxyTool:Win/Luminati.gyf
Avast	Win32:PUP-gen [PUP]	AVG	Win32:PUP-gen [PUP]

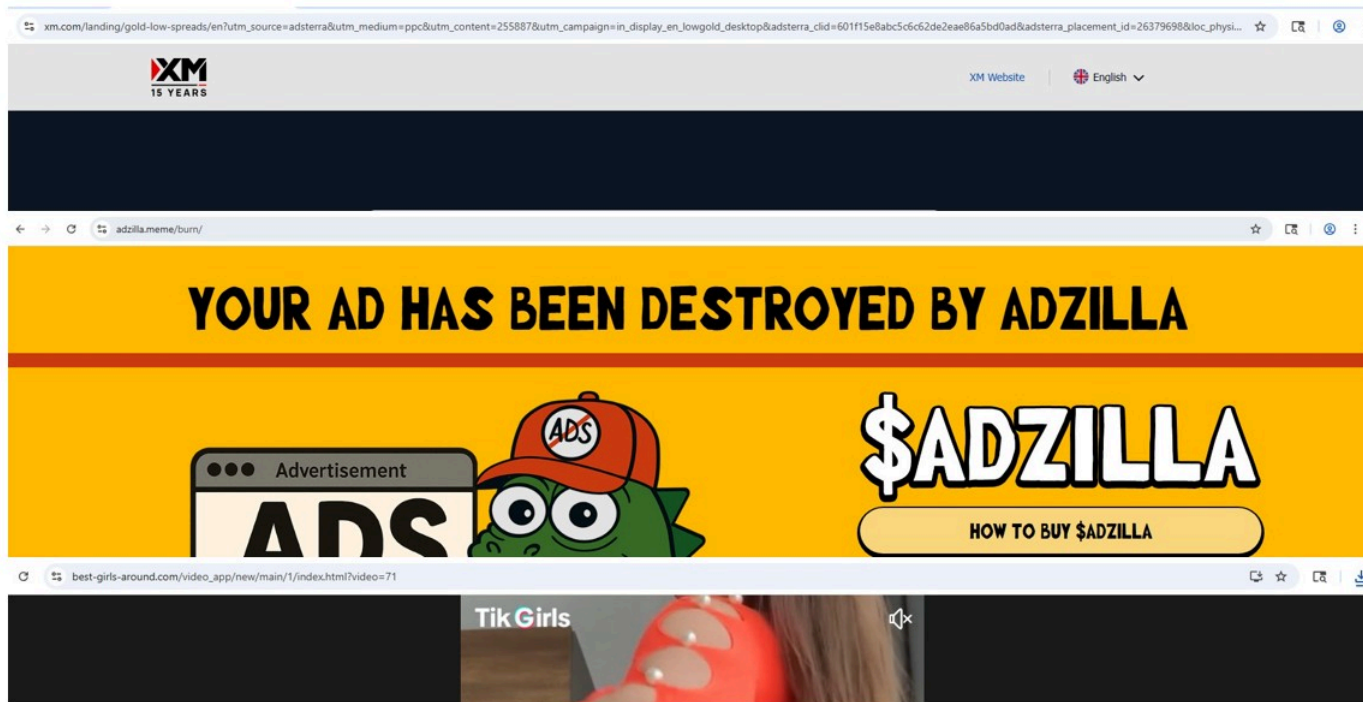
Inconsistent Outcomes and Traffic Monetization

Revisiting the same download URLs does not consistently result in the same behavior.

In multiple attempts, instead of receiving a file, the browser was redirected to completely unrelated destinations, including:

- TikTok video pages
- XM trading platform landing pages
- Ad-related sites such as adzilla/.meme
- Adult-themed click-through domains like best-girls-around/.com

This inconsistency strongly indicates the use of a traffic distribution system (TDS). Depending on conditions such as IP reputation.



VPN and Sandbox Detection Blocking Visibility

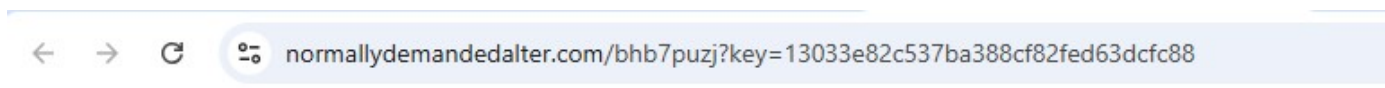
When accessing normallydemandedalter[.]com through a VPN or sandbox environment, the site responds with a simple message

“Anonymous Proxy detected.”

Once this message appears, no further redirects or downloads occur. This behavior effectively blocks

- VPN users
- Cloud-based sandboxes
- Automated analysis systems

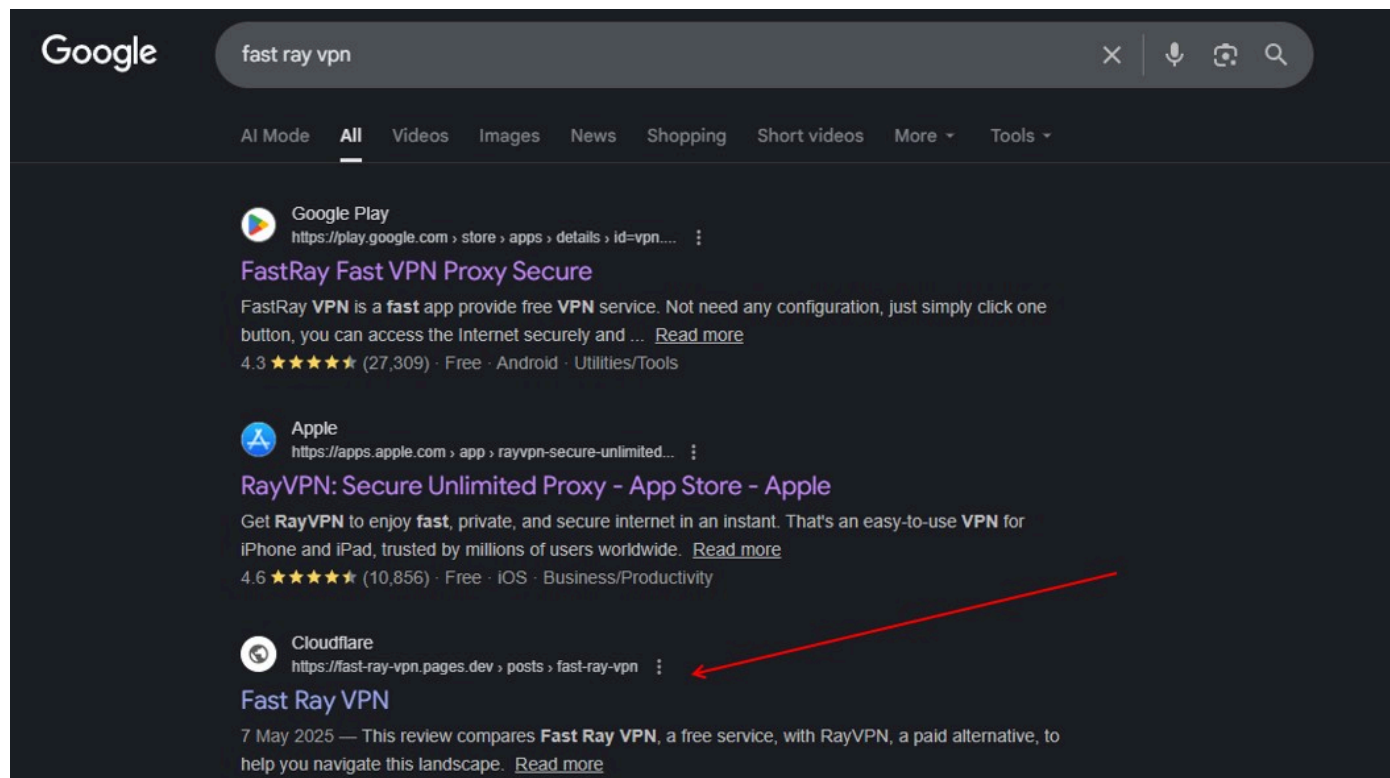
This explains why the site can remain live for months while still evading deeper inspection. The actual payload delivery only happens when the visitor appears to be a **“real”** user.



Anonymous Proxy detected.

Visibility in Google Search Results

An additional point worth highlighting is that the Fast Ray VPN site is not buried or obscure. A simple Google search for “**fast ray vpn**” currently surfaces the Cloudflare Pages site within the top search results, appearing alongside legitimate Google Play and Apple App Store listings. This positioning significantly increases the likelihood of real users landing on the page organically, especially those searching for a VPN by name and expecting an official or review-based result. Combined with the site's long uptime and clean presentation, this search visibility further amplifies its effectiveness as a traffic funnel.



Indicators of Compromise (IOCs)

The following indicators were observed during hands-on analysis and sandbox testing. They are linked to a deceptive VPN-themed page that redirects users through third-party infrastructure and, in some cases, delivers potentially unwanted applications. The redirects do not behave consistently. Sometimes a file is downloaded, other times users are sent to unrelated advertising or affiliate pages. This kind of behavior suggests traffic is being routed and monetized dynamically rather than through a single, fixed download path.

Domains

- fast-ray-vpn.pages.dev
- normallydemandedalter.com
- insecthoney.xyz
- valueeye.xyz
- pixel-see.com

- adzilla.meme
- best-girls-around.com
- xm.com

URL's

- hxxps://fast-ray-vpn.pages.dev/
- hxxps://normallydemandedalter[.]com/y4gw4zmhi3?key=14baee5d6a64addb406346147543b508
- hxxps://normallydemandedalter[.]com/bhb7puzj?key=13033e82c537ba388cf82fed63dcfc88
- hxxps://insecthoney.xyz/?affld=2266&o=519&title...
- hxxps://valueeye[.]xyz/?affld=2266&o=473&title=SETUPFILE&t=download_s1.....

File Hashes (PUA)

MD5: 3856355ad00016cf21e0492fc5db2fd6

The **Fast Ray VPN** site is not a legitimate VPN service and not a genuine review platform. It functions as a persistent traffic lure, redirecting users into affiliate and PUA distribution chains while actively blocking VPNs and sandboxes.

Its long lifespan suggests an effective design that prioritizes persistence and user reach while avoiding signals that typically lead to rapid takedown.