

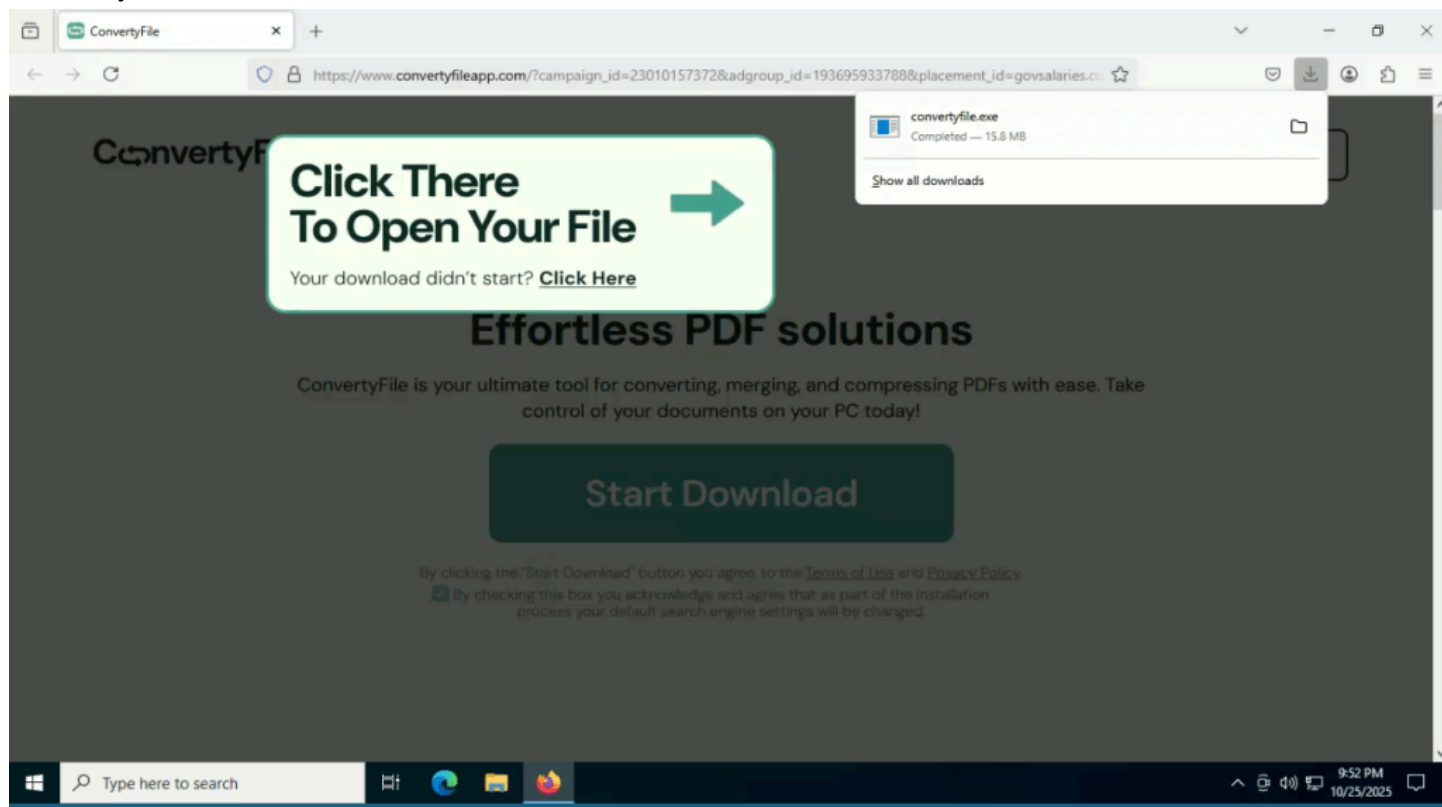
# ConvertyFile Browser Hijacker

: 10/28/2025

## Malware Research



By Aaron Samala October 29, 2025



## TL;DR

ConvertyFile is a browser hijacker, delivered via ads, that changes the browser's default search engine.

## Tactical Pause

THE CONTENT, VIEWS, AND OPINIONS EXPRESSED ON THIS DOCUMENT ARE MY OWN AND DO NOT REFLECT THOSE OF MY EMPLOYER OR ANY AFFILIATED ORGANIZATIONS. ALL RESEARCH, ANALYSIS, AND WRITING ARE CONDUCTED ON MY PERSONAL TIME AND USING MY OWN PERSONALLY-ACQUIRED RESOURCES. ANY REFERENCES, TOOLS, OR SOFTWARE MENTIONED HERE ARE LIKEWISE USED INDEPENDENTLY AND ARE NOT ASSOCIATED WITH, ENDORSED, OR FUNDED BY MY EMPLOYER.

# Summary Up Front

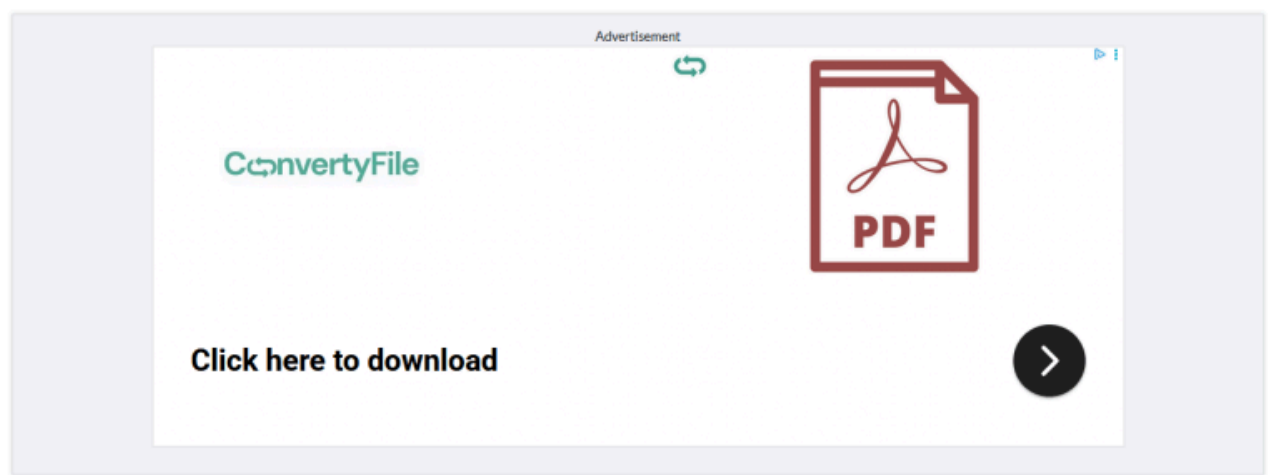
ConveryFile is a Browser Hijacker. This documents my analysis on ConveryFile. It starts with an ad on govssalaries[.]com from Red Root LTD for ConveryFile. This was written in GO, and I'm not at that level to RE it yet. I used Any Run to interact with the sample, and to pull PCAP. I assess that ConveryFile is linked to ConvertMaster.

## Intro

This continues from my analysis on ConvertMaster [1]. ConveryFile is a Browser Hijacker.

## Google Advertisement

This ad was served again from govssalaries[.]com. I will likely continue to pull converter ads from their site as the browser hijackers become available.



The advertiser is Red Root LTD. The snip below is from Google Ad Transparency.


← → ↻ 🏠 🔒 🔑 adstransparency.google.com/?region=US&domain=convertyfileapp.com 📄 ⭐ ⬇️ 👤 Sign in 🏠 ☰

Google Ads Transparency Center ⋮ 👤

All topics Political ads 🔍 Find the ads you've seen by searching by advertiser name or website ✓ Ads in United States ▾

convertyfileapp.com This domain includes results for multiple advertiser accounts with ads pointing to this domain. You can filter by individual advertiser below.

56 ads 📅 Any time ▾ 🌐 All platforms ▾ 📄 All formats ▾



ConvertyFile


Click here to download

Works on Windows 10 / 8 / 7 / Vista / XP | Start download

Open >

Red Root LTD  
Verified


Converty File



Download | ConvertyFile  
[Open](#)

Red Root LTD  
Verified

Converty File




Download | ConvertyFile  
[Open](#)

Red Root LTD  
Verified

ConvertyFile

Convert in Seconds!

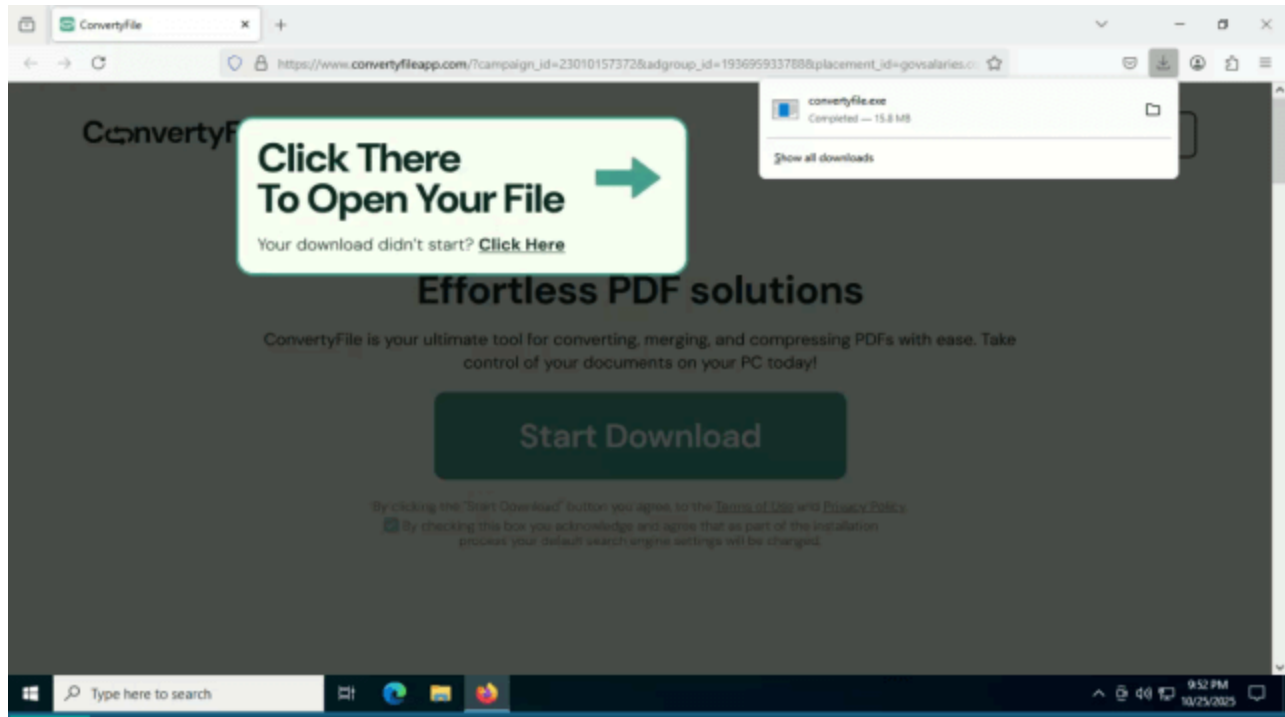


Try It Now

Red Root LTD  
Verified

## Delivery

The link leads you to “hxxps[:]//convertyfileapp[.]com”. Follow my work here [2]!



Convertyfile.exe (SHA256: 3d82200083a86df09c3b16c9095b844738a76863b1b01092b6c4dbef3b974b12) is served from “hxxps[:]//lukgiop[.]com/cond1”. Keep in mind that there will be parameters in the lukgio domain.

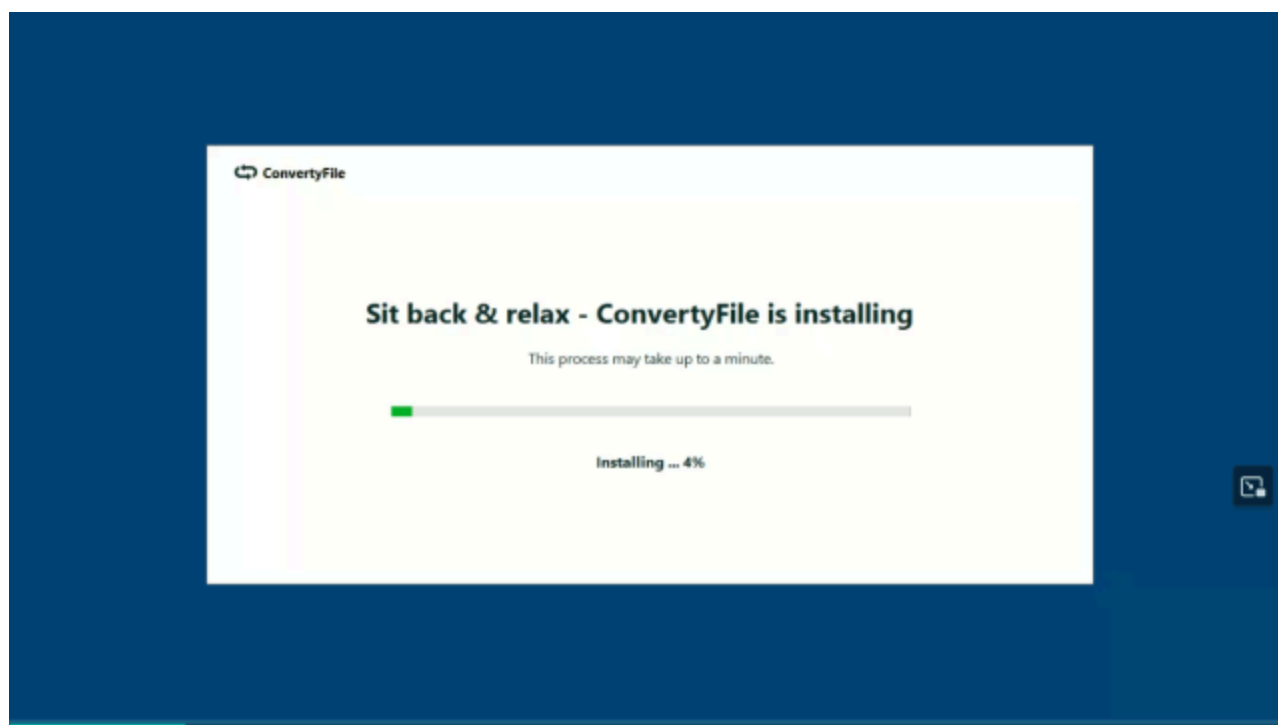
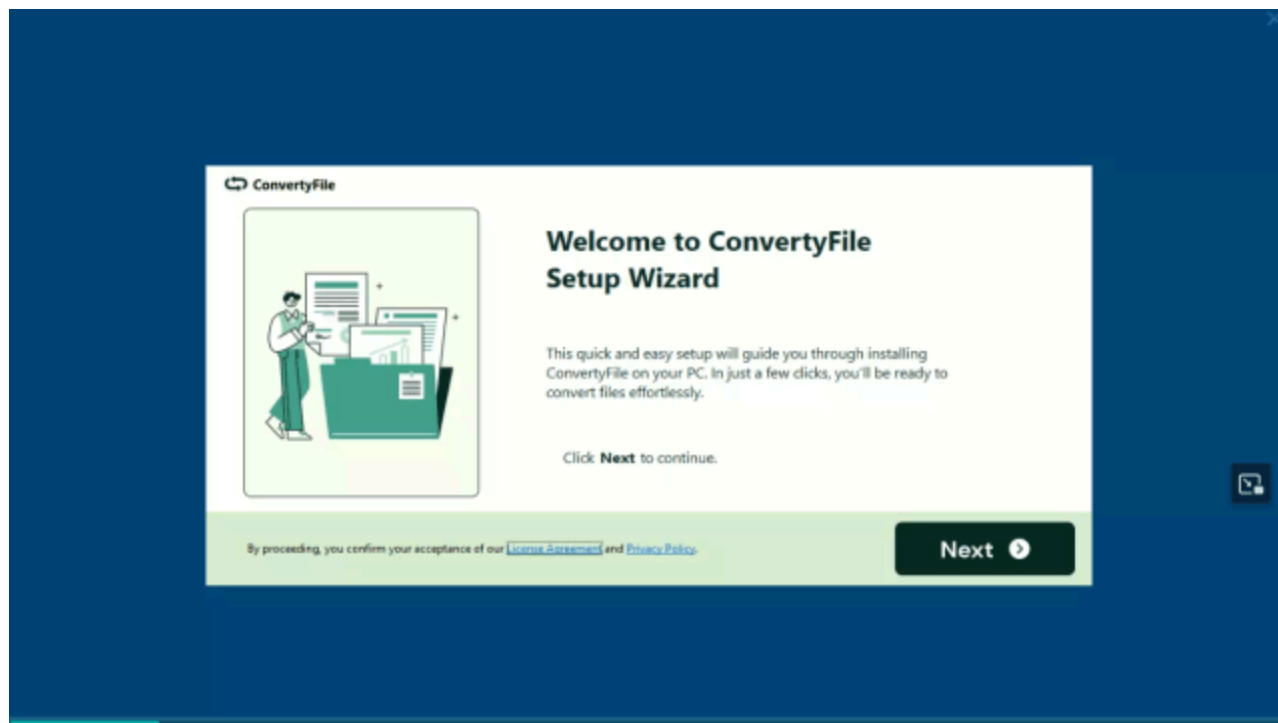
```
<a href="https://lukgiop.com/cond1" class="cta-button cta_click static_indicator" event_action="download_main">
  <div class="cta2" >Start Download</div>
</a>
```

I’m A/B testing with the snip width... be a bear with me.

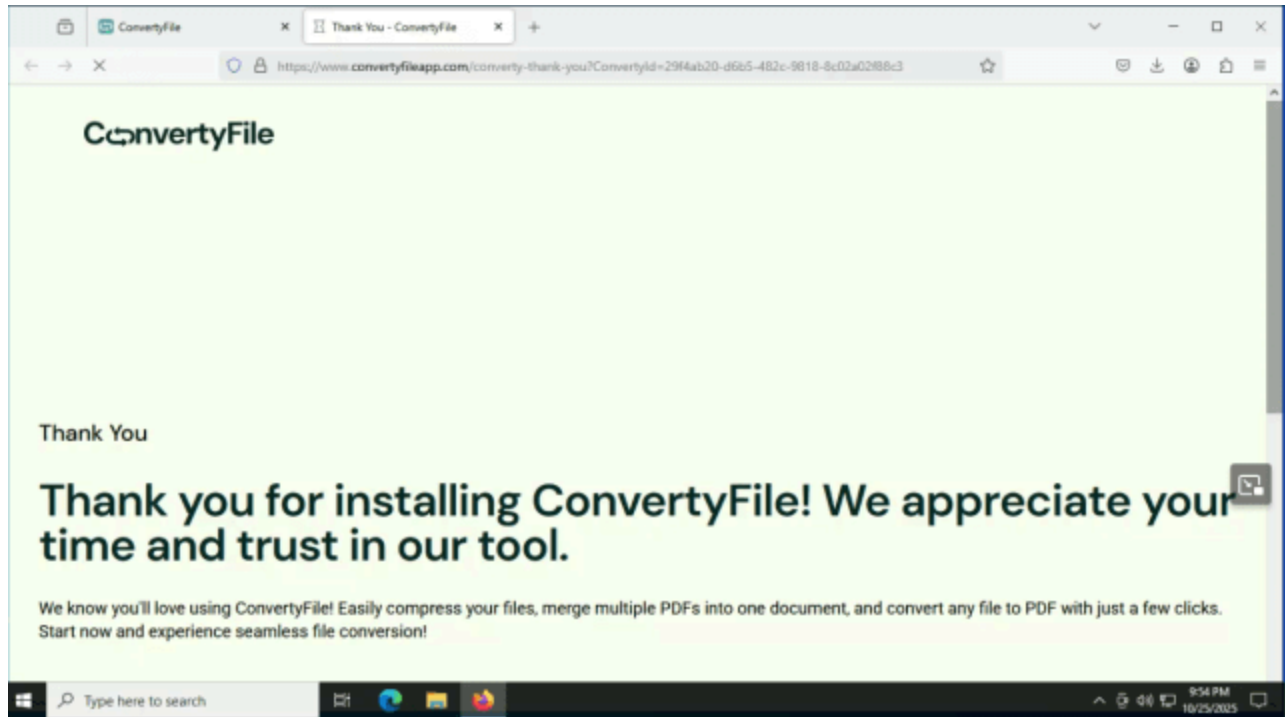
```
<div class="hero-cta">
  <a href="https://lukgiop.com/cond1" class="cta-button cta_click static_indicator" event_action="download_main">
    <div class="cta2" >Start Download</div>
  </a>
```

## Execution

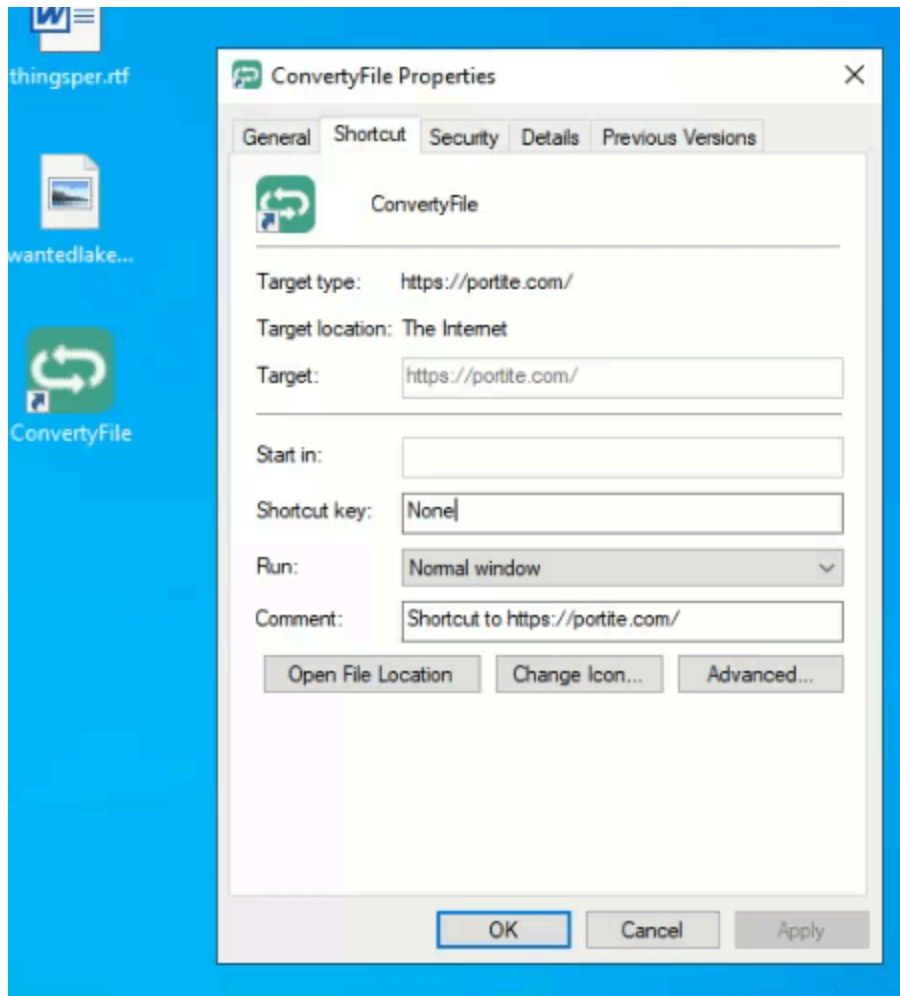
These are the install views that are similar to Convert Master. It covers the screen to ensure you don’t see the browser activities in the background.



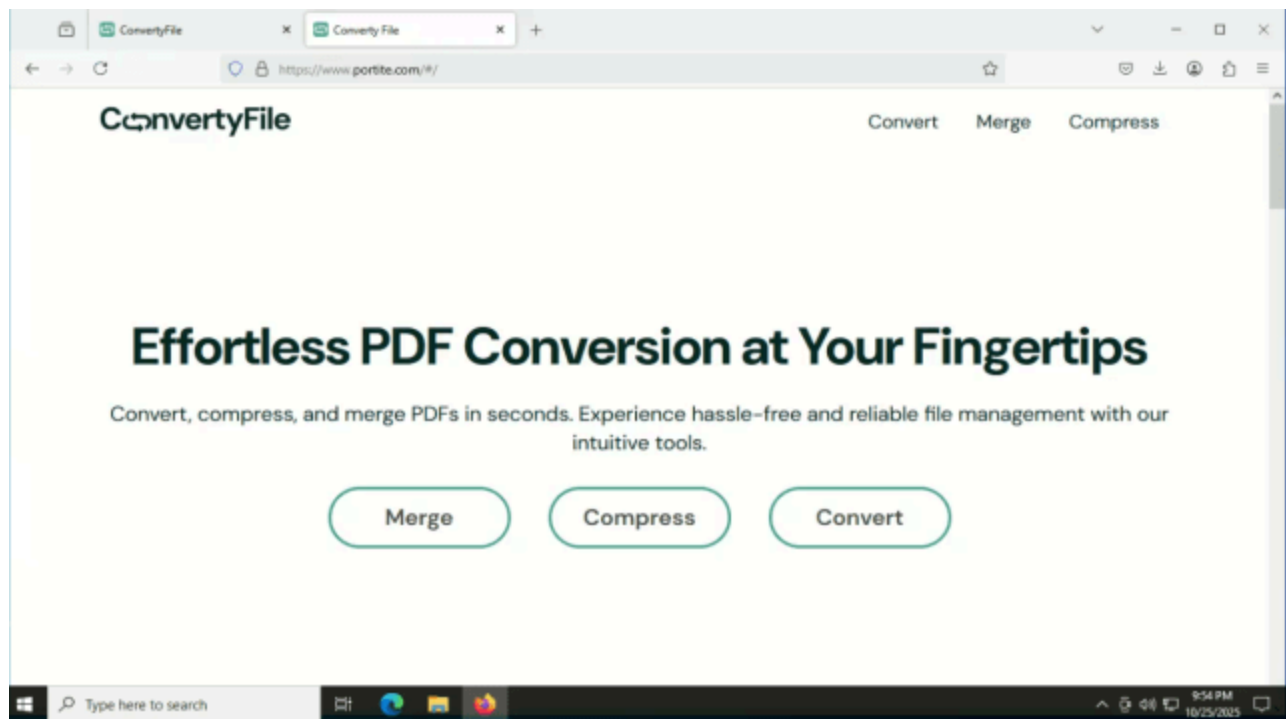
This is the success page.



The snip below shows the shortcut on the desktop, and the properties. I show this because this is the same behavior as Convert Master. The online converter is portite[.]com.

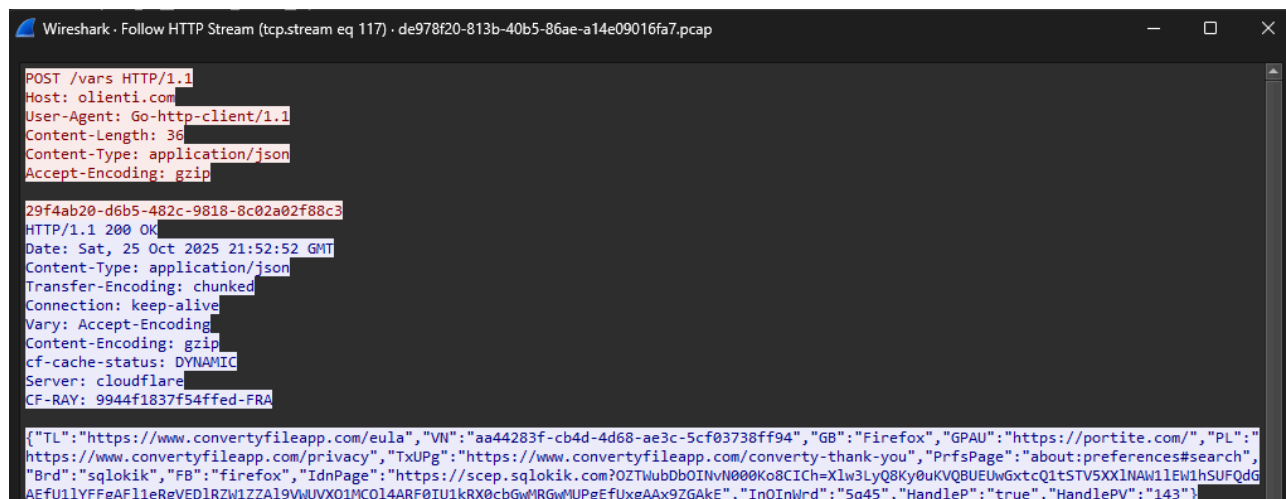


This is a snip of the portite site. Note how Convert Master also used a desktop link to bring the user to an online converter.



## Config Server

The snip shows the response to the POST request to “hxxps[:]//olienti[.]com/vars” contains the dynamic configs. From this I glean the target browser is FireFox, and the injected search URL starts with “hxxps[:]//scep.sqlokik[.]com”.



I assume the POST request to “hxxps[:]//olienti[.]com/boom” must mean “success”.

```

POST /boom HTTP/1.1
Host: olienti.com
User-Agent: Go-http-client/1.1
Content-Length: 0
Content-Type: application/json
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Sat, 25 Oct 2025 21:53:55 GMT
Content-Type: application/json
Content-Length: 0
Connection: keep-alive
cf-cache-status: DYNAMIC
Server: cloudflare
CF-RAY: 9944f30fed0bffd-FRA

```

The POST request to “hxps[:]/olienti[.]com/pass” appears to contain metrics. I assume this must be for chargeback to the “sqlokik” customer.

```

POST /pass HTTP/1.1
Host: olienti.com
User-Agent: Go-http-client/1.1
Content-Length: 304
Content-Type: application/json
Accept-Encoding: gzip

cont=true&accepted=true&backUsr=false&JobCancel=false&bv=136.0&bldVer=19045&id=29f4ab20-d6b5-482c-9818-8c02a02f88c3&scrDem=1360x768&txUp=true&monNum=false&guestId=aa44283f-cb4d-4d68-ae3c-5cf03738ff94&db=Firefox&more=false&brd=sqlokik&winTp=Windows+10&appVer=1.30.3.16&appUp=true&cancel=false&jobDone=true
HTTP/1.1 200 OK
Date: Sat, 25 Oct 2025 21:53:58 GMT
Content-Type: application/json
Content-Length: 0
Connection: keep-alive
cf-cache-status: DYNAMIC
Server: cloudflare
CF-RAY: 9944f3208955ffed-FRA

```

## Search Hijack Flow

The snip below shows my search “what is sqlokik and does it use searchretrorevive[.]com too” goes to scep.sqlokik[.]com.

```
Wireshark · Follow HTTP Stream (tcp.stream eq 312) · de978f20-813b-40b5-86ae-a14e09016fa7.pcap

GET /?OZTWubDb0INvN000Ko8CICH=Xlw3LyQ8Ky0uKVQBUEUwGxtcQ1tSTV5XXlNAW1lEW1hSUFQdGAefU1lYFFgAF1leRgVEDlRZW1ZZA19VWUVXQ1
1MCQl4ARF0IU1kRX0cbGwMRGwMUPgEfUxgAAx9ZGAkE&q=what%20is+sqlokik+and+does+it+use+searchretrorevive.com+too%3F HTTP/1.1
Host: scep.sqlokik.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Cookie: JSESSIONID=4CECB148F1C86DEEF5674CA3103E593C
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i

HTTP/1.1 200
Date: Sat, 25 Oct 2025 21:57:01 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Access-Control-Allow-Origin, Access-Control-Allow-Credentials
Vary: Accept-Encoding
cf-cache-status: DYNAMIC
Server: cloudflare
CF-RAY: 9944f79bae346957-FRA
```

The snip below shows that search is redirected to “hxxps[:]//searchdreamytab[.]com/search/?”

```
GET /p?OZTWubDb0INvN000Ko8CICH=Xlw3LyQ8Ky0uKVQBUEUwGxtcQ1tSTV5XXlNAW1lEW1hSUFQdGAefU1lYFFgAF1leRgVEDlRZW1ZZA19VWUVXQ
.314 HTTP/1.1
Host: scep.sqlokik.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Cookie: JSESSIONID=4CECB148F1C86DEEF5674CA3103E593C
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=0, i

HTTP/1.1 302
Date: Sat, 25 Oct 2025 21:57:02 GMT
Content-Length: 0
Connection: keep-alive
CF-RAY: 9944f79f68896957-FRA
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Access-Control-Allow-Origin, Access-Control-Allow-Credentials
Location: https://searchdreamytab.com/search/?chnm2=1739195227804691&chnm3=sags8lfj&q=what+is+sqlokik+and+does+it+us
e+searchretrorevive.com+too%3F
cf-cache-status: DYNAMIC
Server: cloudflare
```

The snip below shows that gets redirected to Yahoo search.

```
Wireshark · Follow HTTP Stream (tcp.stream eq 322) · de978f20-813b-40b5-86ae-a14e09016fa7.pcap

GET /search/?chnm2=1739195227804691&chnm3=sags8lfj&q=what+is+sqlloik+and+does+it+use+searchretrorevive.com+too%3F&asb=1&asb_sg=a0%7Cb0%7Cc0%7Cd2%7Ce0%7Cf0%7Cg0%7Ch0%7Ci0%7Ck0&asb_uid=176142942247041738893856 HTTP/1.1
Host: searchdreamytab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=0, i

HTTP/1.1 302 Found
date: Sat, 25 Oct 2025 21:57:03 GMT
server: Apache
cache-control: no-cache, no-transform
pragma: no-cache
expires: -1
x-mnt-w: 22-xr41
x-frame-options: SAMEORIGIN
location: http://de.search.yahoo.com/yhs/search?hspart=sz&hsimp=yhs-033&p=what+is+sqlloik+and+does+it+use+searchretrorevive.com+too%3F&type=type80176-1871945066&gdr=1&param1=3006825451
Content-Length: 0
content-type: text/html; charset=UTF-8
via: 1.1 google
Alt-Svc: h3=":18006"; ma=2592000,h3-29=":18006"; ma=2592000
```

## Closing Thoughts

This shares many similarities with Convert Master. I think they're related based on the deliver ads, the delivery chain, the objectives of browser hijacking to inject the default search engine, and the unique behavior of creating a desktop shortcut that just goes to an online converter. In addition to those similarities, I present to you the Silent Push snip below that shows both domains were observed using the same Google Ad ID.

datasource = ["webscan"] AND body\_analysis.google-GA4 = "G-SS88ENC0JT"

| Results                        |                                |              |                      |          |                                    |   |               |              |        |
|--------------------------------|--------------------------------|--------------|----------------------|----------|------------------------------------|---|---------------|--------------|--------|
| Basic Raw Data                 |                                |              |                      |          |                                    |   |               |              |        |
| origin_url                     | url                            | ip           | scan_date            | response | title                              | html_body_snippet   | favicon_icons | header_serve |        |
| https://convertmasterapp.co.nj | https://convertmasterapp.co.nj | 104.35.26.91 | 2025-10-25T16:24:10Z | 200      | Convert Master - The Best PDF Tool | 2025-10-25T16:24:10Z<br/>GdWdOpe=KXWMPg<br/>lgk0k0P-WdR0V000<br/>D0WGA=00 |               | cloudfl      | Expand |
| https://convertmasterapp.co.in | https://convertmasterapp.co.nj | 104.35.26.91 | 2025-07-07T05:02:14Z | 200      | Convert Master - The Best PDF Tool | 2025-07-07T05:02:14Z<br/>GdWdOpe=KXWMPg<br/>lgk0k0P-WdR0V000<br/>D0WGA=00 |               | cloudfl      | Expand |
| https://convertmasterapp.co.in | https://convertmasterapp.co.nj | 104.35.26.91 | 2025-06-07T21:00:20Z | 200      | Convert Master - The Best PDF Tool | 2025-06-07T21:00:20Z<br/>GdWdOpe=KXWMPg<br/>lgk0k0P-WdR0V000<br/>D0WGA=00 |               | cloudfl      | Expand |
| https://convertmasterapp.co.in | https://convertmasterapp.co.nj | 104.35.26.91 | 2025-06-05T03:30:10Z | 200      | Convert Master - The Best PDF Tool | 2025-06-05T03:30:10Z<br/>GdWdOpe=KXWMPg<br/>lgk0k0P-WdR0V000<br/>D0WGA=00 |               | cloudfl      | Expand |
| https://portfile.com           | https://www.portfile.com/W     | 104.35.18.35 | 2025-03-07T09:50:02Z | 200      | Converty File                      | 2025-03-07T09:50:02Z<br/>GdWdOpe=KXWMPg<br/>lgk0k0P-WdR0V000<br/>D0WGA=00 |               | cloudfl      | Expand |

## Summary

ConvertyFile is a Browser Hijacker. This documents my analysis on ConvertyFile. It starts with an ad on govsalaries[.]com from Red Root LTD for ConvertyFile. This was written in GO, and I'm not at that level to

RE it yet. I used Any Run to interact with the sample, and to pull PCAP. I assess that ConverytyFile is linked to ConvertMaster.

## References

- 1 – <https://malasada.tech/convert-master-browser-hijacker-analysis/>
- 2 – <https://app.any.run/tasks/de978f20-813b-40b5-86ae-a14e09016fa7>

## IOCs

```
3d82200083a86df09c3b16c9095b844738a76863b1b01092b6c4dbef3b974b12
converytyfileapp[.]com
lukgio[.]com
portite[.]com
olienti[.]com
scep.sqlokik[.]com
searchdreameytab[.]com
hxxps[:]//converytyfileapp[.]com
hxxps[:]//lukgio[.]com/condl
hxxps[:]//portite[.]com/
hxxps[:]//olienti[.]com/vars
hxxps[:]//scep.sqlokik[.]com
hxxps[:]//olienti[.]com/boom
hxxps[:]//olienti[.]com/pass
hxxps[:]//searchdreameytab[.]com/search/
```

## WITH PLANNY ALOHA, MAHALO FOR YOUR TIME

## Post navigation

[Convert Master Browser Hijacker Analysis](#)