SAMPLE DATA

This is a real whack.sh report — rendered from example data.

The layout, fields and PDF are exactly what a scan produces. The target, redirect chain, addresses and file hash are fabricated and use **RFC 2606** reserved names, so this makes no claim about any real site.

whack.sh

Shared scan report · #e3b0c44298fc · 2026-08-14 00:00 UTC · 9 credits

hxxp://example[.]com/invoice/download?id=8f21c4

Malware 96/100

85 Cross-egress divergence: the datacenter vantage was served nothing while the residential and mobile vantages were served a file

90 Served executable captured (PE/EXE, sha 4b1d9c07e2af)

55 Forced binary/installer download [residential, mobile]

45 Redirect chain crosses three unrelated registrable domains before delivery

SUMMARY

Malware — a file was delivered to two of three vantages (96/100).

The datacenter vantage was served an empty 404 and nothing else. The residential and mobile vantages, requesting the same URL at the same time, were redirected through two further domains and handed a Windows executable. The file was captured from both.

A scanner checking this URL from a datacenter address alone would record it as dead. The delivery only happens for traffic that looks like a real consumer connection, which is what the target is filtering for.

EVIDENCE SHA-256 `9f2c1a7e4d6b8035ca1f47e290b6d3517c8ae04f2b91d6835e7a0c4f18d29b6e`

3	2	3	7
Egress vantages	Max redirects	Unique hosts	Requests · 2.8 MB

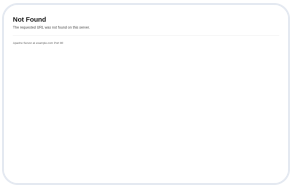
2.1s	2
Load time	Payloads

Cross-egress divergence — vantages landed on different destinations: `datacenter → example.com` · `residential → cdn.example.org` · `mobile → cdn.example.org`. This is the cloaking tell a single-vantage scanner can't see.

ℹ Origin IP / ASN are shown as **observed on the wire** wherever an un-proxied vantage saw the host. When every vantage is proxied, the IP is **resolved from DNS** by the scanner node and labelled as such — a resolution can differ from what the vantage actually reached, so we never present it as an observation. Where neither is available the hop shows "— *via proxy*".

Datacenter Done 1 hop · 404 412 B · 6.1s render · 1s queued

Exit IP: **198.51.100.24** · US · AS64500 Example Hosting LLC ✓ **Verified**



→ 404 **example[.]com** · text/html · 104[.]20[.]23[.]154

Residential Done 3 hops · 302 › 302 › 200 1.4 MB · 10.5s render · 1s queued

Exit IP: **192.0.2.145** · US · AS64501 Example Broadband ✓ **Verified**

→ 200 **cdn[.]example[.]org** · application/x-msdownload · 203[.]0[.]113[.]199

Proxied egress — a proxy can't reveal origin IPs on the wire. IPs here come from an un-proxied vantage that observed the host, or (when every vantage was proxied) from the node's own DNS resolution, marked *resolved*. Hops with neither show "—".

#	ST	HOST	IP · PTR	ASN · ORG · CC	AN
1	302	**example[.]com**	104[.]20[.]23[.]154	…	…
2	302	**www[.]example[.]net**	203[.]0[.]113[.]71	…	…
3	200	**cdn[.]example[.]org**	203[.]0[.]113[.]199	…	…

No TLS — served over HTTP, or certificate not captured.

Final IP	203[.]0[.]113[.]199
Country	US
ASN / Org	AS64501 · Example Broadband
PTR	–
Flags	—

No cookies set.

No response headers captured.

No assets recorded.

⚠ **captured payload** payload · PE/EXE · 1.4MB

4b1d9c07e2afd35180f6ba2ce9471d8a5c30e7f24b96a8d1e05c7f3924ab61d0

MalwareBazaar ↗ **Search VT ↗** retained server-side · not distributed

Mobile Done 3 hops · 302 › 302 › 200 1.4 MB · 8s render · 2s queued

Exit IP: **192.0.2.201** · US · AS64502 Example Mobile Network ✓ **Verified**

→ 200 **cdn[.]example[.]org** · application/x-msdownload · 203[.]0[.]113[.]199

Proxied egress — a proxy can't reveal origin IPs on the wire. IPs here come from an un-proxied vantage that observed the host, or (when every vantage was proxied) from the node's own DNS resolution, marked *resolved*. Hops with neither show "—".

#	ST	HOST	IP · PTR	ASN · ORG · CC	A
1	302	**example[.]com**	172[.]66[.]147[.]243	…	…
2	302	**www[.]example[.]net**	203[.]0[.]113[.]71	…	…
3	200	**cdn[.]example[.]org**	203[.]0[.]113[.]199	…	…

No TLS — served over HTTP, or certificate not captured.

Final IP	203[.]0[.]113[.]199
Country	US
ASN / Org	AS64502 · Example Mobile Network
PTR	–
Flags	—

No cookies set.

No response headers captured.

No assets recorded.

⚠ **captured payload** payload · PE/EXE · 1.4MB

4b1d9c07e2afd35180f6ba2ce9471d8a5c30e7f24b96a8d1e05c7f3924ab61d0

MalwareBazaar ↗ **Search VT ↗** retained server-side · not distributed