PDF Forensic Analysis Log

Treadstone — Domestic Terrorism in the United States: Executive Summary

Analysis Date: 2026-04-21 21:43 UTC

Analyst: Allison Criten | Disinfo Forensics

OVERALL VERDICT: NO MALICIOUS CONTENT DETECTED

1. File Identity & Provenance

Field	Value
Filename	Treadstone-Domestic Terrorism in the United States - Executive Summary.pdf
File Size	130,034 bytes (127 KB)
PDF Version	1.4
Page Count	5
Creation Date	2025-10-06 01:25:50 UTC
Modification Date	2025-10-06 01:25:50 UTC (matches creation — no post-creation tampering)
Creator	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Producer	Skia/PDF m141

Hybrid Analysis Verification

The following Hybrid Analysis sandbox report provides independent verification of file origin and behavior. No URLs were found embedded in the original PDF itself (confirmed by annotation scan, in-text extraction, and raw binary scan) — this link is the sole provenance reference.

Field	Value
Hybrid Analysis URL	https://hybrid-analysis.com/sample/b0dabe8818ae476e9baaa454de2b8617a823d6f09de079912147f13ffcc27cf
SHA-256	b0dabe8818ae476e9baaa454de2b8617a823d6f09de079912147f13ffcc27cfd
Embedded URLs in original PDF	NONE — no URIs, hyperlinks, or annotations present in file

Creator string identifies Chrome 141 on Linux x86_64 via Skia rendering engine — consistent with a 'Print to PDF' or Puppeteer/headless Chrome workflow. Creation and modification timestamps are identical, confirming no post-creation alteration.

2. Security Checks Performed

Check	Method	Finding	Result
JavaScript (doc-level)	/Names → /JavaScript	NOT PRESENT	**PASS**
JavaScript (annotation)	/A → /S /JavaScript	NOT PRESENT	**PASS**
OpenAction (auto-exec)	/Root → /OpenAction	NOT PRESENT	**PASS**
Additional Actions (AA)	/Root → /AA	NOT PRESENT	**PASS**

Embedded Files (.dat, .exe…)	/Names → /EmbeddedFiles	NOT PRESENT	PASS
Launch Actions	/A → /S /Launch	NOT PRESENT	PASS
AcroForm / Submit Actions	/Root → /AcroForm	NOT PRESENT	PASS
RichMedia (Flash/SWF)	/RichMedia key	NOT PRESENT	PASS
URI Actions in Annotations	/A → /S /URI	NOT PRESENT	PASS
Embedded URLs (raw binary)	Regex scan of full binary	NONE FOUND	PASS
Embedded URLs (text layer)	pdfplumber extraction + regex	NONE FOUND	PASS
Suspicious stream content	eval, exec, powershell, shellcode, ActiveXObject, base64, fromCharCode	NONE FOUND	PASS
Compressed stream anomalies	13 streams, printable-ratio analysis	All standard glyph/content data	PASS
Font steganography	FontDescriptor + font program inspection	4 standard subsetted fonts (AAAAAA+ prefix = normal PDF behavior)	PASS
XRef integrity	XRef table structure	Standard; no obfuscation streams	PASS
Metadata anomalies	/Info dictionary inspection	Title, Creator, Producer, dates — consistent with Chrome/Skia PDF	PASS

3. PDF Object Inventory

All object types found are standard for a Chrome/Skia-generated PDF.

Object Type	Count	Notes
/Pages	1	Root page tree
/Page	5	No per-page actions or suspicious keys
/Font / /FontDescriptor	4	LiberationSerif-Bold, LiberationSerif, LiberationSans-Bold, LiberationSans
Compressed streams	13	All FlateDecode (standard zlib); no encrypted or obfuscated streams
/XObject	Present	Image and Form subtypes only
/StructTreeRoot	1	Accessibility/tagged PDF — benign
/MarkInfo	1	PDF/UA marker — benign
/ViewerPreferences	1	Display preferences only — no auto-execute
/Lang	1	Language tag — benign

4. Items Removed in Sanitized Output

NO MALICIOUS CONTENT FOUND OR REMOVED

No malicious payloads existed. The sanitized PDF was rebuilt from scratch using only extracted plain text, which eliminates all risk from the original binary structure regardless. The following were stripped as part of standard sanitization practice:

- Original compressed font streams (replaced with standard ReportLab fonts)
- Original page content streams (recomposed from plain-text extraction)
- /StructTreeRoot, /MarkInfo, /ViewerPreferences, /Lang objects (non-content)
- Original XObject image/form data (only text content preserved)
- Original PDF metadata — replaced with sanitized provenance metadata

5. False Positives During Analysis

One match was flagged and cleared:

```
grep pattern "exec" matched title string "Executive Summary" — confirmed false positive. No executable code associated.
```

The AAAAAA+ font prefix (e.g., /FontName /AAAAAA+LiberationSerif-Bold) is standard Chrome/Skia behavior — a random 6-char subset tag per PDF spec. Not an indicator of compromise.

6. Conclusion

This PDF is a clean, standard Chrome-generated document. No embedded scripts, executable payloads, auto-launch behaviors, hidden files, or embedded URLs were found. It is consistent with a document produced via 'Print to PDF' in Chrome 141 on Linux on October 6, 2025. The sanitized rebuild is safe to distribute, archive, and open in any PDF viewer.

Log generated: 2026-04-21 21:43 UTC | Disinfo Forensics / Allison Criten

Hybrid Analysis: https://hybrid-analysis.com/sample/b0dabe8818ae476e9baaa454de2b8617a823d6f09de079912147f13ffcc27cfd/69e821fa08bf25f03e0322b5

SHA-256: b0dabe8818ae476e9baaa454de2b8617a823d6f09de079912147f13ffcc27cfd