PDF Forensic Analysis Log

Treadstone — Domestic Terrorism in the United States: Executive Summary

Analysis Date: 2026-04-21 21:31 UTC

Analyst: Allison Criten | Disinfo Forensics

OVERALL VERDICT: NO MALICIOUS CONTENT DETECTED

1. File Identity

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 (same as creation — not altered)
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

Note: Creator string identifies a Chrome 141 browser on Linux x86_64 using the Skia rendering engine. This is consistent with a 'Print to PDF' or programmatic PDF generation via Chrome/Puppeteer. Creation and modification timestamps match, confirming no post-creation tampering.

2. Security Checks Performed

Check	Method	Finding	Result
JavaScript (document-level)	/Names → /JavaScript key	NOT PRESENT	PASS
JavaScript (annotation-level)	/A → /S /JavaScript in page annots	NOT PRESENT	PASS
OpenAction (auto-execute on open)	/Root → /OpenAction	NOT PRESENT	PASS
Additional Actions (AA)	/Root → /AA	NOT PRESENT	PASS
Embedded Files (.dat, .exe, .zip, etc.)	/Names → /EmbeddedFiles	NOT PRESENT	PASS
Launch Actions	/A → /S /Launch	NOT PRESENT	PASS
AcroForm (form fields / submit actions)	/Root → /AcroForm	NOT PRESENT	PASS
RichMedia (Flash/SWF)	/RichMedia key in any object	NOT PRESENT	PASS
URI Actions	/A → /S /URI in annotations	NOT PRESENT	PASS
Suspicious stream content	Decompressed stream scan: eval, exec, powershell, Shellcode, ActiveXObject, CreateObject, base64, fromCharCode	NONE FOUND	PASS
Binary anomalies in streams	Printable-ratio analysis of 13 compressed streams	All streams are standard glyph/font/content data	PASS
Font steganography	FontDescriptor + embedded font program inspection	Inspected subsetting markers (AAAAAA+ prefix = normal Chrome PDF behavior)	PASS
Binary keyword scan	grep/strings for .dat, JavaScript, Launch, EmbeddedFile, shellcode, exec	Only benign 'exec' (false positive), no other hits	PASS

Cross-reference integrity	XRef table structure	Standard; no XRef streams indicating obfuscation	PASS
Metadata anomalies	Inspect /Info dictionary	Title, Creator, Producer, dates — all consistent with Chrome PDF origin	PASS

3. PDF Object Inventory

The following object types were identified in the PDF structure. All are standard for a Chrome-generated PDF.

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

4. Items Removed in Sanitized Output

NO MALICIOUS CONTENT

No JavaScript, embedded files (.dat or otherwise), launch actions, or exploit payloads were found. Nothing was removed for security reasons. The sanitized PDF was rebuilt from scratch using only the extracted plain text content, which eliminates any risk from the original PDF's binary structure entirely — including fonts, stream metadata, XObjects, and viewer-preference objects.

What was stripped in the rebuild (standard sanitization practice):

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

5. False Positives Noted During Analysis

One binary keyword match was flagged and resolved:

```
grep pattern "exec" matched the document title string "Executive Summary" — confirmed
false positive. No executable code or action of any kind was associated with this match.
```

The AAAAAA+ font name prefix (e.g., /FontName /AAAAAA+LiberationSerif-Bold) is standard Chrome/Skia behavior. It indicates a font subset tag — a random 6-character prefix used to mark subsetted (compressed)

fonts per PDF spec. This is not an indicator of compromise.

6. Conclusion

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