ForensicLab X Enterprise - Forensic Report

27million_eur.dat

Type: Unknown / data (unknown)
Size: 206569472 bytes
SHA256: 2bc3b298470c1b86fb3de0e8039b93c8eea1639ebaa93aeb11488d6869c4f562
MD5: 90004b12ed944388ce3d545d279d9028
Entropy avg: 7.999825 bits/byte
Verdict: Sangat mungkin encrypted / random / proprietary blob
Likelihood encrypted: 85%
Risk score: 30/100
Fuzzy hash:
`3145728:qXBJGddQWn0QzmONoQXC3PrXy4fahdBeiAJWFpa/liAHzqFz0it:qTidQC0QzfyD3P+4+BeiAwaVqFwit`

Forensic Flags (2)

[MEDIUM] [Suspicious_PDF_Action] PDF berisi JavaScript / auto-action.
[MEDIUM] 18 file tertanam terdeteksi (BZIP2, GZIP, JPEG, Script shebang).

File Carving

Polyglot: tidak
Trailing data: tidak
Embedded @3466172: BZIP2
Embedded @5637854: BZIP2
Embedded @5837109: Script shebang
Embedded @13124903: BZIP2
Embedded @13451739: Script shebang
Embedded @17085291: GZIP
Embedded @17730211: Script shebang
Embedded @18518956: JPEG
Embedded @21083785: JPEG
Embedded @38038684: Script shebang
Embedded @39743147: GZIP
Embedded @40824875: JPEG
Embedded @51223531: Script shebang
Embedded @56206658: JPEG
Embedded @59486190: Script shebang

IOC Extracted (35)

ipv6 (1): 0:e:C
domain (1): f.uk
windows_path (32): h:\y!m■p■■■, e:\■■N■T■■x, G:\;zm■■■■■■■=■■, A:\&5■■■■■■ ■,P, I:\■+■■ }■■H%
■$■■E■1[u■Mk■■■■[■Z■■■■■r■, P:\a3■}■■■■■■■{■■■
unc_path (1): \\7\■■$)■S ■■q■^■OBJ■8■■■■■U3WP■EJ■■L■■■■■w■■■y'■l■■07

MITRE ATT&CK (1 teknik)

T1204.002 User Execution: Malicious File: Execution

Assessment Reasons

• Entropy sangat tinggi, mendekati ciphertext/random.

• Tidak ada blok 16-byte berulang (konsisten dengan cipher mode acak).
• Tidak ada header format publik yang dikenali di awal file.
• Distribusi byte relatif merata (chi-square rendah).