Shannon Entropy: Measuring Randomness in File Content

Encrypted Rootkits (~7.9)

ELF Binaries (~6.1)

Text Files (~4.2)

$$H = -\sum_{i=0}^{255} p(x_i) \cdot \log_2\left(p(x_i)\right)$$

Shannon Entropy (bits/byte)

Byte Value Distribution Uniformity (%)