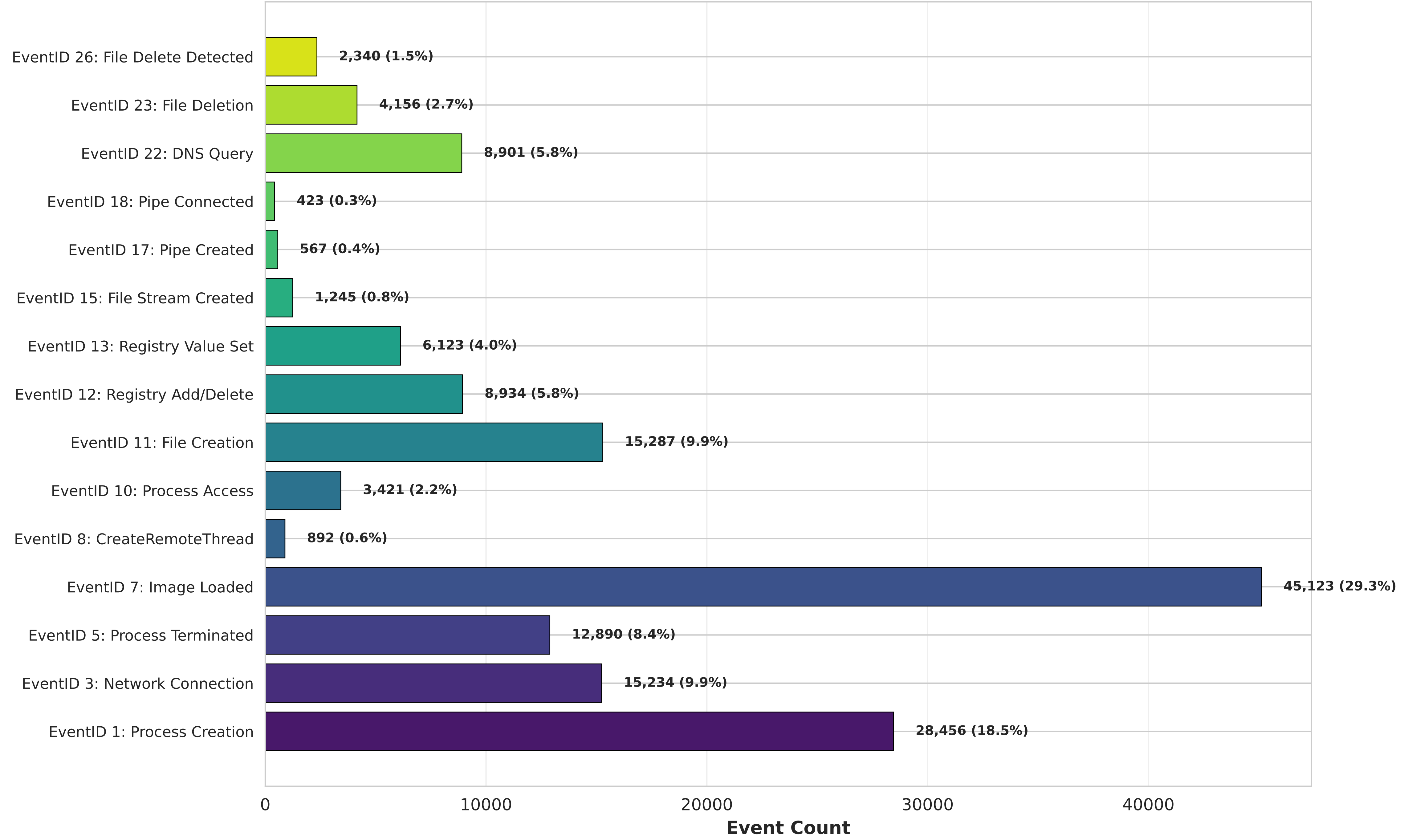
Figure 2.3: Sysmon EventID Distribution
Typical APT Run Dataset (145,832 total events)


EventID 26: File Delete Detected
2,340 (1.5%)
EventID 23: File Deletion
4,156 (2.7%)
EventID 22: DNS Query
8,901 (5.8%)
EventID 18: Pipe Connected
423 (0.3%)
EventID 17: Pipe Created
567 (0.4%)
EventID 15: File Stream Created
1,245 (0.8%)
EventID 13: Registry Value Set
6,123 (4.0%)
EventID 12: Registry Add/Delete
8,934 (5.8%)
EventID 11: File Creation
15,287 (9.9%)
EventID 10: Process Access
3,421 (2.2%)
EventID 8: CreateRemoteThread
892 (0.6%)
EventID 7: Image Loaded
45,123 (29.3%)
EventID 5: Process Terminated
12,890 (8.4%)
EventID 3: Network Connection
15,234 (9.9%)
EventID 1: Process Creation
28,456 (18.5%)
Event Count