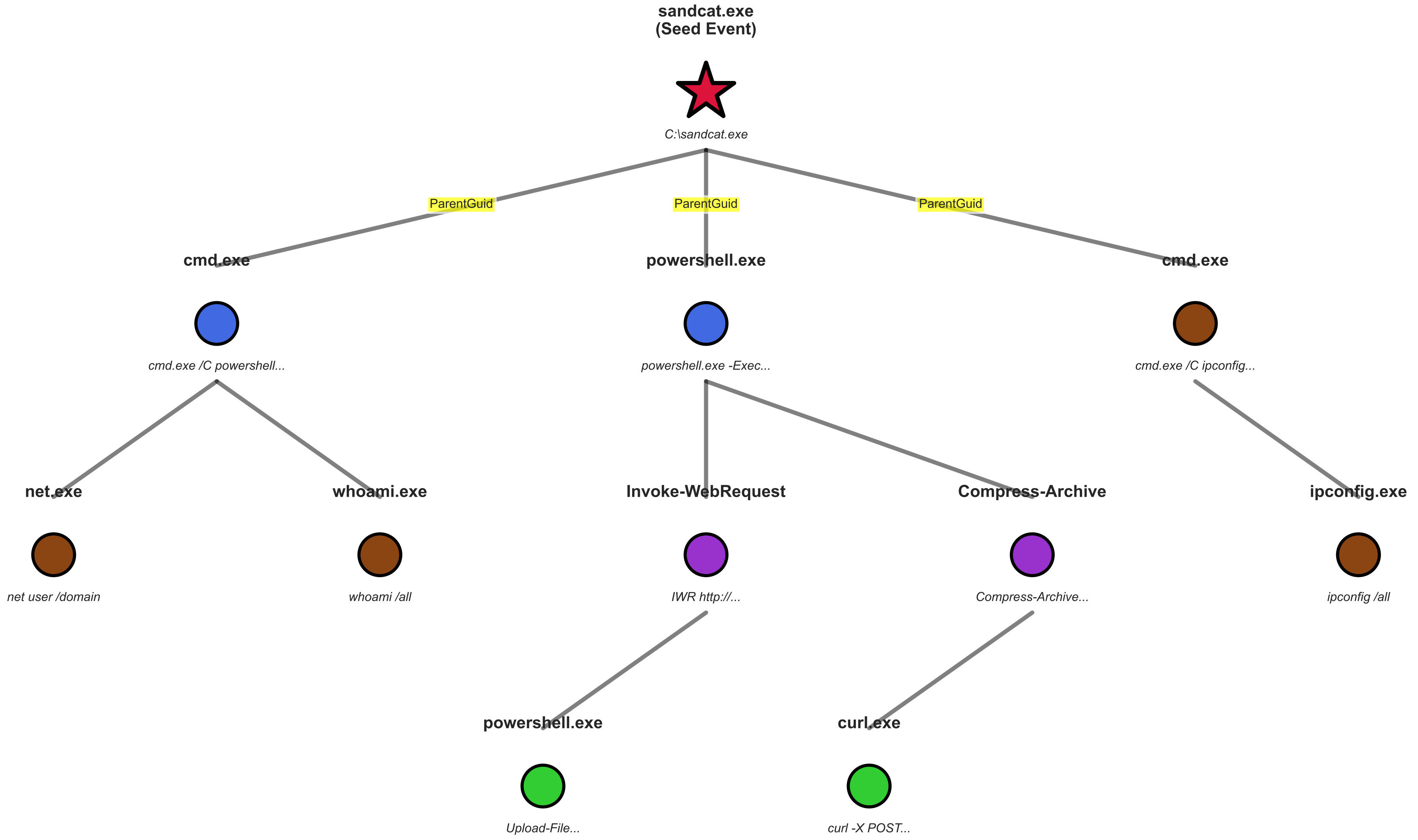
Figure 7.1: ProcessGuid Correlation Tree

Attack Lifecycle Expansion via Parent-Child Process Relationships



Seed Events: 1 | Total Traced: 12 | Expansion: 12x | Max Depth: 3 levels
Correlation Method: ProcessGuid (child) matched to ParentProcessGuid (parent)

🟥 Seed Event (□) 🟦 Execution 🟫 Discovery 🟩 Persistence 🟪 Collection 🟩 Exfiltration