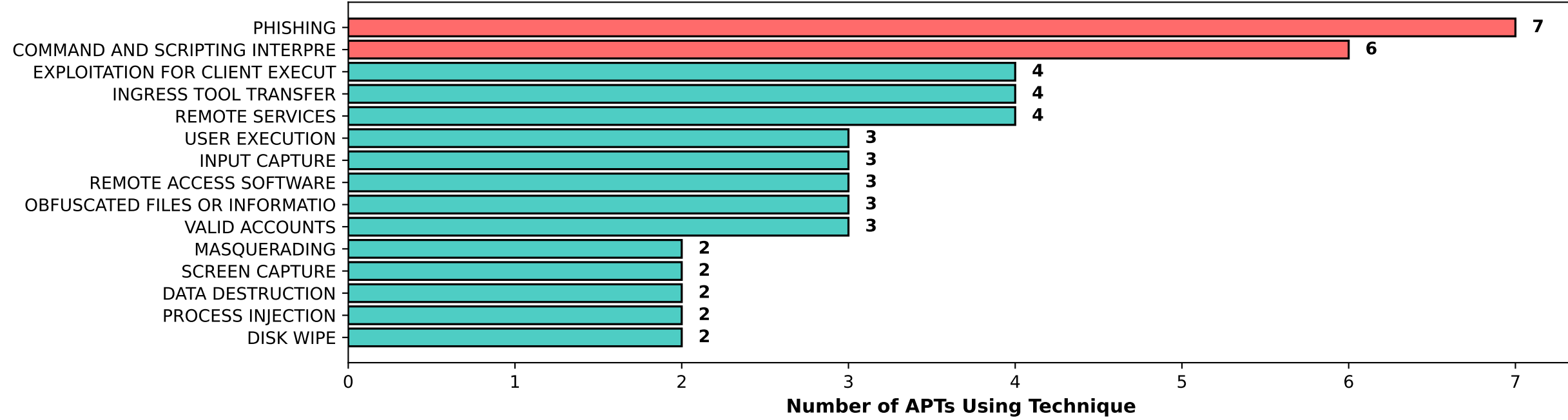# CTI Knowledge Graph - Research Analysis Metrics
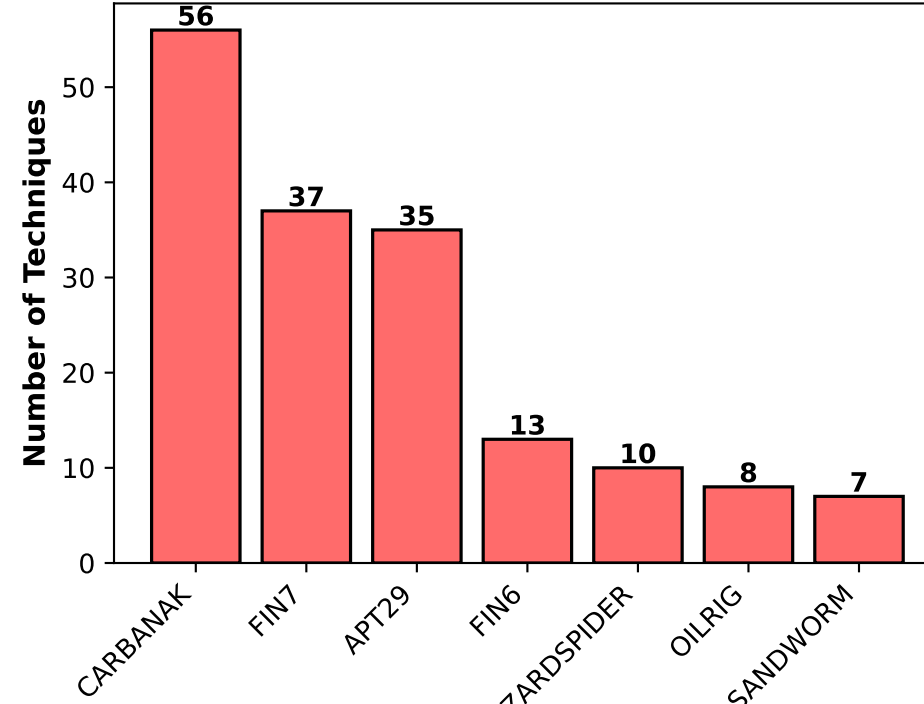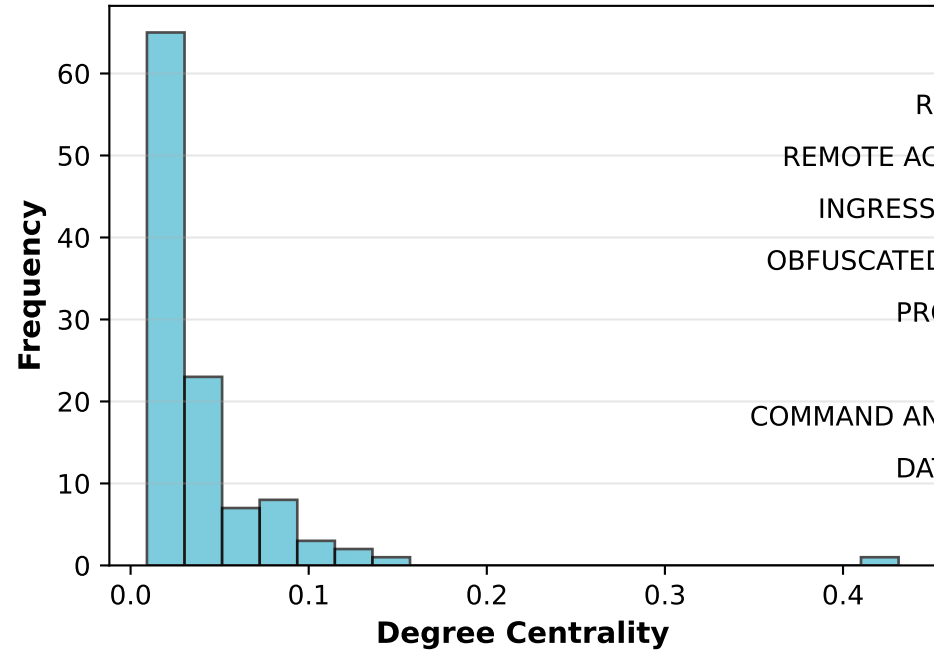
Top 15 Techniques by APT Usage (Hub Techniques)
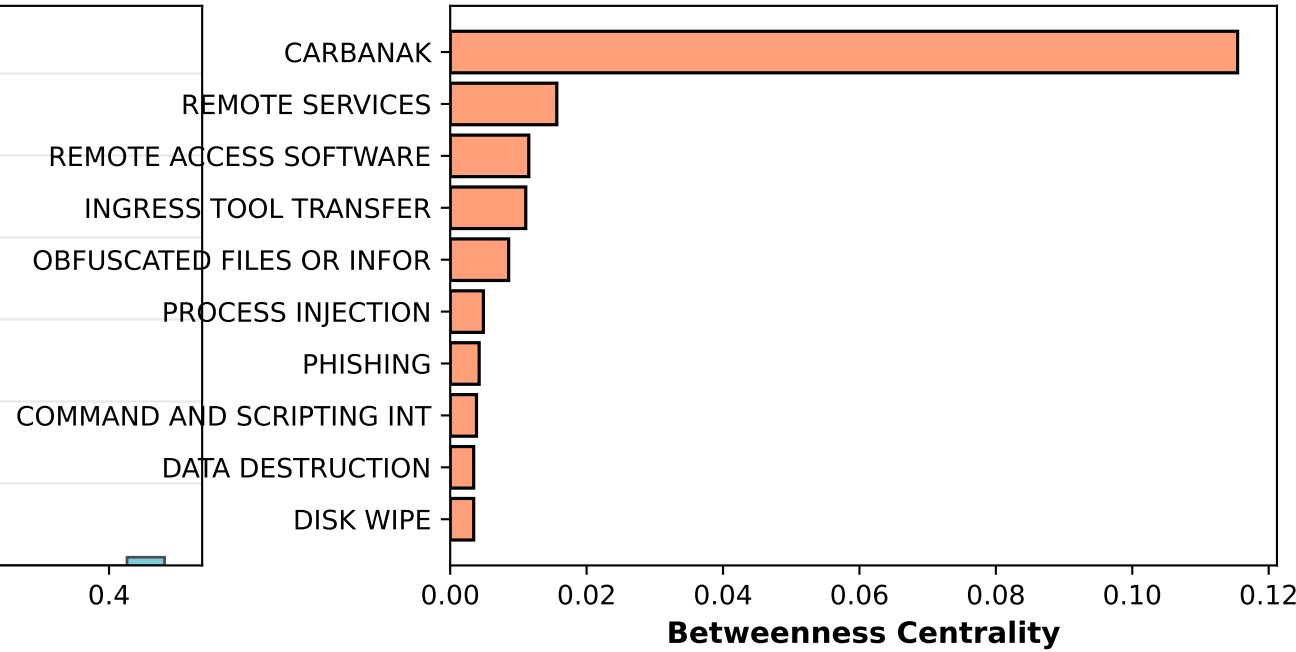
Technique	Number of APTs Using Technique
PHISHING	7
COMMAND AND SCRIPTING INTERPRE	6
EXPLOITATION FOR CLIENT EXECUT	4
INGRESS TOOL TRANSFER	4
REMOTE SERVICES	4
USER EXECUTION	3
INPUT CAPTURE	3
REMOTE ACCESS SOFTWARE	3
OBFUSCATED FILES OR INFORMATIO	3
VALID ACCOUNTS	3
MASQUERADING	2
SCREEN CAPTURE	2
DATA DESTRUCTION	2
PROCESS INJECTION	2
DISK WIPE	2

APT Actor Activity

APT	Number of Techniques
CARBANAK	56
FIN7	37
APT29	35
FIN6	13
WIZARDSPIDER	10
OILRIG	8
SANDWORM	7

Degree Centrality Distribution

(Histogram: Frequency vs Degree Centrality, ranging 0.0 to ~0.45)

Top 10 Bridge Nodes (Betweenness)

Node	Betweenness Centrality
CARBANAK	~0.115
REMOTE SERVICES	~0.015
REMOTE ACCESS SOFTWARE	~0.011
INGRESS TOOL TRANSFER	~0.011
OBFUSCATED FILES OR INFOR	~0.008
PROCESS INJECTION	~0.005
PHISHING	~0.005
COMMAND AND SCRIPTING INT	~0.004
DATA DESTRUCTION	~0.004
DISK WIPE	~0.003

MITRE Tactic Coverage

Tactic	Number of Techniques
COMMAND AND CONTROL	10
DEFENSE EVASION	8
PERSISTENCE	6
EXECUTION	5
IMPACT	5
COLLECTION	4
INITIAL ACCESS	4
DISCOVERY	4
PRIVILEGE ESCALATION	4
EXFILTRATION	3
CREDENTIAL ACCESS	3
RESOURCE DEVELOPMENT	2
CREDENTIALS ACCESS	2
LATERAL MOVEMENT	1
COMMAND AND CONTROLE	1
RECONNAISSANCE	1
COMMUNICATION AND CO	1

```
GRAPH METRICS SUMMARY

Network Properties:
• Total Nodes: 110 | Total Edges: 236 | Density: 0.0197
• Connected Components: 1

Key Findings:
• Most Active APT: CARBANAK with 56 techniques
• Most Connected Hub Node: CARBANAK (Degree: 47)
• Most Common Technique Hub: PHISHING (Used by 7 APTs)
• Top Bridge Node (Betweenness): CARBANAK (0.1154)

APT Intelligence:
• Total APT Groups: 7
• Total Techniques Represented: 53
• Total MITRE Tactics Covered: 17
• Average Techniques per APT: 23.7

Research Implications:
✓ CARBANAK demonstrates the highest connectivity, suggesting sophisticated and diverse TTPs
✓ Technique "PHISHING" is a critical hub - appears in 7 APT arsenals
✓ Graph structure shows interconnected threat landscape with shared tactics across APT groups
```