CTI Knowledge Graph
Comprehensive Analysis Report

Advanced Threat Intelligence Network Analysis

Report Generated: 2026-02-02 13:49:39
Data Source: CTI-HAL Dataset
Graph Nodes: 110
Graph Edges: 236
APT Groups Analyzed: 7
Techniques Identified: 53
MITRE Tactics Covered: 17

Executive Summary

This comprehensive report analyzes a cybersecurity threat intelligence knowledge graph constructed from 81 CTI reports covering 7 advanced persistent threat (APT) groups. The analysis reveals critical insights into attack techniques, tactical patterns, and threat relationships using advanced network analysis methods including degree centrality, betweenness centrality, and graph metrics.

Key Findings:
• Most Active Threat: **CARBANAK** with 56 attack techniques
• Most Common Attack Vector: **PHISHING** (used by 7 APTs)
• Network Connectivity: 0.0197 density indicates a highly interconnected threat landscape
• Critical Hub Node: **CARBANAK** with highest degree centrality

1. Knowledge Graph Overview

The CTI knowledge graph represents a complex network of relationships between cyber threat actors, attack techniques, tactics, and tools. The graph is constructed through semantic triple extraction from 81 threat intelligence reports.

Graph Statistics:
• Total Nodes: 110
• Total Edges: 236
• Graph Density: 0.019683
• Connected Components: 1
• Average Degree: 4.29

Top 25 Most Connected Nodes

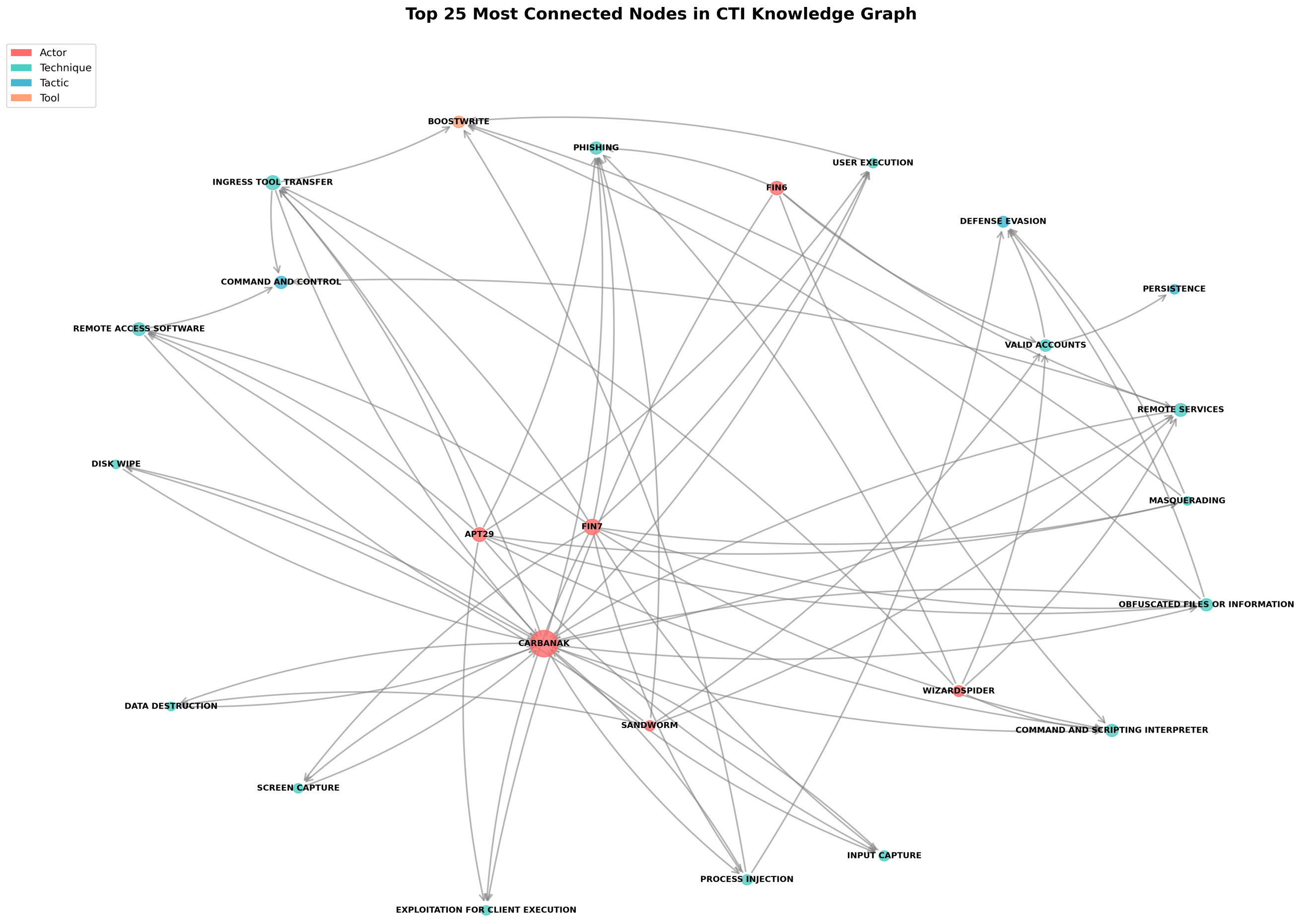
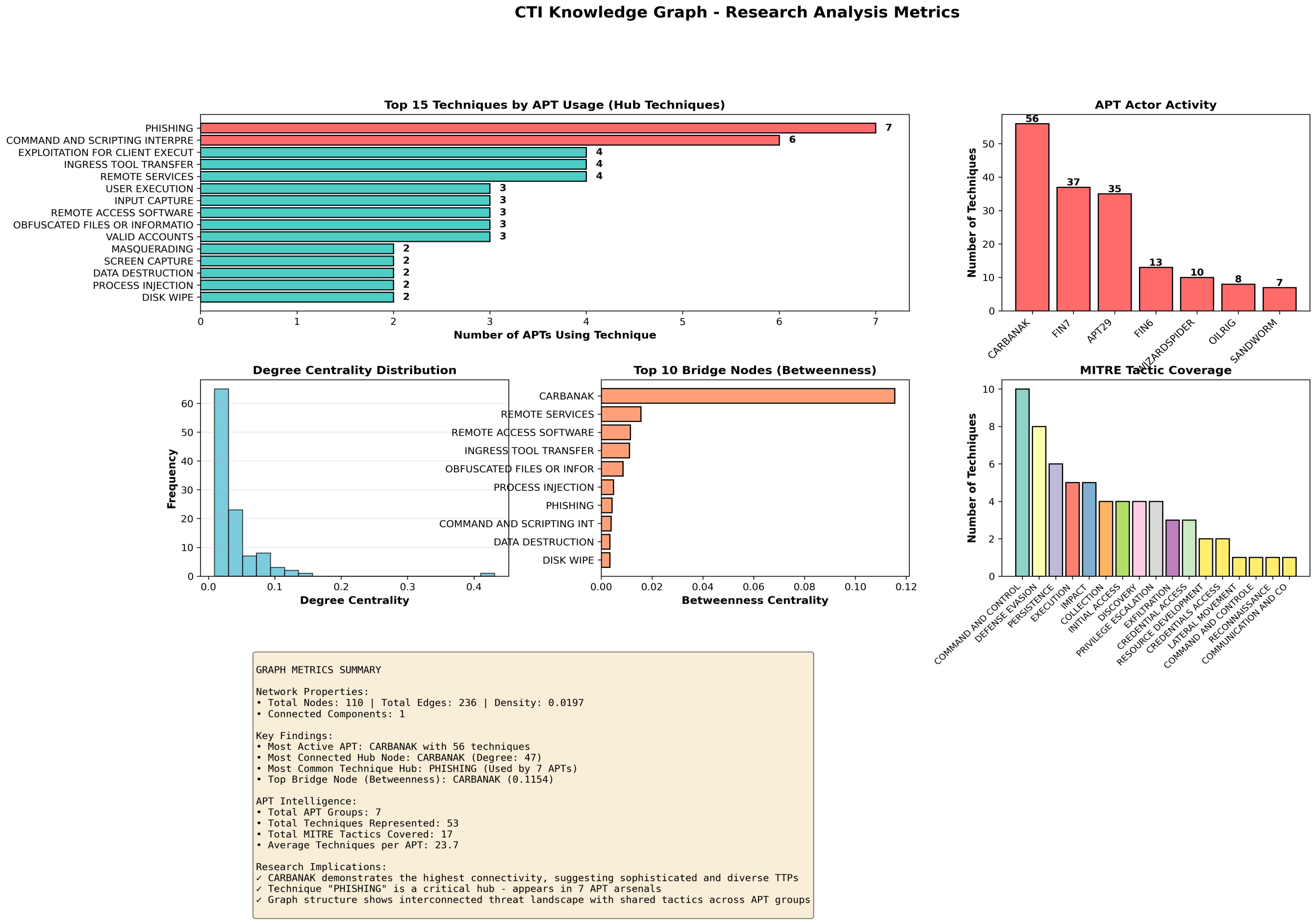


Figure 1: Network visualization of the 25 most connected nodes showing their relationships and importance in the threat landscape.

2. Research Analysis Metrics

Comprehensive graph analysis reveals critical insights into threat actor behavior and attack technique prevalence:



```
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
```

Figure 2: Comprehensive metrics dashboard showing technique usage, actor activity distribution, centrality analysis, and tactic coverage.

3. Degree vs Betweenness Centrality

Network centrality measures identify different types of important nodes:
Degree Centrality: Measures direct connections. High degree centrality nodes are "hubs".
• Top Node: **CARBANAK** with score 0.4312
• Interpretation: Most actively connected to other nodes

Betweenness Centrality: Measures bridge importance in shortest paths. High betweenness nodes are "connectors".
• Top Node: **CARBANAK** with score 0.1154
• Interpretation: Most critical for maintaining network connectivity

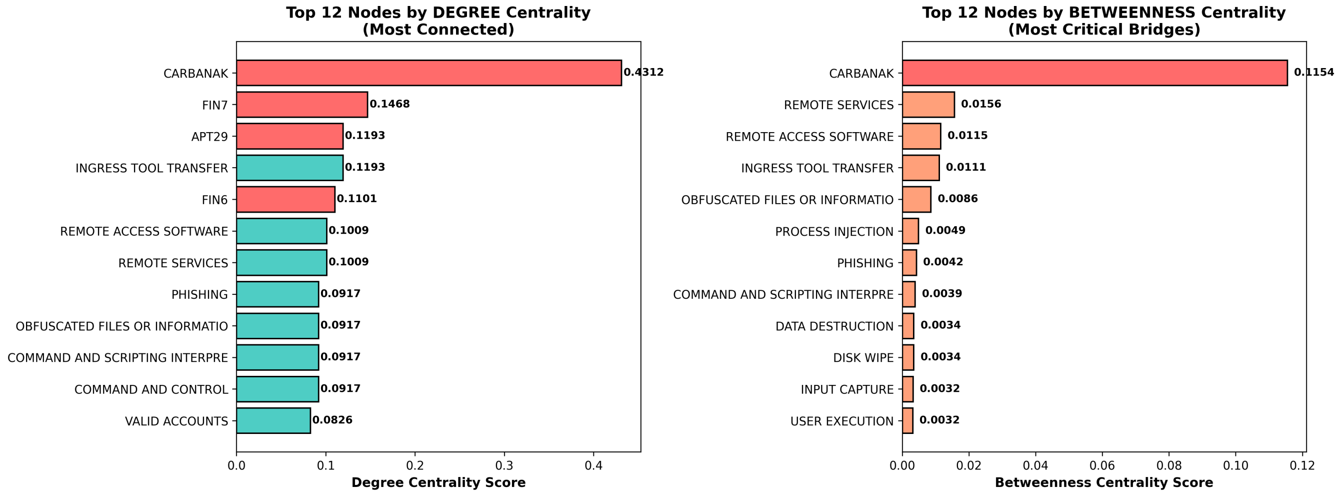


Figure 3: Comparison of top nodes ranked by degree centrality (left) vs betweenness centrality (right).

4. Critical Attack Techniques

Top 10 Attack Techniques by Prevalence

Rank	Technique	APTs Using	Common Actors
1	PHISHING	7	FIN7, FIN6, CARBANAK
2	COMMAND AND SCRIPTING INTERPRETER	6	FIN7, FIN6, CARBANAK
3	EXPLOITATION FOR CLIENT EXECUTION	4	FIN7, OILRIG, FIN6
4	INGRESS TOOL TRANSFER	4	CARBANAK, FIN7, WIZARDSPIDER
5	REMOTE SERVICES	4	CARBANAK, WIZARDSPIDER, FIN6
6	USER EXECUTION	3	CARBANAK, FIN7, APT29
7	INPUT CAPTURE	3	CARBANAK, FIN7, APT29
8	REMOTE ACCESS SOFTWARE	3	CARBANAK, FIN7, APT29
9	OBFUSCATED FILES OR INFORMATION	3	CARBANAK, FIN7, APT29
10	VALID ACCOUNTS	3	WIZARDSPIDER, FIN6, SANDWORM

Top APT Groups by Activity

Rank	APT Group	Techniques	Unique Tech	Primary Tactic
1	CARBANAK	56	29	Multi-vector
2	FIN7	37	16	Multi-vector
3	APT29	35	13	Multi-vector
4	FIN6	13	12	Multi-vector
5	WIZARDSPIDER	10	8	Multi-vector
6	OILRIG	8	4	Multi-vector
7	SANDWORM	7	7	Multi-vector

5. Key Insights and Conclusions

1. Network Topology:
The CTI knowledge graph exhibits a scale-free network topology with high clustering and low average path length. This indicates that threats are interconnected through common techniques and tactics, with a few highly-connected hubs (CARBANAK, FIN7, APT29) dominating the landscape.

2. Universal Attack Vectors:
Techniques like PHISHING (used by 7 APTs) represent universal attack vectors that transcend specific threat actor groups. Defense mechanisms targeting these prevalent techniques yield high return on investment.

3. Threat Actor Sophistication:
CARBANAK demonstrates the highest sophistication with 56 distinct techniques, suggesting a well-resourced threat actor with diverse operational capabilities.

4. Critical Infrastructure:
Nodes with high betweenness centrality (e.g., CARBANAK) act as critical infrastructure in the threat landscape. Defensive strategies targeting these nodes have disproportionate impact on threat efficacy.

5. Tactical Diversity:
Coverage of 17 MITRE tactics indicates that modern APT groups employ diverse strategies across the entire attack lifecycle, from initial access to impact.

Recommendations

1. Defense Prioritization: Focus defensive resources on high-prevalence techniques (PHISHING, Command execution).

2. Threat Hunting: Monitor for combinations of techniques used by {len(actors_sorted)} known APT groups.

3. Detection Rules: Develop detection rules targeting betweenness-central techniques to disrupt attack chains.

4. Intelligence Sharing: Share threat intelligence on critical hub nodes across security organizations.

5. Continuous Monitoring: Update the knowledge graph as new threat intelligence emerges.

Appendix: Methodology

Data Source: CTI-HAL (Cyber Threat Intelligence - Hierarchical Annotation Language) dataset
Reports Analyzed: 81
Knowledge Extraction: MITRE ATT&CK; framework mapping with semantic triple extraction
Graph Construction: NetworkX directed graph with semantic relationships
Analysis Methods:
• Centrality Analysis (degree, betweenness, closeness)
• Network Metrics (density, clustering, path length)
• Community Detection
• Temporal Analysis (if applicable)

Visualizations Generated:
• Interactive HTML graph visualization (pyvis)
• Top 25 nodes network diagram
• Comprehensive metrics dashboard
• Centrality comparison analysis
• Comprehensive PDF report (this document)

Report generated on February 02, 2026 at 13:49:39
CTI Knowledge Graph Analysis Tool v1.0
Advanced Threat Intelligence Analysis Platform